Scraping PDF

Mobility Master Configuration Hierarchy

Mobility Master (ArubaOS 8.x.x.x) uses a centralized, multi-tier architecture under a brand new UI that provides a clear separation between management, control, and forwarding functions. The entire configuration for both the Mobility Master and managed devices is set up from a centralized point, thereby simplifying and streamlining the configuration process. Mobility Master consolidates all-master, single master-multiple local, and multiple master-local deployments into a single deployment model.

Whereas, the architecture of ArubaOS 6.x and earlier versions consist of a flat configuration model that contains global and local configurations. The global configurations are applied to the master controller which propagates those to its local controllers. The local configurations are applied to the master or the local controller directly.

Mobility Master takes the place of a master controller in the network hierarchy. Mobility Master oversees controllers that are co-located (on-premises local controllers or off-campus branch office local controllers). All the controllers that connect to Mobility Master act as managed devices.

Understanding Configuration Hierarchy

The Mobility Master hierarchy simplifies the configuration process by supporting multiple configurations for multiple deployments using a single Mobility Master. Configuration elements can be mapped to one or more end devices, such as a managed device or VPN concentrator. Common configurations across devices are extracted to a shared template, which merges with device-specific configurations to generate the configuration for an individual device.

Figure 1 *Example of the Configuration Hierarchy*

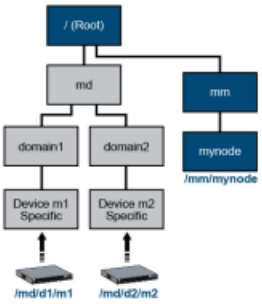


Figure 1 provides an example of the configuration hierarchy. The solid lines represent the hierarchy, the dotted arrows represent the device mapping, and each box represents a node in the hierarchy. When a device is added to Mobility Master, it must be mapped to a node or node-path in order to inherit configurations from the hierarchy. An explicit configuration node is also created for each device so that any device-specific configurations can be added directly to that node. Any device that is managed by Mobility Master is known as a managed device. For example, device **m2** in Figure 1 retrieves all device-specific configurations from the **Device m2 Specific** node. Since the **Device m2 Specific** node is mapped to the **domain2**, **md**, and **Root** nodes, the device also receives configurations from those nodes.

Each node contains a unique combination of common and device-specific configurations. The root node appears by default upon logging in to Mobility Master CLI.

The configuration hierarchy contains the following nodes and node structure:

Table 1: *Nodes and Node Structure*

Category	Node Name	Node Description
Mobility Master	/	Configurations common to Mobility Master and its managed devices (the root node). **NOTE:** Configuration changes are not allowed on the root node.
	/md	Configurations common to all managed devices. The user can create additional nodes under this node.
	/mm	Configurations common to the primary and standby Mobility Master (VRRP pair).
	/mm/mynode	Configurations specific to a particular Mobility Master. This can only be edited on the respective Mobility Master.
Stand-alone Controller	/mm	Configurations common to the primary and standby stand-alone controllers (VRRP pair).
	/mm/mynode	Configurations specific to a particular stand-alone controller. This can only be edited on the respective stand-alone controller.

The term "mm" refers to Mobility Master and "md" refers to managed device.

Understanding the Node Hierarchy

You can view the hierarchy of the devices and groups on a Mobility Master at a global level. Mobility Masters are placed into the **/mm** group and managed devices are in the **/md** group.

- **/md**—This is the global or root level where anything configured is applicable to all the nodes globally. It is recommended not to edit or add additional configuration at this level.
- **/md/<group name>**— This is used to differentiate the sites physically or by the type of deployment such as DMZ, Branch, Campus, RAPs, and so on.

When you log in to the Mobility Master, you are placed in the **/mm/mynode** prompt by default.

Navigating through Node Hierarchy

You can use one of the following two commands to navigate to any node from the current node:

- **change-config-node**
- **cd**

Both commands auto complete the group or folder names. You can also use the device hostname as an alias to navigate to a device node in the hierarchy. In doing so, your prompt changes to reflect where you are in the hierarchy:

```
(host) [mynode] #change-config-node Aruba7010
(host) [00:0b:86:99:97:57] #
```

The following CLI command displays your current node:

```
(host) [00:0b:86:99:97:57] #pwd
/md/Home-Production/00:0b:86:99:97:57
```

The following CLI command allows you to navigate one group up in the hierarchy:

```
(host) [00:0b:86:99:97:57] #cd ..
(host) [Home-Production] #
```

Centralized Configuration

Mobility Master uses a centralized configuration application to maintain all configurations under the management domain, eliminating the use of multiple points of contact to apply global and local configurations to each managed device. You can organize all common configurations at a higher level of the hierarchy.

Mobility Master Configuration

The Mobility Master that provides this configuration service to other devices in the network also contains its own configuration. The Mobility Master configuration is obtained through nodes in the hierarchy labeled **/mm** or **/mm/mynode**. Configurations under the **/mm** node, which are shared by the redundant Mobility Master pair (primary and standby Mobility Masters), are synced to the standby Mobility Master. Configurations under **/mm/mynode** are synced to individual Mobility Master devices.

Allowed Node Operations

The following node operations are allowed on Mobility Master:

- **Create Node**: Creates a new node as the child of an existing node in the configuration hierarchy (system-generated or user-created)
- **Add Device**: Associates a device to an existing node in the hierarchy. This device inherits configurations from all nodes between the root node and the device (node-path).
- **Delete Node**: Deletes an existing user-created node or node without any child nodes. System-generated nodes cannot be deleted. Only leaf nodes without any child nodes can be deleted.
- **Delete Device**: Deletes a currently associated device from the configuration hierarchy. This will cause the device to reload and erase all configurations received from Mobility Master.
- **Clone Node**: Copies the configuration of an existing node into a new node. The new node is created as a child of an existing node in the hierarchy.
- **Move Node**: Moves an existing user-created node in the hierarchy to the specified destination node. System-generated nodes cannot be moved. Ensure the following points while moving a node or device, otherwise the move operation will fail:
  - The node to be moved is a leaf node and does not have any group node or a device node as a child node under it.
  - No configuration is pending on the parent nodes of the child node to be moved.
  - The configuration on the node to be moved is complaint with the configuration in the new ancestor nodes chain.
- **Rename Node**: Renames the existing node name to the specified name. The node paths of the child nodes under the renamed node are automatically updated.
- **Drag and Drop Node**: Allows you to move any controller from one group to another group within the hierarchy, without deleting the controller from the Mobility Master.

  Moving multiple controller or group within the network hierarchy is not supported.

- **Edit Action**: Allows you to rename a controller or a group in the managed network hierarchy.

Refer to the ArubaOS *Command Line Interface Reference Guide* for more details on the configuration commands for node and device management.

Access Permissions

The Mobility Master management domain can be large and widespread across various geographic regions. In a Mobility Master, the editing scope of the admin user can be restricted to individual node-paths within the configuration hierarchy, unlike the legacy ArubaOS management domain where an administrator can modify any configuration in the system.

Each management user is granted editing permissions for a given node, allowing the user to modify the configuration for that node and any child node within its node-path. The user, however, cannot modify any parent nodes or nodes on a different path in the hierarchy. Users can view configurations for any node in the hierarchy to refer to a parent node configuration or verify that the derived configuration for a device matches the parent node

Configuration Validation

Mobility Master uses a centralized validation model that performs various types of validations for different targets. Configuration validation falls under one of the following categories:

- **Syntax Validation**: Basic parser validations (for example, making sure the syntax of a command is correct, the data type is correct, or a value is within a valid range).

  > Roles, ACLs, and pools (DHCP, VLAN, tunnel, and NAT) must be written in lower-case. Passwords, crypto keys, and ESSIDs can be written in both upper-case and lower-case.

- **Semantic Validation**: Custom application-specific validations (for example, dependency checks across commands or instance count limits). Dependency checks are limited to the nodes from which the target device inherits the configuration.
- **Platform Validation**: Platform model-specific validations (for example, determining which features are supported on a platform or the type and count of ports on a platform).

  > Validation is not available on the setup dialogue. Users must manually verify the setup dialogue information for each managed device.

Validation Failures

If a command does not pass validation, it is rejected and will not be included in the pending configuration for that node. If a new device that cannot support an existing configuration is added, the device add is rejected.

Serviceability

Managed devices are always serviceable from the centralized management location. When a managed device boots up for the first time under the factory default state, it auto-provisions and establishes connectivity to Mobility Master through ZTP. Managed devices can also be provisioned manually through the setup dialog box. Managed devices can encounter connectivity loss due to bad configurations, network connectivity issues, and so on. The system attempts to recover from these situations when possible.

This section includes the following topics:

Bad Configuration Recovery

Certain configurations, such as those in the following list, can interfere with the connectivity between managed devices and Mobility Master:

- Uplink port shut
- Partially configured uplink VLAN
- Limiting bandwidth contract policy
- Bad ACL

Bad configurations can be caused by simple typo errors. Even if the user discovers the error, the bad configuration may have already caused connectivity loss, preventing the user from pushing the correct configuration to the managed device.

Mobility Master supports an auto-rollback mechanism that reverts the managed device to the last known good configuration prior to the management connectivity loss. Mobility Master also indicates if a device has recovered from a bad configuration through the **show switches** command output. The output for this command labels the **Configuration State** for the managed device as **CONFIG ROLLBACK** if the device has recovered connectivity using the rollback configuration. When the user fixes the bad configuration on Mobility Master, the managed device recovers automatically, and the state changes to UPDATE SUCCESSFUL.

Example output for the **show switches** command:

```
(host) [mynode] #show switches

Thu Jun 09 12:13:45.735 2016

All Switches
------------
IP Address     IPv6 Address  Name              Location          Type     Model         Version                  Status  C
onfiguration State  Config Sync Time (sec)  Config ID
----------     ------------  ----              --------          ----     -----         -------                  ------  -
------------------  ----------------------  ---------
192.192.192.1  None          TECHPUB_MASTER    Building1.floor1  master   ArubaMM       8.0.0.0-svcs-ctrl_55038  up      U
PDATE SUCCESSFUL    0                       27
192.192.192.2  None          TECHPUB_STANDBY   Building1.floor1  standby  ArubaMM       8.0.0.0-svcs-ctrl_55038  up      U
PDATE SUCCESSFUL    10                      27
192.192.189.1  None          TECHPUB_LC1_189.1 Building1.floor1  MD       Aruba7010     8.0.0.0-svcs-ctrl_55038  up      U
PDATE SUCCESSFUL    0                       27
192.192.192.3  None          TECHPUB_x86_LC    Building1.floor1  MD       VMC-TACTICAL  8.0.0.0-svcs-ctrl_55038  up      U
PDATE SUCCESSFUL    0                       27
192.192.189.2  None          TECHPUB_LC2_189.2 Building1.floor1  MD       Aruba7005     8.0.0.0-svcs-ctrl_55038  up      U
PDATE SUCCESSFUL    0                       27
Total Switches:5
```

Disaster Recovery

If auto-rollback from a bad configuration fails, and connectivity between the managed device and Mobility Master remains disrupted, users can enable **Disaster Recovery** mode on the managed device using the **disaster-recovery on** command. Under the regular mode, the **/mm** node downloads configurations from Mobility Master that cannot be modified directly on each managed device. **Disaster Recovery** mode grants users access to the **/mm** node through the managed devices while blocking any further configuration synchronizations from Mobility Master. With full control of the **/mm** node, users can make local modifications on each managed device to restore connectivity to Mobility Master.

Mobility Master User Interface

The Mobility Master user interface provides ease-of-use through an intuitive layout and simple navigation model.

Navigation Model

Each page of the Mobility Master UI is divided into the following sections:

- **Header**, which includes the following:
  - **Aruba logo**: The Aruba logo.
  - **Deployment mode and hostname**: The deployment mode and hostname of the Mobility Master or managed device.
  - **Network Status Counters**: Counters for reachable and unreachable controllers, reachable and unreachable access points, clients, and alerts.
  - **Help**: Initiates help mode to display available help information in the UI. See "Help Mode" on page 1 for more details.
  - **User menu**: Drop-down menu that displays your username. It allows you to logout of the Mobility Master or managed device. The **Preferences** option allows you to enable or disable the **Profiles** link in the following pages:
    - **All Profiles** table of the Mobility Master node.
    - **WLANs** table and **AP Group** table of the Managed Device node.

      The **Profiles** link is displayed only when the **show advanced profiles** check box is selected in the **Preferences** option of the User menu.

    Limitations
    - Advanced profile configuration is controller specific (domain name)
    - Advanced profile configuration is not per-user specific
    - It is browser specific, irrespective of user login—for example, if a user enabled Preferences in the Chrome browser it will not carry forward to IE or Firefox.
- **Node-path**: Node-path within the network hierarchy.
- **Pending Changes**: List of all pending configuration changes. See "Pending Changes" on page 1 for more details.
- **Menu**: Main menu, which includes the **Dashboard**, **Configuration**, **Diagnostics**, and **Maintenance** menu items. Select a menu item to reveal the corresponding sub-menu items. See "Navigation Levels" on page 1 for more details.
- **Collapsible network tree**: Complete network hierarchy that is revealed or hidden when you click the menu or arrow button, respectively, next to the node-path. See "Network Tree" on page 1 for more details.
- **Work-screen**: Content description for a menu item or tab.

Figure 1 *Overview of the User Interface*

Network Tree

The Mobility Master UI allows users to create, modify, and delete any node in the network hierarchy from a central location. By clicking the menu

MultiVersion Support

Starting with ArubaOS 8.2.0.0, Mobility Master provides the essential infrastructure for multiversion support across all managed devices in the network. With this enhancement, the ArubaOS version on each managed device can be different from that in the Mobility Master in the network.

The multiversion infrastructure performs the centralized validation for the configurations of different ArubaOS versions run on the managed devices. The configurations that are not compatible with the managed device's ArubaOS version will not be sent to the managed device.

This feature supports the following scenarios:

- Customers want to upgrade only the Mobility Master with the latest ArubaOS version to use centralized services.
- Customers want to upgrade only a few managed devices in their network with the latest ArubaOS version to test some features of their interest.
- Customers want to upgrade their network in certain geographical locations and plan to upgrade the entire network incrementally.

Important Points to Note

The following are important points to note before implementing the multiversion support in your network:

- ArubaOS 8.2.0.0 is the minimum supported version on the managed devices and the Mobility Master.
- The Mobility Master can run an ArubaOS version that is either the same or a higher version of ArubaOS than the versions on the managed devices; the minimum supported version on both platforms is ArubaOS 8.2.0.0.
- Multiversion is supported only if the Mobility Master is running two code versions higher than the code versions running on the managed devices. For example multiversion is supported if a Mobility Master is running ArubaOS 8.5.0.0 and the managed devices are running ArubaOS 8.3.0.0 and will not be supported if the managed devices are running ArubaOS 8.2.0.0 or ArubaOS 8.4.0.0.

UI Support for Multiversion

When the managed devices and the Mobility Master run different ArubaOS versions, the following rules apply:

- At all levels of hierarchy, the WebUI elements of the later ArubaOS version is always shown to the user.
- At the group level, the following rules apply:
  - All WebUI elements that are new in the ArubaOS version of the Mobility Master are shown.
  - The WebUI elements that are obsolete in the ArubaOS version of the Mobility Master are not shown.
- At the device level, the following rules apply:
  - The WebUI elements that are obsolete in the ArubaOS version of the Mobility Master but not obsolete on the ArubaOS version of the device are shown.
  - The WebUI elements that are obsolete on the ArubaOS version of the device are not shown.
  - The WebUI elements that are introduced in the ArubaOS version later than that on the device are not shown.

Display of ArubaOS Version Identifiers

The UI displays the ArubaOS versions running on the Mobility Master and the managed device:

The following changes are applicable in the WebUI of the managed device:

- **Mobility Master ArubaOS version identifier**: The ArubaOS version of the Mobility Master is displayed at the bottom of the left navigation pane. The Mobility Master version identifier is displayed as *Mobility Master: Version <version #>*.
- **Managed device ArubaOS version identifier:** If the ArubaOS version running on the managed device is different from that running on the Mobility Master, an information icon is displayed. It shows the ArubaOS version running on the managed device. The managed device version identifier is displayed as *Version <version #>*.

> The managed device version identifier is not displayed when the ArubaOS version running on the managed device and the Mobility Master are the same.

Dashboard Monitoring

The **Dashboard** page provides an enhanced visibility into your network to view and monitor various information of the devices in the network.

You can view the context sensitive help for each field in the **Dashboard** UI by clicking the **help** link at the top-right corner of the WebUI. The field for which the help is defined appears as green. You can turn off the help by clicking **Done**.

The ArubaOS 8.0.0.0 adds the Mobility Master and managed device in a topology that permits the Mobility Master to manage and monitor one or more managed devices. For this, the administrator has to configure mgmt-server as the Mobility Master from the managed device's path. The Mobility Master can only manage and monitor managed devices and cannot manage APs.

> New dashboard is not supported in the Master controller mode.

In the **Managed Network** node hierarchy, navigate to **Dashboard**. You can view the **Dashboard** of a managed device without logging out of the Mobility Master. To view the **Dashboard** page of a managed device, click the managed device. See Table 1 for dashboard pages available in managed network and managed device.

Dashboard Pages

Starting from ArubaOS 8.4.0.0, the dashboard page contains the following sub-categories:

- Overview
- Infrastructure
- Traffic Analysis
- Security
- Services

The following table shows the dashboard pages available in Mobility Master mode:

Table 1: *Dashboard Pages in Various Views*

Dashboard Pages	Managed Network	Managed Device
Overview		
Action Bar	Yes	Yes
WLANs	Yes	Yes
Usage	Yes	Yes
Radios	Yes	Yes
Infrastructure		
Action Bar	Yes	Yes
Action Bar	Yes	Yes
Action Bar	Yes	Yes
Cluster	Yes	—

Overview

The **Overview** dashboard provides the summary of CLIENTS, WLANs, USAGE, and RADIOS. See Figure 1 for **Overview** page.

Figure 1 *Overview Page*

The **Overview** dashboard contains the following windows:

- **CLIENTS**—This window displays the information about all the clients connected to a managed device within the network hierarchy. The number of wired and wireless clients is displayed in the bottom right corner of the **CLIENTS** window. This is the default page. For more information, see Action Bar.

You can view the following information using the **Grouped by** drop-down list.

  - **Health** — Displays the health score of the wireless clients connected to APs. The health score are Good, Fair, Poor, or Unknown. Click the donut chart area or hyperlinked number to navigate to the **Wireless clients** table and view the details of the wireless clients connected to APs.
  - **Band** — Displays the list of wireless clients under the 2.4 GHz and 5 GHz radio bands. Click the donut chart area or hyperlinked number to navigate to the **Wireless clients** table and view the details of the wireless clients connected to APs.
  - **Data Speed** — Displays the data speed (bps) of the wireless clients connected to APs. Click the vertical bar to navigate to the **Wireless clients** table and view the details of the selected wireless clients.
  - **Signal Quality** — Displays the SNR (dB) ranges of the wireless clients connected to APs. Click the vertical bar to navigate to the **Wireless clients** table and view the details of the selected wireless clients.
  - **Operating System** — Displays the number of clients that are running each type of operating systems. Click the OS area in the donut chart or hyperlinked number to navigate to the **Wireless clients** table and view the details of the wireless clients running the selected operating system type.

- **WLANS**—This window displays the summary of all active WLANs in the managed device. This is the default page. Click the horizontal bar or hyperlinked number to navigate to the **WLANs** table and view the details of the active WLANs. For more information, see WLANs.

You can view the following information using the **Show WLANs** drop-down list.

  - **With most clients** — Displays five WLANs currently accessed by highest number of clients, in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the **WLANs** table and view the details of the selected WLAN.
  - **With highest usage** — Displays five WLANs with highest number of bytes transmitted and received, in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the **WLANs** table and view the details of the selected WLAN.

- **USAGE**—Displays the throughput data (bps) transmitted and received in the last 15 minutes. Click the hyperlinked number to navigate to the **Usage** page and view the details of the data transmitted and received. For more information, see Usage.

Click **Current** icon in the top right corner of the window to display the data transmitted and received in the last 15 minutes.

- **RADIOS**— Displays the information of all radios of APs controlled by the managed device. For more information, see Radios.

You can view the following information using the **Grouped by** drop-down list.

  - **Channel Quality** — Displays the channel quality of the 2.4 GHz and 5 GHz radio bands. This is a default page. Click the vertical bar to navigate to the **Radios** table and view the details of the 2.4 GHz or 5 GHz radio bands.
  - **Interference** — Displays the percentage of interference in the 2.4 GHz and 5 GHz radio bands. Click the vertical bar to navigate to the **Radios** table and view the details of the 2.4 GHz or 5 GHz radio bands.
  - **Channel Busy** — Displays the percentage of busy channel in the 2.4 GHz and 5 GHz radio bands. Click the vertical bar to navigate to the **Radios** table and view the details of the 2.4 GHz or 5 GHz radio bands.
  - **Channel** — Displays the active channels on the 2.4 GHz or 5 GHz radio bands. Click the vertical bar to navigate to the **Radios** table and view the details of the individual radio bands.

Clients

Navigate to **Dashboard > Overview** and click the **CLIENTS** icon. This page displays the summary of the active **Wireless Clients** connected to the managed device. See Figure 1 for **Clients** Page.

Figure 1 *Clients Page*

Clicking the icon on top right-hand corner of the table displays the list of wired clients connected to the managed device. The information displayed in the **Role** column will provide details on the following:

- User-based tunneled users
- Port-based tunneled users
- Controller wired users
- AP wired users
- VIA-VPN users

Use the **Customize columns** option to choose the columns you want to view.

Action Bar

The Action bar displays the total number of wireless clients depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, **Add to blacklist**, and **Customize columns**.

> Aruba now allows you to manage blacklisted clients in stand-alone controllers as well as in a Mobility Master-Managed Device topology.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the wireless clients in the table that you want to view.
- **Add to blacklist** — Click the **Add to blacklist** icon to blacklist a wireless client.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

To blacklist a client manually, perform the following steps:

1. Select a client from the **Wireless Clients** table.
2. Click **Add to blacklist** icon as shown in Figure 2.

Figure 2 *Add to Blacklist Page*

The **Add to Blacklist** pop-up window is displayed.

3. In the **Add to Blacklist** pop-up window, click **Add**.

The client is blacklisted and is listed in the **Blacklisted Clients** table.

Details

Expand the wireless client from the **Wireless clients** table to view the detailed information of individual client. See Figure 3 for Details Page.

The **Wireless clients** table displays the following details:

- **Details** — Displays detailed information about the selected wireless client.
- **Signal** — Displays detailed information about throughput, transferred frames, signal quality, and data speed of the wireless clients.

You can view the following information using the **Show information about** drop-down list

WLANs

Navigate to **Dashboard > Overview** and click **WLANS** icon. The **WLANs** page displays the summary of all the active WLANs in the managed device. See Figure 1 for **WLANs** page.

Figure 1 *WLANs page*

Action Bar

The Action bar displays the total number of wireless clients depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the WLANs in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand the WLAN from the **WLANs** table to view the detailed information of individual WLAN. See Figure 2 for **Details page**.

The **WLANs** table displays the following details:

- **Details** — Displays detailed information about the selected WLAN.
- **Usage** — Displays detailed information about health, band, and throughput of the wireless clients.

You can view the following information using the **Show** drop-down list.

- **Client Health** — Displays the health score of the wireless clients connected to APs. The health score are Good, Fair, Poor, or Unknown. Click the donut chart area or hyperlinked number to navigate to the **Wireless clients** table and view the details of the wireless clients connected to APs.
- **Client by band** — Displays the list of wireless clients under the 2.4 GHz and 5 GHz radio band. Click the donut chart area or hyperlinked number to navigate to the **Wireless clients** table and view the details of the wireless clients connected to APs.
- **Throughput** — Displays the transmitted or received data (bps) in the last 15 minutes.

Traffic Analysis — Displays detailed information about active applications, destinations, clients and clients by OS.

You can view the following information using the **Show** drop-down list.

- **Top 5 Applications** — Displays five applications with highest usage (bytes), in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the **Applications** table and view the details of the wireless clients using the application.
- **Top 5 Destinations** — Displays five destinations with highest usage (bytes), in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the **Destinations** table and view the details of the wireless clients using the destination.
- **Top 5 Clients** — Displays five clients with highest usage (bytes), in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the **Hosts** table and view the details of the hosts.
- **Clients by OS** — Displays the number of hosts that are running each type of OS. Click the OS area in the donut chart to display the hosts running the selected OS type.

Figure 2 *Details Page*

Usage

Navigate to **Dashboard > Overview** and click **USAGE** icon. The **Usage** page displays the usage summary of APs, Clients, Low Performing Wi-Fi, and Low Performing Clients on the managed devices in the network. See Figure 1 for **Usage** page.

Figure 1 *Usage Page*

TOP ACCESS POINTS — Displays five access points with highest number of bytes transmitted or received, in decreasing order. Click the horizontal bar to navigate to the **Access points** table and view the details of the selected access point. For more information, see Details.

TOP CLIENTS — Displays five clients with highest number of bytes transmitted or received, in decreasing order. Click the horizontal bar to navigate to the **Wireless clients** table and view the details of the selected wireless client. For more information, see Details.

LOW PERFORMING WI-FI — Displays the details of low performing access points in the network. You can view the following information using the **Show APs with** drop-down list.

- **Highest noise floor** — Displays five access points with noise floor (dBm) in the 2.4 GHz or 5 GHz band. Click the horizontal bar to navigate to the **Access points** table and view the details of the selected access point. For more information, see Details.
- **Busiest Channel** — Displays five access points with percentage of busy channel in the 2.4 GHz or 5 GHz band. Click the horizontal bar to navigate to the **Access points** table and view the details of the selected access point. For more information, see Details.
- **Highest Interference** — Displays five access points with percentage of interference in the 2.4 GHz or 5 GHz band. Click the horizontal bar to navigate to the **Access points** table and view the details of the selected access point. For more information, see Details.

LOW PERFORMING CLIENTS — Displays the details of low performing access points in the network. You can view the following information using the **Show clients with** drop-down list.

- **Lowest signal quality** — Displays five wireless clients with lowest SNR (dB) ranges. Click the horizontal bar to navigate to the **Wireless clients** table and view the details of the selected wireless client. For more information, see Details.
- **Lowest Goodput** — Displays five wireless clients with lowest goodput (bps). Click the horizontal bar to navigate to the **Wireless clients** table and view the details of the selected wireless client. For more information, see Details.
- **Lowest data speed** — Displays five wireless clients with lowest data speed (bps). Click the horizontal bar to navigate to the **Wireless clients** table and view the details of the selected wireless client. For more information, see Details.

Radios

Navigate to **Dashboard > Overview** and click **RADIOS** icon. The **Radios** page displays the summary of all the active radios in the managed device. See Figure 1 for the **Radio** page.

Figure 1 *Radios Page*

Action Bar

The Action bar displays the total number of radios depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the radios in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand the radios from the **Radios** table to view the detailed information of individual radios. See Figure 2 for Details page.

The **Radios** table displays the following details:

DETAILS — Displays detailed information about the selected radio.

USAGE — Displays detailed information about client health, connected clients, throughput, and goodput of the radio.

You can view the following information using the **Show information about** drop-down list.

- **Client Health** — Displays the health score of the wireless clients connected to APs. The health score are Good, Fair, Poor, or Unknown. Click the donut chart area or hyperlinked number to navigate to the **Wireless clients** table and view the details of the wireless clients connected to APs.
- **Clients Connected** — Displays the number of clients connected in the last 15 minutes.
- **Throughput** — Displays the transmitted and received data (bps) in the last 15 minutes.
- **Goodput** — Displays the goodput data (bps) in the last 15 minutes.
- **Channel** — Displays the detailed information about channel utilization, noise floor, transmitted or received frames, and WLANs.

You can view the following information using the **Show information about** drop-down list.

- **Channel Utilization** — Displays the percentage of the current channel utilization. The channel utilization information is categorized as: **Tx time**, **Rx time**, **Interference** and **Free**.

Click **Historical** icon in the top right corner of the window to display the channel utilization percentage in the last 15 minutes.

- **Noise Floor** — Displays the information about noise floor (dBm) in the last 15 minutes.
- **Transferred Frames** — Displays the percentage of transmitted or received frames in the channel. The transmitted or received frame information is categorized as: **Successful**, **Retried**, and **Dropped**.

Click **Historical** icon in the top right corner of the window to display the transmitted or received frames in the last 15 minutes.

Click **Clients** button in the bottom right corner of the window to navigate to the **Wireless clients** table and view the details of the wireless clients.

- **WLANs** — Displays the details of the throughput data (bps) of the selected channel. Click the horizontal bar to navigate to the **Wireless clients** table and view the details of the wireless clients connected to this WLAN. For more information, see Details.

Figure 2 *Details Page*

Infrastructure

The **Infrastructure** provides the summary of Controllers, Access devices, WAN and Clusters. See Figure 1 for **Infrasructure** page.

Figure 1 *Infrastructure Page*

The **Infrastructure** dashboard contains the following windows:

- **CONTROLLERS**—This window displays the summary of all the controllers in the network. This is the default page. Click the donut chart or hyperlinked number to navigate to the **Controllers** table and view the details of all the controllers. For more information, see Controller.

You can view the following information using the **Grouped by** drop-down list.

  - **Status** — Displays the status of all the controllers in the network. The controller status is categorized as: **Up**, and **Down**
- **Health** — Displays the health of all the controllers in the network. The controller health is categorized as:
  - **Poor**- The health status is displayed as **Poor** when any one of the following scenarios is observed:
    - the controller itself is down.
    - at least one of its uplinks has poor health score.
    - 10% or more of the APs are Down.
  - **Fair** - The health status is displayed as **Fair** when when any one of the following scenarios is observed:
    - at least one of its uplinks has a fair health score.
    - 1% or more (less than 10%) of the APs are Down.
  - **Good**- The health status is displayed as **Good** if APs and WAN uplinks are up.
  - **Unknown**- The health status is displayed as **Unknown** when the health status of the controller cannot be identified as good, fair, or poor.

Click **Network map** button to display the location of the managed devices in the network. If a managed device is not positioned, it is listed in a red balloon in the top-right corner of the map.

- **ACCESS DEVICES**—This window displays the summary of all the access points connected to a managed device. This is the default page. Click the donut chart or hyperlinked number to navigate to the **Access Points** table and view the details of all the access points connected to the network. For more information, see Access Devices.

You can view the following information using the **Grouped by** drop-down list.

  - **Status** — Displays the status of all the access points connected to a managed device. The access point status is categorized as: **Up**, and **Down**.
  - **AP Group** — Displays five access point groups with the number of access points connected per group.

Click **Tunneled Switches** button in the bottom right corner of the window to navigate to the **Tunneled Switches** table and view the details of tunneled switch.

- **WAN** — The window displays the summary of status and health of uplink in the network. This is the default page. Click the donut chart or hyperlinked number to navigate to the **Uplinks** table and view the details of all the uplinks in the network. For more information, see Details.

You can view the following information using the **Uplink grouped by** drop-down list.

  - **status** — Displays the status of all uplinks in the network. The uplink status is categorized as: **Up**, **Down** and **WAN disabled**
  - **health** — Displays the health of all uplinks in the network. The uplink health is categorized as: **Good**, **Fair**, **Poor** and **Unknown**
- **CLUSTERS** — The **Cluster** dashboard provides a visual overview on each cluster deployed on the network. The cluster dashboard displays total AP load, client load per cluster, health of each cluster, and status of each controller and access point connected to the cluster.
- **Clients**—This window displays the summary of all active wired and wireless clients in the managed device. This is the default page. Click the horizontal bar or hyperlinked number to navigate to the **Clients** table and view the details of the active clients. For more information, see Details.

Controller

Navigate to **Dashboard > Infrastructure** and click **CONTROLLERS** icon. The **Controllers** page lists all the managed devices in the network and provides its status and health related information. See Figure 1 for **Controllers** page.

Figure 1 *Controller Page*

Action Bar

The Action bar displays the total number of controllers depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the controllers in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand the controller from the **Controllers** table to view the detailed information of individual controller. See Figure 2 for Details page.

The **Controllers** table displays the following details:

- **Details** — Displays detailed information about the managed device.
- **Ports** — Displays the status of all the ports in the managed device.

Figure 2 *Details Page*

Access Devices

Navigate to **Dashboard > Infrastructure** and click **ACCESS DEVICES** icon. The **Access Points** page lists all the access points connected to managed devices in the network and provides its status and access point group related information. See Figure 1 for **Access Points** page.

Figure 1 *Access Points Page*

Action Bar

The Action bar displays the total number of APs depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the access points in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.
- **Sort**: Click a column header of the Access Points table to sort the complete list based on the entries on the active column. You can also use the sort icon that appears when you click on a column for sorting.
- **View client details**: Click on the number of clients associated with the AP to view the details of the clients on the **Clients** page.
- **View AP or radio summary**: Expand the access point from the **Access Points** table to view the summary of the individual APs. See Details for more information.
- **Capture and download packets:** Click Packet Capture icon of an access point from the Action column to start, pause, or stop capturing and downloading the AP packets.
- **Delete**: Select the check box for APs with **Down** status, and click the trash icon to remove the APs from the table. The APs with **Down** status are either unused or replaced when deployed.

> You can delete the APs with **Down** status only on Mobility Master or standalone controllers, and not on managed devices.

Details

Expand a access point from the **Access Points** table to view the detailed information of individual access point. See Figure 2 for Details page.

The **Access Points** table displays the following details:

Details — Displays detailed information about the selected access point.

Radio 2.4 GHz Channel — Displays the about channel utilization, noise floor, transmitted or received frames, and WLANs in the 2.4 GHz band.

You can view the following information using the **Show information about** drop-down list.

- **Channel Utilization** — Displays the percentage of the current channel utilization in the 2.4 GHz band. The channel utilization information is categorized as: **Tx time**, **Rx time**, **Interference**, and **Free**.

Click **Historical** icon in the top right corner of the window to display the percentage of the current channel utilization in the last 15 minutes.

- **Noise Floor** — Displays the information about noise floor (dBm) in the last 15 minutes.
- **Transferred Frames** — Displays the information about transmitted or received frames in the 2.4 GHz band. The transmitted or received frame information is categorized as: **Successful**, **Retried**, and **Dropped**.

Click **Historical** icon in the top right corner of the window to display the transmitted or received frames in the last 15 minutes.

- **WLANs** — Displays the throughput data (bps) in the 2.4 GHz band. Click the horizontal bar to navigate to the **Wireless clients** table and view the details of the wireless clients connected to this WLAN. For more information, see Details.

Radio 5 GHz Channel — Displays the detailed information about channel utilization, noise floor, transmitted or received frames, and WLANs in the 5 GHz band.

You can view the following information using the **Show information about** drop-down list

WAN

Navigate to **Dashboard > Infrastructure** and click **WAN** icon. The **Uplinks** page provides the status and health related information of uplinks in the network. See Figure 1 for **Uplinks** page.

Figure 1 *Uplinks Page*

Action Bar

The Action bar displays the total number of uplinks depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the uplinks in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand a uplink from the **Uplinks** table to view the detailed information of individual uplink. See Figure 2 for Details page.

The **Uplinks** table displays the following details:

- **HEALTH** — Displays detailed information about jitter, latency, and health score of the uplink in the network.

You can view the following information using the **Show** drop-down list.

  - **Jitter and Latency** — Displays the jitter and latency (Msec) in the last 15 minutes.
  - **Health Score** — Displays the percentage of health score in the last 15 minutes.

THROUGHPUT — Displays detailed information about transmitted or received data, and global compression on the uplink.

You can view the following information using the **Show** drop-down list.

  - **Tx and Rx** — Displays the transmitted or received data (bps) in the last 15 minutes.
  - **Global Compression** — Displays the aggregated compression saving on every uplink of the controller in the last 15 minutes.

Figure 2 *Details Page*

Cluster

The **Cluster** dashboard provides a visual overview on each cluster deployed on the network, displaying the following information:

- Total AP load per cluster
- Total Client load per cluster
- Status of each controller and access point in a cluster
- Health of each cluster

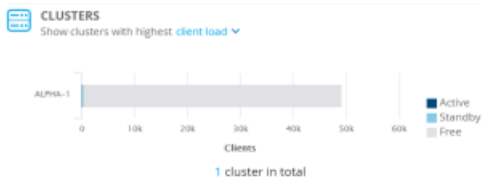
The **Cluster** dashboard can only be accessed from the root (Managed Network) node of the Mobility Master hierarchy. This information is not displayed on any stand-alone controllers, managed devices, or other nodes in the hierarchy. To view the **Cluster** dashboard, navigate to **Dashboard > Infrastructure > Clusters** in the WebUI. By default, the cluster dashboard displays the cluster with the highest AP load.

Following dashboard displays the cluster with the highest AP load. It also displays the number of active, standby and free APs for a given cluster.

Figure 1 *The Cluster Dashboard with Highest AP Load*

To view the client load, you can select client load to display the clusters with the highest client load from the drop-down menu.

Figure 2 *The Cluster Dashboard with Highest Client Load*



The **Cluster** dashboard consists of an **Cluster** section and **Cluster Member** section. Click on the AP load page or client load page to view more details.

- **Cluster > AP Load**: Displays the proportional distribution and number of active, standby, and free APs. Hover your mouse above a section of the chart to view the count for that AP type:
  - Free AP Load
  - Active AP Load
  - Standby AP Load
  - Total AP Load
- **Cluster > Client Load**: Displays the proportional distribution and number of active, standby, and free stations (clients). Hover your mouse above a section of the chart to view the count for that station type:
  - Free STA Load
  - Active STA Load
  - Standby STA Load
  - Total STA Load

To view in-depth information of each cluster member, click on the hyperlinked number under the **Controllers** column of the **Clusters** table. A **Cluster Members** pop-up window is displayed that contains a summary of each cluster member such as hostname, IP address, the cluster roles and so on.

Traffic Analysis

The **Traffic Analysis** page provides the summary of APPLICATIONS, DESTINATIONS, HOSTS, and WEBSITES features. See Figure 1 for **Traffic Analysis** page.

Figure 1 *Traffic Analysis Page*

You can click the hyperlinked number of a particular feature to navigate to its table to view more information.

> The **Traffic Analysis** dashboard application visibility feature is supported only in 7000 Series, 7200 Series , and x86 managed devices, and requires WebCC and PEFNG license.

The **Traffic Analysis** dashboard contains the following windows:

- **APPLICATIONS**—This window displays the summary of all applications in the managed device. This is the default page. Click the Applications window or hyperlinked number to navigate to the **Applications** table and view the details of the applications currently in use. For more information, see Applications.

You can view the following information using the **Show applications** drop-down list.

  - **By categories** — Displays all the applications by categories.
  - **With highest usage** — Displays five applications with highest number of bytes transmitted or received, in decreasing order. Click the horizontal bar to display the details of the selected application.
  - **With most hosts** — Displays five applications with highest number of hosts, in decreasing order. Click the horizontal bar to display the details of the selected application.

- **DESTINATIONS**—This window displays the summary of all active destinations in the managed device. This is the default page. Click the horizontal bar or hyperlinked number to navigate to the **Destinations** table and view the details of the active destinations. For more information, see Destinations.

You can view the following information using the **Show destinations** drop-down list.

  - **With highest usage** — Displays five destinations with highest number of bytes transmitter or received, in decreasing order. Click the horizontal bar to display the details of the selected destination.
  - **With most hosts** — Displays five destinations currently accessed by highest number of hosts, in decreasing order. Click the horizontal bar to display the details of the selected destination.

- **WEBSITES**—This window displays the summary of all websites visited using the managed device in the network hierarchy. This is the default page. For more information, see Websites.

You can view the following information using the **Show websites** drop-down list.

  - **By reputation** — Displays percentage of traffic based on reputation or score of web traffic in the managed device. The reputation levels are Trustworthy, Low risk, Moderate risk, Suspicious, High risk, and Unknown. Click the pie chart to display details of the selected reputation level.
  - **By web categories** — Displays the number of bytes transmitted or received by web categories in tree chart presentation. Click on the rectangle tile of a selected web category to show the number of bytes transferred for the selected web category that is grouped by reputation.
  - **With highest usage** — Displays five websites with the highest number of bytes transmitted or received, in decreasing order in chart presentation. Click the horizontal bar to display details of the selected website.
  - **With most hosts** — Displays five websites with the highest number of clients currently connected, in decreasing order in chart presentation. Click the horizontal bar to display details of the selected website.

- **HOSTS**—This window displays the summary of all active hosts in the managed device. This is the default page. Click the horizontal bar or

Applications

Applications performs DPI of local traffic and detects over 1500 applications on the network. **Applications** allows you to configure both application and application category policies within a given user role.

Enable DPI to enhance the benefit of the existing visualization or dashboard, To enable DPI, see the ArubaOS 8.6.0.0 Help Center section.

Navigate to **Dashboard > Traffic Analysis** and click **APPLICATIONS** icon. The **Applications** page displays the summary of all the applications in the managed device. See Figure 1 for **Applications** page.

Figure 1 *Applications Page*

Action Bar

The Action bar displays the total number of applications depending on filters applied. The action bar includes action icons namely, **Show/Hide table filters**, **Block/Unblock applications**, **Customize columns**, and **Set application QoS**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the applications in the table that you want to view.
- **Block/Unblock applications** — This button allows you to permit or deny an application or an application category for a given role. You can create global and per-role rules. For example, you can block the YouTube application, which belongs to the Streaming application category for the guest role within the enterprise.

To **Block/Unblock applications**, perform the following steps:

1. Select a application from the **Applications** table.

Details

Expand the application from the **Applications** table to view the detailed information of individual application. See Figure 2 for Details page.

The application table displays the following details:

- **HOSTS** — Displays five hosts with highest application usage, in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the **Hosts** table and view the details of the hosts using this application.
- **DESTINATIONS** — Displays five destinations with highest usage, in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the **Destinations** table and view the details of the destination using this application.
- **TRAFFIC DISTRIBUTION** — Displays the distribution of traffic. You can view the following information using the **Show sessions** drop-down list.
  - **By WLAN** — Displays the number of sessions established by the application for each WLAN in a donut chart. Click the donut chart area or hyperlinked number to navigate to the **Sessions** table and view the details of the sessions established by this application.
  - **By OS** — Displays the number of sessions established by the application for each OS in a donut chart. Click the donut chart area or hyperlinked number to navigate to the **Sessions** table and view the details of the sessions established by this application.
  - **By Role** — Displays the number of sessions established by the application for each role in a donut chart. Click the donut chart area or hyperlinked number to navigate to the **Sessions** table and view the details of the sessions established by this application.

Figure 2 *Details Page*

Destinations

Navigate to **Dashboard > Traffic Analysis** and click **DESTINATIONS** icon. The **Destinations** page displays the summary of all the active destinations in the managed device. See Figure 1 for **Destinations** page.

Figure 1 *Destinations Page*

Action Bar

The Action bar displays the total number of destinations depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the destinations in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand the destination from the **Destinations** table to view the detailed information of individual destination. See Figure 2 for Details page.

The destination table displays the following details:

- **HOSTS** — Displays five hosts with highest destination usage, in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the **Hosts** table and view the details of the hosts using this application.
- **APPLICATIONS** — Displays five applications with highest usage, in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the **Applications** table and view the details of the application used by the destination.
- **Traffic Distribution** — Displays the distribution of traffic. You can view the following information using the **Show sessions** drop-down list.
  - **By WLAN** — Displays the number of sessions established by the destination for each WLAN in a donut chart. Click the donut chart area or hyperlinked number to navigate to the **Sessions** table and view the details of the sessions established by this destination.
  - **By OS** — Displays the number of sessions established by the destination for each OS in a donut chart. Click the donut chart area or hyperlinked number to navigate to the **Sessions** table and view the details of the sessions established by this destination.
  - **By Role** — Displays the number of sessions established by the destination for each role in a donut chart. Click the donut chart area or hyperlinked number to navigate to the **Sessions** table and view the details of the sessions established by this destination.

Figure 2 *Details Page*

Hosts

Navigate to **Dashboard > Traffic Analysis** and click **HOSTS** icon. The **Hosts** page displays the summary of all the active hosts in the managed device. See Figure 1 for **HOSTS** page.

Figure 1 *Hosts Page*

Action Bar

The Action bar displays the total number of hosts depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the clients in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand the host from the **Hosts** table to view the detailed information of individual host. See Figure 2 for Details page.

The host table displays the following details:

- **APPLICATIONS** — Displays five applications with highest usage, in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the **Applications** table and view the details of the applications used by the selected host.
- **DESTINATIONS** — Displays five destinations with highest usage, in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the **Destinations** table and view the details of the destinations used by the selected host.

Figure 2 *Details Page*

Websites

Navigate to **Dashboard > Traffic Analysis** and click the **WEBSITES** tab. The implementation of **WebCC** feature can be viewed in this tab. **WebCC** uses a cloud-based service to dynamically determine the types of websites being visited, and their safety.

> The **WebCC** feature requires the WebCC subscription license.

When the **WebCC** feature is enabled, all web traffic (http and https) is classified. The classification is done in data path as the traffic flows through the managed device and updates dynamically.

Starting from ArubaOS 8.4.0.0, the **WebCC** feature supports classification of both IPv4 and IPv6 sessions.

Aruba has partnered with Webroot®, a Web classification service to provide the **WebCC** feature in the Mobility Master. Aruba uses the URL database of Webroot and the cloud look-up service to classify the web traffic. Aruba uses Webroot classified categories and score for web categories and reputation for **WebCC**. The following **Websites** Reputation table lists the risk level and score associated to each reputation level:

Table 1: *Websites Reputation Table*

Risk Level	Score
High-risk	1 - 20
Suspicious	21 - 40
Moderate-risk	41 - 60
Low-risk	61 - 80
Trustworthy	81 - 100

As indicated in Table 1, if the risk level of the content reputation goes high, the score goes down. So, when a WebCC reputation is configured to be denied in a policy, all traffic with the specified risk level and higher are denied. Similarly, when a WebCC reputation is configured to be permitted in a policy, all traffic with the specified risk level and lower are permitted. For example, if a policy is configured to deny moderate-risk traffic, then all the traffic categorized under moderate-risk, suspicious, and high-risk levels are denied. If a policy is configured to permit moderate-risk traffic, then all the traffic categorized under moderate-risk, low-risk, and trustworthy levels are permitted.

Action Bar

The Action bar displays the total number of websites depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, **Block/Unblock web category**, **Set web category QoS**, and **Customize columns**.

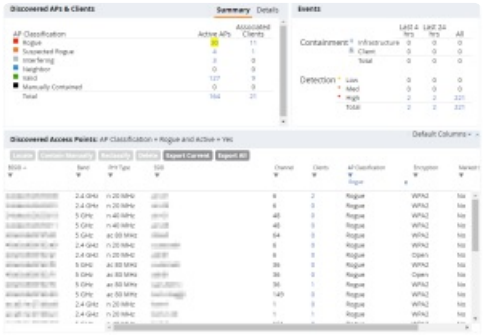
You can perform the following tasks on this page:

- **Show/Hide table filters** — Click the **Show/Hide table filters** icon to filter the websites by **NAME**, **CATEGORY**, or **REPUTATION**.
- **Block/Unblock web category** — This button allows you to permit or deny a website or web category for a given role.

Security

The **Security** page displays the summary of detected radios, detected clients, events , and blacklisted clients in your network. See Figure 1 for **Security** Page.

Figure 1 *Security Page*



The **Security** dashboard contains the following windows:

- **Detected Radios** — Displays the active detected radios in the managed device. This is the default page. The detected radios is categorized as: **Authorized**, **Neighbor**, **Interfering**, **Suspected Rogue**, **Rogue**, and **Contained**. Click the donut chart area or hyperlinked number to navigate to the **Detected Radios** table and view the details of the detected radios in the managed device. For more information, see Detected Radios.
- **Detected Clients** — Displays the active detected clients in the managed device. This is the default page. The detected clients is categorized as: **Authorized**, **Interfering**, and **Contained**. Click the donut chart area or hyperlinked number to navigate to the **Detected clients** table and view the details of the detected clients in the managed device. For more information, see Detected Clients
- **Events** — Displays the information about all detected and containment events that occur during specified time frame. For more information, see Events

You can view the following information using the **Grouped by** drop-down list.

- **Severity** — Displays low, medium and high severity of the events occurred in **last 4 hours**, **last 24 hours**, or **anytime**. This is the default page. Click the vertical bar or hyperlinked number to navigate to the **Events** table and view the details of the events you wish to view.
- **Target type** — Displays the details of the events by infrastructure and client occurred in **last 4 hours**, **last 24 hours**, or **anytime**. Click the vertical bar or hyperlinked number to navigate to the **Events** table and view the details of the events you wish to view.
- **Feature type** — Displays the details of the events by detection and containment occurred in **last 4 hours**, **last 24 hours**, or **anytime**. Click the vertical bar or hyperlinked number to navigate to the **Events** table and view the details of the events you wish to view.
- **Blacklisted Client** — Displays the clients that are blacklisted in stand-alone controllers or in Mobility Master-Managed Device topology. This is the default page. Click the **Blacklist** icon or donut chart area or hyperlinked number to navigate to the **Blacklisted Clients** table and view the details of the clients that are blacklisted in the managed device.

Detected Radios

Navigate to **Dashboard > Security** and click **DETECTED RADIOS** icon. The **Detected Radios** page displays the summary of all the detected radios in the managed device. See Figure 1 for **Detected Radios** page.

Figure 1 *Detected Radios*

Action Bar

The Action bar displays the total number of detected clients depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, **Reclassify detected radios**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the detected clients in the table that you want to view.
- **Reclassify detected radios** — Allows you to reclassify a single detected radio or all the selected detected radios.

To **Reclassify detected radios**, perform the following steps:

1. Select a detected radio from the **Detected Radios** table.
2. Click **Reclassify detected radios** icon as shown in Figure 2.

Figure 2 *Reclassify Detected Radios*

3. In the **Reclassify Detected Radios** dialog box, select classification from **Classification** drop-down list and click **Reclassify**.
4. Click **Pending Changes**.
5. In the **Pending Changes** window, select the check box and click **Deploy changes**.

- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Detected Clients

Navigate to **Dashboard > Security** and click **DETECTED CLIENTS** icon. The **Detected Clients** page displays the summary of all the detected clients in the managed device. See Figure 1 for **Detected Radios** page.

Figure 1 *Detected Clients Page*

Action Bar

The Action bar displays the total number of detected clients depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, **Reclassify detected clients**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the detected clients in the table that you want to view.
- **Reclassify detected clients** — Allows you to reclassify a single detected client or all the selected detected clients.

To **Reclassify detected clients**, perform the following steps:

1. Select a detected client from the **Detected Clients** table.
2. Click **Reclassify detected clients** icon as shown in Figure 2.

Figure 2 *Reclassify Detected Clients*

3. In the **Reclassify Detected Clients** dialog box, select classification from **Classification** drop-down list. Click **Reclassify**.
4. Click **Pending Changes**.
5. In the **Pending Changes** window, select the check box and click **Deploy changes**.

- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Events

Navigate to **Dashboard > Security** and click **EVENTS** icon. The **Events** page displays the summary of all the events in the managed device. See for **Events** page.

Figure 1 *Events Page*

Action Bar

The Action bar displays the total number of wireless clients depending on the filters applied. The Action bar includes Action buttons namely, **Show/Hide table filters**, **Delete Event**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the wireless clients in the table that you want to view.
- **Delete Event** — Allows you to delete a selected event from the **Events** table.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand a event from the **Events** table to view the detailed information of individual event. See Figure 2 for Details page.

Figure 2 *Details Page*

Blacklisted Clients

Navigate to **Dashboard > Security** and click the **BLACKLIST** icon. The **Blacklisted Clients** page displays the summary of all the blacklisted clients in the managed device. See Figure 1 for **Blacklisted Clients** page.

Figure 1 *Blacklisted Clients*

Action Bar

The Action bar displays the total number of blacklisted clients depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, **Add to blacklist**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the blacklisted clients in the table that you want to view.
- **Add to blacklist** — Click **Add to blacklist** icon to add a client to the blacklist table.

To blacklist a client manually, perform the following steps:

1. Select a client from the **Wireless Clients** table.
2. Click **Add to blacklist** icon as shown in Figure 2.

Figure 2 *Add to Blacklist*

The **Add to Blacklist** pop-up window is displayed.

3. In the **Add to Blacklist** pop-up window, enter the MAC address of the client,
4. Click **Add**.

The client is blacklisted and is listed in the **Blacklisted Clients** table.

- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Services

The **Services** provides the summary of AirGroup servers, AirGroup clients, and UCC. See Figure 1 for **Services** page.

Figure 1 *Services Page*

The **Services** dashboard contains the following windows:

- **AIRGROUP SERVERS**—This window displays the summary of all the AirGroup servers in the network. This is the default page. For more information, see AirGroup Servers.

You can view the following information using the **Show** drop-down list.

  - **Most offered services** — Displays five services advertised by the servers, in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the **Airgroup Servers** table and view the details of the AirGroup servers that offer the selected services.
  - **Servers with highest throughput** — Displays five AirGroup servers with highest throughput (bps), in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the AirGroup server table and view the details of the servers currently advertising AirGroup services.

    The **Servers with highest throughput** option from the **Show** drop-down list is displayed only if an AppRF license is installed and DPI is enabled.

- **AIRGROUP CLIENTS**—This window displays the summary of all the AirGroup clients in the network. This is the default page. For more information, see AirGroup Clients.

You can view the following information using the **Show clients** drop-down list.

  - **Sending most service requests** — Displays five AirGroup clients that sends the most mDSN and DLNA control packets, in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the AirGroup clients table and view the details of the mDSN and DLNA control packets.
  - **With highest throughput** — Displays five AirGroup servers with highest throughput (bps), in decreasing order. Click the horizontal bar or hyperlinked number to navigate to the AirGroup clients table and view the details of the selected clients.

    The **With highest throughput** option from the **Show** drop-down list is displayed only if an AppRF license is installed and DPI is enabled.

- **UCC**— This window displays the summary of all the wireless calls made in the managed devices. The number of external calls made is displayed in the bottom right corner of the **UCC** window. This is the default page. For more information, see UCC.

You can view the following information using the **Show** and drop-down list.

  - **Call Quality** — Displays the call quality of the wireless calls. The call quality is categorized as Good, Fair, Poor, or Unknown. Select **wireless only** or **end-to-end** from **measures on** drop-down list to display the call quality of wireless only or end-to-end calls in the managed device. Click the donut chart area or hyperlinked number to navigate to the **Wireless clients** table and view the details of the wireless only or end-to-end calls in the managed device.

AirGroup Servers

Navigate to **Dashboard > Services** and click **AIRGROUP SERVERS** icon. The **AirGroup Servers** page displays the summary of all the active AirGroup servers in the managed device. See Figure 1 for **AirGroup Servers** page.

Figure 1 *AirGroup Servers Page*

Action Bar

The Action bar displays the total number of AirGroup servers depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the AirGroup servers in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

AirGroup Clients

Navigate to **Dashboard > Services** and click **AIRGROUP CLIENTS** icon. The **AirGroup Clients** page displays the summary of all the active AirGroup clients in the managed device.See Figure 1 for **AirGroup Clients** page.

Figure 1 *AirGroup Clients Page*

Action Bar

The Action bar displays the total number of AirGroup clients depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the AirGroup clients in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand a AirGroup client from the **AirGroup Clients** table to view the detailed information of individual AirGroup client. See Figure 2 for Details page.

Figure 2 *Details Page*

UCC

Navigate to **Dashboard > Services** and click **UCC** icon. The **Wireless Calls** page displays the summary of all the wireless calls made in the managed device. See for **Wireless Calls** page

> The UCC feature requires the PEFNG license.

Figure 1 *Wireless Calls Page*

Action Bar

The Action bar displays the total number of wireless calls depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the wireless clients in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand a wireless call from the **Wireless calls** table to view the detailed information of individual call like Callers, Call Information, and Call Health. See Figure 2 for Details page.

Figure 2 *Details Page*

Controller Clustering

Cluster is a combination of multiple managed devices working together to provide high availability to all the clients and ensure service continuity when a failover occurs.

The APs are managed by a single managed device. The client load is shared by all the managed devices. The goal of a cluster is to provide full redundancy to APs and wireless clients alike in case of a malfunction of one or more of its cluster members.

All the members in a cluster are active managed devices.

Cluster facilitates a large roaming domain, minimizes fault-domain, and helps in speedy recovery.

> The master controller mode does not support cluster.

The objectives of a cluster are:

- **Seamless Campus Roaming:** When a client roams between APs of different managed devices within a large L2 domain, the client retains the same subnet and IP address to ensure seamless roaming. The clients remain anchored to a single managed device in a cluster throughout their roaming area which makes their roaming experience seamless because their L2 or L3 information and sessions remain on the same managed device.
- **Hitless Client Failover:** When a managed device fails, all the users fail over to their standby managed device seamlessly without any disruption to their wireless connectivity or existing high-value sessions.
- **Client and AP Load Balancing:** When there is excessive workload among the managed devices, the client and AP load is evenly balanced among the cluster members. Both clients and APs are load balanced seamlessly.

Following sections describe the pre-requisites, key considerations, and features supported in a cluster.

Requirements

Cluster is supported only on the Mobility Master and cluster members can only be managed devices.

The following managed devices support clustering:

- 7200 Series controllers - Support for up to 12 nodes in a cluster.
- 7000 Series controllers - Support for a maximum of 4 nodes in a cluster.
- 9004 controllers - Support for a maximum of 4 nodes in a cluster.
- Mobility Controller Virtual Appliance - Support for a maximum of 4 nodes in a cluster.

Even with a 12-node cluster, the maximum supported APs and client counts are limited to 10K and 100K, respectively.

Key Consideration

Some of the key considerations are:

- All the managed devices within the cluster need to run the same software version.
- If HA-AP fast failover is enabled, then cluster cannot be enabled.
- A 12-node cluster is supported for Remote APs. Starting from ArubaOS 8.6.0.0, Remote APs can now terminate on the cluster with more than 4 nodes.
- A mix of hardware devices and the Mobility Controller Virtual Appliance-based controller is not supported.
- A Mobility Controller Virtual Appliance cluster can be set up only with same SKU models. Only homogenous clusters are supported for Mobility Controller Virtual Appliance.
- A mix of 7200 Series controllers and 7000 Series controllers within the same cluster is not recommended due to disparity in capacity between the two controller series models. However, you can use these devices in the same cluster when you want to migrate from a smaller cluster like 7000 series controllers to a larger cluster with 7200 Series controllers

Cluster Configuration

This section describes the procedure for setting up a cluster and editing a cluster profile using the WebUI and the CLI.

Configuring a Cluster

Following section describes how to configure a cluster using the WebUI. The configuration is carried out in two stages:

- Creating a cluster profile.
- Attaching the created profile to the cluster group membership.

Perform the following steps to add a cluster profile:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Services > Clusters** tab.
2. Click **+** in the **Clusters** table.
3. Enter a name for the cluster profile in the **Name** field.
4. Click **Submit**.
5. To configure the cluster created, select the cluster from **Clusters** table.
6. In the **Cluster Profile > <cluster name>** window, expand **Basic**.
7. To add controllers to the cluster, click **+** in the **Controllers** table. The **Add Controller** window is displayed.
8. Define the parameters listed in Table 1 .
9. Click **OK**.
10. Expand **Advanced**.
11. Select the **Redundancy** check box to enable redundancy in the cluster.
12. Optionally, the **Active client rebalance threshold, Standby client rebalance threshold, Unbalance threshold, and Heartbeat threshold** can be set. However, these parameters have default settings and Aruba strongly recommends you to use the default settings.

    For **Minimum Heartbeat Threshold in milliseconds**, the default setting is based on the latency determined between each pair of managed devices and the cluster. It also depends on the connection type between managed device and distribution switch (single ethernet cable, or port channel, and so on).

13. Click **Submit**.

Perform the following steps to attach the cluster profile to the cluster group membership.

14. In the **Managed Network** node hierarchy, select a managed device that you want to add to the cluster.
15. Navigate to the **Configuration > Services > Cluster** tab and expand **Cluster profile**.
16. Select a cluster profile from the **Cluster group-membership** drop-down list.
17. Set the **Exclude VLAN** field by either typing or selecting from the drop-down list to build a list of VLAN IDs separated by commas.

    In the **Exclude VLAN** drop-down list, if the user selects a VLAN ID, the selected value gets added to the already existing content in the field. For example, if the text field contains '2' and the user selects '5' from the drop-down list, the field must display '2,5'. A range of value can also be added, for example, 1-5.

18. Click **Submit**.
19. Click **Pending Changes**.
20. In the **Pending Changes** window, select the check box and click **Deploy changes**.

Cluster Load Balancing

Cluster load-balancing is achieved through the features, Client load-balancing and AP load-balancing. Both these features are explained in this section.

Client Load Balancing

The client load balancing feature ensures that clients are evenly distributed across the cluster members, thereby using the system resources efficiently.

If the system detects a distorted distribution of load, it balances the load on the managed devices by changing the UAC of these clients. The load across all the managed devices is balanced in the cluster regardless of the type of platform.

The cluster manager calculates the ratio of the existing number of clients on a managed device and its maximum capacity. Based on this ratio and additional threshold triggers, client load balancing is triggered.

When any new managed device, including the managed device that comes up after a failover, is added to an existing cluster, it is considered for load balancing and accordingly, APs and clients are moved to balance the load in the cluster.

> Load balancing is enabled by default when a cluster is configured.

Threshold triggers

- **Active client rebalance threshold:** The actual active load on a cluster member. The threshold is set at 20%, that is, 20% of the capacity of a platform.
- **Standby client rebalance threshold:** The standby load on a cluster member. The threshold is set at 40%.
- **Unbalanced threshold:** The difference between the loads on maximum loaded cluster node and the minimum loaded cluster node. The threshold is set at 5%, that is, there must be at least a 5% disparity in load between the managed devices.
- **AP Total Load Balance threshold:** The total load balance threshold is set to 40%. This is the default value and cannot be configured.

For load balancing to be triggered for active clients, the active client rebalance threshold and the unbalanced threshold percentages must be met. Similarly, for the standby client, the standby client rebalance threshold and the unbalanced threshold percentages must be met.

> When the redundancy mode is enabled, the capacity of the cluster is reduced to half.

AP Load Balancing

The AP load balancing feature ensures that the cluster leader manages the load balancing based on the platform capacity. The AP is dynamically assigned an AAC when it connects to a cluster. Here, instead of client load, AP load is considered.

Both active and standby APs are considered for load balancing.

Following is the AP load balancing criteria if a managed device is newly added:

- When an AP threshold is already met in the cluster nodes, if a new managed device is added, the Active AP table of the new managed device is filled first based on AP count set.
- When the threshold is not met, APs are moved to standby AP table of the newly added managed device.
- The count of these APs will increment based on the AP count set only after the stabilization of the cluster, however, the APs that were moved during this phase cannot be always based on AP Count.

> Starting from ArubaOS 8.3.0.0, the Active AP load balancing feature is enabled by default. In previous releases, this feature is disabled by default.

Cluster Deployment Scenarios

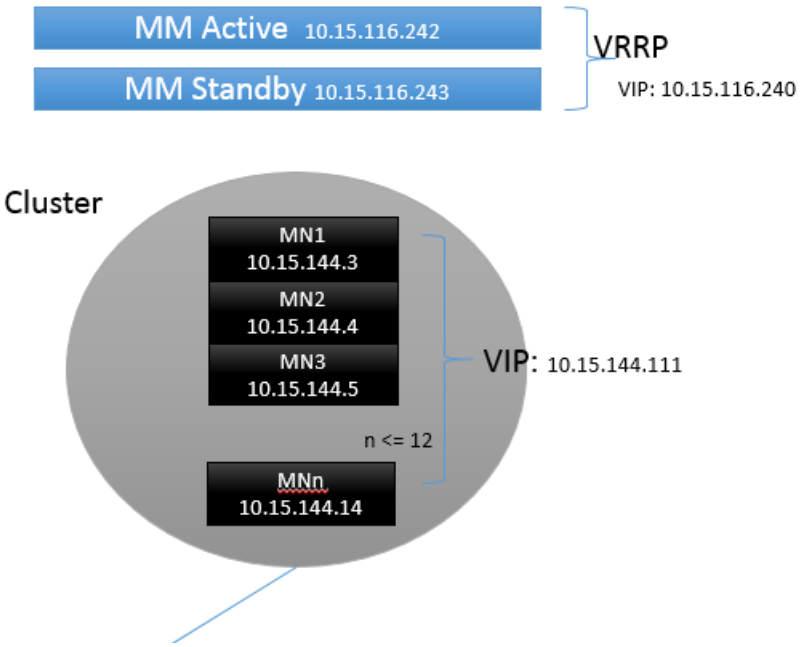
Clusters can be deployed in four different scenarios. The following section describes the guidelines for these different cluster deployment scenarios.

> Aruba recommends you to enable AP load balancing for cluster using the CLI command **active-ap-lb**. It is enabled by default.

> If **active-ap-lb** is disabled, LMS is used for the initial termination. LMS preemption is used as described in all scenarios mentioned.

Scenario 1: Cluster with Virtual IP Setup

In this scenario, an AP performs a cluster failover to the S-AAC if the A-AAC (LMS) is down. The APs perform internal rebootstrap if both A-AAC and S-AAC are down at the same time. If the AP reboots on any node including the LMS, the AP remembers the nodelist and tries all the entries in the nodelist. The AP performs a legacy rebootstrap only when it cannot reach any of the nodes.



Following are the guidelines to ensure a successful deployment of the cluster in a Virtual IP :

- Master of the APs must be configured as the virtual IP on the cluster nodes.
- If the cluster has VRRP IP configured, set the VRRP IP in LMS IP address and backup-LMS IP addresses.
- Nodelist from the cluster node is saved on the AP. If the A-AAC and S-AAC are down at the same time, the AP will perform an internal rebootstrap and tries different nodes from the nodelist till the nodelist is exhausted.

Scenario 2: Cluster with Multiple Master via DNS resolution

In this scenario, an AP will perform a cluster failover to the S-AAC if the A-AAC (LMS) is down. The AP internally rebootstraps if both A-AAC and S-AAC are down at the same time and the AP tries to contact another node in the cluster till it is unable to reach the entire nodelist in the cluster. If the

Upgrading Cluster

The Live Upgrades feature allows you to upgrade the managed devices and APs in a cluster to the latest ArubaOS version. Managed devices in a cluster can be seamlessly upgraded by specifying the new image file and a target partition. This is a real-time network upgrade where managed devices and APs upgrade automatically without any planned maintenance downtime.

You can also schedule an upgrade to a specified time to avoid manual intervention. The cluster is upgraded automatically at the scheduled time. You can view, delete, or reschedule the scheduled cluster upgrade.

When a cluster is upgraded, the following actions take place:

1. The cluster upgrade manager sends information of the APs to AirMatch.
2. The AirMatch creates logical groups of APs and updates the cluster upgrade manager with this information.
3. A target managed device is assigned to all APs in each partition.
4. The managed devices download the new firmware. The following events happen after the firmware download:
   a. One of the target managed devices is rebooted.
   b. All APs on the managed device that is rebooted move to their standby managed device.
   c. APs for which the target managed device is rebooted are preloaded.
5. The AP image is preloaded on the APs.
6. All APs in one partition are upgraded first.
7. The upgraded APs are then moved to the managed device.
8. Subsequently, all APs belonging to different partitions are preloaded, rebooted, and moved to the upgraded managed device.
9. The second target managed device is also reloaded.
10. Steps 4a to 9 are repeated till all the managed devices in the cluster are upgraded.

Following section describes how to configure Live upgrade and the limitations of live upgrade:

Configuring Live Upgrade

The following procedure describes how to upgrade the cluster:

1. Log in to a Mobility Master.
2. In the **Managed Network** node hierarchy, navigate to **Maintenance > Software Management**..
3. Select one or multiple clusters from the table. The table only lists the clusters and not the cluster members.

   The table displays the Name of the cluster, the number of managed devices, the number of APs in the cluster, and the version of software running on the managed devices of the cluster.

4. In the **INSTALLATION SETTINGS > When** menu, select **Now**.
5. In the **Image File** section, specify the image file location, name, and the protocol to use. Enter values for the following parameters:

- **Server IP address**—IP address of the server
- **Image path**—Path of image file
- **Software to Install**—Version to upgrade to
- **Protocol**—Protocol to use to transfer file. Valid values are: FTP, TFTP, and SCP. Default value is FTP.
- **Username**—Username of the account on the image server.
- **Password**—Password of the account on the server.

6. Click **Next.**
7. In the **Target Partition** section, specify the managed device partition where you want to install the firmware and where you want it to boot from

Scheduling a Cluster Upgrade

Starting from ArubaOS 8.4.0.0, scheduled cluster upgrade allows you to schedule the upgrade to a specified time to avoid manual intervention. The cluster is upgraded automatically at the scheduled time. You can view, delete, or reschedule the scheduled cluster upgrade.

You can also schedule cluster upgrade for one or more profiles at the same time or different times.

When a Mobility Master reboots or a process restarts, this feature has the ability to preserve the configured scheduled upgrades. It also allows you to synchronize the scheduled upgrades to a standby Mobility Master. If a Mobility Master has active and standby devices configured, then the scheduled upgrade information will be synchronized between active and standby through database synchronization. The upgrade is initiated when the Mobility Master becomes active.

Key Considerations

- Upgrades can be schedule only to a future time, maximum of 30 days from the managed device's current time.
- The time scheduled is always in reference to the managed devices in a cluster.
- All the network nodes have to be NTP synchronized.

Limitation

- DST time change hour is not automatically adjusted for a scheduled upgrade.
- Time changed manually in a managed device is not automatically adjusted for a scheduled upgrade.

Configuring a Scheduled Upgrade

To configure a scheduled upgrade, perform the following steps either through WebUI or CLI:

To configure a scheduled cluster upgrade, refer to the Scheduling Upgrade of Clusters section.

To schedule a scheduled cluster upgrade:

```
(host) [mm] (config) #lc-cluster <cluster_prof> schedule upgrade <version> <year> <month> <day> <hh> <mm> <ss>
```

Parameter	Description
cluster_prof	Cluster profile for which upgrade is scheduled
version	The version to which the cluster will get upgraded to
year	Year of the upgrade
month	Month of the upgrade
day	Day of the upgrade
hh	Hour of the upgrade
mm	Minutes of the upgrade
ss	Seconds of the upgrade

Example:

```
(host) [mm] (config) #lc-cluster <cluster_prof> schedule upgrade version 8.4.0.0-sangiovese_73823 2018 04 10 00 00 00
```

Viewing the Scheduled Cluster Upgrade Status

```
(host) [mm] #show lc-cluster scheduled-upgrades
```

Troubleshooting Cluster

This section provides commands that can be used to troubleshoot different scenarios in a cluster configuration.

The different control plane processes in the cluster are GSM manager (GSM), cluster manager (CM), Station Manager (STM), and AUTH. On the AP, the main modules are A-STM and ASAP (datapath).

The following is a list of some common troubleshooting scenarios in a cluster:

Cluster Formation Unsuccessful

All managed devices in a cluster are collectively known as cluster members. The cluster formation is successful when all the managed devices in the cluster are connected to each other.

Some of the reasons because of which a cluster formation is unsuccessful are as follows:

1. If the cluster group membership is not executed.
2. If all the managed devices are not listed in cluster.
3. If there is a connectivity issue and managed devices are not able to reach their peer.
4. If IPsec SA is not formed.

To check the status of the cluster formation, execute the **show lc-cluster group membership** command.

```
(host) [mynode] #show lc-cluster group-membership
Mon Dec 21 17:30:51.952 2015
Cluster Enabled, Profile Name = "6NodeCluster"
Redundancy Mode On
Active Client Rebalance Threshold = 50%
Standby Client Rebalance Threshold = 75%
Unbalance Threshold = 5%
Cluster Info Table
------------------
Type IPv4 Address    Priority Connection-Type STATUS
---- --------------- -------- --------------- ------
self     10.15.116.3      128             N/A ISOLATED (Leader)
peer     10.15.116.4      128    L3-Connected CONNECTED-FROM-SELF-DISCONNECTED-FROM-PEERS
peer     10.15.116.5      128    L3-Connected CONNECTED-FROM-SELF-DISCONNECTED-FROM-PEERS
peer     10.15.116.8      128    L3-Connected CONNECTED-FROM-SELF-DISCONNECTED-FROM-PEERS
peer     10.15.116.9      128             N/A SECURE-TUNNEL-NEGOTIATING
peer    10.15.116.10      128             N/A SECURE-TUNNEL-NEGOTIATING

DISCONNECTED
INCOMPATIBLE
DISCONNECTED-FROM-SELF-CONNECTED-FROM-PEERS",
CONNECTED-FROM-SELF-DISCONNECTED-FROM-PEERS",
SECURE-TUNNEL-NEGOTIATING
SECURE-TUNNEL-ESTABLISHED
CONNECTED
```

Table 1: *Cluster state*

State	Reason
INCOMPATIBLE	This error can occur in the following scenario: ▪ If two managed devices are running different ArubaOS versions, then a build string mismatch is found and the managed devices are not part of the cluster.
DISCONNECTED	This error can occur in the following scenario:

Managed Devices at Branch Offices

Many distributed enterprises with branch and remote offices and locations use cost-effective hybrid WAN connectivity solutions that include low-cost DSL, 4G and LTE technologies, rather than relying solely on traditional E1/T1 or T3/E3 dedicated circuits. 7000 Series Cloud Services Controllers are optimized for these types of locations, which are more likely to use cloud security architectures instead of dedicated security appliances, and where clients are likely to access applications in the cloud, rather than on local application servers.

Provision and Configure Managed Devices

This chapter describes ArubaOS features designed to optimize the configuration and performance of managed devices in branch and remote offices, and lists the procedures to configure these features.

Learn more about Managed Device Optimization

Select any of the links below to view detailed information about ArubaOS features for managed device configuration and management, and examples of deployment topologies that support these features.

- Managed Device Feature Overview
- Zero-Touch Provisioning Overview
- WAN Authentication Survivability Overview
- Managed Device WAN Dashboard

Provision and Configure a Managed Device

The following sections describe the procedures to configure your network for zero-touch managed device provisioning, and to define configuration settings for a group of managed devices.

- Using ZTP with DHCP to Provision a Managed Device
- Health Check Services for Managed Devices
- WAN Optimization Through IP Payload Compression
- WAN Interface Bandwidth Priorities
- Uplink Monitoring and Load Balancing
- Hub and Spoke VPN Configuration
- IP Routes Configuration
- Uplink Routing using Next-hop Lists
- Policy Based Routing
- Address Pool Management
- Configuring WAN Authentication Survivability
- Preventing WAN Link Failure on Virtual APs
- Managed Device Integration with a Palo Alto Networks Portal

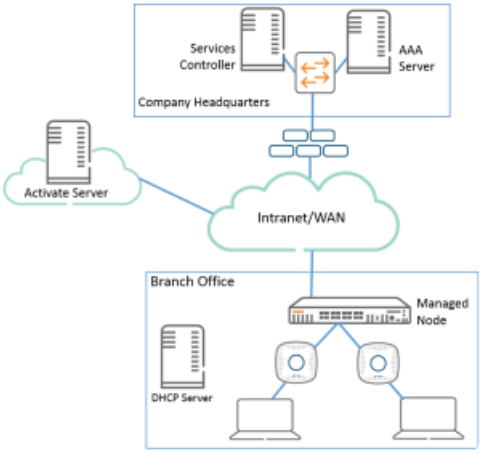
Managed Device Feature Overview

ArubaOS supports these distributed enterprises through the following features designed specifically for managed devices in branch and remote offices:

- Authentication survivability allows managed devices to store user access credentials and key reply attributes whenever clients are authenticated with external RADIUS servers or LDAP authentication servers, providing authentication and authorization survivability when remote authentication servers are not accessible.
- Integration with existing Palo Alto Networks Firewalls, like WildFire™ anti-virus and anti-malware detection services. In deployments with multiple Palo Alto Networks firewalls, managed devices can select the best PAN firewall based on priority and availability.
- Policy-based routing on each uplink interface, which allows you specify the next hop to which packets are routed. ArubaOS supports multiple next-hop lists, to ensure connectivity in the event that a device on the list becomes unreachable.
- Uplink and VPN redundancy, and per-interface bandwidth contracts to limit traffic for individual applications (or categories of applications) either sent from or received by a selected interface.
- Packet compression between Aruba devices (such as devices at the branch and main office), to maximize the amount of data that can be carried by the network.
- A WAN health-check feature that uses ping-probes to measure WAN availability and latency on each uplink.

The following diagram depicts a managed device topology where a managed device in the branch office learns the address, routing information, and other provisioning information from the Mobility Master.

Figure 1 *Managed Device Topology*



Scalable Site-to-Site VPN Tunnels

ArubaOS supports site-to-site IPsec tunnels based on an FQDN. When you identify the remote peer for a managed device using an FQDN, that node configuration can be applied across multiple branch managed devices, as the configured FQDN can resolve to different IP addresses for each local branch, based on local DNS settings.

Crypto maps for site-to-site VPNs support a VLAN ID as the identifier for the source network. When the VPN settings are pushed to a managed device, the IKE negotiation process uses the IP address range for the VLAN. This feature allows multiple managed devices to use a single group of configuration settings defined at a configuration node, as each managed device negotiates a different source network IP for its VLAN, based on the IP pool for the managed devices defined for that configuration node.

WAN Health Check

Zero-Touch Provisioning Overview

Traditionally, the deployment of controllers was a multiple step process where the master controller information and local configurations were first pre-provisioned. After the managed device connected to the network, it established a secure tunnel to the master and downloaded the global configuration. ZTP automates deployment of managed devices plug-n-play. The managed device now learns the required information from the network and provisions itself automatically. ArubaOS allows a managed device to automatically get its local and global configuration and license limits from Mobility Master.

This section includes the following topics:

> For more information about the procedures to prepare your network for ZTP, see Using ZTP to Provision a Managed Device.

Why use ZTP?

ZTP offers the following advantages over a standard managed device configuration:

- Simple deployment
- Reduced operational cost
- Limits to provisioning errors

A managed device configured using ZTP automatically discovers the Mobility Master, downloads its local configuration from that Mobility Master, and is provisioned with its device role, and country code.

> The local configuration is the configuration that is specific to a managed device. That is, not the global configuration shared by a network of managed devices. This includes, but is not limited to, IP addresses and VLANs.

Once the managed device is provisioned, it is ready to obtain its global configuration in either of two ways:

- The administrator enters the global configuration via the WebUI or CLI of the Mobility Master.
- The managed device retrieves its global configuration from the Mobility Master.

Device-specific configurations that are common across multiple devices can be modified from a central location using the bulk edit feature. Users can apply common device configurations to a group of devices without having to update each device individually. Bulk edit supports, but is not limited to, the following configurations:

- Time zone
- Daylight savings time setting
- VLANs
- Managed device IP addresses
- DHCP pools

Managed Device Provisioning Modes

The administrator has the choice of provisioning modes that select how the managed device is supplied with its own IP address, role, country code, and configuration settings.

Once the managed device learns the IP address of the primary Mobility Master, the managed device contacts that Mobility Master and retrieves its configuration from its assigned configuration node.

> Before you deploy a managed device, use you must create a configuration for that device at a configuration node on Mobility Master. Mobility Master pushes this configuration to the managed device when the device becomes active on the network.

WAN Authentication Survivability Overview

Authentication survivability is critical to managed device WLANs since most managed devices use geographically remote authentication servers to provide authentication and authorization services. When those authentication servers are not accessible, clients cannot access the WLAN because the managed device cannot authenticate them. ArubaOS authentication survivability allows managed devices to provide client authentication and authorization survivability when remote authentication servers are not accessible. When this feature is enabled, ArubaOS stores user access credentials and key reply attributes whenever clients are authenticated with external RADIUS servers or LDAP authentication servers. When external authentication servers are not accessible, the managed device uses its internal survival server to continue providing authentication and authorization functions by using the user access credentials and key reply attributes that were stored earlier.

When authentication survivability is enabled, an internal survival server on the managed node performs authentication functions, as well as EAP-termination using the RADIUS protocol. The survival server performs authentication or query requests when authentication survivability is enabled, *and* one of the following is true:

1. All servers are out of service in the server group if fail-through is disabled.
2. All in-service servers failed the authentication and at least one server is out of service when fail-through is enabled.

All access credentials and key reply attributes saved in the local survival server remain in the system until they expire. The system-wide lifetime parameter **auth-survivability cache-lifetime** has a range from 1 to 168 hours, and a default value of 24 hours. Expired user credential attributes and key reply attributes stored in the survival server cache are purged every 10 minutes.

> Best practices is to import a customer server certificate into the managed device and assign it to the local survival server.

The survival server can store the following types of client data:

- Client username
- Encrypted Passwords. For PAP authentication, the survival server receives the password provided by the client and then stores the encrypted SHA-1 hashed value of the password.
- EAP indicator: When employing 802.1X with disabled termination using EAP-TLS, the EAP indicator is stored.
- The CN lookup *EXIST* indicator

Supported Client and Authentication Types

The following combination of clients and authentication types are supported with the authentication survivability feature see the table below:

Table 1: *Clients and Supported Authentication Types*

Clients	Authentication Methods
Captive Portal clients	PAP
802.1X clients	▪ *Termination disabled*: Extensible Authentication Protocol-Transport Layer Security with an external RADIUS server ▪ *Termination enabled*: EAP-TLS with CN lookup with an external authentication server
External Captive Portal clients using the XML-API	PAP
MAC-based Authentication clients	PAP
VPN clients	▪ PAP with an external authentication server ▪ CN lookup with an external authentication server
VIA and other VPN clients	PAP method and CN lookup

Managed Device WAN Dashboard

The **WAN** dashboard, in the **Monitoring** section of the WebUI, is the default landing page for a managed device with uplinks defined via the uplink manager. Starting with ArubaOS 8.1.0.0, the WAN dashboard also appears in the Mobility Master WebUI when a branch office controller is selected in the network hierarchy.

> For more information on defining a WAN uplink, see Uplink Monitoring and Load Balancing . For information on enabling and the uplink health check features, see Health Check Services for Managed Devices.

The WAN dashboard provides the WAN summary details for uplink VLANs, and contains the following tables:

- **Uplinks**: This section displays the **link** status and **WAN** status for VLANs monitored using the uplink manager utility. For each VLAN, the green check mark icon indicates an up status and red down arrow represents a down status for the link and WAN. The uplink health-check feature is disabled by default on managed devices. If it is enabled , the WAN status link will appear with a yellow icon, indicating that this feature is in an error state.
- **Health Score**: The health score rates the health of the uplink on a scale of 1-5, with score of 1 being lower quality and a score of 5 being the highest quality.
- **Throughput**: Displays the inbound and outbound traffic rates for the selected uplink.
- **Latency & Jitter**: Jitter is a variation in the delay times of received packets. If the **jitter measurement** option is enabled in the uplink manger, the uplink manger uses UDP packets on UDP port 4500 to measure jitter on the WAN links, and includes jitter statistics in the uplink quality calculations. Jitter statistics will not be measured if jitter measurement is not enabled in the uplink manager settings.
- **Aggregate Compression**: Displays the aggregate percentage compression on all VLANs with the compression feature enabled.

Figure 1 *WAN Monitoring Dashboard*

Using ZTP to Provision a Managed Device

When a factory-default controller boots, it starts the auto-provisioning process. The following sections describe the provisioning workflow, and the process to prepare your network for ZTP for a managed device.

When a managed device establishes an HTTPS connection to the Activate server and requests provisioning information, the Activate server authenticates the managed device and provides that device with provisioning information, including the IP address of its Mobility Master and secondary Mobility Master, and its country code.

If the managed device is unsuccessful in retrieving the provisioning parameters from Activate, it will retry in 30 seconds. The managed device will keep trying to retrieve the provisioning parameters from Activate until it is successful, or the administrator initiates Mini-Setup or Full-Setup provisioning.

Before you can use Activate to associate a managed device to Mobility Master, you must configure Activate with additional device settings for each managed device and Mobility Master, create a folder for those local devices, then assign a provisioning rule to the folder that associates the managed devices to a specified master and configuration node. Use the following procedures to configure device details for the Mobility Master and managed devices, create folders, and define the provisioning rule.

Upgrading a Legacy Device via Activate

Starting with ArubaOS 8.1.0.0, a factory-default controller running ArubaOS 6.0.0.0 can use Activate Zero-Touch Provisioning to upgrade its software as part of the provisioning process. If Activate detects that a factory-default managed device running ArubaOS 6.x has been assigned a **Managed Device to Master Controller** provisioning rule, Activate will automatically send that managed device the information it needs to automatically download and upgrade to the latest version of ArubaOS.

Configuring Device details for a Managed Device

When you place an order for a controller, that device appears in the Activate **Devices** list displaying the preconfigured settings for its serial number, MAC address, and software image. Before you can add a managed device to a whitelist, you must use the Activate interface to assign a name to each managed device, and use the Activate interface to identify the Mobility Master in a managed device deployment.

The following procedure describes how to configure managed device or Mobility Master device settings using Activate:

1. Click the **Devices** icon at the top of the page to display the **Devices** page.
2. Select a managed device or Mobility Master from the **Devices** list. If the list is very large, you can click the **filter** icon by any **Devices** list column heading and choose which entries to display, then select the managed device from the smaller, filtered list.
3. If the device will be used as the Mobility Master, select the **Master Controller** check box.
4. In the **Device Detail** section of the **Devices** page, enter the following values:
   - **Device name**: (Required) an IP address or fully-qualified domain name for the managed device or Mobility Master
   - **Full name**: (Optional) a user-friendly name for the device
   - **Description**: (Optional) a short text string describing the device
5. Click **Done** to save your settings.

Figure 1 *Device Details for a Managed Device*

Creating a New Managed Device Folder

Associate multiple managed devices to the same Mobility Master by moving those managed devices into a single Activate folder.

> A folder can contain only one model of managed device, using the same country code and mapping to the same configuration node. Different folders need to be created for managed devices of different model types, or that use a different country code or local configuration group.

Using ZTP with DHCP to Provision a Managed Device

The auto-provisioning process begins when a factory-default controller boots up. The following section describes the provisioning work flow, and also details the process to prepare your network for ZTP using DHCP.

In the absence of an Activate server, DHCP servers aid the managed devices to get information about the Mobility Master. The information required for provisioning managed devices is obtained from a DHCPv4 or DHCPv6 server.

Option 43 of DHCPv4 contains information about the Mobility Master to the managed devices. Similarly, for DHCPv6 Option 16 provides vendor related information and Option 17 provides information such as master IPv6 address, VPNC information and so on.

Following are the list of supported topologies:

- VMM with VPNC
- HMM with VPNC
- HMM without VPNC

  VPNC must be a hardware controller and not a virtual machine.

  In scenarios where both Activate and DHCP Option 43 are available, DHCP option 43 takes precedence over the Activate server. If an Activate server has to be used, then Option 43 should be removed from the DHCP server.

This feature also supports L2 Mobility Master Redundancy scenarios, where the managed device gets information about the primary Mobility Master and standby Mobility Master.

In VPNC scenarios, the managed devices get information related to primary Mobility Master, standbyMobility Master, Primary VPNC, and standby VPNC.

IPv4 Deployment Scenario

Option 43 of DHCPv4 contains the following information required to provision a managed device:

- masterip, country-code, master-mac1 (No L2 redundant Master)
- masterip, country-code, master-mac1, master-mac2 (L2 Redundant Master)
- masterip, country-code, vpnc ip, vpnc-mac1 (No L2 , Redundant VPNC)
- masterip, country-code, vpnc ip, vpnc-mac1, vpnc-mac2 (L2 Redundant VPNC)

Enter the details using one of the formats given below:

```
mip=10.9.186.001, mm1=aa:aa:aa:aa:aa:aa, cc=US
mip = 10.9.195.111 , cc= US,   vm2= 00:0C:20:C9:10:34 , vm1= 00:0C:29:B1:05:56A, vip=10.45.12.111
```

Following is an example of a DHCPv4 configuration used for ISC DHCP server software:

```
subnet 10.3.91.0 netmask 255.255.255.0 {
option vendor-class-identifier  "ArubaMC";
option vendor-encapsulated-options "mip = 10.9.196.160 , cc= US, vm2= 00:0C:29:B9:20:64 , vm1= 00:0C:29:B9:20:5A, vip=10.45
.34.187";
option domain-name-servers 10.1.10.10;
option routers 10.3.91.254;
range 10.3.91.2 10.3.91.253;
authoritative;
}
```

IPv6 Deployment Scenario

For DHCPv6, Option 16 contains Vendor Class Identifier (VCI), which is a text string that uniquely identifies a type of vendor device and Option 17 contains the following information required to provision a managed device:

- Master IPv4
- Master IPv6
- VPNC IPv6

Health Check Services for Managed Devices

The health-check feature uses ping-probes to measure WAN availability and latency on selected uplinks. Based upon the results of this health-check information, the managed device can continue to use its primary uplink, or failover to a backup link. Latency is calculated based on the round-trip time of ping responses. You must define an uplink interface via the uplink manager and enable the health check feature before the results of this health check appear in the **WAN** section of the Monitoring Dashboard.

> For more information on the WAN Dashboard, see WAN.

ArubaOS supports policy-based routing on each uplink interface, which allows you specify the next hop to which packets are routed. ArubaOS supports multiple next-hop lists, to ensure connectivity in the event that a device on the list becomes unreachable. If you are using Policy Based Routing, you can define global ping settings for all next-hop list destinations.

The **Health Check** section of the **Configuration > Services > WAN** tab allows you to configure probe measurement settings ping probe settings for the primary **WAN** uplink on the managed device, as well as for next hop links used by the policy-based routing feature

Table 1: *WAN Health Check Settings*

Parameter	Description
Health Check	Click this check box to enable the health check features.
Remote Host IP/FQDN	IP address or FQDN of a remote host to which the managed device is connected. The WAN health check feature will check the connectivity to the managed device uplink to this device.
WAN	
Probe Mode	Click the **Probe Mode** drop-down list and select **ping** or **UDP** to enable this feature.
Probe Interval (sec)	The **Probe Interval** field specifies the probe interval, in seconds. The WAN health-check feature sends the number of probes defined by the **Pocket Burst per Probe** parameter during each probe interval. To change the default interval of 10 seconds, enter a new value into this field.
Packet Burst Per Probe	The **Pocket Burst per Probe** field specifies the number of probes to be sent during the probe interval. To change the default value of 5 probes, enter a new value into this field.
Probe Retries	The number of times the managed device will attempt to resend a probe.
Jitter Measurement	If the health check feature is configured to use **UDP** probe mode, the WAN health-check feature can measure jitter on the connection to the remote host by sending and measuring packets at fixed intervals.
PBR	
Probe Mode	Click the **Probe Mode** drop-down list and select **ping** to enable this feature.
Probe Interval (sec)	The **Probe Interval** field specifies the probe interval, in seconds. The WAN health-check feature sends the number of probes defined by the **Pocket Burst per Probe** parameter during each probe interval. To change the default interval of 10 seconds, enter a new value into this field.
Packet Burst Per Probe	The **Pocket Burst per Probe** field specifies the number of probes to be sent during the probe interval. To change the default value of 5 probes, enter a new value into this field.
Probe Retries	The number of times the managed device will attempt to resend a probe. To change the default value of 3 retries, enter a new value into

WAN Optimization Through IP Payload Compression

Data compression reduces the size of data frames that are transmitted over a network link, thereby reducing the time required to transmit the frame across the network. IP payload compression is one of the key features of the WAN bandwidth optimization solution, which is comprised of the following elements:

- IP Payload Compression
- Traffic Management and QoS

> WAN optimization through IP payload compression is not supported in a 7205 controller.

The managed device can send traffic to destinations other than the corporate headquarters on the same link, so payload compression is enabled on the IPsec tunnel between the managed device and Mobility Master. Dynamic compression is used for the IP payload to achieve a high compression ratio. No compression is applied to data such as an embedded image file that might already be in a compressed format. Such data does not compress well, and may even increase in size.

The following procedure describes how to enable payload compression:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Services > WAN** tab.
2. Expand the **WAN Optimization** accordion.
3. Select the **Compression** option.
4. Click **Submit.**
5. Click **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

WAN Interface Bandwidth Priorities

ArubaOS supports minimum bandwidth guarantees per traffic class, and allows critical delay-sensitive applications like voice and video to use more bandwidth and/or be scheduled with higher priority. Each interface can be associated with a scheduler profile that supports four queues with different priority levels. If you use session ACLs to define traffic policies on the managed device, you can use the scheduler profile to automatically associate these different priority levels assigned by these policies to a scheduler profile queue.

> For information on creating a traffic policy that assigns 802.1p priority levels to a specific application or application type, see Firewall Policies

Each scheduler profile queue is assigned a priority level and one of the following scheduler discipline types:

- **Strict priority**: The queue service is based exclusively on the priority of the queue, where the lower priority queues are not serviced until the higher priority queue is clear. With this option, the highest level priority is guaranteed as much bandwidth as possible, but there can be phases where the 2nd, 3rd and 4th priority queues may receive little or no bandwidth.
- **Deficit Round Robin Weight**: The queue is assigned a percentage of available bandwidth.

> You can define both strict priority and DDR Weight discipline types for a single scheduler profile.

The following procedure describes how to enable WLAN interface bandwidth priorities using the WAN scheduler feature:

1. In the **Managed Network** node hierarchy, navigate to **Configuration > Services > WAN** tab.
2. Expand the **WAN Scheduler** accordion.
3. Click + below the **WAN Scheduler Profiles** table to define a new scheduler profile.
   a. Enter a **Profile name**.
   a. In the **Priority** fields, enter one or more 802.1p priority levels (0-7) for each queue type. Each of the seven priority levels must be supported by one of the four queues.
   b. For each queue, click the **Scheduler Discipline** drop-down list and select the **Strict Priority** or **DDR Weight** discipline type. If you select the **DDR weight** option, enter the percentage of available bandwidth that should be made available to traffic in the selected queue. This field appears to the right of the **DDR weight** option.

   > If you configure both of strict priority and Deficit Round Robin weighted queues, the strict priority queues should be specified together continuously, followed by the Deficit Round Robin weighted queues. For example, if you want to specify two strict priority queues and two DDR weighted queues, configure queue 0 and 1 with the strict priority type, then configure queues 2 and 3 with a Deficit Round Robin priority type. You cannot alternate between strict priority and DDR weighted queues.

4. To assign the scheduler profile to a cellular or Gigabit Ethernet interface, click + below the **Assignments** table.
   a. Click the **Ports** drop-down list to select an interface.
   b. In the **Transmit Rate** field, enter the maximum transmit rate for the selected interface, in Mbps.
5. Create a firewall session policy that assigns a priority level to an application or application group. For details, see Firewall Policies

The following CLI commands enable WLAN interface bandwidth priorities:

```
(host)[node](config) #scheduler-profile <map-name> {priority-map <q0-q3> <que0-prio-list>} | {queue-weights <q0-q3> <percentage_weight>}
(host)[node](config) #interface cellular|gigabitethernet <slot/module/port> transmit max-rate rate mbits <mbps> scheduler-profile <profile>
(host)[node](config) #ip access-list session  any any app salesforce permit priority 3
```

Uplink Monitoring and Load Balancing

ArubaOS 8.5.0.0 and later versions do not support the uplink load balancing feature.

Wi-Fi Uplink

Starting from ArubaOS 8.5.0.0, Wi-Fi uplink is introduced to provide connectivity of AP to an external wireless network. The 3G/4G cellular uplink and the Wi-Fi uplink can be used to extend the connectivity to places where a wired uplink cannot be configured.

Wi-Fi uplink allows an AP running ArubaOS to connect to an external wireless network or a managed device by using a third-party AP, such as a Mi-Fi device or a smart phone running a hotspot. This requires the Aruba AP running ArubaOS to work as a standard Wi-Fi client. When the standard Wi-Fi client is used as an uplink, the AP requires MAC Address Translation (MAT) to bridge the traffic between wireless or wired users of the AP and the uplink network. Wi-Fi uplink can also be used to connect the AP to another Wi-Fi service, such as a hospital wireless network.

> It is recommended to use Aruba mesh between one uplink Aruba AP and another Aruba AP. Wi-Fi uplink is used only when mesh is not suitable.

The ArubaOS AP must be provisioned with the necessary Wi-Fi uplink client parameters. After the AP reboots, it works as a standard client with the provisioned client parameters and connects with a Mi-Fi device or another AP to reach the managed device. The provisioned AP acts as both client and AP when it receives configurations from the managed device, which allows other wireless and wired clients to connect to the Aruba AP.

> Wi-Fi uplink is applicable to 802.11ac AP platforms and is supported on AP-203R, AP-203H, AP-203RP, AP-303, AP-303H, AP-303P, and AP-325 access points only.

The following sections describe how to configure a Wi-Fi Uplink profile and provision an AP with Wi-Fi uplink:

Configuring a Wi-Fi Uplink Profile

The following configuration conditions apply to Wi-Fi uplink:

- If the Wi-Fi uplink is used on 2.4 GHz or 5 GHz band, mesh or cellular uplink is disabled. The two links are mutually exclusive.
- To bind or unbind the Wi-Fi uplink on 2.4 GHz or 5 GHz band, reboot the AP.
- An AP provisioned with Wi-Fi uplink client parameters can failover to wired uplink and vice-versa, depending on the priority specified for Wi-Fi uplink and wired uplink. However, preemption is not allowed in this release.

The following procedure describes how to configure an AP with Wi-Fi uplink profile:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** tab.
2. Expand the **AP** accordion.
3. Select **WiFi uplink**.
4. Select the Wi-Fi uplink profile that you want to edit or click **+** and enter a name into the **Profile Name** dialog box to create a new profile.

   > You can create up to 16 Wi-Fi uplink profiles with different priorities in an ap-group or ap-name.

5. Configure the Wi-Fi uplink profile settings described in Table 1.

Table 1: *Wi-Fi Uplink Profile Parameters*

Parameter	Description
General	

Hub and Spoke VPN Configuration

Mobility Master supports the hub and spoke VPN topology for Aruba branch office solutions. In this topology, one or more VPN routers (remote branches or spokes) communicate with a central VPN router (VPN Concentrator or hub) using a secured tunnel. The VPN Concentrator identifies the endpoints using the TPM certificates to establish the secured tunnel. This topology allows users at remote sites to access the main network and is best suited for networks where the traffic between the remote sites and the main network is predominant with minimal inter-site traffic.

Ensure to configure the VPN Concentrator and the managed devices at the branch locations to set up a hub and spoke VPN. You can configure 7200 Series Mobility Controllers as VPN Concentrators and 7000 Series Mobility Controllers as branch office devices.

This section includes the following topics:

- Whitelisting Managed Devices on VPN Concentrator
- Configuring Auto-VPN on Managed Devices

Whitelisting Managed Devices on VPN Concentrator

In a hub and spoke VPN topology, where remote branches connect to the VPN Concentrator, newer branches are added in a staggered way. Each time a managed device is added to a branch, the branch information needs to be populated in the VPN Concentrator to whitelist the branch device. With large-scale deployments, this method is error prone and very cumbersome. The automatic whitelisting feature enables automating the process of whitelisting the branch devices to avoid extra configuration for each device at the headend.

For automatic whitelisting of managed devices in the VPN Concentrator, the authentication code method is used. In this method, the whitelisting of the device is achieved through the authentication token.

Configuring Passcode Based Whitelisting

You must configure the same VPN peer authentication passcode on the managed devices as well as the VPN Concentrator to whitelist the device in the database.

The following procedure describes how to whitelist a managed device automatically on a VPN Concentrator:

1. In the **Managed Network** node hierarchy, navigate to **Configuration> Services > VPN**.
2. Expand the **Hub and Spoke** accordion.
3. Enable the toggle switch **Hub and Spoke settings.**
4. Select **Hub (VPNC)** in **Deployment mode**.
5. Select **Automatic** in **Connection mode**.
6. Enter the same passphrase that is configured on the managed device in the **Passphrase** field for automatic whitelisting.
7. Select an encryption method from the **Encryption** drop-down list.
8. For **Custom Cert** encryption method, enter the **CA cert** and **Server cert** details.
9. Select **Route** or **Session** from the **ACL type** drop-down list based on your requirement and then select the appropriate ACL.
10. If you have overlapping uplink IP address across branches, then enter the branch pool details.
11. Click **Submit**.

The following CLI command configures the authenticate code on the Mobility Master which is used for automatic whitelisting of managed devices on a VPN concentrator where the same authenticate code is configured.

```
(host)[mynode] (config) #vpn-peer pass-code Aruba123 cert-auth factory-cert
```

Configuring MAC Address Based Whitelisting

The following procedure describes how to whitelist a managed device manually on a VPN Concentrator:

1. In the **Managed Network** node hierarchy, navigate to **Configuration> Services > VPN**.
2. Expand the **Hub and Spoke** accordion.
3. Enable the toggle switch **Hub and Spoke settings.**
4. Select **Hub (VPNC)** in **Deployment mode**.
5. Select **Manual** in **Connection mode**.
6. Click **+** from the **Branch Gateways** table to add the MAC address of the managed devices:
   - **MAC ADDRESS**—Enter the MAC address of the primary VPN Concentrator.
   - **ENCRYPTION**—Specify the encryption method. It can be **Factory Cert** or **Custom Cert**
   - **CA CERT**—Select the CA certificate for the custom certificate.
   - **SERVER CERT**—Select the server certificate for the custom certificate.
7. Click **Submit**.
8. Click **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy changes**.

Configuring VPN Tunnels on Managed Devices

You can configure the managed devices to establish a VPN tunnel with the VPN Concentrator using one of the following methods:

- By configuring Auto-VPN to automatically establish a VPN tunnel with a VPN Concentrator by advertising the branch devices.
- By configuring a VPN endpoint for the managed devices to establish a VPN tunnel.

Configuring Auto-VPN on Managed Devices

The following procedure describes how to configure Auto-VPN using branch advertisement:

1. In the **Managed Network** node hierarchy, navigate to **Configuration> Services > VPN**.
2. Click **Hub and Spoke**.
3. Enable the toggle switch **Hub and Spoke settings**.
4. Select **Hub (VPNC)** in **Deployment mode**.
5. Select **Automatic** in **Connection mode**.
6. Enter the same passphrase that is configured on the VPN Concentrator for automatic whitelisting in the **Passphrase** field.
7. Re-enter the passphrase in **Confirm Passphrase** field.
8. Click **Submit**.
9. Click **Pending Changes**.
10. In the **Pending Changes** window, select the check box and click **Deploy changes**.

Configuring VPN Endpoint for Managed Devices

The following procedure describes how to configure a specific VPN endpoint for the managed devices:

1. In the **Managed Network** node hierarchy, navigate to **Configuration> Services > VPN**.
2. Click **Hub and Spoke**.
3. Enable the toggle switch **Hub and Spoke settings**.
4. Select **Spoke (Branch Gateway)** in **Deployment mode**.
5. Select **Manual** in **Connection mode**.
6. Click **+** from the **Hubs** table to add the following VPN Concentrator hub information:
   - **Primary VPNC**—Enter the MAC address of the primary VPN Concentrator.
   - **Backup VPNC**—(Optional) Enter the MAC address of the backup VPN Concentrator.
   - **IP Address**—Enter the IP address of the VPN Concentrator.
   - **Source VLAN**—Specify the source VLAN of the managed device if more than one IP address is configured for the same VPN Concentrator.
   - **Encryption**—Specify the encryption method. It can be **Factory Cert** or **Custom Cert**.
7. Click **Submit**.
8. Click **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy changes**.

IP Routes Configuration

The managed devices and VPN Concentrator in a branch network must have IPv4 routes to determine how each device must reach Mobility Master and its VPN peers over any intermediate public or private IPv4 networks (underlay routes). Routes are also required to determine the internal networks that must be reached by the branch devices through the overlay VPN tunnels (overlay routes).

Underlay Routes

To reach WAN or the internet, the VPN Concentrators in data centers can use static routes. In case of private WAN deployments, the administrators can configure Open Shortest Path First (OSPF) routes.

managed devices, however, use the default routes obtained from service providers through DHCP or PPPoE. For private WAN deployments or MPLS routing, the administrators can configure static routes.

Overlay Routes

For overlay routes, the administrators can use IKEv2 extensions to dynamically learn networks from each connected branch. The routes can be populated in the forwarding table for each VPN Concentrator as static routes. These routes can also be redistributed into OSPF. The administrators can define static routes for each destination network and VPN Concentrator, and then configure VPN Concentrators to redistribute routes at different costs to prevent routing loops.

Configuring Static IP Routes

For overlay routing using static IP routes, ensure that you define static routes for each branch network and data center as follows:

- Static routes for each branch network must be defined on the router in the data center.
- Static routes for each branch network must be defined on the VPN Concentrator for each remote network, peer, and link.
- Static routes for each data center or a hub site must be defined for each managed device.

Creating a Static IP Route

To configure a static IP route, perform the following steps in the WebUI:

1. In the **Managed Network** node hierarchy, navigate to **Configuration> Interfaces > IP Routes** tab.
2. Expand **IP Routes** and click **+** to add a static route to a destination network or host.
3. Enter the IP address and netmask for the **Destination IP address** and **Destination network mask**, respectively.
4. Configure a forwarding setting:
   - **Using Forwarding Router Address**—Enter the next hop IP address in dotted decimal format (A.B.C.D). You can also enter the distance metric (cost) for this route. The cost prioritizes routing to the destination. The lower the cost, the higher the priority.
   - **Using IPsec Tunnel to VPNC**—Select the VPN Concentrator and the uplink to use. Select this option for a Hub and Spoke VPN configuration. For more information, see Hub and Spoke VPN Configuration.
   - **Using Site-to-Site IPsec**—Enter the IPsec map name to use in a static IPsec route map. Select this option for a site-to-site VPN. For more information, see Working with Site-to-Site VPNs.
   - **Using Null Interface**—Designate a null interface.
5. Specify a value for the **Cost**.
6. Click **Submit**.

Uplink Routing using Next-hop Lists

If the managed device uses policy-based routing to forward packets to a next-hop device, a next-hop list ensures that if the primary next-hop device becomes unreachable, the packets matching the policy can still reach their destination. ArubaOS now also allows IPv6 next-hop lists in policy-based routing. For more information on next-hop configuration, see Policy Based Routing.

Defining Next-hop Lists

The following procedure describes how to define a next-hop list:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration> Services> WAN** tab.
2. Expand the **Next Hop Configuration** accordion.
3. (Optional) In the **Health check probe interval** field, specify the probe interval, in seconds.

   The default value is 10 seconds.
4. (Optional) In the **Pocket Burst per Probe** field, specify the number of probes to be sent during the probe interval.

   The default value is 5 probes.
5. Click + below the **NextHop Lists** table to open the **NextHop** section that allows you to configure the following next-hop settings:

Table 1: *Managed Device Next-Hop Settings*

Parameter	Description
NextHop list name	Add a name for the new next-hop list. **NOTE:** You cannot use the same name for both IPv4 and IPv6 next-hop lists.
IP version	Select either **IPv4** or **IPv6** from the drop-down list, which you want to assign for the new next-hop list.

NextHops	IPv4 or IPv6 address of the next-hop device or the VLAN ID of the VLAN used by the next-hop device. If the VLAN gets an IPv4 address using DHCP, and the default gateway is determined by the VLAN interface, the gateway IP is used as the next-hop IP address.
	▪ Click + to open the **Add IPv4 NextHop** pop-up window, if you selected **IPv4** option in the **IP version** field. In the **Add IPv4 NextHop** pop-up window, select one of the following radio buttons:
	  ◦ **IP**— Enter the IPv4 address and priority of the next-hop device In the **IP address** and **Priority** fields respectively.
	  ◦ **DHCP**— Enter the VLAN ID and priority of the next-hop device In the **VLAN ID** and **Priority** fields respectively.
	▪ Click + to open the **Add IPv6 NextHop** pop-up window, if you selected **IPv6** option in the **IP version** field.
	In the **Add IPv6 NextHop** pop-up window, enter the IPv6 address and priority of the next-hop device in the **IPv6 address** and **Priority** fields.
	Use the optional **Priority** field to assign priority to next-hop device. The range is 1-255 and default value is 128.
	NOTE: You can configure a maximum of 16 next-hop devices for a next-hop list, and a maximum of 32 next-hop lists are currently supported.
	NOTE: You cannot configure IPv6 multicast, link-local, unspecified, loopback, and subnet anycast addresses as IPv6 next-hop addresses.

IPsec map name	A next-hop list may require policy-based redirection of traffic to different VPN tunnels. Select an IPsec map to redirect traffic through IPsec tunnels. Click + to open the **Add New IPsec Map** pop-up window. Select either **Using site-to-site IPSec** or **Using IPSec Tunnel to VPNC** option from the drop-down list of **Forward Settings** field, and specify the priority in the **Priority** field. **NOTE:** For IPv6 address, only **Using site-to-site IPSec** option is supported under **Forward Settings** field. If a managed device terminates a secure tunnel on a VPN concentrator, you can issue the **vpn-peer peer-mac** command on the VPN concentrator configuration to enable load balancing on secure uplinks between the VPN concentrator and a managed device. The following example enables uplinks between a managed device with the MAC address 01:00:5E:00:00:FF and a VPN concentrator, this automatically enables load balancing (host)[node](config) #vpn-peer peer-mac 01:00:5E:00:00:FF cert-auth factory-cert **NOTE:** If the peer device is an x86 server, then configure the MAC address of the management interface of the managed device. However, if the peer device is a hardware platform, you must provide the MAC address of the VLAN interface of the managed device
Preemptive-failover	If preemptive failover is disabled and the highest-priority device on the next-hop list is disabled, the new primary next-hop device remains the primary even when the original device comes back online.

6. Click **Submit.**

Policy Based Routing

A policy-based routing rule is an ACL that can forward traffic as normal, or route traffic over a VPN tunnel specified by an IPsec map, routed to a next-hop router on a next-hop list, or redirected over an L3 GRE tunnel or tunnel group.

ArubaOS now also supports IPv6 address in policy-based routing rule.

> A Policy Based Routing rule does not become active until it is applied to a VLAN interface or user role.

Associating PBR Rule with Managed Device

The following procedure describes how to associate a policy based routing rule with a managed device:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration> Services > WAN** tab.
2. Expand the **Policy-Based Routing** accordion.
3. Click **+** below the **Policies** table to create a new policy.
4. Enter the **Policy Name** in the **New Routing Policy** pop-up window and click **Submit**.

The policy type (route) is predefined in this window.

5. Select the policy created in the **Policies** table.

The **Policy > (policy name)** table is displayed.

6. Click **+** to add a new policy.
7. The **New Rule** pop-up window opens.
8. Select one of the following rule types:

- **Access Control:** Applies the rule to all traffic, or traffic using a specific service, protocol, or TCP/UDP port or range of ports.
- **Application**: Applies a rule to a traffic for an application or application category.

> The **Application** rule type is not supported for IPv6 traffic.

9. Configure the rule parameters.

Table 1: *Policy Based Routing ACL Rule Parameters*

Field	Description
IP version	Select either **IPv4** or **IPv6** from the drop-down list to specify whether the policy applies to IPv4 or IPv6 traffic.
Source (required)	Source of the traffic, which can be one of the following: ▪ **Any**: Acts as a wildcard and applies to any source address. ▪ **User**: This refers to traffic from the wireless client. ▪ **Host**: This refers to traffic from a specific host. When this option is chosen, you must configure the IP address of the host. ▪ **Network**: This refers to a traffic that has a source IP from a subnet of IP addresses. When this option is chosen, you must configure the IP address and network mask of the subnet. ▪ **Alias**: This refers to using an alias for a host or network. You configure the alias by navigating to the **Configuration > Advanced Services > Stateful Firewall > Destination** page. **NOTE:** When you select **IPv6** option in the **IP version** field, only **Any**, **Host**, and **Network** options are available as source of the traffic. **NOTE:** You cannot configure IPv6 multicast, link-local, unspecified, loopback, and subnet anycast addresses as IPv6 source addresses.

Address Pool Management

Each managed device supports one or more client DHCP pools; a pool of IP addresses that can be assigned to clients associated to that managed device, or to the node itself. In addition to the DHCP pool, the Mobility Master also allows you to create separate pools of addresses a managed device can use to dynamically assign to its uplink VLANs, use for NAT translation, or use to create a GRE tunnel to the Mobility Master. These address pools are pushed out to each managed node when it comes up on the network. If a managed node is removed from the master, the IP addresses allocated to that managed device can be reused and reassigned to a new managed node.

ArubaOS supports the following pool types:

- Configuring DHCP Address pool—When you create DHCP pool for a configuration group, that pool defines a set of IP addresses that can be assigned to client associated to managed devices in that group.
- Creating Address Pools for VLANs—Mobility Master must have a separate VLAN pool defined for each VLAN used by its managed device. A VLAN pool allocates a static, continuous block of multiple IP addresses to each managed device. The managed device acts as a DNS proxy server and dynamically assign IP addresses from its allocated pool to each AP or client on the VLAN.
- ArubaOS 8.6.0.0 Help Center—The tunnel pool on a managed node defines a range of IP addresses that the managed node uses to create a GRE tunnel within the IPsec tunnel back to the Mobility Master. Unlike VLAN pools, which allocates multiple addresses to each managed node VLAN, the tunnel DHCP pool assigns a single tunnel IP address to each managed node.
- ArubaOS 8.6.0.0 Help Center—Used by the managed device for source NAT translation. You can use a NAT pool to create a firewall policy rule to perform NAT on packets matching the rule.
- ArubaOS 8.6.0.0 Help Center—The VPN pool defines a group of IP addresses assigned to VPN clients.

DHCP Address Pools

Use the **Configuration > Services > DHCP Server** page to configure a pool of DHCP addresses. The managed device can use one of the addresses from this pool for its own IP address, and/or assign addresses in the pool to clients associating to that node.

Configuring DHCP Address pool

The following procedure describes how to configure a DHCP address pool:

1. In the **Managed Network** node hierarchy, navigate to **Configuration > Services > DHCP > DHCP Server.**
2. Click **+** below the **Pool Configuration** table.
3. Define the following values for the pool, then click **Submit**.
4. Click **Pending Changes**.
5. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Table 1: *DHCP Pool Configuration Parameters*

Parameter	Description
IP version	Assign IPv4 or IPv6 addresses
Pool Name	Give a name to the new address pool
Default router	IP address of the default router for the DHCP client. The client should be on the same subnetwork as the default router. You can specify up to eight IP addresses.
DNS Server	IP address of the DNS server. You can specify up to eight IP addresses. Multiple IP addresses must be separated by spaces.
Import from DHCP/PPPoE	Select this option to use the DNS server address obtained through PPPoE or DHCP.
Domain Name	Domain name to which the client belongs.
WINS	IP address of a NetBIOS Windows Internet Naming Service server. You can specify up to eight IP addresses. Multiple IP addresses must be separated by spaces.
Import from DHCP/PPPoE	Use the NetBIOS name server address obtained through PPPoE or DHCP.
Lease Days	The number of days that the assigned IP address is valid for the client.
Lease Hours	The number of hours that the assigned IP address is valid for the client.
Lease Minutes	The number of minutes that the assigned IP address is valid for the client.
Network IP Address Type	Choose **Static** to add a static IP address and netmask to the pool, or select **Dynamic** to define a range of addresses that the DHCP server may assign to clients. ▪ If you select **Static**, enter an IP address and netmask. ▪ If you select **Dynamic**, enter the starting and ending IP address for the address range, as well as the maximum number of hosts to be supported by the pool.
Option	Click + in **Option** to apply a client-specific option code and IP address or text string. See RFC 2132, "DHCP Options and BOOTP Vendor Extensions".

VLAN Pools

You can create address pools for VLAN and assign them to the required VLAN interfaces. This topic includes the following sections:

Creating Address Pools for VLANs

The following procedure describes how to create a VLAN pool for uplink interfaces on a managed device:

1. In the **Managed Network** node hierarchy, navigate to **Configuration > Interfaces> Pool Management** tab.
2. Expand the **VLAN Pools** accordion.
3. Click + below the **VLAN Pools** table to create a new VLAN pool
4. In the **Pool name** field, enter a name to the new pool.
5. In the **Start IP address** field, enter the IP address at the start of the range of addresses.
6. In the **End IP address** field, enter the IP address at the end of the range of addresses.
7. Click **Submit**.
8. Click **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Assigning Address Pool to VLAN

The following procedure describes how to assign a VLAN address pool to a VLAN:

1. Navigate to **Configuration > interfaces > VLAN** tab.
2. In the **VLANs** table, select the name of the VLAN to which you want to assign the DHCP pool. A **VLANS > (selected VLAN)** table appears
3. Select the VLAN ID of the VLAN to use the address pool. The **Port Members** table opens.
4. In the **Port Members** table, select the IPv4 subtab.
5. For **IP assignment**, and select VLAN Pool.
6. Click the **VLAN Pool** drop-down list and select a DHCP to associate to the VLAN.

Tunnel Pools

The following procedure describes how to use tunnel pools to create a pool of IP addresses used by the managed device to create a GRE tunnel to the Mobility Master. Each managed device uses a single IP address from this pool.

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Interfaces> Pool Management** tab.
2. Expand the **Tunnel Pools** accordion.
3. Click + below the **Tunnel Pools** table to create a new VLAN pool
4. In the **Pool name** field, enter a name to the new pool.
5. In the **Start IP address** field, enter the IP address at the start of the range of addresses.
6. In the **End IP address** field, enter the IP address at the end of the range of addresses.
7. Click **Submit**.
8. Click **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

The following procedure describes how to associate a tunnel pool to a GRE tunnel:

1. In the **Managed Network** node hierarchy, navigate to **Configuration > Interfaces > GRE Tunnels** tab.
2. Select an entry in the **GRE Tunnels** table to associate a tunnel pool to that GRE tunnel.
3. In the **IPv4 Address Type** field, select the **Dynamic** option.
4. Click the **Dynamic IP Address Pool** drop-down list and select a tunnel pool.
5. Click **Submit**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

NAT Pools

The following procedure describes how to create a pool of addresses the managed device can use for Network Address Translation:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Interfaces> Pool Management** tab.
1. Expand the **VLAN Pools** section
2. Click **+** below the **VLAN Pools** table to create a new VLAN pool.
3. In the **Pool name** field, enter a name to the new pool.
4. In the **Start IP address** field, enter the IP address at the start of the range of addresses.
5. In the **End IP address** field, enter the IP address at the end of the range of addresses.
6. Click **Submit**.
7. Click **Pending Changes**.
8. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Nat pools can associated to firewall policy rules and VPN configurations.

- For information on creating a firewall policy rule that uses the NAT pool to performs NAT translation on matching packets, see Firewall Policies.
- To apply network address translation to VPN clients , navigate to **Configuration > Services > VPN > General VPN**, enable the **Source-NAT** option, then click the **NAT** drop-down list and select the NAT pool you just created.

VPN Pools

The following procedure describes how to create a pool of addresses used by VPN clients:

1. In the **Managed Network** node hierarchy, navigate to **Configuration > Services > VPN**.
1. Expand the **General VPN** accordion.
2. Click **+** below the **Address Pools** table to create a new VPN address pool
3. In the **Pool name** field, enter a name to the new pool.
4. In the **Start address IPV4 or V6** field, enter the IP address at the start of the range of addresses.
5. In the **End address IPV4 or V6** field, enter the IP address at the end of the range of addresses.
6. Click **Submit**.
7. Click **Pending Changes**.
8. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Configuring WAN Authentication Survivability

Enable WAN survivability for managed devices on your network by navigating to the **Configuration > Authentication> Advanced** tab, then selecting the Survivability tab.

The survivability settings on this tab are described in Table 1.

> For additional information on WAN Authentication Survivability, including authentication workflows and supported client and authentication types see the WAN Authentication Survivability Overview.

Table 1: *WAN Authentication Survivability for a Managed Device*

Parameter	Description
Enable Auth-Survivability	This parameter controls whether to use the Survival Server when no other authentication servers in the server group are in-service. This parameter also controls whether to store the user access credential in the Survival Server when it is authenticated by an external RADIUS or LDAP server in the server group. Authentication Survivability is enabled or disabled at each managed device. This parameter is disabled by default. **NOTE:** Authentication Survivability will not activate if Authentication Server Dead Time is configured as 0. For more information on configuring Authentication Server Dead Time, see Configuring Authentication Timers.
Authentication Server Certificate	This parameter allows you to view the name of the server certificate used by the local Survival Server. The local Survival Server is provided with a default server certificate from ArubaOS. The customer server certificate must be imported into the managed device first, and then you can assign the server certificate to the local Survival Server.
Cache Lifetime (hrs)	This parameter specifies the lifetime in hours for the cached access credential in the local Survival Server. When the specified cache-lifetime expires, the cached access credential is deleted from the managed device. Configured authentication servers are put into the out-of-service state when authentication requests time out. The managed device picks the next server from the server group when the previous server times out or fails. When there are no more servers available from the server group, the local Survival Server processes the authentication request. When the client is authenticated with the local Survival Server, the previously stored Key Reply attributes are included in the RADIUS response. The Cache Lifetime range is from 1 to 168 hours. The default is 24 hours.
Certificate Type	Select the certificate to be used for client authentication.

Preventing WAN Link Failure on Virtual APs

In managed device deployments, the managed devices are connected across the WAN link from the Mobility Master to the RADIUS server. A WAN link outage will result in service outage as new users cannot be authenticated to 802.1X Virtual APs. This feature provides limited connectivity to managed devices even when the WAN link is down. To provide connectivity when the WAN link is down, open and PSK SSID Virtual APs are available at all times and the user can connect to these Virtual APs instead of the main 802.1X Virtual AP.

> Currently, this feature is targeted for Campus APs in managed device deployments.

When all the WAN links are down, an AP management module in the controller updates the link state using the notification it receives from the health check manager. Depending on the link state, the new set of Virtual APs are made available to the users, ensuring minimum service depending on the deployment. The Virtual APs for WAN link failure feature can be configured using the Mobility Master WebUI or command-line interface.

The following procedure describes how to prevent the WAN link failure on virtual APs:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration> System> Profiles** tab.
2. In the **All Profiles** pane, expand the **Wireless LAN** menu.
3. Expand the **Virtual AP** menu.
4. Select an existing virtual AP profile.
5. Expand the **Advanced** accordion.
6. The **WAN Operation Mode** drop-down list supports the **primary**, **always**, and **backup** WAN modes. To enable WAN link failure, set this mode to **backup**.
7. Click **Submit.**
8. Click **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Managed Device Integration with a Palo Alto Networks Portal

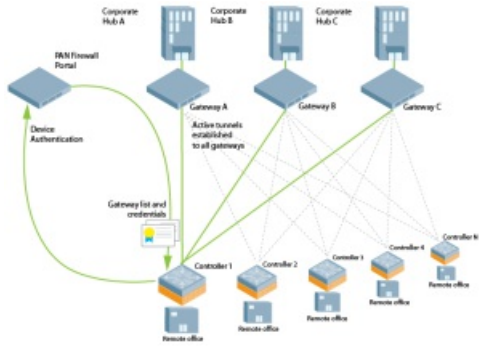
Managed devices can leverage their networks' existing Palo Alto infrastructure to access more advanced security services, including antivirus services, malware detection and seamless integration with the Palo Alto Networks WildFire™ cloud-based threat detection.

Overview

Enable Palo Alto firewall integration on Mobility Master to securely redirect internet inbound traffic from managed devices into the PAN firewall. Although this configuration setting can be used on a stand-alone Mobility Master, this feature can only be used in this types of deployments when used in conjunction with the Uplink VLAN manager feature.

The uplink VLAN manager is enabled by default on managed device uplinks. Stand-alone Mobility Masters using the PAN portal feature must enable the uplink VLAN manager using the **uplink** command in the Mobility Master command-line interface.

Figure 1 *Managed Device and PAN Firewall Integration*

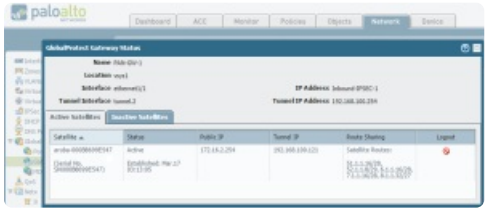


Integration Workflow

The following steps describe the work flow to integrate a managed device with a Palo Alto Networks Large-Scale VPN firewall.

1. Palo Alto Portal certificates are installed on Mobility Master, and the managed device is configured with the Palo Alto portal IP address or FQDN, Palo Alto certificate, and the username and password for device authentication using the **Configuration > Services > External Services > PAN Portal** section of the Mobility Master WebUI.
2. The managed device is provisioned via Aruba Activate and downloads its configuration (including Palo Alto Networks integration settings).
3. The Palo Alto portal may be configured with the device number (a text string comprised of the device serial number followed by its MAC address) of the managed device at each remote office site. This allows the managed device to bypass the username and password challenge to authenticate to the portal.
4. The managed device initiates a secure connection to the Palo Alto portal. Once the managed device is authenticated, the Palo Alto portal sends the managed device a list of PAN gateways and priority levels. Once the managed device is authenticated, that device appears in the PAN satellite list, as shown in the figure below.

Figure 2 *Palo Alto Networks Active Satellites List*



RF Planning and Channel Management

AirMatch is the next generation radio resource management service introduced in ArubaOS 8.0.0.0 for devices in a Mobility Master/managed device topology. AirMatch provides RF network resource allocation with unprecedented quality. It analyzes the past 24 hours of RF network statistics and proactively optimizes the network for the next day. Any RF plan change is applied in the early morning to minimize client disruption and maximize the user experience. AirMatch can react to detrimental RF events, such as radar and high noise levels, to allow the network to manage sudden changes in the RF environment.

Stand-alone controllers support only the ARM and ClientMatch features, which use automatic, infrastructure-based controls to maximize client performance and enhance the stability and predictability of the Wi-Fi network.

> AirMatch and ARM cannot be used together. ArubaOS does not support AirMatch on a standalone controller in master controller mode. A Mobility Master deployment that includes managed devices does not support Adaptive Radio Management.

This section describes the following topics:

RF Management for Mobility Master Deployments with Managed Devices

The following sections provide a general overview of the RF management used by a multi-managed device deployment managed by Mobility Master.

- AirMatch RF Management Overview
- ClientMatch Overview

The sections below describe the procedures to configure AirMatch and ClientMatch:

- Configuring AirMatch
- Configuring ClientMatch

RF Management for Deployments with a Stand-alone Controller

The following sections provide a general overview of the RF management used by stand-alone controllers:

- RF Management for Stand-alone Controller Deployments
- ClientMatch Overview

The sections below describe the steps to configure advanced ARM settings and troubleshoot common ARM issues:

- ARM Coverage and Interference Metrics
- Configuring ARM Profiles
- Troubleshooting ARM

AirMatch RF Management Overview

> ArubaOS does not support AirMatch in master controller mode.

The AirMatch channel and EIRP optimization features deprecate the channel planning and EIRP optimization features in the legacy ARM feature. AirMatch is supported on Mobility Master only, while legacy ARM channel optimization and EIRP features continue to be supported by stand-alone controllers running ArubaOS.

AirMatch channel planning evens out channel distributions in any size of network, and in any subset of the contiguous network (as much as allowed by the network configuration, regulatory domain, and AP hardware capability). AirMatch also minimizes channel coupling, where adjacent radios are assigned to the same channel. The computing power of Mobility Master impacts channel distribution calculations, so channel coupling may occasionally be allowed in complex networks to keep the computing time practical.

AirMatch EIRP planning automatically considers the local density of the network to manage the APs' coverage and MCS operation, and optimizes EIRP changes across neighboring AP radios in order to offer users the best roaming experience.

Table 1 describes some of the differences between the channel and EIRP optimization features supported by ArubaOS AirMatch and ArubaOSARM.

Table 1: *AirMatch and ARM in ArubaOS*

Features	AirMatch	ARM
Initial Release	ArubaOS 8.0.0.0	ArubaOS 2.x
Supported Topology	Mobility Master / Managed device	Stand-alone controller
Run Period	24 hours	As little as 5 minutes
RF information used	Past 24 hours of RF data	Instantaneous snapshot of the RF environment
Deployment Time	5 AM (by default) , or any time necessary **NOTE:** Starting with ArubaOS 8.1.0.0, the deployment time for each managed device is based upon the time zone configured for that device. In ArubaOS 8.0.x, the deployment time for all managed devices was based upon the time zone of the Mobility Master server.	Any time necessary
Computing Time	Depends upon network size	Less than 1 second
Optimization Scope	The entire RF network	Each individual AP

AirMatch Channel Assignments

Each AP in a Mobility Master deployment measures its RF environment for a five minute period, every 30 minutes by default. The AP then sends AMON messages about the radio feasibility to the managed device based on the AP hardware capability, radio and regulatory domain, and RF neighbors. The managed device forwards these messages to the Mobility Master. The Mobility Master adds this information to a database, computes an optimal solution, and deploys the latest RF plan by sending updated settings to the APs. By default, this configuration update is sent to each device at 5 AM (as per the system clock for each managed device), but time of this configuration update can be modified via the AirMatch profile.

> An exception to this daily update is an automatic channel change due to a radar detection event or high noise interference. If an AP detects a radar event on its current operating channel, that AP automatically changes to another supported channel to avoid radar interference, and does not wait for the daily RF configuration update from the Mobility Master. An AP may also automatically change channels if a very high noise level is detected on the current channel, if at least one other channel is free of noise.

ClientMatch Overview

ClientMatch continually monitors the RF neighborhood for each client to provide ongoing client bandsteering and load balancing, and enhanced AP reassignment for roaming mobile clients.

> Legacy 802.11a/b/g devices do not support ClientMatch. When you enable ClientMatch on 802.11n-capable devices, ClientMatch overrides any settings configured for the legacy bandsteering or load balancing features. 802.11ac-capable devices do not support the legacy bandsteering, station hand off or load balancing settings, so these APs must be managed on using ClientMatch.

The managed device aggregates information it receives from all APs using ClientMatch, and maintains information for all associated clients in a database. The managed device shares this database with the APs (for their associated clients), and the APs use the information to compute the client-based RF neighborhood and determine which APs should be considered candidate APs for each client. When the managed device receives a client steer request from an AP, the managed device identifies the optimal AP candidate and manages the client's relocation to the desired radio. This is an improvement from previous releases, where ARM was managed exclusively by APs, without the larger perspective of the client RF neighborhood.

In Mobility Master / managed device deployments where APs are connected to a managed device that is associated to Mobility Master, the AP sends RF neighborhood information to the managed device, which then forwards that information to the Mobility Master. The Mobility Master receives probe reports from all managed devices and generates a VBR for each client. These VBRs are sent from the Mobility Master to the managed device, and then to the AP to which the client is associated. APs associated to a stand-alone controller receive and collect information about clients in their neighborhood, and periodically send this information to the controller, which in turn generates VBRs and sends them directly back to the APs.

The following client or AP mismatch conditions are managed by ClientMatch:

- **Load Balancing**: ClientMatch balances clients across APs on different channels, based upon the client load on the APs and the SNR levels that the client detects from an underused AP. If an AP radio can support additional clients, the AP will participate in ClientMatch load balancing, and clients can be directed to that AP radio, subject to predefined SNR thresholds.
- **Sticky Clients**: ClientMatch also helps mobile clients that tend to stay associated to an AP despite low signal levels. APs using ClientMatch continually monitor the client RSSI as it roams between APs, and moves the client to an AP when a better radio match is found. This prevents mobile clients from remaining associated to APs with a less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients associated with that AP.
- **Band Steering/Band Balancing**: APs using the ClientMatch feature monitor the RSSI for clients that advertise dual-band capability. If a client is currently associated to a 2.4 GHz radio, and the AP detects that the client has a good RSSI from the 5 GHz radio, the managed device attempts to steer the client to the 5 GHz radio, as long as the 5 GHz RSSI is not significantly worse than the 2.4 GHz RSSI, and the AP retains a suitable distribution of clients on each of its radios.
- **HE Steering**: 802.11ax clients are best compatible with 802.11ax capable radios, resulting in better throughput and spectral efficiency. When an 802.11ax client is associated with a lower radio, ClientMatch pushes the client to the best compatible 802.11ax radio for advanced capabilities. Though STA is in good health, and is 802.11ax capable, it still sometimes connects to lower radios. ClientMatch finds a potential 802.11ax radio on the same band and the client moves to the new 802.11ax radio.

This section describes the following topics:

Incremental Rules-Based ClientMatch Updates

The ClientMatch rules that manage client associations are based primarily upon the client RF environment and apply uniformly to all client types, regardless of device type or operating system. ArubaOS 8.0.0.0 supports incremental updates to ClientMatch rules to support network devices running newer operating systems that may be incompatible with the existing ClientMatch client association rules. This feature allows the managed device to use a newer set of ClientMatch rules without updating the entire operating system, reducing network downtime.

BSS Transition Management Support

The BSS Transition Management Support feature allows ClientMatch to steer devices using 802.11v BSS transition management standards for

Configuring AirMatch

The range of RF settings that can be assigned to an the AP via the AirMatch feature is defined in the 2.4 GHz and 5 GHz radio profiles on the managed device. You can access these settings on the Mobility Master WebUI by selecting the configuration for the managed device from the configuration hierarchy, then navigating to the **Configuration > AP Groups** and **Configuration > Access Points** pages. Use these pages to specify the radio mode and range of channels and maximum channel bandwidth that can be assigned to an AP or AP group via an AirMatch solution. The AirMatch feature will not assign an AP a channel that does not fall within the group of valid channels or channel bandwidth ranges allowed by that 2.4 GHz and 5 GHz radio profile used by that AP.

The AirMatch feature performs automatic daily updates by default, but you can use the Mobility Master WebUI or command-line interface to disable daily updates for APs at one or more configuration nodes, allowing those APs and retaining their existing RF configuration. If the AirMatch updates are changed from the default **enabled** setting to **disabled**, the Mobility Master continues to receive RF updates from the APs but Mobility Master does not execute any channel or EIRP changes.

> The AirMatch **disabled** setting is different from the ARM **disable** or **maintain** setting on a standalone controller. The ARM **disable** setting changes the AP radio channel and EIRP values back to the default values specified in the 2.4 GHz and 5 GHz radio profiles for that radio. The ARM **maintain** setting freezes the current radio channel and EIRP settings. In contrast, if you use AirMatch in a Mobility Master/Managed Device topology, the AirMatch **disabled** option simply means the centralized algorithm will stop selecting a new channel, bandwidth, or EIRP setting; the network operator still can override the previous settings assigned by AirMatch with static channel or EIRP values, and the AP radio can continue to voluntarily change channels to avoid radar interference or high noise levels.

> AirMatch supports manual dual 5 GHz mode selection in AP-344 access points and auto dual 5 GHz mode selection in AP-345 access points.

The following procedure describes how to define the most commonly used AirMatch configuration settings, but some advanced AirMatch settings are only available in the CLI. The following steps hold the existing AirMatch RF configuration and will disable future updates in ArubaOS 8.0.1.0 or later:

1. In the **Mobility Master** node hierarchy, navigate to **Configuration > Services > AirMatch**.
2. Click the **Automatically deploy AirMatch optimizations** toggle switch to enable this setting.
3. To change the time of the daily AirMatch RF updates, click the **Deploy daily at** drop-down list and select an update interval (in 24-hour format).
4. Click **Submit**.
5. Select **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy changes**.

> In ArubaOS 8.0.0.0, the AirMatch WebUI was available at **Configuration > Services > More > AirMatch** page of the ArubaOS WebUI.

The following CLI command holds the existing AirMatch RF configuration and disable future updates in ArubaOS 8.0.1.0 or later:

```
(host) [mynode] (config) #airmatch profile schedule disable
```

The following CLI commands changes the time of the daily AirMatch RF updates from the default 5 AM to 2 AM, in the time zone of each managed device:

```
(host) [mynode] (config) #airmatch profile deploy-hour 2
```

Use the **quality-threshold** parameter to change the percentage of channel quality improvement that triggers a scheduled AirMatch RF update. If a proposed channel change will not produce an improvement that meets or exceeds this threshold, AirMatch does not trigger a channel plan.

```
(host) [mynode] (config) #airmatch profile quality-threshold <quality-threshold>
```

> If scheduled updates are enabled, the new channel plan is deployed on the specified deployment hour only if it is improved by greater than this threshold value. A new EIRP plan is deployed on the deployment hour every day.

Configuring ClientMatch

Use the following procedures to disable or re-enable ClientMatch, and upload a Rules-Based ClientMatch update package.

Enabling and Disabling ClientMatch

ClientMatch is enabled by default. The procedure to disable and re-enable ClientMatch varies, depending upon whether your deployment consists of multiple managed devices managed by a Mobility Master, or whether your APs are all associated to a stand-alone controller.

Mobility Master Deployments

The following procedure describes how to enable or disable the 2.4 GHz and 5 GHz radio settings for an AP:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > AP Groups** page.
2. Select the AP group from the **AP Groups** table.
3. Click the **Radio** tab below the **AP Groups** table to display the AP radio settings.
4. Expand the **Client Control** section.
5. Click the **Client match** checkbox to enable or disable both 2.4 GHz and 5 GHz radio settings. Click **Submit.**
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy changes**.

For more information on managing 2.4 GHz and 5 GHz radio settings, see 2.4 GHz and 5 GHz Radio RF Management .

Stand-alone Controller Deployments

For stand-alone controllers that do not have any associated managed devices, the ClientMatch feature is enabled and disabled in the ARM profile used by the AP, as described in Configuring ARM Profiles. Although default ClientMatch settings are recommended for most users, advanced ClientMatch settings can be configured using **rf arm-profile** commands in the command-line interface.

Uploading a Custom ClientMatch Rule Update Package

Use the WebUI or CLI to upload a custom update file of ClientMatch rules to the **/flash/config** folder on Mobility Master. This feature is not available for stand-alone controller deployments.

The following procedure describes how to upload a ClientMatch rule update package in ArubaOS 8.0.1.0 or later:

1. In the **Mobility Master** node hierarchy, select the device and navigate to **Diagnostics > Technical Support > Client Match Rules**.
2. Click **Upload File**, and then select a file to upload.
3. Click **Submit**.
4. Click **Pending Changes**.
5. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

The following CLI commands upload a ClientMatch rule update package in ArubaOS 8.0.1.0 or later:

```
(host) [mynode] (config) #copy tftp: <tftphost> <filename> flash: <destname>
(host) [mynode] (config) #copy ftp: <ftphost> <user> <password> flash: <destname>
(host) [mynode] (config) #copy scp: <scphost> <username> <password> flash: <destname>
```

RF Management for Stand-alone Controller Deployments

Aruba's ARM technology maximizes WLAN performance even in the highest traffic networks by dynamically and intelligently choosing the best 802.11 channel and transmit power for each Aruba AP in its current RF environment.

Aruba's ARM technology solves wireless networking challenges for stand-alone controllers in a large network deployment, dense deployment, or a network that must support VoIP or mobile users. Deployments with dozens of users per access point can cause network contention and interference, but ARM dynamically monitors and adjusts the network to ensure that all users are allowed ready access.

ARM continually monitors and adjusts radio resources to provide optimal network performance for APs associated to a stand-alone controller. Automatic power control can adjust AP power settings if adjacent APs are added, removed, or moved to a new location within the network, minimizing interference with other WLAN networks. ARM adjusts only the affected APs, so the entire network does not require systemic changes.

This section describes the following features:

- ARM Monitoring and Management
- Traffic Shaping
- Cellular Handoff Assist

ARM Monitoring and Management

When ARM is enabled, the Aruba AP dynamically scans all 802.11 channels in its regulatory domain at regular intervals and will report everything it sees to the controller on each channel it scans (by default, 802.11n-capable APs scan channels in all regulatory domains). This includes, but is not limited to, data regarding WLAN coverage, interference, and intrusion detection. You can retrieve this information from the controller to get a quick health check of your WLAN deployment without having to walk around every part of a building with a network analyzer. For additional information on the individual matrix gathered on the AP's current assigned RF channel, see ARM Coverage and Interference Metrics.

This section describes the following topics:

Maintaining Channel Quality

Hybrid APs and Spectrum Monitors determine channel quality by measuring channel noise, non-Wi-Fi (interferer) utilization and duty-cycles, and certain types of retries. Regular APs using ARM derive channel quality values by measuring the noise floor for both 802.11 and non-802.11 noise on that channel.

The ARM algorithm is based on what the individual AP hears, so each AP on your WLAN can effectively "self heal" by compensating for changing scenarios like a broken antenna or blocked signals from neighboring APs. Additionally, ARM periodically collects information about neighboring APs to help each AP better adapt to its own changing environment.

Configuring ARM Scanning

The default ARM scanning interval is determined by the **scan-interval** parameter in the ARM profile. If the AP does not have any associated clients (or if most of its clients are inactive), ARM will dynamically readjust this default scan interval, allowing the AP to obtain better information about its RF neighborhood by scanning non-home channels more frequently. If an AP attempts to scan a non-home channel but is unsuccessful, the AP will make additional attempts to rescan that channel before skipping it and continuing on to other channels.

The **Over the Air Updates** feature allows an AP to get information about its RF environment from its neighbors, even if the AP cannot scan. If you enable this feature, when an AP on the network scans a foreign (non-home) channel, it sends an Over-the-Air update in an 802.11 management frame that contains information about that home channel for that APl, the current transmission EIRP value of the home channel, and one-hop neighbors seen by that AP.

If ARM reports a high noise floor on a channel within a 40 MHz channel pair or 80 MHz channel set, ARM performs an additional 20 MHz scan on each channel within that channel pair or set, to determine the actual noise floor of each affected channel. This allows ARM to avoid assigning the overused channel, while still allowing channel assignments to the other unaffected channels in that channel pair or set.

Understanding ARM Application Awareness

Aruba APs keep a count of the number of data bytes transmitted and received by their radios to calculate the traffic load. When a WLAN gets very busy and traffic exceeds a predefined threshold, load-aware ARM dynamically adjusts scanning behavior to maintain uninterrupted data transfer on heavily loaded systems. ARM-enabled APs will resume their complete monitoring scans when the traffic has dropped to normal levels. You can also define a firewall policy that pauses ARM scanning when the AP detects critically important or latency-sensitive traffic from a specified host or network.

ARM's band steering feature encourages dual-band capable clients to stay on the 5 GHz band on dual-band APs. This frees up resources on the 2.4 GHz band for single-band clients like VoIP phones.

The ARM Mode Aware option is a useful feature for single radio, dual-band WLAN networks with high density AP deployments. If there is too much AP coverage, those APs can cause interference and negatively impact your network. Mode aware ARM can turn APs into Air Monitors if necessary, then turn those Air Monitors back into APs when they detect gaps in coverage. Note that an Air Monitor will not turn back into an AP if it detects client traffic (or client traffic increases), but will change to an AP only if it detects coverage holes.

Using Multi-Band ARM for 802.11a/802.11g Traffic

It is recommended that you use the **multi-band** ARM assignment and **Mode Aware** ARM feature for single-radio APs in networks with traffic in the 802.11a and 802.11g bands. This feature allows a single-radio AP to dynamically change its radio bands based on current coverage on the configured band. This feature is enabled via the ARM profile used by the AP.

When you first provision a single-radio AP, it initially operates in the radio band specified in its AP system profile. If the AP finds adequate coverage on multiple channels in its current band of operation, the **mode-aware** feature allows the AP to temporarily turn itself off and become an AP Air

Cellular Handoff Assist

Some dual-network-capable devices, such as mobile phones, prefer to connect to Wi-Fi networks and may remain associated to a Wi-Fi network even when they experience poor performance at the edge of the Wi-Fi coverage area. When both the ClientMatch and the cellular handoff assist features are enabled, the cellular handoff assist feature can help a dual-mode, 3G or 4G-capable Wi-Fi device, such as an iPhone, iPad, or Android client at the end of a Wi-Fi network, switch from Wi-Fi to an alternate 3G or 4G radio that provides better network access. This feature is supported by iOS and Android devices only.

This feature is enabled via the Virtual AP profile for an AP or AP group. For more information on Virtual AP profiles and other WLAN configuration settings, see Basic WLAN Configuration

Traffic Shaping

In a mixed-client network, it is possible for slower clients to bring down the performance of the whole network. To solve this problem and ensure fair access to all clients independent of their WLAN or IP stack capabilities, an AP can implement the traffic shaping feature. This feature has the following three options:

- **default-access:** Traffic shaping is disabled, and client performance is dependent on MAC contention resolution. This is the default traffic shaping setting.
- **fair-access:** Each client gets the same airtime, regardless of client capability and capacity. This option is useful in environments like a training facility or exam hall, where a mix of 802.11a/g, 802.11g and 802.11n clients need equal to network resources, regardless of their capabilities.
- **preferred-access:** High-throughput (802.11n) clients do not get penalized because of slower 802.11a/g or 802.11b transmissions that take more air time due to lower rates. Similarly, faster 802.11a/g clients get more access than 802.11b clients.

With this feature, an AP keeps track of all BSSIDs active on a radio, all clients connected to the BSSID, and 802.11a/g, 802.11b, or 802.11n capabilities of each client. During every sampling period, airtime is allocated to each client, giving it the opportunity to receive traffic. The specific amount of airtime given to an individual client is determined by the following factors:

- Client capabilities (802.11a/g, 802.11b or 802.11n).
- Amount of time the client spent receiving data during the last sampling period.
- Number of active clients in the last sampling period.
- Activity of the current client in the last sampling period.

The **bw-alloc** parameter of a traffic management profile allows you to set a minimum bandwidth to be allocated to a virtual AP profile when there is congestion on the wireless network. You must set traffic shaping to **fair-access** to use this bandwidth allocation value for an individual virtual AP.

Traffic shaping is configured in a traffic management profile.

The following procedure describes how to configure traffic shaping:

1. In the **Mobility Master** node hierarchy, navigate to **Configuration > System > Profiles**.
2. From the **All Profiles** list, expand **QoS**.
3. Select the **Traffic management** profile.
4. In the **Profiles Details** window, select the name of the traffic management profile for which you want to configure traffic shaping. If you do not have any traffic management profiles configured, click **+** and enter a name for a new profile.

The following table describes configuration settings available in the **General** and **Advanced** sections of the traffic management profile.

Table 1: *Traffic Management Profile Parameters*

Parameter	Description
General Settings	
Station Shaping Policy	Define Station Shaping Policy This feature has the following three options: ▪ **default-access:** Traffic shaping is disabled, and client performance is dependent on MAC contention resolution. This is the default traffic shaping setting. ▪ **fair-access:** Each client gets the same airtime, regardless of client capability and capacity. This option is useful in environments like a training facility or exam hall, where a mix of 802.11a/g, 802.11g, and 802.11n clients need equal to network resources, regardless of their capabilities. The bw-alloc parameter of a traffic management profile allows you to set a minimum bandwidth to be allocated to a virtual AP profile when there is congestion on the wireless network. You must set traffic shaping to fair-access to use this bandwidth allocation value for an individual virtual AP. ▪ **preferred-access:** High-throughput (802.11n) clients do not get penalized because of slower 802.11a/g or 802.11b transmissions that take more air time due to lower rates. Similarly, faster 802.11a/g clients get more access than 802.11b clients.
Advanced Settings	

802.11ad

IEEE 802.11ad (WiGig) is a multi-gigabit Wi-Fi technology that allows managed devices to communicate at multi-gigabit speeds over a 60 GHz band. This technology comprises two radios, 5 GHz and 60 GHz.

The 802.11ad technology is supported by mesh networks and its radios support the following 2 GHz channels:

- 1 (58320MHz)
- 2 (60480MHz)
- 3 (62640MHz)
- 4 (64800MHz)

Managed devices can add the 802.11ad radio profile to store related configurations and to add 60 GHz channel entries to the regulatory domain profile.

ARM Coverage and Interference Metrics

ARM computes coverage and interference metrics for each valid channel, and chooses the best performing channel and transmit power settings for each AP's RF environment. Each AP gathers other metrics on their ARM-assigned channel to provide a snapshot of the current RF health state.

The information described below appears in the output of the **show ap arm rf-summary** command.

The following two metrics help the AP decide which channel and transmit power setting is best:

- **Coverage Index:** The AP uses this metric to measure RF coverage. The coverage index is calculated as x/y, where "x" is the AP's weighted calculation of the SNR on all valid APs on a specified 802.11 channel, and "y" is the weighted calculation of the AP SNR the neighboring APs see on that channel.

  To view these values for an AP in your current WLAN environment, issue the **show ap arm rf-summary ap-name <ap-name>** CLI command, where **<ap-name>** is the name of an AP for which you want to view information.
- **Interference Index:** The AP uses this metric to measure co-channel and adjacent channel interference. This metric is calculated and weighted for all APs, including third-party APs seen on a specified 802.11 channel and its adjacent channels. An adjacent channel is 25 MHz of the primary 20 MHz channel. For example, channel 40 is adjacent, because it is 20 MHz away from channel 36. The Interference Index is calculated as a/b/c/d, where:
  - Metric value "a" is the channel interference the AP sees on its selected channel.
  - Metric value "b" is the interference the AP sees on the adjacent channel.
  - Metric value "c" is the channel interference the AP's neighbors see on the selected channel.
  - Metric value "d" is the interference the AP's neighbors see on the adjacent channel.

  To manually calculate the total Interference Index for a channel, issue the **show ap arm rf-summary ap-name <ap-name>** CLI command, then add the values *a+b+c+d*.

  The following CLI example describes the interference index calculation involving four metric values:

```
(host) [md] (config) # show ap arm rf-summary ap-name ap1
Channel Summary
---------------
channel  retry  phy-err  mac-err  noise  util(Qual)    cov-idx(Total)  intf_idx(Total)
-------  -----  -------  -------  -----  ----------    --------------  ---------------
149      0      0        0        96     8/7/0/0/99    8/0(8)          18/11//4/1(34)
153      0      0        0        92     6/3/2/0/99    3/0(3)          32/22//3/0(57)
157      0      0        0        92     3/0/2/0/99    7/0(7)          50/13//2/5(70)
161      0      0        0        92     3/0/2/0/95    0/1(1)          7/17//5/0(29)
```

  For channel 149, the interference index values are 18/11//4/1 where:

  a= 18 (due to neighbors on channel 149)

  b = 11 (due to neighbors on channel 153)

  c = 4 (due to two-hop neighbors on channel 149)

  d = 1 (due to two-hop neighbors on channel 153)

  Hence, the interference index total on channel 149 is a+b+c+d i.e., 18+11+4+1 = 34.

Each AP also gathers the following additional metrics, which can provide a snapshot of the current RF health state. View these values for each AP using the **show ap arm rf-summary ip-addr <ap ip address>** or **show ap arm rf-summary ap-name <ap-name>** CLI command.

- Amount of Retry frames (measured in %)
- Amount of Bandwidth seen on the channel (measured in kbps)
- Amount of PHY errors seen on the channel (measured in %)
- Amount of MAC errors seen on the channel (measured in %)
- Noise floor value for the specified AP

The following enhancements are introduced in ArubaOS 8.0.0.0 to resolve issues that occur with the distributed channel/power algorithm:

Configuring ARM Profiles

ARM profile settings are divided into two categories: **General, Scanning** and **Advanced.** The general ARM settings include general configuration parameters such as channel and power assignments and minimum and maximum allowed EIRP values.

> Most network environments do not require any changes to the **Scanning** or **Advanced** categories of ARM configuration settings. If, however, your network supports a large amount of VoIP or Video traffic, or if you have unusually high security requirements you may want to manually adjust the basic ARM thresholds.

Default Profiles

When you create a new AP group and modify any of the ARM settings for that group, ArubaOS creates a unique profile for that AP group. The settings in these default profiles may vary, depending upon the radio type. The default ARM profile for a 2.4 GHz radio is Default-g, and the default profile for a 5 GHz radio is Default-a.

This section describes how to manually configure an ARM profile.

Manually Configuring an ARM Profile

The range of RF settings that can be assigned to an AP are defined in the 2.4 GHz and 5 GHz radio profiles. You can access these settings on the Mobility Master WebUI by selecting the configuration for the managed device from the configuration hierarchy, then navigating to the **Configuration > AP Groups > Radio** page. However, advanced ARM settings can be edited using the WebUI or CLI.

> The ARM profile also includes advanced ClientMatch settings that can be configured through the command-line interface only. The default values for these settings are recommended for most users, and caution should be used when changing them to a non-default value. For complete details on all ClientMatch configuration settings, refer to the

The following procedure describes how to configure an ARM profile:

1. In the **Mobility Master** node hierarchy, navigate to **Configuration > System > Profiles**.
2. Select **RF Management** from the **All Profiles** list, and then click **Adaptive Radio Management (ARM)**.
3. Select the ARM profile you want to edit, or create a new profile by clicking **+** and entering a name for the new profile in the **Profile Name** field. The ARM profile settings are divided into three sections, **General, Scanning** and **Advanced.** The profile parameters in each section are described in Table 1.

Table 1: *ARM Profile Configuration Parameters*

Parameter	Description	Default
General		
ClientMatch	The ClientMatch feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the managed device is responding to the wireless clients' probe requests. If enabled, the managed device compares whether an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is enabled by default. For details, see ClientMatch Overview .	Enabled
Scanning		
Scanning	The **Scanning** check box enables or disables AP scanning across multiple channels. This check box is selected by default. Do not disable scanning unless you want to disable ARM and manually configure AP channel and transmission power. Disabling this option also disables the following scanning features: ▪ Multi Band Scan ▪ Rogue AP Aware ▪ VoIP Aware Scan ▪ Power Save Scan	Enabled
Multi Band Scan	If enabled, single radio channel APs scan for rogue APs across multiple channels. This option requires that **Scanning** is also enabled. (The **Multi Band Scan** option does not apply to APs that have two radios, as these devices already scan across multiple channels. If one of these dual-radio devices are assigned an ARM profile with Multi Band enabled, that device will ignore this setting.)	Enabled

Dynamic Bandwidth Switch

ARM's dynamic bandwidth switch feature provides capability for ARM to detect the 20 Mhz interferer by reading the CCA statistics and other radio statistics. Once the signatures are detected, ARM moves to another 80 Mhz channel or downgrades to 40 Mhz. This feature only works when **dynamic-bw** parameter is enabled and ARM is set to use 80 Mhz assignment.

> If ARM decides to downgrade the bandwidth to 40 MHz, then it will upgrade back to 80 Mhz after the clear time based on the volume of the traffic.

Enabling Dynamic Bandwidth Switch

The following CLI commands enable and set dynamic bandwidth switch:

```
(host) [mynode] (config) #rf arm-profile default
(host) [mynode] (Adaptive Radio Management (ARM) profile "default") #dynamic-bw
(host) [mynode] (Adaptive Radio Management (ARM) profile "default") #dynamic-bw-beacon-failed-thresh
(host) [mynode] (Adaptive Radio Management (ARM) profile "default") #dynamic-bw-cca-ibss-thresh
(host) [mynode] (Adaptive Radio Management (ARM) profile "default") #dynamic-bw-cca-intf-thresh
(host) [mynode] (Adaptive Radio Management (ARM) profile "default") #dynamic-bw-clear-time
(host) [mynode] (Adaptive Radio Management (ARM) profile "default") #dynamic-bw-wait-time
```

Troubleshooting ARM

If ARM is enabled but does not seem to be working properly, try some of the troubleshooting tips below.

Too many APs on the Same Channel

If many APs are selecting the same RF channel, there may be excessive interference on the other valid 802.11 channels. Issue the CLI commands **show ap arm rf-summary ap-name <ap-name>** or **show ap arm rf-summary ip-addr <ap ip address>**and calculate the Interference index (*intf_idx*) for all the valid channels.

An AP will only move to a new channel if the new channel has a lower interference index value than the current channel. The ARM Free Channel Index parameter specifies the required difference between two interference index values. If this value is set too high, the AP will not switch channels, even if the interference is slightly lower on another channel. Lower the Free Channel Index to improve the likelihood that the AP will switch to a better channel.

Wireless Clients Report a Low Signal Level

If APs detect strong signals from other APs on the same channel, they may decrease their power levels accordingly. Issue the CLI commands **show ap arm rf-summary ap-name <ap-name>** or **show ap arm rf-summary ip-addr <ap ip address>** for all APs and check their current coverage index (*cov-idx*). If the AP's coverage index is at or higher than the configured coverage index value, then the APs have correctly chosen the transmit power setting. To manually increase the minimum power level for the APs using a specific ARM profile, define a higher minimum value with the command **rf arm-profile <profile> min-tx-power <dBm>**.

If wireless clients still report that they see low signal levels for the APs, check that the AP's antennas are correctly connected to the AP and correctly placed according to the manufacturer's installation guide.

Transmission Power Levels Change Too Often

Frequent changes in transmission power levels can indicate an unstable RF environment, but can also reflect incorrect ARM or AP settings. To slow down the frequency at which the APs change their transmit power, set the ARM backoff time to a higher value.

APs Detect Errors but Do Not Change Channels

First, ensure that ARM error checking is enabled. The ARM Error Rate Threshold should be set to a percentage higher than zero. The suggested configuration value for the ARM Error Rate Threshold is 30–50%.

APs Don't Change Channels Due to Channel Noise

APs will only change channels due to interference if you enable ARM noise checking. Check to verify that the ARM Noise Threshold is set to a value higher than 0 dBm. The suggested setting for this threshold is 75 dBm.

Access Points

Overview of Access Points

This gives an overview of the basic functions of APs, and describes the process to install and configure the APs on your network. When an AP is first installed on the network and powered on, the AP locates the managed device and the AP's designated configuration is sent from the managed device to the AP.

> APs cannot terminate either on Mobility Master or a master controller. They must terminate on managed devices only.

The default management credentials for IAP and UAP for WebUI, SSH, and console access are:

- **Username**: admin
- **Password**: serial number of the AP

The same credentials will be used if IAPs running ArubaOS versions prior to ArubaOS 8.5.0.0 are upgraded to ArubaOS 8.5.0.0 and factory reset. If the IAP is part of a cluster, the username will be admin and the password will be the serial number of any of the APs in the cluster.

If the IAP is running software version prior to ArubaOS 8.5.0.0, **admin** would continue to be the default password.

Before Deploying an AP

Before you install APs in a network environment, you must ensure that the APs are able to locate and connect to the managed device. Specifically, you must configure firewall settings to allow APs to obtain software images and configuration settings from the managed device. You must also verify that the APs are able to locate the Mobility Master, and verify that each AP is assigned a valid IP address when connected to the network.

> Mobility Master cannot be used as an AP master since APs are not allowed to terminate on a Mobility Master. If the AP manager on Mobility Master receives an AP HELLO message, the message is dropped.

The following topics describe the pre-deployment tasks. Click any of the following links for more information.

- Controller Licenses
- Understanding Firewall Port Configuration in Aruba Devices
- Discovery of Controller
- Enable DHCP to Provide APs with IP Addresses
- AP Provisioning

Mesh AP Pre-configuration

Mesh APs require the following additional steps to define the mesh networking environment.

- Configuring Mesh Cluster Profiles
- Creating and Editing Mesh Radio Profiles

Remote AP Pre-configuration

Remote APs require the following additional step to identify valid APs in the remote AP whitelist.

- Creating a Remote AP Whitelist

Controller Licenses

ArubaOS supports a centralized licensing architecture, which allows a group of managed devices to share a pool of licenses. A primary and backup Mobility Master can share a single set of licenses, eliminating the need for a redundant license set on the backup server. For information on license types, usage, and license installation, see *ArubaOS Licensing Guide*.

Understanding Firewall Port Configuration in Aruba Devices

This section describes the network ports that need to be configured on the firewall to allow proper operation of the network.

Communication Between Managed Devices

Configure the following ports to enable communication between any two managed devices:

- IPsec (UDP port 4500) for communication between Mobility Master and a managed device.
- IPsec (UDP ports 500 and 4500) and ESP (protocol 50). PAPI between Mobility Master and a managed device is encapsulated in IPsec.
- IP-IP (protocol 94) and UDP port 443 if Layer-3 mobility is enabled
- GRE (protocol 47) if tunneling guest traffic over GRE to DMZ managed device
- IKE (UDP 500)
- ESP (protocol 50)
- NAT-T (UDP 4500)

Communication Between APs and the Managed Device

APs use Trivial File Transfer Protocol (TFTP) during their initial boot to grab their software image and configuration from the managed device. After the initial boot, the APs use FTP to retrieve their software images and configurations from the managed device. In many deployment scenarios, an external firewall is situated between various Aruba devices.

Configure the following ports to enable communication between an AP and the managed device:

- PAPI (UDP port 8211). If the AP uses DNS to discover the LMS managed device, the AP first attempts to connect to the managed device. (Also allow DNS (UDP port 53) traffic from the AP to the DNS server.)
- PAPI (UDP port 8211). All APs running as Air Monitors (AMs) require a permanent PAPI connection to managed device.
- FTP (TCP port 21)
- TFTP (UDP port 69). All campus APs; If there is no local image on the AP or if the image needs to be upgraded (for example, a new AP), the AP will use TFTP to retrieve the initial image. For remote APs, upgrade the image only by FTP and not TFTP.
- SYSLOG (UDP port 514)
- PAPI (UDP port 8211)
- GRE (protocol 47)
- Control Plane Security (CPsec) uses UDP port 4500

Communication Between Remote APs and the Managed Device

Configure the following ports to enable communication between a remote AP (IPsec) and a managed device:

- NAT-T (UDP port 4500)
- TFTP (UDP port 69)

> TFTP is not needed for normal operation. If the remote AP loses its local image for any reason, it will use TFTP to download the latest image.

Discovery of Controller

An AP can discover the IP address of the controller from a DNS server, from a DHCP server, or using the Aruba Discovery Protocol.

At boot time, the AP builds a list of managed device IP addresses and then tries these addresses in order until it successfully reaches a managed device. The AP constructs its list of managed device addresses as follows:

- If the provisioning parameter is set to a DNS name, that name is resolved and all resulting addresses are put on the list. If it is set to an IP address, that address is put on the list.
- If the provisioning parameter is not set and a managed device address was received in DHCP Option 43, that address is put on the list.
- If the provisioning parameter is not set and no address was received via DHCP option 43, ADP is used to discover a managed device address and that address is put on the list.
- Managed device addresses derived from the **server-name** and **server-ip** provisioning parameters and the default managed device name **aruba-master** are added to the list. Note that if a DNS name resolves to multiple addresses, all addresses are added to the list.

This list of IP addresses provides an enhanced redundancy scheme for managed device that are located in multiple data centers separated across Layer-3 networks.

Controller Discovery Using DNS

When using DNS, AP learns multiple IP addresses to associate with a managed device. If the primary node is unavailable or does not respond, the AP continues through the list of learned IP addresses until it establishes a connection with an available managed device. This takes approximately 3.5 minutes per managed device.

> It is recommended you use a DNS server to provide APs with the IP address of the managed device because it involves minimal changes to the network and provides the greatest flexibility in the placement of APs.

APs are factory-configured to use the host name **aruba-master** for the managed device that terminates the APs. For the DNS server to resolve this host name to the IP address of the managed device, configure an entry on the DNS server for the name **aruba-master**.

Controller Discovery Using Aruba Discovery Protocol

ADP is enabled by default on all Aruba APs and managed devices. With ADP, APs send out periodic multicast and broadcast queries to locate the Mobility Master. ADP requires that all APs and managed devices are connected to the same Layer-2 network. If the devices are on different networks, you must use a Layer-3 compatible discovery mechanism, such as DNS, DHCP, or IGMP forwarding.

To use ADP discovery:

1. Execute the command **show adp config** to verify that ADP and IGMP join options are enabled on the managed device, If ADP is not enabled, you can re-enable ADP using the command **adp discovery enable** and **adp igmp-join enable**.
2. If the APs are not in the same broadcast domain as the Mobility Master, you enable multicast on the network (ADP multicast queries are sent to the IP multicast group address 239.0.82.11) for the Mobility Master to respond to the APs' queries. Ensure that all routers are configured to listen for IGMP join requests from the controller and can route these multicast packets.

Controller Discovery Using a DHCP Server

You can configure a DHCP server to provide the IP address or VRRP IP address of the Mobility Controller. Configure the DHCP server to send the managed device's IP address using the DHCP vendor-specific attribute option 43. The APs identify themselves with a vendor class identifier set to **ArubaAP** in their DHCP requests. When the DHCP server responds to a request, it will send the managed device's IP address as the value of option 43.

When using DHCP option 43, the AP accepts only one IP address. If the IP address of the managed device provided by DHCP is not available, the AP can use the other IP addresses provisioned or learned by DNS to establish a connection. For more information on how to configure vendor-specific information on a DHCP server, see "DHCP with Vendor-Specific Options" on page 1 or refer to the documentation included with your server.

AP Provisioning

AP provisioning settings allow you to define a set of additional provisioning information for an AP, such as USB modem settings, PPPoE values, or configuration settings to provision an AP as a Remote AP.

Ensure that any provisioning changes you make are complete and accurate before you save those settings. If an AP is configured incorrectly with erroneous parameters, that AP may be lost. If you want to provision APs with more than one interface, you can also configure the USB settings and interface priority levels using an AP provisioning profile.

The following procedure describes how to provision APs.

1. Navigate to the **Configuration > Access Points** window.
2. Select the AP to which you want to add new provisioning settings, then click **Provision**. The AP provisioning settings divided into two groups. By default, the ArubaOS WebUI displays configuration settings described in Table 1.

Table 1: *AP Provisioning Profile Parameters*

Parameter	Description
Name	Name assigned to an AP An AP requires a reboot before a new AP name takes effect. Therefore, wait until there is little or no client traffic passing through the AP before renaming it.
AP Group	AP group to which the AP is assigned.
Remote-AP	Select this check box to provision the APs as Remote APs. If you are provisioning Remote APs, you must also add the remote APs to the Remote AP whitelist. For details, see Remote Access Points.
Controller Discovery	Select **Use AP discovery protocol (ADP)** if you want to provide the AP with its managed device IP address, or select **Static** to manually define the managed device IP for that AP. If you select the **Static** option, you are prompted to enter the managed device's DNS name or IP address. ADP is enabled by default on all Aruba APs and managed devices. With ADP, APs send out periodic multicast and broadcast queries to locate the Mobility Master. ADP requires that all APs and managed devices are connected to the same Layer-2 network. If the devices are on different networks, you must use a Layer-3 compatible discovery mechanism, such as DNS, DHCP, or IGMP forwarding.
IP	Select **DHCP** if you have configured a DHCP server to provide the AP with the AP IP address, or select **Static** to manually define the AP IP address. If you select the **Static** option, you are prompted to enter the following information for the selected AP: ▪ IPv4 address, netmask, internet gateway used by the AP, and DNS server. ▪ IPv6 address, netmask, internet gateway used by the AP, and DNS server.
TFTP Server (Select **Show advanced options**)	IPv4 / IPv6 address of the TFTP server from which the AP can download its boot image.
Coverage Area	This setting defines the type of installation (**indoor** or **outdoor**). The **default** option indicates that the installation mode is determined by the AP model type.
Single Chain Mode	If this option is enabled for an 802.11n-capable radio, the radio will operate in single-chain mode, and will transmit and receive data using only legacy rates and single-stream HT rates up to MCS 7. This parameter is disabled by default.
PEAP username	Username of AP so that AP can authenticate to 802.1X using PEAP.
PEAP password	Password of AP so that AP can authenticate to 802.1X using PEAP.
EAP-TLS	Enable AP to 802.1x using EAP-TLS.
EAP-TLS use factory	Enable AP to use factory certificates when doing 802.1x EAP-TLS.

Overview of Basic Functions of an AP

APs use AI-powered RF optimization, rich user and application intelligence, and smart management options to improve user experiences, enhance Quality of Service (QoS), and support digital workplace initiatives. This section describes the basic functionalities of an AP. Use the Mobility Master WebUI and command-line interface to configure APs.

Table 1: *AP Configuration Function Overview*

Features and Function	Description
WLANs	A WLAN permits wireless clients to connect to the network. An AP broadcasts the SSID (which corresponds to a WLAN configured on the Mobility Master to wireless clients. APs support multiple SSIDs. WLAN configuration includes the authentication method and the authentication servers by which wireless users are validated for access. The WebUI includes a WLAN Wizard that provides easy-to-follow steps to configure a new WLAN. **NOTE:** All new WLANs are associated with the ap-group named "default".
AP operation	An AP can function as an AP that serves clients, as an AM performing network and RF monitoring, or as a hybrid AP that serves both clients and performs spectrum analysis a single radio channel. You can also specify the regulatory domain (the country) which determines the 802.11 transmission spectrum in which the AP will operate. Within the regulated transmission spectrum, you can configure 802.11a, 802.11b/g, or 802.11n (high-throughput) radio settings. **NOTE:** The 802.11n features, such as high-throughput and 40 MHz configuration settings, are supported on APs that are 802.11n standard compliant.
Quality of Service (QoS)	Configure Voice over IP call admission control options and bandwidth allocation for 5 GHz (802.11a) or 2.4 GHz (802.11b/g) frequency bands of traffic.
RF Management	Configure settings for balancing wireless traffic across APs, detect holes in radio coverage, or other metrics that can indicate interference and potential problems on the wireless network. ARM is an RF spectrum management technology that allows each AP to determine the best 802.11 channel and transmit power settings. ARM provides several configurable settings.
Intrusion Detection System	Configure settings to detect and disable rogue APs, adhoc networks, and unauthorized devices, and prevent attacks on the network. You can also configure signatures to detect and prevent intrusions and attacks.
Mesh	Configure Aruba APs as mesh nodes to bridge multiple Ethernet LANs or extend wireless coverage. A mesh node is either ▪ mesh portal: an AP that uses its wired interface to reach the managed device ▪ mesh point: an AP that establishes a path to the managed device via the mesh portal ▪ mesh auto: an AP that automatically detects the mesh role and configures mesh portal or mesh point. **NOTE:** Starting from ArubaOS 8.4.0.0, you can set mesh role to **auto** under AP provisioning. Mesh auto enables auto-detection of mesh role based on system initialization or operation. The role switches between mesh point or mesh portal depending on the ethernet link and mesh role detected packets. Mesh environments use a wireless backhaul to carry traffic between mesh nodes. This allows one 802.11 radio to carry traditional WLAN services to clients and one 802.11 radio to carry mesh traffic and WLAN services. Secure Enterprise Mesh contains more specific information on the Mesh feature.

AP Configuration Profiles

An AP configuration profile is a general name to describe any of the different groups of settings that can be defined, saved, and applied to an Access Point. ArubaOS has many different types of profiles that each allow you to configure a different aspect of an overall configuration of an AP. ArubaOS also contains a predefined “default” profile for each profile type. You can use the predefined settings in these default profiles, or create entirely new profiles that you can edit as required.

Each different AP configuration profile type can be managed using the CLI or the WebUI. To see a full list of available configuration profiles using the command-line interface, access the CLI and issue the command **show profile-hierarchy**.

To view available configuration profiles using the WebUI, navigate to **Configuration > System**, then select the **Profiles** tab.

> The profile types that appear in the **All Profiles** list may vary, depending upon the controller configuration and available licenses.

The following sections provide information on AP profiles and RF Management profiles:

AP Profiles

The AP profiles configure AP operation parameters, radio settings, port operations, regulatory domain, and SNMP information.

- **AM Filter:** Clients may assign APs or AP groups to AM filter profiles. These profiles collect data that is used to identify and monitor APs, wireless clients, and mesh nodes within the network.
- **AP Authorization:** Allows you to assign a provisioned but unauthorized AP to a AP group with a restricted configuration profile. For details see Configuring Remote AP Authorization Profiles.
- **AP Ethernet Link**: Sets the duplex mode and speed of the AP’s Ethernet link. The configurable speed is dependent on the port type, and you can define a separate Ethernet Interface profile for each Ethernet link. For details on configuring this profile, see Table 1.
- **AP LACP LMS map information:** Maps a LMS IP address to a GRE striping IP address. If the AP fails over to a standby or backup Mobility Master, the AP LACP LMS map information profile on the new LC defines the striping IP address that the AP uses for link aggregation. For details, see Configuring Port Channel LACP.
- **AP LLDP and AP LLDP-MED Network Policy:** LLDP is a Layer 2 protocol that allows network devices to advertise their identity and capabilities on a LAN. The LLDP-MED Network Policy profile defines the VLAN, priority levels, and DSCP values used by a voice or video application. Wired interfaces on Aruba APs support LLDP by periodically transmitting LLDP Protocol Data Units comprised of selected TLV elements. The AP LLDP profile identifies which TLVs will be sent by the AP. For details, see Understanding Extended Voice and Video Features.
- **AP MultiZone:** The MultiZone feature allows an AP to terminate to multiple managed devices that reside in different zones. A zone is a collection of managed devices under a single administration domain. For details, see Limitations.
- **AP system:** Defines administrative options for the managed device, including the IP addresses of the local, backup, and master controllers, RTLS server values and the number of consecutive missed heartbeats on a GRE tunnel before an AP reboots. For details on configuring this profile, see Optional AP Configuration Settings.
- **AP Wired Port:** Specifies a AAA profile for users connected to the wired port on an AP.
- **Dump Collection:**Specifies the profile for collecting core dump when an AP process crashes. For details, see Configuring the Dump Collection Profile.
- **EDCA Parameters (AP):** AP-to-client traffic prioritization, including EDCA parameters for background, best-effort, voice and video queues. For additional information on configuring this profile, see Working with QoS for Voice and Video.
- **EDCA Parameters (Station):** Client-to-AP traffic prioritization parameters, including EDCA parameters for background, best-effort, voice and video queues. For additional information on configuring this profile, see Working with QoS for Voice and Video.
- **Regulatory Domain:** Defines the AP’s country code and valid channels for both legacy and high-throughput 802.11a and 802.11b/g radios.
- **Spectrum Local Override:** configure an individual AP radio as a spectrum monitor, For details, see Converting AP to Spectrum Monitor.
- **Wi-Fi Uplink:** Configure a Wi-Fi uplink profile that allows an AP running ArubaOS to connect to an external wireless network or a managed device by using a third-party AP, such as a Wi-Fi device. For details on configuring this profile, see Uplink Monitoring and Load Balancing

Converting APs to Instant APs

Starting from ArubaOS 8.6.0.0, you can convert a Campus AP or a Remote AP to an Instant AP that is managed by Aruba Central, by using a new command—**ap convert**. However, Aruba does not support this feature for Instant AP deployments that are managed through AirWave or local WebUI, and recommends using this command only in lab or test environments for such deployments.

You can convert the APs, AP lists, or AP groups using local-flash or local image server options like ftp, tftp, http, https, or scp by copying the downloaded image from Aruba support to the local ftp/tftp/scp server. From that server, the managed device downloads the image to its ftp or tftp folder and then distributes the ftp or tftp URLs to Campus APs.

> The converted APs are limited to the highest supported version of the corresponding Instant APs. For example, if IAP-225 runs only up to Aruba Instant 8.6.0.0 version, the converted AP-225 will also support up to Aruba Instant 8.6.0.0 version.

This feature also supports conversion of APs based on AP groups or AP lists, which allows the user to manage the conversion seamlessly and also, avoid the high load on a managed device.

> Ensure to disable the load balancing feature in a cluster to avoid the AP's movement to different managed devices during conversion.

To convert APs using local-flash option, upload the images in flash before executing the following commands:

```
(host) [mynode] #ap convert active specific-aps local-flash <images>
(host) [mynode] #ap convert active all-aps local-flash <images>
```

To convert APs using image servers, execute one of the following commands depending on the mode:

```
(host) [mynode] #ap convert all-aps server ftp: <ftphost> <user> <images >
(host) [mynode] #ap convert specific-aps server ftp: <ftphost> <user> <images>
(host) [mynode] #ap convert all-aps server scp: <scphost> <user> <images >
(host) [mynode] #ap convert specific-aps server scp: <scphost> <user> <images>
(host) [mynode] #ap convert all-aps server tftp: <tftphost> <images >
(host) [mynode] #ap convert specific-aps server tftp: <tftphost> <images>
```

To add specific AP groups or AP names to convert, execute the following command:

```
(host) [mynode] #ap convert add ap-group <ap-group>
(host) [mynode] #ap convert add ap-name <ap-name>
```

To remove specific AP groups or AP names from list of conversion, execute the following command:

```
(host) [mynode] #ap convert delete ap-group <ap-group>
(host) [mynode] #ap convert delete ap-name <ap-name>
```

To clear all the APs from the list of conversion, execute the following command:

```
(host) [mynode] #ap convert clear-all
```

To abort the conversion of APs:

```
(host) [mynode] #ap convert cancel
```

Configuring Installed APs

APs and AMs are designed to require only minimal setup to make them operational in a user-centric network. Once APs have established communication with the managed device, apply advanced configuration to individual APs or groups of APs in the network using the WebUI on the managed device.

You can either connect the AP directly to a port on the managed device, or connect the AP to another switch or router that has layer-2 or layer-3 connectivity to the managed device. If the Ethernet port on the managed device is an 802.3af PoE port, the AP automatically uses it to power up. If a PoE port is not available, get an AC adapter for the AP. For more information, see the *Installation Guide* for the specific AP.

> It is recommended not to connect both the Ethernet ports of the APs to the uplink switch, because the APs act as DHCP servers to wired clients when LACP is not configured on the uplink switch. This occurs when APs with more than one Ethernet interface are not under a managed device.

If you are configuring a new AP that has never been provisioned before, first connect the AP to the managed device according the instructions included with that AP. If you are re-provisioning or reconfiguring existing active APs, this step is not necessary, as the APs are already communicating with the managed device.

You can configure an AP using the AP wizard, the provisioning profile in the WebUI, or the managed device command-line interface. The individual configuration steps vary, depending on whether the AP is deployed as a Campus AP, Remote AP, or a Mesh AP.

This following sections describe the procedure to configure an installed AP with the basic settings it requires to become operational on the network:

- Configuring an AP using AP Wizard
- Configuring a Remote AP
- Verifying the Configuration

Configuring an AP using AP Wizard

The easiest way to provision any AP is to use the AP Wizard in the managed device WebUI. This wizard will walk you through the specific steps required to provision a Campus, Remote or Mesh AP. The Wizard includes a help tab that further describes each of the configuration tasks for that deployment type.

The following procedure describes how to access the AP wizard to provision an AP:

1. Select the managed device to which the AP will be provisioned.
2. Navigate to the **Configuration** > **Access Points** page.
3. Select the new AP from the **Campus APs** list, then click **Provision.**
4. In the **General** section, click the **AP Group** drop-down list and select the AP group to which this AP should be assigned. The AP group must have at least one virtual AP.
5. (Optional) Some AP models support an external antenna in addition to their internal antenna. If the AP you are provisioning supports an external antenna, the Provisioning window displays an additional **Antenna Parameters** section.
6. (Optional) To allow the remote AP to use PEAP to authenticate to 802.1X networks, select **Show Advanced Options** under the **General** tab, then enter a user name and password in the 802.1X Parameter using PEAP section.
7. In the **IP Settings** section, define how the AP should obtain its IP address. If you have configured a DHCP server to allow APs to get addresses using DHCP, select **Obtain IP address using DHCP**. For more information on configuring a DHCP server, see Enable DHCP to Provide APs with IP Addresses. Otherwise, select **Use the Following IP address** and enter the appropriate values in the following fields:
   - **IP address**: IP address for the AP, in dotted-decimal format
   - **Subnet mask**: Subnet mask for the IP, in dotted-decimal format.
   - **Gateway IP address**: The IP address the AP uses to reach other networks.
   - **DNS IP address**: The IP address of the Domain Name Server.
   - **Domain name**: (optional) The default domain name.
8. (Optional) Access points can be configured in single-chain mode, allowing the radios of those APs to transmit and receive data using only legacy rates and single-stream HT and VHT rates on a single radio chain and single antenna or antenna interface. On APs with external antennas, this feature uses the external antenna interface labeled **A0** or **ANT0** (radio chain 0); the other (one or two) antenna interfaces are left unused. If you are provisioning an 802.11n-capable AP, select the **Enable for Radio-0** or **Enable for Radio-1** check boxes in the **Single-Chain Mode** section to enable single-chain mode for the selected radio. AP radios in single-chain mode will transmit and receive data using only legacy rates and single-stream HT rates up to MCS 7. This feature is disabled by default.
9. (Optional) Define the AP name or SNMP location. The **AP list** section displays current information for an AP, and allows you to define additional parameters for your AP, such as AP Name, SNMP System Location.
10. Click **Submit** (Re-provisioning the AP causes it to automatically reboot).

Configuring a Remote AP

A Remote AP is recommended when the network between the AP and managed device is an un-trusted/non-routable network, such as the Internet. Furthermore, a Remote AP supports an internal DHCP server, while a Campus AP does not.

The following sections provide information on Remote authentication and RAP configuration:

Remote Authentication

The two most common ways to provision an AP for remote authentication are certificate-based AP provisioning and provisioning using a pre-shared key. Although both options allow for a simple secure setup of your remote network, you should make sure that the procedure you select is supported by your managed device, the AP model type and the end user's client software. If you must provision your APs using a pre-shared key, you need to know which managed device models you have that do not support certificate-based provisioning.

- **Certificate based authentication** allows a managed device to authenticate a AP using its certificates instead of a PSK. You can manually provision an individual AP with a full set of provisioning parameters, or simultaneously provision an entire group of APs by defining a provisioning profile which contains a smaller set of provisioning parameters that can be applied the entire AP group. When you manually provision an individual AP to use certificated-based authentication, you must connect that AP to the managed device before you can define its provisioning settings.
- Use **Pre-Shared Key (PSK) authentication** to provision an individual Remote AP or a group of Remote APs using an IKE PSK.

Remote AP Configuration

Following procedure describes how to configure Remote APs:

1. Select the managed device to which the AP will be provisioned.
2. Navigate to the **Configuration > Access Points** page.
3. Open the **Remote APs** tab
4. Select the new Remote AP from the **Remote AP** list, then click **Provision**.
5. In the **General** section, click the **AP Group** drop-down list and select the AP group to which this AP should be assigned. The AP group must have at least one virtual AP.
6. (Optional) Some AP models support an external antenna in addition to their internal antenna. If the AP you are provisioning supports an external antenna, the Provisioning window displays an additional **Antenna Parameters** section.
7. (Optional) To allow the Remote AP to use PEAP to authenticate to 802.1X networks, select **Show Advanced Options** under the **General** tab, then enter a user name and password in the 802.1X Parameter using PEAP section.

Verifying the Configuration

After the AP has been configured, navigate to **Dashboard** page and verify that the AP has an **up** status. The AP on your network *does not* appear in this table, it may have been classified as an inactive AP for any of the following reasons:

- The AP is configured with a missing or incorrect VLAN. (For example, the AP is configured to use a tunneled SSID of VLAN 2 but the controller does not have a VLAN 2.)
- The AP has an unknown AP group.
- The AP has a duplicate AP name.
- An AP with an external antenna is not provisioned with external antenna gain settings.
- Both radios on the AP are disabled.
- No virtual APs are defined on the AP.
- The AP has profile errors. For details, access the command-line interface and issue the command “show profile errors”.
- The GRE tunnel between the AP and the managed device was blocked by a firewall after the AP became active.
- The AP is temporarily down while it is upgrading its software. The AP will become active again after upgrading.

Optional AP Configuration Settings

Once the AP has been installed and provisioned, you can use the WebUI or CLI to configure the optional AP settings described in the following sections:

- Spanning Tree
- PortFast
- AP Console Access Using a Backup ESSID
- Defining an RTLS Server
- AP Redundancy
- AP Maintenance Mode
- Energy Efficient Ethernet
- Smart Rate
- Configuring Energy Efficient Ethernet and Ethernet Link Speed
- Associating Ethernet Interface Link Profile with a Wired Port profile
- AP LEDs
- Suppressing Client Probe Requests
- BLE Operation Mode
- Configuring the AP System Profile
- Configuring the AP Wired Port Profile
- Configuring the Dump Collection Profile
- ArubaOS 8.6.0.0 Help Center
- ArubaOS 8.6.0.0 Help Center

Spanning Tree

The STP can prevent loops in bridged Ethernet local area networks. Spanning tree settings can be configured via the WebUI and command-line interface.

To enable this feature, enable both the **Spanning Tree** parameter in the AP system profile and the **Spanning Tree**parameter in the AP wired port profile. For details, see Configuring the AP System Profile .

PortFast

The PortFast feature is introduced to avoid network connectivity issues. These issues are caused by delays in STP enabled ports moving from blocking-state to forwarding-state after transitioning from the listening and learning states. STP enabled ports that are connected to devices such as a single switch, workstation, or a server can access the network only after passing all these STP states. Some applications need to connect to the network immediately, else they will timeout.

Spanning Tree should be enabled on the access point before enabling PortFast. If PortFast is configured, it is enabled only on access mode ports and if PortFast-Trunk is configured, it is enabled on trunk-mode ports only. Only one of them can be set based on the port's switchport mode.

Enabling PortFast on an Access Port

Before enabling PortFast ensure that the switchport mode is set to **access**:

```
(host)[mynode] #show ap wired-port-profile <profile>
```

Execute the following commands in config mode to enable PortFast on an access port:

```
(host)[mynode] (config) #ap wired-port-profile "default"
(host)[mynode] (AP wired port profile "default") #portfast
```

Enabling PortFast on a Trunk Port

Before enabling PortFast ensure that the switchport mode is set to **trunk**:

```
(host)[mynode] #show ap wired-port-profile <profile>
```

Execute the following commands in config mode to enable PortFast on a trunk port:

```
(host)[mynode] (config) #ap wired-port-profile "default"
(host)[mynode] (AP wired port profile "default") #portfast-trunk
```

AP Console Access Using a Backup ESSID

This failover system allows users to access an AP console after the AP has disconnected from the managed device. By advertising backup ESSID in either static or dynamic mode, the user is still able to access and debug the AP remotely through a virtual AP. Settings for this feature are configured using the **Password for Backup**, **RF Band for Backup**, and **Operation for backup** parameters in the AP system profile. For details, see Configuring the AP System Profile .

Defining an RTLS Server

The RTLS server configuration enables the AP to send RFID tag information to an RTLS server. Currently, when configuring the RTLS server under **ap system-profile**, you can set the **station-message-frequency** parameter in the 1-3600 seconds range. Setting the frequency to 1 means a report is sent for every station every second. A value of 5 means that a report for any particular station would be sent at 5 second intervals.

- Sending more frequent reports to the server can improve the accuracy of the location calculation.
- Configuring an AP to send reports more frequently adds additional load in terms of CPU usage.

Settings for this feature are configured using the **RTLS Server configuration** parameters in the **Advanced** section the AP system profile. For details, see Configuring the AP System Profile .

AP Redundancy

In conjunction with the managed device redundancy features described in Increasing Network Uptime With Redundancy Services the information in this section describes redundancy for APs. Remote APs also offer redundancy solutions via a backup configuration, backup managed device list, and remote AP failback. For more information relevant to remote APs, see Remote Access Points.

The AP failback feature allows an AP associated with the backup managed device (backup LMS) to fail back to the primary managed device (primary LMS) if it becomes available.

If configured, the AP monitors the primary managed device by sending probes every 600 seconds by default. If the AP successfully contacts the primary managed device for the entire hold-down period, it will fail back to the primary managed device. If the AP is unsuccessful, the AP maintains its connection to the backup managed device, restarts the LMS hold-down timer, and continues monitoring the primary managed device.

Settings for this feature are configured using the LMS IP parameters in the **LMS settings** section of the AP system profile. For details, see Configuring the AP System Profile .

AP Maintenance Mode

You can configure APs to suppress traps and syslog messages related to those APs. Known as AP maintenance mode, this setting in the AP system profile is particularly useful when deploying, maintaining, or upgrading the network. If enabled, APs stop flooding unnecessary traps and syslog messages to network management systems or network operations centers during a deployment or scheduled maintenance. The managed device still generates debug syslog messages if debug logging is enabled. After completing the network maintenance, disable AP maintenance mode to ensure all traps and syslog messages are sent. AP maintenance mode is disabled by default.

The AP maintenance mode is configured by enabling **Maintenance Mode** parameter in the **Advanced** section of the AP system profile. For details, see Configuring the AP System Profile .

The following CLI commands display the status of APs in maintenance mode:

```
show ap config {ap-group <name>|ap-name <name>|essid <name>}
show ap debug system-status {ap-name <name>|bssid <name>| ip-addr <ipaddr>}
```

Energy Efficient Ethernet

Most new models of Aruba APs support the 802.3az Energy Efficient Ethernet standard, which allows the APs to consume less power during periods of low data activity. This setting can be enabled for provisioned APs or AP groups through the Ethernet Link profile. If this feature is enabled for an AP group, any APs in the group that do not support 802.3az will ignore this setting. For more information on configuring Energy Efficient Ethernet, see Configuring Energy Efficient Ethernet and Ethernet Link Speed.

802.3az is not supported on AP-215, AP-315, and 330 Series access points.

Thermal Shutdown Support in Access Points

The Aruba 530 Series and 550 Series APs support operating temperatures of up to 50°C (indoor) or 60°C (outdoor). Starting from ArubaOS 8.6.0.0, these APs are enabled with thermal shutdown feature. The APs are equipped with an internal temperature sensor that initiate a shutdown when the AP's operating temperature crosses the set threshold. The AP then disconnects from the controller till an internal cool down is initiated. Once the AP reaches an optimum temperature, it reconnects to the controller. This process of rebootstrap and reconnection is carried out for 5 times, until the connection is restored. If the connection between the AP and the controller still does not secure, the AP remains in the shutdown state till it is manually turned on.

Smart Rate

HPE Smart Rate is a new multi-gigabit (1, 2.5, 5, 10 Gbps) twisted-pair network interface that is interoperable with the NBASE-T ecosystem of 2.5 or 5 Gbps products as well as with existing industry standard 1 GbE or 10 GbE devices. It allows the majority of existing cable installations found in campus LAN environments to provide higher bandwidth connectivity, distribute PoE power to connected devices, and secure the wired-link for next-generation 802.11ac applications.

With smart rate configuration enabled, an AP is capable of negotiating more than 1Gbps of link speed with a smart rate capable switch. 330 Seriesaccess points are capable of negotiating up to 5 Gbps speed. By default, the Ethernet interface speed is configured as **auto** (auto-negotiate) and the eth0 interface of 330 Series access points negotiate a 2.5 Gbps speed. To obtain 5 Gbps speed negotiation, enforce the speed value in the AP Ethernet Link profile. For more information on configuring the link speed, see Configuring Energy Efficient Ethernet and Ethernet Link Speed.

Configuring Energy Efficient Ethernet and Ethernet Link Speed

You can configure 802.3az or link speed using the WebUI or CLI.

The following procedure describes how to configure 802.3az EEE and Ethernet link speed:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** page.
2. Select **AP > AP Ethernet Link**, and select the Ethernet link profile you want to modify. The parameters for the profile are described in Ethernet Interface Link Profile Parameters.
3. The selected profile appears in the **Profile Details** window. The configuration parameters for the profile are described in Ethernet Interface Link Profile Parameters.
4. Select the **803.az** checkbox to enable energy efficient ethernet.
5. Select the required value from the **Speed** drop-down list to configure the Ethernet link speed. The speed value can be one of the following values:
   - **10**— 10 Mbps
   - **100**— 100 Mbps
   - **1000**—1 Gbps
   - **2500**— 2.5 Gbps
   - **5000**— 5 Gbps
   - **auto**— Auto-negotiate. This is the default value.
6. Save your changes.

The following CLI command enables support for 803.az EEE:

```
(host)[mynode] (config) #ap enet-link-profile <profile>
  dot3az
```

The following CLI commands configure the Ethernet link speed:

```
(host) [mynode] (config) #ap enet-link-profile <profile>
(host) [mynode] (AP Ethernet Link profile "<profile>") #speed <speed>
```

where <speed> can take any of the following values:

- **10**— 10 Mbps
- **100**— 100 Mbps
- **1000**—1 Gbps
- **2500**— 2.5 Gbps
- **5000**— 5 Gbps
- **auto**— Auto-negotiate. This is the default value.

Table 1 describes the Ethernet Interface Link profile parameters.

Table 1: *Ethernet Interface Link Profile Parameters*

Parameter	Description
Speed	The speed of the Ethernet interface, either 10 Mbps, 100 Mbps, 1000 Mbps (1 Gbps), or auto-negotiated.
Duplex	The duplex mode of the Ethernet interface, either full, half, or auto-negotiated.
802.3az (EEE)	Select this check box to enable support for 802.1az Energy Efficient Ethernet.
Power Over	Enable PoE for APs that support PoE.

Associating Ethernet Interface Link Profile with a Wired Port profile

By default, AP wired port profiles reference the Default Ethernet interface link profile. If you created a new Ethernet interface link profile to support 803.az, you can associate an AP wired port profile or Ethernet interface port configuration with the new Ethernet Interface link profile.

The following procedure describes how to associate a new Ethernet Interface link profile with an AP wired port profile.

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** page.
2. Navigate to **AP > AP Wired Port Profile** on the **Profile** pane, then select the AP Wired Port profile you want to modify.
3. Click the Ethernet interface link profile currently associated with the AP wired port profile you want to modify. This profile appears below the AP Wired Port Profile in the **All Profiles** list.
4. Click the **Ethernet interface link profile** drop-down list at the top of the **Profile Details** window, and select a new Ethernet interface link profile.
5. Save your changes.

The following CLI commands associate a new Ethernet Interface link profile with an AP wired port profile.

```
(host)[node] (config) #ap wired-port-profile <profile>
  enet-link-profile <profile>
```

AP LEDs

AP LEDs on 802.11n and 802.11ac APs can be configured in two modes: **normal** and **off**. In normal mode, the AP LEDs will light as expected. When the mode is set to off, all of the LEDs on the affected APs are disabled. The AP LED mode is configured by enabling the **LED Operating Mode** parameter in the **General** section of the AP system profile. For details, see Configuring the AP System Profile .

Suppressing Client Probe Requests

The anyspot client probe suppression feature decreases network traffic by suppressing probe requests from clients attempting to locate and connect to other known networks. By reducing the frequency at which these messages are sent, this feature frees up network resources and improves network performance.

When an AP is configured to use this feature, the anyspot AP radio hides its configured ESSID in beacons, and compiles a list of other ESSIDs from detected neighboring APs. If the client sends a probe request without a specified ESSID, the anyspot AP will respond with a preconfigured ESSID.

When a client searches for a preferred network, that client sends the SSID of the preferred network in the probe request. The anyspot AP checks to see if there is a neighboring AP using that ESSID that can respond to the client request. If no matching network is found, the anyspot AP sends a response to the client using the SSID from the client request. If the client is authorized to connect to the anyspot AP, that client associates to AP. Once connected to the anyspot AP, the client recognizes the ESSID to which it is connected as one associated with its preferred network, and does not send out any further probe requests.

> An AP radio can only use this feature when encryption is disabled. (That is, when the **operation mode** parameter in the AP radio WLAN SSID profile is set to **opensystem**.)

You can define a list of excluded ESSIDs to which the anyspot AP will not respond. If a client sends probe request with an ESSID on the excluded ESSID list, the anyspot AP will not respond to the request, even if there is no neighboring AP using that ESSID. Excluded ESSIDs can be identified by exact name or a matching string.

The following procedure describes how to configure an anyspot profile:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** page.
2. Navigate to **Wireless LAN> Anyspot** on the **Profile** pane, then select the anyspot profile you want to modify.
3. Configure the anyspot parameters described in Table 1.

Table 1: *Anyspot Client Probe Suppression Configuration Parameters*

Parameter	Description
Enable Anyspot	Select this check box to enable the anyspot feature. Note that you must associate the anyspot profile with a virtual AP profile for the settings to take effect.
Exclude ESSID(s) (exact match)	An anyspot-enabled radio will not respond to client probe requests using an ESSID in the **Exclude ESSID** lists. To add an ESSID to the list, enter the full name of the ESSID, then click **Add**. To remove an ESSID from the list, select it and click **Delete**. ESSIDs from neighboring APs will automatically appear in this list as long as the anyspot-enabled AP can detect that ESSID.
Exclude ESSID(s) (containing string(s)	An anyspot-enabled radio will not respond to client probe requests using an ESSID in the **Exclude ESSID** list. To exclude ESSIDs that partially match a text string, enter that string then click **Add**. To remove a matching string from the list, select it and click **Delete**.
Preset ESSID(s)	The anyspot-enabled AP will not send an ESSID in beacons, but if a client sends a probe requests without ESSIDs (that is, the probe request is not looking for a specific network)then the anyspot-enabled AP will respond to the probe request with an ESSID from this list.

If you create a new Anyspot profile, use the procedure below to associate the anyspot profile with a selected WLAN via the virtual AP profile.

The following procedure describes how to associate a new Ethernet interface link profile with a wired port profile:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** page.
2. Select **AP > Virtual AP** on the **Profile** pane, then select the Virtual AP profile for the WLAN you want to modify.
3. Click the **Anyspot** profile currently associated with the Virtual AP profile. This profile appears below the Virtual AP Profile in the **All Profiles** list.
4. Click the **Anyspot profile** drop-down list and select the new **Anyspot** profile.

BLE Operation Mode

The **BLE Operation Mode** setting determines how the built-in BLE chip in the AP functions. You can configure this setting using the Mobility Master WebUI or CLI.

> Starting from ArubaOS 8.5.0.0, BLE functionality is enabled on ArubaOS 203H Series, 203R Series, 210 Series/220 Series (external USB -based BLE radio), 207 Series, 300 Series, 530 Series and 550 Series FIPS APs. The **BLE Operation Mode** setting is currently supported in 320 Series access points only.

This feature supports the following modes:

- **Beaconing**: The built-in BLE chip in the AP functions as an iBeacon combined with beacon management functionality.
- **Disabled**: The built-in BLE chip in the AP is turned off. This is the default setting.
- **DynamicConsole**: The built-in BLE chip in the AP functions as a regular iBeacon combined with beacon management functionality. However, when the link to the managed device is lost, the built-in chip temporarily enables access to the AP console over BLE. This state of the BLE device may be rolled back to any of the other modes if the AP receives a different configuration setting for the **ble-op-mode** parameter from the new LMS.
- **PersistentConsole**: The built-in chip in the AP provides access to the AP console over BLE using a mobile application. This functionality is the superset of the **Beaconing** mode.

Settings for this feature are configured using the **BLE Operation Mode** parameter in the **Advanced** section the AP system profile. For details, see Configuring the AP System Profile .

Configuring the AP System Profile

The AP system profile configuration settings are divided into four groups, **General**, **LMS Settings**, **Remote AP** and **Advanced**. The **General**, **LMS Settings**, and **Remote AP** sections of this profile include configuration settings that often need to be adjusted to suit a specific network. The **Advanced** tab includes settings that do not need frequent adjustment or should be kept at their default values.

The following procedure describes how to configure AP settings using the AP system profile:

1. In the **Managed Network** node hierarchy, navigate to **Configuration > System > Profiles** tab.
2. In the **All Profiles** list, expand the AP menu, then select **AP system**.
3. Select the AP system profile you want to edit, or click + to create a new profile.
4. Configure the profile parameters described in AP System Profile Configuration, then click **Submit**.
5. Click **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

> To specify the server details to receive the core dump when an AP process crashes, select an AP system profile and click on **Dump Collection**. To allow the core dump files to be sent to the managed device, access the managed device command-line interface and issue the **ap-crash-transfer** command.

Table 1: *AP System Profile Configuration*

Parameter	Description
Profile Name	
General	
RF Band	For APs that support both 802.11a and 802.11b/g RF bands, specify the RF band in which the AP should operate: ▪ g = 2.4 GHz ▪ a = 5 GHz
RF Band for AM Mode scanning	For Air Monitors that support both 802.11a and 802.11b/g RF bands, specify the RF band which the AM should scan: ▪ a = 5 GHz ▪ all = both radio bands ▪ g = 2.4 GHz
Native VLAN ID	Native VLAN for bridge mode virtual APs (frames on the native VLAN are not tagged with 802.1q tags).
WIDS AMPDU Optimization	Reduce the number of frames copied for the purpose of WIDS aggregate MPDU Optimization. Default: Enabled.
Session ACL	Session ACL configured with the **ip access-list session** command. **NOTE:** This parameter requires the PEFNG license.
Corporate DNS Domain	Name of domain that is resolved by corporate DNS servers. Use this parameter when configuring split-tunnel forwarding.
SNMP sysContact	SNMP system contact information.
LED operating mode	The operating mode for the LEDs on 802.11n-capable indoor AP. supported options are normal mode, and off, which disables all LEDs.
LED override	Override the LED action for single-LED APs in normal LED operating mode. If enabled, this feature disables the LED auto-turn-off function.
Driver log level	Level of AP driver logs sent to the syslog server. Supported options are:

Configuring Preferred Uplink

Starting ArubaOS 8.4.0.0 ethernet port1 can be configured as the primary uplink and ethernet port0 can be configured as the downlink interface, in an active-standby uplink mode of deployment. This enhancement is supported in AP-318, AP-374, AP-375, AP-377.

The following CLI commands configure ethernet port1 as the primary uplink:

```
(host) [mynode] (config) #provision-ap
(host) [mynode] (config-submode)#read-bootinfo
(host) [mynode] (config-submode)#read-bootinfo ap-name ap_318
(host) [mynode] (config-submode)#preferred_uplink
(host) [mynode] (config-submode)#preferred_uplink eth1
```

Configuring the AP Wired Port Profile

This profile is only applicable to APs with Ethernet ports. Use this profile to enable or disable the wired port, define an AAA profile for wired port devices, and associate the port with an Ethernet link profile that defines its speed and duplex values.

The following procedure describes how to configure the AP wired port profile:

1. Navigate to the **Configuration > System > Profiles** page.
2. Select **AP > AP Wired Port**, and select the AP wired port profile you want to modify. The parameters for the profile are described in Ethernet Interface Link Profile Parameters.

Table 1: *AP Wired Port Profile Parameters*

Parameter	Description
Shut down	Disable the wired AP port.
Remote AP Backup	Enable this option to use the wired port on a Remote AP for local connectivity and troubleshooting when the AP cannot reach the managed device. If the AP is not connected to the managed device, no firewall policies will be applied when this option is enabled. (The AAA profile will be applied when the AP is connected to managed device).
Bridge Role	Role that is assigned to a user if split-tunnel authentication fails.
Time to wait for authentication to succeed	Authentication timeout value, in seconds, for devices connecting the AP's wired port. The supported range is 1-65535 seconds, and the default value is 20 seconds.
Spanning Tree	Enables the spanning-tree protocol.
Portfast	Enables portfast for AP wired access ports. Spanning tree must be enabled before this command can be used.
Portfast on trunk	Enables portfast for AP wired trunk ports. Spanning tree must be enabled before this command can be used.
Loop Protect Enable	Enables loop protection on AP wired ports.
Loop Detection Interval	Time, in seconds, to send loop detection packet. The supported range is 1 to 10 seconds and the default value is 2 seconds.
Storm Control Broadcast	Enables storm control broadcast. If the number of broadcast packets per second on one port in the AP exceeds the configured threshold, the port is shutdown.
Storm Control Broadcast Threshold:	Storm control broadcast threshold in packets per second after which the port is shutdown. The default value is 2000 packets per second.
Auto Recovery Enable	Enables automatic recovery of the port in the AP that is shut down because of loop protection. After the automatic recovery, if the loop re-occurs, then the port is shut down again.
Auto Recovery Interval	Time, in seconds, to automatically recover the port in the AP that is shut down because of loop protection. The supported range is 30 to 43200 seconds and the default value is 300 seconds.

The following CLI command configures the AP wired port profile:

```
(host)[node] (config) #ap wired-port-profile <profile>
```

Tri-Radio Mode for 550 Series Access Points

Starting from ArubaOS 8.6.0.0, 550 Series Access points will support 802.11ax 8x8 dual-radio with optional 4x4 tri-radio operating mode.

In tri-radio mode or split 5GHz mode, 8x8:8SS 5GHz radio is split into dual 4x4:4SS 5GHz radio. The two radios can work on AP mode and also work on AP+AM or AP+ Spectrum mode, where one radio provides wireless access and the other radio performs scanning. Tri-radio mode works only under BT POE or DC power.

The Tri-radio mode in 550 Series Access Points supports the following features:

- Station Management
- AirMatch
- SAPD/SAPM
- Spectrum Analysis
- Cluster
- MultiZone
- Mesh
- ClientMatch
- Firmware

> When an AP is in a mode in which there are two radios on A-band,ClientMatch will not try to steer or load balance clients between the two A-band radios on the same AP. This limitation also applies to access points in dual-5G mode.

Follow the procedure below to enable tri-radio mode in the WebUI,

1. In the **Managed Network** Node hierarchy, navigate to **Configuration > AP groups**.
2. Select an AP group. In the **AP group > <Name of the AP group> table**, select **Radios** and expand the **Advanced** accordion.
3. Under **5 GHz**, enable the **Split radio** toggle switch.
4. Enable the **Set second radio differently** toggle switch to select the radio mode.
5. Select the radio mode **am-mode / ap-mode / spectrum-mode** from the **Radio mode** drop-down list.
6. Click **Submit**.
7. Click **Pending Changes**.
8. In the **Pending Changes** window, select the check box and click **Deploy changes**.

For other technical specifications, refer 550 Series*Campus Access Points Installation Guide*.

Validating and Optimizing AP Connectivity

The ArubaOS AP system profile contains multiple configuration settings to help you validate and optimize your AP connections to a managed device.

This section includes the following information:

AP Health Checks

The AP Health check feature uses ping probes to check reachability and latency levels for the connection between the AP and the managed device. The recorded latency information appears in the output of the **show ap ip health-check** command. If the managed device IP address becomes unreachable from the AP uplink, this feature records the time that the connection failed, and saves that information in a log file (tmp/ap_hcm_log) on the AP.

> This feature is disabled by default, and is enabled by selecting the Health Check option in the AP system profile. For details see Optional AP Configuration Settings.

Optimizing AP Connections over Low-Speed Links

Depending on your deployment scenario, you may have APs or remote APs that connect to a managed device located across low-speed (less than 1 Mbps capacity) or high-latency (greater than 100 ms) links.

With low-speed links, if heartbeat or keep alive packets are not received between the AP and managed device during the defined interval, APs may reboot causing clients to re-associate. You can adjust the bootstrap threshold and prioritize AP heartbeats to optimize these types of links. In addition, high bandwidth applications may saturate low-speed links. For example, if you have tunnel-mode SSIDs, use them with low-bandwidth applications such as barcode scanning, small database lookups, and Telnet to avoid saturating the link. If you have traffic that will remain local, deploying remote APs and configuring SSIDs as bridge-mode SSIDs can also prevent link saturation.

With high-latency links, consider the amount and type of client devices accessing the links. Aruba APs locally process 802.11 probe-requests and probe-responses, but the 802.11 association process requires interaction with the managed device.

When deploying APs across low-speed or high-latency links, the following best practices are recommended:

- Connect APs and managed devices over a link with a capacity of 1 Mbps or greater.
- Maintain a minimum link speed of 64 Kbps per AP and per bridge-mode SSID. This is the minimum speed required for downloading software images.
- Adjust the bootstrap threshold to 30 if the network experiences packet loss. This makes the AP recover more slowly in the event of a failure, but it will be more tolerant to heartbeat packet loss.
- Prioritize AP heartbeats to prevent losing connectivity with the managed device.
- If possible, reduce the number of tunnel-mode SSIDs. Each SSID creates a tunnel to the managed device with its own tunnel keep alive traffic.
- If most of the data traffic will remain local to the site, deploy remote APs in bridging mode. For more information about remote APs, see Access Points.
- If high-latency links such as transoceanic or satellite links are used in the network, deploy a managed device geographically close to the APs.
- If high-latency causes association issues with certain handheld devices or barcode scanners, check the manufacturer of the device for recent firmware and driver updates.

The following topics provide information on configuring bootstrap threshold and prioritizing AP heartbeats:

Configuring the Bootstrap Threshold

To configure the bootstrap threshold using the WebUI, enter a value into the **bootstrap threshold** field in the advanced AP system profile settings (For details, see Configuring the AP System Profile).

To configure this setting using the command-line interface, issue the command **ap system-profile <profile> bootstrap-threshold <bootstrap-threshold>**.

Prioritizing AP Heartbeats

To configure the AP heartbeat priority using the WebUI, enter a value greater than zero into the **Heartbeat DSCP** field in the advanced AP system profile settings (For details, see Configuring the AP System Profile).

To configure this setting using the command-line interface, issue the command **ap system-profile <profile> heartbeat-dscp <number>**.

AM Copy Optimization

Starting from ArubaOS 8.4.0.0, the AM Copy feature is significantly enhanced to reduce the burden on CPU and increase the AP performance. The optimization impacts the following features:

IDS Signature Match

This feature will no longer be reliable in matching the packet payload or sequence number. You need to disable the **wids-ampdu-optimization** parameter to detect the filtered packets and match all the packets with a given payload pattern or sequence number.

Frame Rate Anomaly Checks

2.4 GHz and 5 GHz Radio RF Management

The two 802.11a and 802.11g RF management profiles for an AP configure its 802.11a (5 Ghz) and 802.11b/g (2.4 Ghz) radio settings. You can either use the “default” version of each profile, or create a new 802.11a or 802.11g profile using the procedures below. Each RF management radio profile includes a reference to an ARM profile. If you would like ARM to dynamically select the best channel and transmission power for the radio, verify that the RF management profile references an active and enabled ARM profile. It can be useful to set the **Max Tx EIRP** parameter in the ARM profile to 127 (the maximum power level permissible) until it determines the signal-to-noise radio on the links. If ARM is active, the **Max Tx EIRP** can also be set to 127 to allow maximum power levels.

If you want to manually select a channel for each AP group, create separate 802.11a and 802.11g profiles for each AP group and assign a different transmission channel for each profile. For example, one AP group could have an 802.11a profile that uses channel 36 and an 802.11g profile that uses channel 11, and another AP group could have an 802.11a profile that uses channel 40 and an 802.11g profile that uses channel 9.

With the implementation of the high-throughput 802.11n standard, 40 Mhz channels were added in addition to the existing 20 MHz channel options. Available 20 Mhz and 40 Mhz channels are dependent on the country code entered in the regulatory domain profile. The newer VHT 802.11ac standard introduces 80 Mhz channel options.

Starting from ArubaOS 8.4.0.0, IEEE 802.11ax standard has been implemented that also supports 40 Mhz, 80 Mhz, and 160 Mhz channels in 5 Ghz frequency bands.

> Changing the country code causes the valid channel lists to be reset to the defaults for the country.

> Starting from ArubaOS 8.4.0.0, 5 GHz band includes 169 and 173 channels, for India only.

This section provides details on the following topics:

- Managing 2.4 GHz and 5 GHz Radio Settings
- Managing High Throughput Radio Settings
- RF Optimization
- RF Event Configuration

Managing 2.4 GHz and 5 GHz Radio Settings

This following sections explain the 2.4 GHz and 5 GHz radio settings and steps to configure the related parameters:

Managing High Throughput Radio Settings

Each radio references a high-throughput profile that manages that AP's 40 Mhz tolerance settings. By default, a 5 GHz radio uses a high-throughput profile named **default-a** and a 2.4 GHz radio uses a high-throughput profile named **default-g**. If you do not want to use these default profiles, use the procedure below to reference a different high-throughput profile for your 802.11a or 802.11g RF management profiles. For more information on configuring these settings, see High-Throughput APs.

RF Optimization

Each AP includes an RF Optimization profile that allows you to configure settings for detecting interference. The controller can detect interference near a wireless client station or AP is based on an increase in the frame retry rate or frame receive error rate.

The following procedure describes how to configure RF Optimization profiles:

1. Navigate to the **Configuration > System > Profiles** tab.
2. Select **RF Management** menu, then click **RF Optimization**.
3. Select the RF Optimization profile you want to edit or click **Add** and enter a name into the **Profile Name** dialog box to create a new profile.
4. Configure your RF Optimization radio settings then click **Submit**. Table 1 describes the parameters

Table 1: *RF Optimization Profile Parameters*

Parameter	Description
Station Handoff Assist	Allows the controller to force a client off an AP when the RSSI drops below a defined minimum threshold. Default: Disabled
RSSI Falloff Wait Time	Time, in seconds, to wait with decreasing RSSI before a de-authorization message is sent to the client. Maximum value: 8 seconds Default : 4 seconds
Low RSSI Threshold	Minimum RSSI above which de-authorization messages should never be sent. Default: 10
RSSI Check Frequency	Interval, in seconds, to sample RSSI. Default: 3 seconds

The following CLI command configures a RF Optimization profiles:

```
rf optimization-profile <profile>
```

RF Event Configuration

An AP's event threshold profile configures RSSI metrics, including high and low watermarks for frame error rates and frame retry rates. When certain RF parameters are exceeded, these events can signal excessive load on the network, excessive interference, or faulty equipment.

> This profile and many of the detection parameters are disabled (value is 0) by default.

The following procedure describes how to configure RF event profiles:

1. Navigate to the **Configuration > Controller > Profiles** tab.
2. Select **RF Management** menu, then click **RF Event Thresholds**.
3. Select the RF Event Thresholds profile you want to edit or click **+** and enter a name into the **Profile Name** dialog box to create a new profile.
4. (Optional) Click **General** then select **Detect Frame Rate Anomalies** to enable or disables detection of frame rate anomalies. This feature is disabled by default.
5. (Optional) Click **Advanced** to configure the parameters described detailed in Table 1.
6. Click **Save**.

Table 1: *RF Event Thresholds Profile Parameters*

Parameter	Description
Bandwidth Rate High Watermark	If bandwidth in an AP exceeds this value, a bandwidth exceeded condition exists. The value represents the percentage of maximum for a given radio. (For 802.11b, the maximum bandwidth is 7 Mbps. For 802.11 a and g, the maximum is 30 Mbps.) The recommended value is 85%.
Bandwidth Rate Low Watermark	After a bandwidth exceeded condition exists, the condition persists until bandwidth drops below this value. The recommended value is 70%.
Frame Error Rate High Watermark	If the frame error rate (as a percentage of total frames in an AP) exceeds this value, a frame error rate exceeded condition exists. The recommended value is 16%.
Frame Error Rate Low Watermark	After a frame error rate exceeded condition exists, the condition persists until the frame error rate drops below this value. The recommended value is 8%.
Frame Fragmentation Rate High Watermark	If the frame fragmentation rate (as a percentage of total frames in an AP) exceeds this value, a frame fragmentation rate exceeded condition exists. The recommended value is 16%.
Frame Fragmentation Rate Low Watermark	After a frame fragmentation rate exceeded condition exists, the condition persists until the frame fragmentation rate drops below this value. The recommended value is 8%
Frame Low Speed Rate High Watermark	If the rate of low-speed frames (as a percentage of total frames in an AP) exceeds this value, a low-speed rate exceeded condition exists. This could indicate a coverage hole. The recommended value is 16%.
Frame Low Speed Rate Low Watermark	After a low-speed rate exceeded condition exists, the condition persists until the percentage of low-speed frames drops below this value. The recommended value is 8%.

AP Groups

In the Aruba user-centric network, each AP has a unique name and belongs to an AP group.

Each AP is identified with an automatically-derived name. The default name depends on if the AP has been previously configured.

- The AP has not been configured—the name is the AP's Ethernet MAC address in colon-separated hexadecimal digits.
- Configured with a previous ArubaOS release—the name is in the format *building.floor.location*

You can assign a new name (up to 63 characters) to an AP; the new name must be unique within your network. For example, you can rename an AP to reflect its physical location within your network, such as "building3-lobby".

An *AP group* is a set of APs to which the same configuration is applied. There is an AP group called "default" to which all APs discovered by the managed device are assigned. By using the "default" AP group, you can configure features that are applied globally to all APs.

Workflow for Configuring an AP Group

You can create additional AP groups and assign APs to that new group. However, an AP can belong to only one AP group at a time. For example, you can create an AP group "Victoria" that consists of the APs that are installed in a company's location in British Columbia. You can create another AP group "Toronto" that consists of the APs in Ontario. You can configure the "Toronto" AP group with different information from the APs in the "Victoria" AP group.

While you can use an AP group to apply a feature to a set of APs, you can also configure a feature or option for a specific AP by referencing the AP's name. Any options or values that you configure for a specific AP will override the same options or values configured for the AP group to which the AP belongs.

> Reassigning an AP from an AP group requires a reboot of the AP for the new group assignment to take effect. Therefore, wait until there is little or no client traffic passing through the AP before reassigning it.

The tasks for configuring an AP group are:

1. Create an AP Group - You can create additional AP groups other than default.

   See ArubaOS 8.6.0.0 Help Center

2. Assign an AP to an AP Group - You can assign APs to that new group. A AP can belong to only one AP group at a time.

   See ArubaOS 8.6.0.0 Help Center

3. Assign channels to an AP Group - The country code in the AP Regulatory Domain profile determines supported channel and channel pairs for that specific AP. Any changes to the country code causes the valid channel lists to be reset to the defaults for the country.

   See ArubaOS 8.6.0.0 Help Center

4. Configure Channel Switch Announcement - CSA, as defined by IEEE 802.11h, enables an AP to announce that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, who support CSA, to transition to the new channel with minimal downtime.

   See ArubaOS 8.6.0.0 Help Center

5. Automatic Channel and Transmit Power Selection - Enable ARM to allow automatic channel and transmit power selection based on the radio environment.

   See ArubaOS 8.6.0.0 Help Center

Creating an AP group

The following procedure describes how to create an AP group:

1. In the **Managed Network** node hierarchy, select the managed device where the AP group are to be added.
2. Navigate to the **Configuration > AP Groups** menu.
3. Click **Add** below the AP Groups table.
4. In the **New AP Groups** window, enter the AP group name in the **New AP groups** field.
5. Click **Submit**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

The following CLI command creates an AP group:

```
(host) [mynode](config) #ap-group <group>
```

When you create an AP group with the CLI, you can specify the virtual AP definitions and configuration profiles you want applied to the APs in the group.

Assigning an AP to an AP Group

Although you will assign an AP to an AP group when you first deploy the device, you can assign an AP to a different AP group at any time.

> Once the **ap-regroup** command is executed, the AP automatically reboots. If the AP is powered off or otherwise not connected to the network or managed device, the executed command is queued until the AP is powered on or reconnected.

The following procedure describes how to assign a single AP to an existing AP group.

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Access Points** menu.
2. Select the check box next to the AP and click **Provision**.
3. From the list of provisioning settings, click the **AP group** drop-down list and choose a new the AP group for the selected AP.
4. Click **Submit**.
5. Click **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

The following CLI commands assign a single AP to an existing AP group.

```
(host) [mynode](config) #ap-regroup {ap-name <name>|serial-num <number>|wired-mac <macaddr>} <group>
```

Assigning Channels to an AP Group

The country code in the AP Regulatory Domain profile determines supported channel and channel pairs for that specific AP. Any changes to the country code causes the valid channel lists to be reset to the defaults for the country.

This section illustrates how to perform the following tasks for an AP group:

- Configure the “default” regulatory domain profile to use a valid country code. This will determine the available channels.
- Configure a 40 MHz channel (bonded pair) for the AP group’s 802.11a (5 Ghz) radio profile.
- Configure a 20 MHz channel for the AP group’s 802.11g (2.4 Ghz) radio profile.

The following procedure describes how to configure channels for an AP group.

1. In the **Managed Network** node hierarchy, select the managed device containing the AP group.
2. Navigate to the **Configuration** > **AP Groups** page.
3. Select the AP group to be configured.
4. Select the **Radio** tab from the AP group menu and click **Basic** accordion.
5. Click the **Radio mode** drop-down list and choose **ap-mode**.
6. Select 2.4 GHz or 5 GHz radio to be configured and click **Edit** in the **Valid Channels** field.
7. In the **Valid Channels** window, select the channels that will be supported by the AP group.
8. Click **OK**.
9. Click **Submit**.
10. Click **Pending Changes**.
11. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

The following CLI commands configure channels for an AP group:

```
(host) [mynode](config) #ap regulatory-domain-profile default
   country-code US
(host) [mynode](config) #rf dot11a-radio-profile ht-corpnet-a
   channel 36+
(host) [mynode](config) #rf dot11g-radio-profile ht-corpnet-g
   channel 1
```

> Country codes are generally specified in ISO 3166 format. To see what channels are available for a given country code, use the **show ap allowed-channels country-code <country-code>** command.

Configuring Channel Switch Announcement

When an AP changes its channel, an existing wireless clients may “time out” while waiting to receive a new beacon from the AP; the client must begin scanning to discover the new channel on which the AP is operating. If the disruption is long enough, the client may need to reassociate, reauthenticate, and request an IP address.

When CSA is enabled, the AP does not change to a new channel immediately. Instead, it sends a number of beacons (the default is 4) which contain the CSA announcement before it switches to the new channel. You can configure the number of announcements sent before the change.

> Clients must support CSA in order to track the channel change without experiencing disruption.

The following procedure describes how to configure CSA.

1. In the **Managed Network** node hierarchy, select the managed device containing the AP group.
2. Navigate to the **Configuration** > **AP Groups** page.
3. Select the AP group to be configured.
4. Select **Radio** tab from the AP group menu and click **Advanced** accordion.
5. Select **Enabled** from the **CSA** drop-down list. This option can be enabled or disabled separately for 2.4 GHz and 5 GHz radios.
6. Click **Submit**.
7. Click **Pending Changes**.
8. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Automatic Channel and Transmit Power Selection

To allow automatic channel and transmit power selection based on the radio environment, enable ARM. Note that ARM assignments will override the static channel and power configurations done using the radio profile. For complete information on the Adaptive Radio Management feature, refer to RF Planning and Channel Management.

AP Channel Scanning

The scanning algorithm is enhanced to reduce the delay between visits to some channel types, by changing their scan priority.

This section provides details on the following topics:

Channel Types and Priority

A channel can belong to one or more channel types, depending on regulatory information and the activity that is detected on the channel. The frequency of visits to a channel depends on the priority of the channel type(s) to which it belongs. The following table describes the priority of channel types.

Table 1: *Channel Types and Priority*

Channel Priority	Channel Type	Description
One	DOS Channels	Channels where the AP is actively containing one more rogue devices in AM mode are marked with an **O** flag in the ARM CLI output (`show ap arm scan-times`).
Two	Active Channels	Channels where AP or Station activity has already been detected are marked with an **A** flag in the ARM CLI output and are visited in all scan-modes.
Three	Reg-Domain Channels	Channels that are in the AP's regulatory domain are marked with a **C** flag in the ARM CLI output and are visited in all scan modes.
Four	All Reg-Domain Channels	Channels that belong to any country's regulatory domain are marked with a **D** flag in the ARM CLI output and are visited only if the **scan-mode** is set to **All-Reg** or **Rare**.

Scanning Optimizations

The following optimizations enable the AP to achieve optimum RF monitoring. Unconventional Scans and Relative Priority of Channel Type Categories optimization apply to all AP types, but Channel Group Scanning optimization applies only to 200 Series models. All optimizations apply to AP and AM mode scanning.

This section provides information on the following topics:

Unconventional (direction) Scans

- Unconventional scans are 40 MHz scans of a channel in the direction away from the channel pair. For example, in the 44-48 channel pair:
  - Conventional scans will be 44+ and 48-
  - Unconventional scans will be 44- and 48+
- Unconventional scans are no longer interspersed with conventional scans. Unconventional scans operate with a lower frequency, because they belong to a new low priority channel type.
- Unconventional scans are performed in all-regulatory and rare scan modes. But these scans will not be performed if the scan mode is set to regulatory domain. This modification enables the AP to scan through active channels, regulatory channels, and all-regulatory channels faster.

> Currently, 200 Series access points do not support unconventional or rare channel scanning.

Modifications in Scan Frequency

A modification is introduced to increase the frequency of visits to active and regulatory domain channels. Channel type categories are:

- DOS
- Active
- Regulatory domain
- All-regulatory domain
- Unconventional or rare

> Unconventional or rare channels are merged for scanning.

Since 11ac AP radio can hear frames sub-channels when it performs an 80 MHz wide scan, scanning can be optimized by categorizing channels into scan groups, which are visited sequentially when a new primary channel is selected. This allows the AP scan through the list of channels faster, so that the delay between visits to channels in a group is reduced.

For more information on Channel Group Scanning, see Channel Group Scanning .

Channel Group Scanning

The following are the salient features of channel group scanning:

- Channel groups can be 80 MHz (4 channels), 40 MHz (2 channels), or 20 MHz wide (1 channel).
- Each channel is mapped to a group depending on the maximum width supported by that channel and the radio's capability. The maximum width supported by a channel is determined by the channel's membership in regulatory domain channel pairs or groups.
  - Channel 36, 40, 44, and 48 belong to 80MHz group
  - Channel 165 belongs to 20MHz group
- Channel groups are visited sequentially and the primary channel is rotated after each visit.
- Group scanning behavior is performed for 200 Series access points on A-band channels.

> Scanning only once in each 80 MHz wide group allows the AP to scan through the channel list faster and also hear frames on sub-channels.

Link Aggregation Support

> Link aggregation is supported by 220 Series, 270 Series, 320 Series, 330 Series, 340 Series, AP-303P, 510 Series, 530 Series, and AP-555 access points.

All 220 Series, 270 Series, 320 Series, 330 Series, 340 Series, AP-303P, 510 Series, 530 Series, and AP-555 access points support link aggregation using either static port channel (configuration based) or Link Aggregation Control Protocol (protocol signaling based) link aggregation. These access points can optionally be deployed with LACP configuration to benefit from higher (greater than 1 Gbps) aggregate throughput capabilities. 330 Series, 340 Series, and 510 Series access points are limited to 1 Gbps on eth1 interface and hence eth0 interface cannot negotiate above 1 Gbps to form LACP.

The Mobility Master uses two different IP addresses for forwarding traffic to wireless clients associated to tunnel mode or decrypt-tunnel mode VAPs. One IP address is Mobility Master's IP address and the other is an unassigned IP address called GRE striping IP. Select the GRE striping IP address to ensure that a different physical interface is used by the load-balancing algorithm on the Ethernet switch. This enables the access points achieve greater than 1 Gbps throughput in both upstream and downstream directions.

> AP LACP striping IP address need not be configured for APs terminating on a cluster.

On 200 Series and 270 Series access points, different IP addresses are used for different GRE tunnels between the AP and the LC. One LC IP address is used for tunnels corresponding to virtual APs using a 5 G radio and the other LC IP address is used for tunnels corresponding to virtual APs using a 2.4 G radio. By associating clients on both bands you can achieve more than 1 Gbps throughput.

A local AP LACP LMS map information profile that maps the device's LMS IP address to a GRE striping IP address. If the AP fails over to a standby or backup controller, the AP LACP LMS map information profile on the new LC defines the striping IP address that the AP uses for link aggregation. This feature allows the access points to continue to support link aggregation to a backup controller in the event of a controller failover, even if the backup controller is in a different L3 network.

In previous releases, the GRE striping IP address was defined in the global AP system profile, which did not allow APs to maintain GRE striping tunnels if the AP failed over to a backup controller in a different L3 network.

> If your topology includes a backup controller you must define GRE striping IP settings in the active and the backup controller For more information on LACP features in ArubaOS, see Configuring Port Channel LACP.

This section describes the following topics:

Configuring LACP

To enable and configure LACP on 220 Series, 270 Series, 320 Series and 330 Series access points, specify the **LMS IP** address and configure the **GRE Striping IP** address in the AP LACP Striping profile. The **GRE Striping IP** value must be an IPv4 address owned by the Mobility Master that has the specified **LMS IP**. The **GRE Striping IP** does not belong to any physical or virtual interface on the Mobility Master, but the Mobility Master can transmit or receive packets using this IP.

> The LMS IP address defined in the AP LACP profile or ap-lacp-striping command **must** be the same LMS IP address defined in the device's AP system profile. The LMS IP address in the device's AP system profile is used as a key to look up entries in the ap-lacp profile on the controllers to which an AP can connect.

The following procedure describes how to configure the LACP parameters in the AP System profile and AP LACP LMS map information profile.

On Mobility Master:

1. In the Mobility Master node hierarchy, select the device.
2. Navigate to **Configuration > System**.
3. Select **Profiles** and expand the **AP** profiles menu.
4. Select the **AP LACP LMS map information** profile.
5. Select the **AP LACP Striping IP** check box to enable the **AP LACP striping IP** feature.
6. Enter a GRE striping IP address in the **IP** field. This IP address must be a in the device's subnet.
7. In the LMS field, enter the LMS IP address specified in the device's AP system profile in the **LMS** field. This LMS IP address *must* match the LMS IP address in Mobility Master's AP system profile.
8. Click **Pending Changes** and save your settings.
9. (Optional) Repeat these settings to configure LACP on a backup Mobility Master.

On an L2-connected High Availability (HA) standby or HA+VRRP controller:

1. In the **Managed Network** node hierarchy, navigate to **Configuration > System.**
2. Select **Profiles** and expand the **AP** profiles menu.
3. Select the **AP LACP LMS map information** profile.
4. Select the **AP LACP Striping IP** check box to enable the **AP LACP striping IP** feature.
5. Click **+**.
6. Enter a GRE striping IP address in the **IP** field. This IP address must be in the managed device's subnet.
7. In the **LMS** field, enter the LMS IP address specified in the device's AP system profile. This LMS IP address must exactly match the LMS IP address in the AP system profile configuration used by the device.
8. Click **OK**.
9. Click **Pending Changes** and save your settings.

On an L3-connected High Availability (HA) standby controller, or an L2- or L3-connected controller in dual-HA mode:

When using high availability between two L3-connected controllers or two dual-mode HA controllers, you must define *two* different striping IPs (one in each controller subnet) to ensure that both the controllers will have striping IPs mapped to their corresponding LMS IP address.

> When two controllers are both deployed in dual HA mode, each dual-mode controller acts as standby for the APs served by the other dual-mode controller. Each controller must therefore have two striping IPs, one for in each controller subnet. Two striping IP addresses are required for these topologies, even if the dual-HA controllers are located within the same subnet.

1. In the **Managed Network** node hierarchy, navigate to **Configuration > System.**

Important Points to Remember

- In the upstream direction when the AP transmits GRE frames to the Mobility Master the bonding driver must be in active-active mode and not in the default active-standby mode to allow link aggregation.
- If an AP's uplink access switch ports are configured in static port-channel mode, then the AP will set the Ethernet bonding mode to static port-channel (xor mode) only if **gre-striping-ip** is configured. If **gre-striping-ip** is not configured, then the AP goes back to **active-standby** mode. In this scenario, the AP may go down depending on the behavior of the upstream switch.
- If an AP's uplink access switch ports are configured in dynamic LACP mode, the AP detects LACP-PDUs and automatically sets the Ethernet bonding mode to LACP. If **gre-striping-ip** is not configured, then the AP's Ethernet bonding mode will continue to be in LACP mode, but the AP will send GRE traffic only through one Ethernet port.
- In 320 Series and 330 Series access points, if AP uplink packet capture is taken, the downstream traffic will have sequence number in GRE header. Wireshark Aruba wlan decoder will not be able to decode these packets correctly since it looks for known Aruba GRE tunnel IDs.
- Ensure that the **gre-striping-ip** is unique and not used by any other host on the subnet.
- LACP support is limited to a use case where Enet 0 and Enet 1 ports of the AP are connected to a switch, and LACP is enabled on the two corresponding switch ports.
- The port priority is not applicable to the AP as both ports need to be used. This value is always set to the maximum numerical priority (0xFF), which is the lowest priority.
- The system priority is not configurable. It is set to the maximum numerical value (0xFFFF), which is the lowest priority. This leaves control of the aggregate to the upstream switch.
- The timeout value is not configurable.
- The key is not configurable and the default key value is 1.
- LACP cannot be enabled if wired AP functionality is enabled on the second port. You cannot enable LACP if the Enet 1 port is shutdown.

Troubleshooting Link Aggregation

The following show commands in the CLI can be used to troubleshoot Link Aggregation on 220 Series , 270 Series, 320 Series and 330 Series access points:

- **show ap debug lacp ap-name <ap-name>**—Using this command, you can view if LACP is active on an AP. It displays the number of GRE packets sent and received on the two Ethernet ports. Using this command with verbose option on 320 Series and 330 Series access points displays packet re-ordering statistics of each wlan client.
- **show ap database**—The output of this command includes an **LACP Striping** flags to indicate of the AP is configured with a LACP striping IP address,
- **show datapath tunnel**—Using this command on 220 Series/270 Series access points, you can verify if the 2.4 GHz tunnels are anchored on the **gre-striping-ip** (The GRE IDs for these tunnels are in a range between 0x8300 and 0x83F0) . On 320 Series and 330 Series access points, use the verbose option to verify that 5 Ghz tunnels have striping IP set in the column **StripIP** (The GRE IDs for these tunnels are in a range between 0x8200 and 0x82F0).
- **show datapath station**—On 320 Series and 330 Series access points, using this command displays the LACP sequence number sent in the GRE header of the last packet to the client. This information is displayed under **Seq** column.
- **show ap remote debug anul-sta-entries**—On 320 Series and 330 Series access points, using this command displays LAG enabled/disabled per station and data drops due to LAG packet reordering.
- **show datapath user**—Using this command, you can verify if the **gre-striping-ip** has an entry with the 'L' (local) flag.
- **show datapath route-cache**—Using this command, you can verify if the **gre-striping-ip** has an entry with the LC MAC.

Support for Port Bounce

Mobility Master provides support for the port bounce feature which enables a client to reinitiate a DHCP request when there is a VLAN change. This is achieved when a RADIUS server such as ClearPass Policy Manager sends Disconnect-Request with a Vendor Specific Attribute (VSA 40) to Mobility Master. Then, Mobility Master forwards the request to the device to trigger an interface shut down for a specified period. This allows the device to re-initiate a DHCP request for obtaining an IP address in the changed subnet.

The Disconnect-Request must include the following information:

- Calling Station-Id—MAC address of the user
- VSA—40
- Integer—0-60

VSA 40 represents **Aruba-Port-Bounce-Host**. The integer value indicates the time in seconds for which Mobility Master must shut the interface down. If the integer value received is greater than 60, then the port is shut down for default value of 12 seconds. If the value is 0, then the port is not shut down.

> During a port bounce, the client connected to the interface is removed from the user table and is added back after the port is up.

Execute the following command to view the security logs during and after a port bounce:

```
[mynode] #show log security all | include bounce
```

The following sample shows the output during a port bounce:

```
Sep 14 22:22:46  authmgr[539]: <124004> <DBUG> |authmgr|  Sending port bounce request for User mac 34:e6:d7:24:c8:3b
Sep 14 22:23:22  authmgr[539]: <124004> <DBUG> |authmgr|  Port Bounce succeeded for User Mac 34:e6:d7:24:c8:3b
```

AP Image Preload

The AP image preload feature minimizes the downtime required for a managed device upgrade by allowing the APs associated to that managed device to download the new images before the managed device actually starts running the new version.

This feature allows you to select the maximum number of APs that are allowed to preload the new software image at any one time, thereby reducing the possibility that the managed device may get overloaded or that network traffic may be impacted by all APs on the managed device attempting to download a new image at once.

APs can continue normal operation while they are downloading their new software version. When the download completes, the AP sends a message to the managed device, informing it that the AP has either successfully downloaded the new software version, or that the preload has failed for some reason. If the download fails, the AP will retry the download after a brief waiting period.

You can allow every AP on a managed device to preload a new software version, or also create a custom list of AP groups or individual APs that can use this feature. If a new AP associates to the managed device while the AP image download feature is active, the managed device will check that AP's name and group to see if it appears in the preload list. If an AP is on the list, (and does not already have the specified image in its Flash memory) that AP will start preloading its image.

> Once a software version has been downloaded, another version cannot be downloaded until the AP reboots.

This section provides information on the following topics:

Managing AP Console Settings

An AP's provisioning parameters are unique to each AP. These parameters are initially configured on the Mobility Master and then pushed out to the AP and stored on the AP itself. Best practices are to configure an AP's provisioning settings using the Mobility Master WebUI. If you find it necessary to alter an AP's provisioning settings for troubleshooting purposes, you can do so using the WebUI and CLI, or alternatively, through a console connection to the AP itself.

To create a console connection to the AP:

1. Connect a local console to the serial port on the AP. You can connect the AP's serial port to a terminal or terminal server using an Ethernet cable, or connect the serial console port to a DB-9 adapter, then connect the adapter to a laptop using an RS-232 cable. For details on connecting to an AP's serial console port, refer to the installation guide included with the AP.
2. Establish a console communication to the AP, then power-cycle the AP to reboot it.
3. To access the AP console command prompt, press **Enter** when the AP displays the message "*Hit <Enter> to stop autoboot.*" If the autoboot countdown expires before you can interrupt it, turn the device off and then back on.
4. Once the AP boot prompt appears, enter the AP console password. You can issue any of the AP provisioning commands described in the Table 1. Remember, though these commands may be useful for troubleshooting, they are all optional and are *not* necessary for normal AP provisioning.

Table 1: *AP Boot Commands*

> The list of AP boot commands may vary based on the APBoot image version.

Command	Description
boot	Boot the ArubaOS image from flash or USB, using currently saved environment variables. Any unsaved changes to the variables will be lost. This command has the following sub-parameters: ▪ ap - Boot the ArubaOS image from flash. ▪ usb:<path> - Boot the ArubaOS image from USB.
clear	Clear the ArubaOS image or other information. This command has the following sub-parameters: ▪ all - Clear the cache and ArubaOS. ▪ cache - Clear the cache sectors (mesh, Remote AP, Campus AP). ▪ os <n> - Clear the image from the specified partition (default: 0). ▪ prov - Clear provisioning image from the flash.
dhcp	Invoke DHCP client to obtain IP/boot parameters.
factory_reset	Reset the AP to factory default.
flash	Upgrade the boot image. **NOTE:** Exercise caution when using this command.
help	Help text for the AP boot commands.
mfginfo	Shows manufacturing information of the AP.
osinfo	Shows the ArubaOS image information on the AP.
ping	Check network connectivity.

AP Console Password Protection

The ArubaOS AP console password feature helps protect systems that manage highly sensitive information, like financial and banking institutions, by requiring users to log in to the AP network with a password. The AP console password is enabled by default. Passwords must be 6 to 32 characters in length, and can include alphanumeric and special characters. If configured, you must enter this password to get AP console access. If not configured, the Mobility Master generates a default random password which can be viewed by executing the **encrypt disable** command followed by the **show ap system-profile <profile-name>** command.

The timeout feature is also supported as an added level of security. If there is no user input or activity during one timeout interval (default of 30 minutes), the user is logged out of the system. The timeout interval cannot be modified.

This section contains the following topics:

AP Discovery Logic

In the earlier versions of ArubaOS, APs are predefined as either controller-based Campus APs or controller-less Instant APs. Each Campus AP is shipped with the ArubaOS manufacturing image and must connect to a controller in order to receive configurations. Campus APs can only run the ArubaOS image and cannot be converted into Instant APs. Each Instant AP is shipped with the Instant manufacturing image and must join an Instant AP cluster in order to receive configurations from a virtual controller. Instant APs run the Instant image and can also be converted into Campus APs.

Starting from ArubaOS 8.2.0.0, selected APs can run in both controller-based mode and controller-less mode. Based on the selected mode, the AP runs a different image:

- Controller-based APs run an ArubaOS image.
- Controller-less APs run an Instant image.

The following APs support both controller-based mode and controller-less mode:

- AP-203H
- AP-203R and AP-203RP
- AP-303H
- AP-365 and AP-367 access points

Each AP is shipped with a manufacturing image based on the Instant image, but containing reduced functions. When the AP is booted up with the manufacturing image, it enters the managed device and Instant discovery process to determine if it will be upgraded to the controller-based mode (ArubaOS image) or controller-less mode (Instant image). After the managed device, Instant virtual controller, or Activate/AirWave/Central is discovered, the AP image is upgraded accordingly.

By default, controller discovery has a higher priority than Instant discovery. APs can discover the IP address of a managed device through one of the following methods. See "Discovery of Controller" on page 1 for more details on the different controller discovery options.

- Static controller discovery
- ADP
- DHCP server
- DNS server

Important Points to Remember

- APs can support up to 12 managed device IP addresses via DHCP/DNS discovery. APs attempt to connect to each managed device 10 times before switching to the next managed device.
- An AP can only be converted into a controller-based AP if the managed device to which it connects is running ArubaOS 8.2.0.0.
- If the AP cannot locate any managed device during the controller discovery process, it enters Instant discovery.

Preference Role

Users can predefine the AP mode by configuring the preference role. APs with the default preference role follow the standard discovery logic by attempting controller discovery before initiating Instant discovery. APs with the controller-less preference role bypass controller discovery and immediately initiate Instant discovery.

The following procedure describes how to set the AP preference role to controller-less:

1. Navigate to **Maintenance > Access Point > Convert to Instant Mode** in the WebUI.
2. Select the AP on which you want to set the preference role to controller-less.
3. Click **Convert to Instant Mode**.

> This option is only available on Stand-alone controllers and managed devices.

> You cannot convert a non-UAP model to an Instant AP. To convert a non-UAP model to an Instant AP, use the reset pin on the AP and reset the AP to factory default state.

The following CLI commands set the AP preference role to controller-less in the CLI:

```
(host) [mynode] #ap redeploy controller-less
  all
  ap-group
  ap-name
  ip-addr
  ip6-addr
  wired-mac
```

> The **ap redeploy controller-less** command works only for UAPs and is applicable to AP-203H, AP-203R, AP-203RP, AP-303, AP-303H, 303P Series, AP-318, AP-344, AP-345, AP-365, AP-367, AP-374, AP-375, AP-377, AP-387, AP-534, and AP-535 access points only.

AP Deployment Policy

The AP deployment policy redirects the specified APs to the Instant discovery process, ensuring that the APs run only in controller-less mode. Users can predefine the AP deployment mode using the AP deployment policy.

The AP deployment policy can be configured on:

- APs in the specified IP address ranges—Policy is applied to the APs in the specified IPv4 or IPv6 address range. You can define up to 128 IPv4 and IPv6 address ranges for the AP deployment policy
- APs in the default AP group—Policy is applied to the APs in the default AP group.
- APs whose MAC address are included in the blacklist table—Policy is applied to the APs whose MAC addresses are included in the UAP blacklist table when the blacklist policy is enabled on the AP deploy profile.

> You must enable the AP deploy profile to enforce the policies configured in the profile.

When the policy is enforced, the managed device automatically identifies the targeted AP, rejects the AP termination, and redirects the AP to upgrade to controller-less mode.

The following CLI commands configure various AP deployment policies.

To enable the AP deploy profile, execute the following commands:

```
(host) [mynode] (config) #ap deploy-profile
(host) [mynode] (ap deploy-profile) #enable
```

To apply the AP deployment policy to the default AP group, execute the following commands:

```
(host) [mynode] (config) #ap deploy-profile
(host) [mynode] (ap deploy-profile) #default-ap-group
```

To apply the AP deployment policy to an IPv4 address range, execute the following commands:

```
(host) [mynode] (config) #ap deploy-profile
(host[mynode] (ap deploy-profile) #ip-range <start> <end>
```

To apply the AP deployment policy to an IPv6 address range, execute the following commands:

```
(host) [mynode] (config) #ap deploy-profile
(host) [mynode] (ap deploy-profile) #ipv6-range <start> <end>
```

To include AP MAC address to the UAP blacklist table, execute the following command:

```
(host) [mynode] (config) #uap-blacklist add mac-address <address> description <description>
```

To apply the AP deployment policy to the blacklisted APs, execute the following commands:

```
(host) [mynode] (config) #ap deploy-profile
(host) [mynode] (ap deploy-profile) #blacklist
```

To remove the IP address range or default AP group from the profile, execute the following command:

```
(host) [mynode] (config) #no ap deploy-profile
```

To view the complete list of IP address ranges to which the AP deployment policy is applied, execute the following command:

```
(host) [mynode] #show ap deploy-profile
```

Discovery Logic Workflow

The following steps describe the AP discovery logic:

Figure 1 *AP Discovery Logic*

1. When an AP boots up, it connects to Activate to obtain a provisioning rule.
2. If provisioning is already done by AirWave or Central, verify if a provisioning rule exists. If yes, the provisioning rule is saved in the flash memory. Compare the saved provisioning rule with the rule in Activate. If the rule in Activate is new, save the new provisioning rule in flash. For example, if the master and slave Instant APs obtain different AirWave addresses or if the master and slave Instant APs obtain a different AirWave or Central rule, the master Instant AP rule takes higher precedence.

   Only the master Instant AP can apply provisioning rules to the Instant AP cluster.

3. If the rule is to perform a mandatory upgrade of the Instant AP, ensure to upgrade the Instant AP to the desired version. The master Instant AP executes the upgrade after a cluster is formed.
4. If the rule is to convert the Instant AP to Campus AP or Remote AP, the conversion takes effect for every Instant AP regardless of whether it is a master or a slave. This requires a manual registration of every master and slave Instant AP with Activate.
5. If there is no rule from Activate or if conversion to Campus AP or Remote AP fails, the master AP conducts local provisioning detection to check the local AirWave configuration.
   - If the AirWave server is configured and is in the configuration file, apply the server details. Otherwise, conduct a DHCP based AirWave or Central detection.
   - If DHCP-based AirWave is not found and the Instant AP is in factory default status, perform a DNS based AirWave discovery.
   - If none of the above methods can detect the AirWave server and if the Instant AP cannot connect to Activate, use the provisioning rule in flash.
6. If the AirWave or Central server is not found, or if the Instant AP is a slave, verify if the following conditions for local controller discovery are met:
   - The Instant AP is factory reset.
   - The **uap_controller_less** mode is not set.
   - There is no provision rule saved in flash.
7. If the controller is found, the Instant AP sends a hello message to the controller and converts to a Campus AP.
8. When a master failover happens, the new master Instant AP connects to Activate to retrieve the provisioning rule. If the new master successfully obtains the provisioning rule, it applies this rule to the cluster.

Manual Upgrade

APs running in unprovisioned mode broadcast a special provisioning SSID to which users can connect to upgrade the AP manually. Upon connecting, users can access a local provisioning page in the WebUI to upgrade the AP to an ArubaOS or Instant image. See "Controller-based AP using Manual Campus AP/Remote AP Conversion" on page 1 and "Controller-less AP using Manual Instant AP Conversion" on page 1 for more details on upgrading APs manually.

Deployment Scenarios

This section describes various AP deployment scenarios in controller, Instant, remote, and hybrid networks.

See the following topics:

- Controller-based AP Deployments
- Controller-less AP Deployments

Troubleshooting the AP Discovery Logic

The following sections describe troubleshooting scenarios users may encounter in the AP discovery logic:

Loop Protection

The loop protect feature detects and avoids the formation of loops on the Ethernet ports of a Campus AP, Remote AP, or Mesh AP.

The loop protect feature can be enabled on all APs that have multiple Ethernet ports and it supports tunnel, split-tunnel, and bridge modes.

The loop protection feature prevents the formation of loops when:

- An unmanaged switch is connected to one port of an AP and a loop forms in the unmanaged switch.
- The WAN port (port 0) and either of ports 1, 2, 3, or 4, if it exists, in an AP are connected to the same switch.
- Multiple ports in an AP are connected to an unmanaged switch.

The loop protection feature transmits a proprietary loop detection packet on one Ethernet port of an AP at the configured loop-protect interval (default value is 2 seconds). The loop protect feature transmits the loop detection packet without a VLAN tag irrespective of whether the Ethernet port of the AP is connected in access mode or trunk mode. That is, for trunk mode, loop protect is supported only in the native VLAN.

- If the same packet is received on the same Ethernet port of the AP, a loop in the downstream switch is detected and the Ethernet port of the AP is shut down.
- If the same packet is received on the WAN port (port 0) of the AP, a loop between the Ethernet and WAN ports of the AP is detected and the Ethernet port of the AP is shut down.
- If the same packet is received on another Ethernet port of the AP, a loop between the Ethernet ports of the AP is detected and the Ethernet port of the AP port with lower priority is shut down. The Ethernet port with smaller port ID has high priority.

The Ethernet port of the AP that is shut down because of loop protection is marked with status **Loop-ERR**. A user can either the recover the shut down port from the managed device with manual intervention or enable automatic recovery mode and configure a automatic recovery interval. At the expiry of the automatic recovery interval, the **Loop-ERR** status of the Ethernet port is cleared and the Ethernet port is re-enabled automatically.

To prevent the downstream switch from dropping the loop detection packet, for example during broadcast storm state, if the AP takes longer time, or if the AP fails to detect a loop, a broadcast storm-control mechanism is provided as part of the loop protection feature. During broadcast-storm control, an AP counts the broadcast packets received on each of its Ethernet port and determines the packet rate in an interval. If the broadcast packet rate on one Ethernet port exceeds the configured threshold (default value is 2000 packets per second), the Ethernet port is shut down.

This section provides information on the following topics:

Configuring Loop Protect

The following procedure describes how to configure loop protect parameters in the AP wired port profile:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** page.
2. Select **AP > AP Wired Port**, and select the AP wired port profile you want to modify. The loop protect parameters for the profile are described in Table 1.

Table 1: *Loop Protect Parameters in AP Wired Port Profile*

Parameter	Description
Loop Protect Enable	Enables loop protection on AP wired ports.
Loop Detection Interval	Time, in seconds, to send loop detection packet. The supported range is 1 to 10 seconds and the default value is 2 seconds.
Storm Control Broadcast	Enables storm control broadcast. If the number of broadcast packets per second on one port in the AP exceeds the configured threshold, the port is shutdown.
Storm	Storm control broadcast threshold in packets per second after which the port is shutdown. The default value is 2000 packets per second.

High-Throughput APs

With the implementation of the IEEE 802.11ac standard, very-high-throughput can be configured to operate on the 5 GHz frequency band. High-throughput (802.11n) can be configured on both the 5 GHz and 2.4 GHz frequency bands. High-throughput is enabled by default, and can be enabled or disabled in the 802.11a and 802.11g radio profiles. For details, see 2.4 GHz and 5 GHz Radio RF Management .

Two different profiles advanced define settings specific to high-throughput APs, the **high-throughput radio** profile and the **high-throughput SSID** profile. Use the **High-throughput radio** profile to configure your APs to advertise intolerance of 40 Mhz operation (by default, this option is disabled, and 40 Mhz operation is allowed). This profile also allows you to enable the **CSD Override** feature. When you turn on CSD override, CSD is disabled and only one antenna transmits data, even if they are being sent to high-throughput stations. The **High-throughput SSID** profile configures the high-throughput SSID settings for 802.11n.

You must create and modify a high-throughput radio or high-throughput SSID profile to change default values for an AP radio, such as activating features not enabled by default, disabling features that are enabled by default, or modifying default values for configuration settings.

> Stations are not allowed to use high-throughput with TKIP stand-alone encryption, although TKIP can be provided in mixed-mode BSSIDs that support high-throughput. High-throughput is disabled on a BSSID if the encryption mode is stand-alone TKIP or WEP.

This section describes the following topics:

- Configuring Advanced High-Throughput Radio Settings
- Configuring Advanced High-Throughput SSID settings

Configuring Advanced High-Throughput Radio Settings

Most deployments do not require manual configuration of the high-throughput radio profile.

However, you can configure advanced high-throughput radio profile settings using the WebUI or CLI.

- In the WebUI
- In the CLI

Configuring Advanced High-Throughput SSID settings

Most deployments do not require manual configuration of the high-throughput SSID profile.

However, you can configure advanced high-throughput SSID profile settings or modify default SSID profile values using the WebUI or CLI.

> De-A-MSDUs is supported with a maximum frame transmission size of 4 k bytes; however, this feature is always enabled and is not configurable. Aggregation is not currently supported.

- In the WebUI
- In the CLI

High-Efficiency (HE) APs

With the implementation of the IEEE 802.11ax standard, you can configure and improve spectrum efficiency and area throughput in dense deployment scenarios of APs or stations in both indoor and outdoor environments. You can configure High-Efficiency (HE) to operate on both the 2.4 GHz and 5 GHz frequency bands. HE is enabled by default, and can be enabled or disabled in the 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac radio profiles.

The 802.11ax certification requires the Wi-Fi Alliance's Agile Multiband Operation (MBO) certification. This certification enables Wi-Fi devices to better adapt to changing network conditions. It helps in improving resource utilization, balanced network load, and various other features.

The MBO certification also includes Cellular Data Capability (CDC). This provides APs or multi-mode capable STAs to advertise CDC support.

The **High-efficiency SSID** profile configures the High-Efficiency SSID settings for 802.11ax. Use the **High-efficiency SSID** profile to configure your APs to allocate the whole channel to a single user at a time or partition a channel to serve multiple users simultaneously.

This section describes the following topic:

Configuring Advanced High-Efficiency SSID settings

Most deployments do not require manual configuration of the High-Efficiency SSID profile. However, you can configure advanced High-Efficiency SSID profile settings or modify default SSID profile values using the WebUI or CLI.

- In the WebUI
- In the CLI

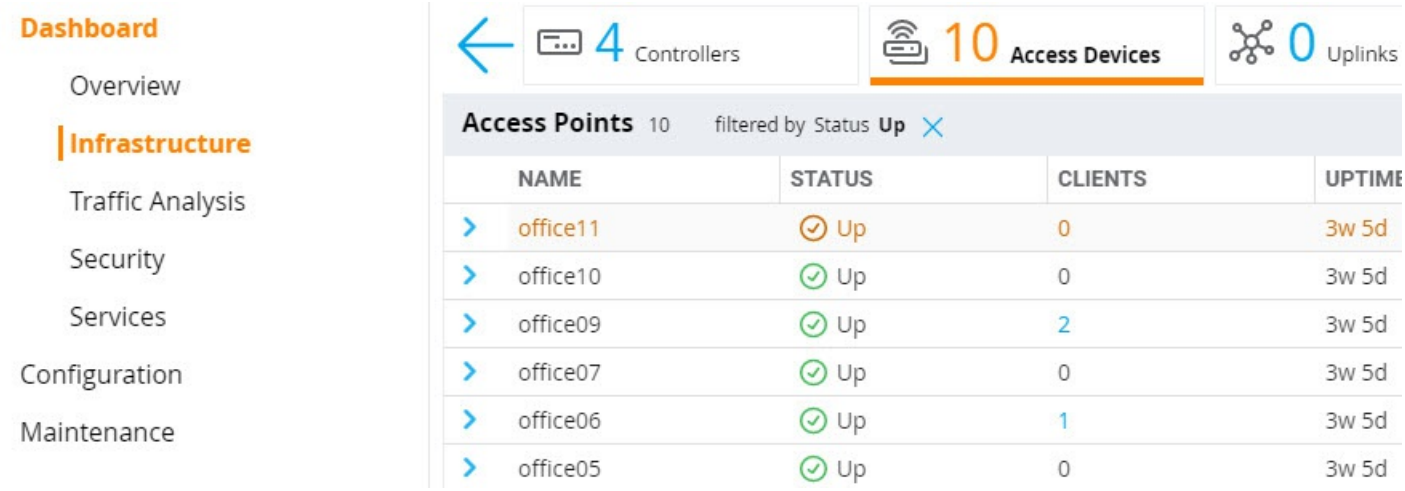
AP Packet Capture

Starting from ArubaOS 8.4.0.0, this feature allows you to manually start and stop capturing 802.11 Wi-Fi packets sent and received by an access point. This feature is supported only on an access point that is Up.

The following procedure describes how to capture packets.

1. In the **Managed Network** hierarchy, navigate to **Dashboard >Infrastructure > Access Devices.**
2. In the **Access Points** table, hover over an access point and then click on packet capture icon of an access point. The **Packet Capture** dialog box is displayed.

Figure 1 *AP Packet Capture*



3. Enter the **Target IP address** and the **Port** number to which you want to send the captured packets to.
4. Select a format from the **Format** drop-down list. The default format is **pcap**.
5. Select the bandwidth using the **Band** drop-down list. You can either select **2.4 GHz** or **5 GHz**. The default value is **2.4 GHz**.
6. Click **Start** to start capturing the packets.

Packet capturing can be stopped or paused using the options, **Pause** or **Stop** from the **Packet Capture** dialog box.

In Remote APs, the captured packets are sent from the AP to the controller. Then, the controller routes the packets to the target IP address. Hence, issue the **ap packet-capture open-port <port>** command to allow access to the UDP port to capture packets and then issue the **ap packet-capture close-port <port>** after capturing packets.

Green AP

Green AP is a feature that helps save energy consumption from common equipment in various areas like airports, offices, universities, hotels and so on. Based on the feeds, the Green AP feature dynamically enables, disables, or reduces functionality of an allocated AP to reduce the consumption of energy.

NetInsight provides the feed for ArubaOS to move the APs into deep-sleep mode or to wake up the APs from deep sleep mode. ArubaOS is responsible for maintaining the state of the APs and forwarding the AMON telemetry in different state.

In a Campus AP setup, the Mobility Master will communicate between NetInsight and the APs. For example, if NetInsight determines that a list of APs are to be put in deep-sleep or power saving mode, NetInsight sends the list to Mobility Master and then, the Mobility Master forwards the request to the APs through the managed device. The AP then, decides to either accept or reject the deep sleep request and sends the status back through AMON messages to the Mobility Master. This is again communicated to NetInsight.

The APs will not fall into deep-sleep mode in the following scenarios:

- The AP does not support WoL functionality.
- In MultiZone where APs need to provide wireless services for Datazone.
- The AP is preloading image.
- The AP is writing flash
- The APs have pending STAs.
- Wired AP is enabled on an AP.
- AP is 802.1X enabled.

Before the AP falls into deep-sleep mode, it performs the following actions:

- Bring down all the virtual APs.
- Send a warning syslog message
- Remove all connections to managed devices.
- Set the reboot reason. This is set to ensure that when the AP wakes up from the deep-sleep mode, this reboot reason indicates that the AP has recovered from deep-sleep mode.
- AP falls into deep-sleep mode.

Whenever the AP wakes up from the deep-sleep mode, the AP gets rebooted and the reason for the reboot is logged as, AP is waken up from deep-sleep mode.

AP-555, AP-534, AP-535 and 510 Series access points support the Green AP, a power saving feature.

> APs wake up automatically every 2 hours using the BLE process and report the status to NetInsight and if the NetInsight communicates that they need to be put back into deep-sleep mode, then the APs are again put into deep-sleep mode.

Limitations

Green AP feature is not supported for the following:

- Legacy APs without WoL support
- Instant APs
- Remote APs
- Mesh portals and mesh points
- Stand-alone controllers deployment

Remote Access Points

The Secure Remote Access Point Service allows AP users, at remote locations, to connect to an Aruba Managed Device over the Internet. As the Internet is involved, data traffic between the Managed Device and the remote AP is VPN encapsulated. That is, the traffic between the Managed Device and AP is encrypted. Remote AP operations are supported on all of Aruba's APs.

Topics in this section include:

About Remote Access Points

Remote APs connect to a managed device using XAuth or IPsec. AP control and 802.11 data traffic are carried through this tunnel. Secure Remote AP Service extends the corporate office to the remote site. Remote users can use the same features as corporate office users. For example, VoIP applications can be extended to remote sites while the servers and the PBX remain secure in the corporate office.

For bothRemote APs and Campus APs, tunneled SSIDs will be brought down eight seconds after the AP detects that there is no connectivity to the managed device. However, Remote AP bridge-mode SSIDs are configurable to stay up indefinitely (always-on or persistent). For Campus AP bridge-mode SSIDs, the Campus AP will be brought down after the keepalive times out (default 3.5 minutes).

Secure Remote AP Service can also be used to secure control traffic between an AP and the managed device in a corporate environment. In this case, both the AP and managed device are in the company's private address space.

The Remote AP must be configured with the IPsec VPN tunnel termination point. Once the VPN tunnel is established, the AP bootstraps and becomes operational. The tunnel termination point used by the Remote AP depends upon the AP deployment, as shown in the following scenarios:

- Deployment Scenario 1: The Remote AP and managed device reside in a private network which secures AP-to-Managed Device communication. (This deployment is recommended when AP-to-Managed Device communications on a private network need to be secured.) In this scenario, the Remote AP uses the managed device's IP address on the private network to establish the IPsec VPN tunnel.
- Deployment Scenario 2: The Remote AP is on the public network or behind a NAT device and the managed device is on the public network. The Remote AP must be configured with the tunnel termination point, which must be a publicly-routable IP address. In this scenario, a routable interface is configured on the managed device in the DMZ. The Remote AP uses the managed device's IP address on the public network to establish the IPsec VPN tunnel.
- Deployment Scenario 3: The Remote AP is on the public network or behind a NAT device and the managed device is also behind a NAT device. (This deployment is recommended for remote access.) The Remote AP must be configured with the tunnel termination point, which must be a publicly-routable IP address. In this scenario, the Remote AP uses the public IP address of the corporate firewall. The firewall forwards traffic to an existing interface on the managed device (The firewall must be configured to pass NAT-T traffic (UDP port 4500) to the managed device).

In any of the described deployment scenarios, the IPsec VPN tunnel can be terminated on a managed device, with a managed device located elsewhere in the corporate network. The remote AP must be able to communicate with the managed device after the IPsec tunnel is established. Make sure that the L2TP IP pool configured on the managed device (from which the Remote AP obtains its address) is reachable in the managed device network by the managed device.

It is not recommended to place a Remote AP in the same subnet as its terminating controller. Each Remote AP is deployed at a remote location that is connected over a multi-hop public or private IP network where a direct Layer 2 path to the Mobility Controllers in the data center is not possible. As a best practice, always place an IP router between the APs and the Mobility Controllers as it establishes Layer 2 fault domains.

Configuring the Secure Remote Access Point Service

The tasks for configuring an Aruba Access Point as a Secure Remote Access Point Service are:

- Configure a public IP address for the Managed Device.

  You must install one or more AP licenses in the Managed Device. There are several AP licenses available that support different maximum numbers of APs. The licenses are cumulative; each additional license installed increases the maximum number of APs supported by the Managed Device.
- Configure the VPN server on the Managed Device. The remote AP will be a VPN client to the server.
- Provision the AP with IPsec settings, including the username and password for the AP, before you install it at the remote location. You can also provision the Remote AP using the ZTP method. For more information, see Provisioning 4G USB Modems on Remote Access Points.

Configuring a Public IP Address for the Managed Device

The remote AP requires an IP address to which it can connect to establish a VPN tunnel to the Managed Device. This can be either a routable IP address you configure on the Managed Device, or the address of an external router or firewall that forwards traffic to the Managed Device. The following procedure describes how to create a DMZ address on the Managed Device.

The following procedure describes how to configure a public IP address for the managed device:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration** > **Interfaces** > **VLANs** page.
2. Click **+** to add a VLAN.
3. Enter the **VLAN name** and **VLAN ID/Range**.
4. Click **Submit**.
5. Click the Vlan Id created. The **VLANs>name** table is displayed.
6. Click the Vlan Id from **VLANs>name** table.
7. Click **Edit** on **Port Members**.
8. Click > to select the port that belongs to this VLAN .
9. Click **OK**.
10. Click **Submit**.
11. Click **IPv4** tab.
12. Enter the IPv4 address in the **IPv4 address** field.
13. Click **Submit**.
14. Click **Pending Changes**.
15. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands configure a public IP address for the managed device:

```
(host) [md] (config) #vlan <id>
(host) [md] (config) #interface vlan <id>
(host) [md] (config-submode) #ip address <ipaddr> <ipmask>
```

Configuring the NAT Device

Communication between the AP and the secure Managed Device uses the UDP 4500 port. When both the Managed Device and the AP are behind NAT devices, configure the AP to use the NAT device's public address as its master address. On the NAT device, you must enable NAT-T (UDP port 4500 only) and forward all packets to the public address of the NAT device on UDP port 4500 to the Managed Device to ensure that the remote AP boots successfully.

Configuring the VPN Server

This section describes how to configure the IPsec VPN server on the Managed Device. For more details, see Virtual Private Networks. The remote AP will be a VPN client that connects to the VPN server on the Managed Device.

The following procedure describes how to configure the VPN server:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration** > **Services** > **VPN** tab.
2. Click **IKEv1** accordion.
3. Click **L2tp** check box to enable L2tp.
4. Select **PAP (Password Authentication Protocol)** check box for **Auth protocols**.
5. To configure the L2TP IP pool, click **General VPN** option.
6. Click **+** in the **Address Pools** table.
7. Enter the **Pool name** to configure the L2TP pool from which the APs will be assigned addresses.
8. Enter the value of the **Start address (ipv4/v6)** and **End address (ipv4/v6)** fields.
9. Click **Submit**.

> The size of the pool should correspond to the maximum number of APs that the Mobility Master is licensed to manage.

10. To configure an ISAKMP encrypted subnet and PSK, click the **Shared Secrets** accordion.
11. Click **+** in the **IKE Shared Secrets** table.
12. In the **Create IKE Group** table, enter the value for **Shared key** and re-enter the key in **Retype shared key**.
13. Click **Submit**.
14. Click **Pending Changes**.
15. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands configure the VPN server:

```
(host) [md] (config) #vpdn group l2tp
(host) [md] (config-submode) #ppp authentication PAP
(host) [md] (config-submode) #ip local pool <pool_name> <pool_start_address> <pool_end_address>
(host) [md] (config) #crypto isakmp key <keystring> address <ipaddr> netmask <mask>
```

Configuring CORP DNS Server

EST servers are generally deployed in a corporate network and EST enrollment can take place only if the DNS requests are resolved. Starting from ArubaOS 8.5.0.0, Remote Access Points will use CORP DNS server for EST enrollment. This will enable the Remote AP to use its own DNS server and not the one provided by the Internet Service Provider, because the ISP provided DNS server will not be reachable within a corporate network and hence will result in failure of DNS requests. EST enrollment cannot not take place if the DNS requests fail. Thus it is necessary for Remote AP to configure corp DNS server for successful EST enrollment.

> CORP DNS server can be configured only for Remote Access Points.

This feature supports both IPv4 and IPv6 addresses and only two CORP DNS servers can be configured.

The following procedure describes how to configure CORP DNS server:

1. In the **Managed Network** node of the hierarchy, navigate to **Configuration** > **System > Profiles**.
2. Expand **AP**. Select **AP system profile**. Click **+** to create a new profile.
3. Enter a **Profile Name.**
4. Expand the **Remote AP** accordion.
5. To configure an IPv4 address, click **+** in **Remote-AP CORP DNS server** and enter the **IP address** in the **Remote-AP CORP DNS server** text box. Click **OK.**
6. To configure an IPv6 address, click **+** in **Remote-AP CORP DNS server IPV6** and enter the **IP address** in the **Remote-AP CORP DNS server IPV6** text box. Click **OK.**
7. Click **Submit**.
8. Select **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands configure a CORP DNS server:

```
(host) [mynode] (config) #ap system profile <profile-name>
(host) [mynode] (AP system profile <profile-name>) #rap-corp-dns-server <ipv4 address>
(host) [mynode] (AP system profile <profile-name>) #rap-corp-dns-server_ ipv6  <ipv6 address>
```

CHAP Authentication Support over PPPoE

RAPs can now establish a PPPoE session with a PPPoE server at the ISP side and get authenticated using the CHAP. The PPPoE client running on a Remote AP is capable of handling the CHAP authentication requests from the PPPoE server.

> The PPPoE client selects either the PAP or the CHAP credentials for the Remote AP authentication depending upon the request from the PPPoE server.

The following procedure describes how to configure CHAP:

1. In the **Managed Network** node of the hierarchy, navigate to the **Configuration** > **Access Points** > **Remote APs** tab. The list of discovered APs are displayed on this page.
2. Select the AP you want to configure using CHAP and click **Provision**.
3. In the popup window click **Continue and Reboot**.
4. Click **Uplink** tab and enter the **CHAP Secret** .

> You can use all the special characters except question mark (?) and the space can be used within double quotes (“ “).

5. Enter the CHAP Secret again in the **Retype** text box for confirmation.
6. Click **Submit** and **Reboot.**
7. Click **Pending Changes**.
8. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands configures CHAP:

```
(host) [md] (config) #provision-ap pppoe-chap-secret <KEY>
(host) [md] (config-submode) #reprovision ap-name <name>
```

Configuring Certificate Remote AP

You can configure the remote AP to use the internal certificate for authentication.

The following procedure describes how to configure the certificate Remote AP:

1. In the **Managed Network** node of the hierarchy, navigate to **Configuration** > **Access Points > Remote APs** tab.
2. Select a check box next to the AP Name in the Remote AP table click **Provision**.
3. In the **General** tab, select **Certificate** from the **Authentication methods** drop-down list.
4. Click **Submit** to apply the configuration and reboot the AP as certificate Remote AP.
5. Click **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI command configures the certificate Remote AP:

```
(host) [mynode] (config) #whitelist-db rap add
(host) [mynode] (config) #whitelist-db rap add mac-address <mac-address>
```

Creating a Remote AP Whitelist

If you use the ZTP method to provision the certificate Remote AP, then you must create a Remote AP whitelist. For more information on ZTP of the Remote AP, see Provisioning 4G USB Modems on Remote Access Points.

Remote AP whitelist is the list of approved APs that can be provisioned on your Managed Device.

The following procedure describes how to create a Remote AP whitelist

1. In the **Managed Network** node of the hierarchy, navigate to **Configuration** > **Access Points > Whitelist** tab.
2. Click **Remote AP Whitelist** tab.
3. Click **+** and provide the following details:
   - **MAC Address** - Enter the MAC address of the AP.
   - **AP Group** - Select a group to add the AP.
   - **AP Name** - Enter a name for the AP. If you do not enter an AP name, the MAC address will be used instead.
   - **Description** - Enter a text description for the AP.
4. Click **Submit** to add the remote AP to the whitelist.
5. Click **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy changes**.

Configuring PSK Remote AP

You can use PSK authentication to provision an individual remote AP or a group of remote APs using an IKE PSK.

The following procedure describes how to configure PSK authentication for Remote AP:

1. In the **Managed Network** node hierarchy, navigate to **Configuration** > **Access Points > Remote APs** tab.
2. Select the required Remote AP and click **Provision**.
3. In the **General** tab, select **Pre-shared Key** from the **Authentication methods** drop-down list.
4. Enter and confirm the IKE PSK.
5. Select **Global User Name/password** or a **Per AP User Name/Password** from**User credential assignment** drop-down list.
   a. If you use the **Per AP User Names/Passwords** option, each Remote AP is given its own username and password.
   b. If you use the **Global User Name/Password** option, all selected RAPs are given the same (shared) username and password.
6. Enter the user name, and enter and confirm the password. If you want the managed device to automatically generate a user name and password, select **Use Automatic Generation**. If this option is not selected, the user has to enter it manually.
7. Click **Submit**.
8. Click **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy changes**.

Add the User to the Internal Database

The following procedure describes how to add the user to the Internal database:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration** > **Authentication** > **Auth Servers** tab.
2. From the **All Servers** table, select **Internal** under the **Name** field.
3. Click **+** in the **Users** tab. The **Internal Server > Add New User** page is displayed.
4. Enter the **User Name** and **Password**.
5. Click **Enabled** check box to activate this entry on creation.
6. Click **Submit**. Note that the configuration does not take effect until you perform this step.
7. Click **Pending Changes**.
8. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands add the user to the Internal database:

Execute the following command:

```
(host) [mynode] (config) #local-userdb add username rapuser1 password <password>
```

Remote AP Static Inner IP Address

The Remote AP static inner IP address feature assigns a static inner IP address to a Remote AP. A new *remote-IP address* parameter is added to the existing configuration commands.

The following procedure describes how to configure Remote AP static inner IP address:

To view IP address parameter in the local database:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration** > **Authentication** > **Auth Servers** tab.
2. In the **All Servers** table, select **Internal** under the **Name** field.
3. A list of **StaticIP for RAPs** is displayed under **Server > Internal** table.

To view the IP Address parameter in the Remote AP Whitelist:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Access Points > Remote APs** tab.

The following CLI commands configure Remote AP static inner IP address:

```
(host) [mynode] (config) #local-userdb add {generate-username|username <name>} {generate-password|password <password>} {remo
te-ip <remote-ip>}
(host) [mynode] (config) #local-userdb modify {username < name>} {remote-ip <remote-ip>}
```

Issue the following command in config mode:

```
(host) [mynode] (config) #whitelist-db rap add {mac-address <address>}{ap-group <ap_group>}{remote-ip <remote-ip>}
(host) [mynode] (config) #whitelist-db rap modify {mac-address <address>} {remote-ip<remote-ip>}
```

> You cannot configure the IP Address parameter using the WebUI.

Provisioning the AP

You need to configure the VPN client settings on the AP to instruct the AP to use IPsec to connect to the Managed Device. You can provision the Remote AP and allow remote users to provision the AP at home. This method of provisioning is referred as ZTP. See Provisioning 4G USB Modems on Remote Access Points for more information about ZTP of remote AP.

You must provision the AP before you install it at its remote location. To provision the AP, the AP must be physically connected to the local network or directly connected to the Managed Device. When connected and powered on, the AP must also be able to obtain an IP address from a DHCP server on the local network or from the Managed Device.

If your configuration has an internal LMS IP address, remote APs may attempt to switch over to the LMS IP address, which is not reachable from the Internet. For remote APs, ensure that the LMS IP address in the AP system profile for the AP group has an externally routable IP address.

Reprovisioning the AP causes it to automatically reboot. The easiest way to provision an AP is to use the Provisioning page in the WebUI, as described in the following steps:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Access Points > Remote APs** tab.
2. Select the remote AP and click **Provision**.
3. Select **Pre-shared Key** from the **Authentication Methods** drop-down list.
4. Enter the **User name**, **Password**, and **Confirm password**.

   The username and password you enter must match the username and password configured on the authentication server for the remote AP.

5. Select the **Static** option in the **Controller Discovery** field.
6. Set the **Controller IP/DNS** name as shown below:

Table 1: *Configuring a Managed device IP Address*

Deployment Scenario	Master IP Address Value
Deployment 1	Managed device IP address.
Deployment 2	Managed device public IP address.
Deployment 3	Public address of the NAT device to which the managed device is connected.

The username and password you enter must match the username and password configured on the authentication server for the remote AP.

7. Select **DHCP** option in the **IP** field.
8. Click **Submit**.
9. Click **Pending Changes**.
10. In the **Pending Changes** window, select the check box and click **Deploy changes**.

Secondary Managed Device

The secondary managed device provides reliability and redundancy; however the functionality of a secondary managed device is initiated only after an AP terminates on a managed device successfully and retrieves the configuration. If the AP boots up and fails to connect to the managed device the AP cannot be managed. To address this, ArubaOS 8.0 introduces the secondary managed device feature.

In a scenario where the managed device is not reachable, the AP will try to reach the secondary managed device and if successful will terminate on the secondary managed device. The secondary managed device details are not stored in the system flash when the AP is deployed for the first time, but only after a successful configuration. An AP can use the secondary managed device feature after the AP reboots.

> If an AP has not been configured to a managed device after deployment, the secondary managed device feature will not be applicable.

The following procedure describes how to enable the secondary managed device feature:

1. In the **Managed Network** node hierarchy, navigate to **Configuration** > **System** > **Profiles**.
2. Select **AP > AP System** under **All Profiles**.
3. Select the AP profile for which the secondary managed device feature is to be enabled. The AP system profile section is displayed.
4. Enter an IP or FQDN value for the secondary managed device in the **Secondary Master IP/FQDN** field.
5. Click **Save**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy changes**.

> The secondary managed device feature can be enabled on the secondary managed device.

The following CLI commands enable the secondary managed device feature.

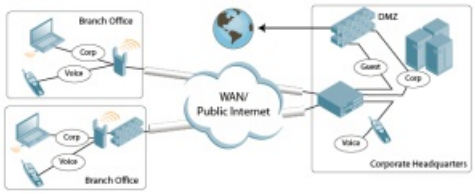
```
(host) [mynode] (config) #ap system-profile <profile name>
(host) [mynode] (AP system profile "profile name")#secondary-master <value>
```

Deploying a Branch or Home Office Solution

In a branch office, the AP is deployed in a separate IP network from the corporate network. Typically, there are one or two NAT devices between the two networks. Branch office users need access to corporate resources such as printers and servers, but traffic to and from these resources must not impact the corporate head office.

Figure 1 is a graphic representation of a remote AP in a branch or home office, with a single Managed Device providing access to both a corporate WLAN and a branch office WLAN.

Figure 1 *Remote AP with Single Managed device*



Branch office users want continued operation of the branch office WLAN, even if the link to the corporate network goes down. The branch office AP solves these requirements by providing the following capabilities on the branch office WLAN:

- Local termination of 802.11 management frames which provides survivability of the branch office WLAN.
- All 802.1X authenticator functionality is implemented in the AP. The Managed Device is used as a RADIUS pass-through when the authenticator has to communicate with a RADIUS server (which also supports survivability).
- 802.11 encryption or decryption is in the AP to provide access to local resources.
- Local bridging of client traffic connected to the WLAN or to an AP enet1 port to provide access to local resources.

Provisioning the Branch AP

You can provision the remote AP either using the Managed Device or using the ZTP method. For more information on Managed Device provisioning, see Configuring Installed APs. For more information on ZTP, see Provisioning 4G USB Modems on Remote Access Points.

Configuring the Branch AP

- Specify forward mode for the ESSID in the virtual AP profile
- Specify remote AP operation in the virtual AP profile (The remote AP operates in standard mode by default.)
- Set how long the AP stays up after connectivity to Managed Device has gone down in the SSID profile
- Set the VLAN ID in the virtual AP profile
- Set the native VLAN ID in the AP system profile
- Set forward mode for enet1 port

> Remote APs support 802.1q VLAN tagging. Data from the remote AP will be tagged on the wired side.

Troubleshooting Remote AP

The following WebUI options are available to troubleshoot issues with remote AP:

- Using local debugging feature
- Viewing the remote AP summary report
- Viewing remote AP connectivity report
- Using remote AP diagnostic options

Local Debugging

Local debugging is a WebUI feature that allows end users to perform diagnostics and view the status of their remote AP through a wired or wireless client. This feature is useful for troubleshooting connectivity problems on remote APs and performing throughput tests. There are three tabs in the **Local Debugging** WebUI window; **Summary**, **Connectivity**, and **Diagnostics**. Each tab displays different information for the AP, but all three tabs include a **Generate & save support file** link that, when clicked, will automatically generate a **support.tgz** file that can be sent to a corporate IT department for additional analysis and debugging.

> A snapshot of the bridge, acl, session, user, and arp tables, current processes, memory, and kernel debug messages are captured in a single **rap_debug.txt** file which is bundled along with **support.tgz** file.

Bringing up Certificate-Based Remote AP in VMC

A certificate-based remote AP does not come up on a virtual mobility controller (VMC) because TPM certificate for the AP is present in the Mobility Master. However, you can bring up the remote AP by using a self-signed certificate.

To do this, first you need to bring up the AP as campus AP. Then, reprovision the AP to come up as remote AP.

The following procedure describes how to bring up a remote AP on the VMC by using a self-signed certificate:

1. Bring up the AP as a campus AP. See the Configuring Installed APs section.

   Before reprovisioning the AP as remote AP, ensure that the AP has come up as campus AP successfully.

2. In the **Managed Network** node hierarchy, navigate to the **Configuration > Access Points > Campus APs** tab.
3. Select the AP name you want to reprovision as remote AP.
4. Click **Provision**.
5. Select **Static** option in the **Controller discovery** field.
6. Enter the IP address or the complete DNS name for the Managed Device, In the **Controller IP/DNS name** field,
7. Select **DHCP** option in the **IP** field.
8. Select the **Remote** option in the **Deployment** field.
9. Select **Certificate** from the **Authentication methods** drop-down list.
10. Select **self-signed** from the **Trust anchor** drop-down list.
11. Click **Submit**.
12. Click **Pending Changes**.
13. In the **Pending Changes** window, select the check box and click **Deploy changes**.

Enabling Remote AP Advanced Configuration Options

This section describes the following features designed to enhance your remote AP configuration:

- ArubaOS 8.6.0.0 Help Center
- ArubaOS 8.6.0.0 Help Center
- Specifying the DNS Managed Device Setting
- Backup Managed Device List
- Configuring Remote AP Failback
- Working with ACL and Firewall Policies
- Understanding Split Tunneling
- Provisioning Wi-Fi Multimedia

> The information in this section assumes you have already configured the remote AP functionality, as described in Configuring the Secure Remote Access Point Service.

Understanding Remote AP Modes of Operation

Table 1 summarizes the different remote AP modes of operation. You specify both the forward mode setting (which controls whether 802.11 frames are tunneled to the Managed Device using GRE, bridged to the local Ethernet LAN, or a combination thereof) and the remote AP mode of operation (when the virtual AP operates on a remote AP) in the virtual AP profile.

The column on the left of the table lists the remote AP operation settings. The row across the top of the table lists the forward mode settings. To understand how these settings work in concert, scan the desired remote AP operation with the forward mode setting, and read the information in the appropriate table cell.

The all column and row lists features that all remote AP operation and forward mode settings have in common regardless of other settings. For example, at the intersection of all and bridge, the description outlines what happens in bridge mode regardless of the remote AP mode of operation.

Table 1: *Remote AP Modes of Operation and Behavior*

Remote AP Operation Setting	Forward Mode Setting				
	all	**bridge**	**split-tunnel**	**tunnel**	**decrypt-tunnel**
all		Management frames on the AP. Frames are bridged between wired and wireless interfaces. No frames are tunneled to the Managed Device. Station acquires its IP address locally from an external DHCP server.	Management frames on the AP. Frames are either GRE tunneled to the Managed Device, to a trusted tunnel or are sent through the NAT and bridged on the wired interface according to user role and session ACL. Typically, the station obtains an IP address from a VLAN on the Mobility Master. Typically, the AP has ACLs that forward corporate traffic through the tunnel and source NAT the non-corporate traffic to the Internet.	Frames are GRE tunneled to the Managed Device to an untrusted tunnel. 100% of station frames are tunneled to the Managed Device.	Management frames on the AP. Frames are always GRE tunneled to Managed Device.
always	ESSID is always up when the AP is up regardless of whether the Managed Device is reachable. Supports PSK ESSID only. SSID configuration stored in flash on AP.	Provides an SSID that is always available for local access.	Not supported	Not supported	Not supported
	all	**bridge**	**split-tunnel**	**tunnel**	**decrypt-tunnel**
backup	ESSID is only up when the Managed Device is unreachable. Supports PSK ESSID only.	Provides a backup SSID for local access only when the Managed Device is unreachable.	Not supported	Not supported	Not supported

Working in Fallback Mode

The fallback mode (also known as backup configuration) operates the remote AP if the master Managed Device or the configured primary and backup LMS are unreachable. The remote AP saves configuration information that allows it to operate autonomously using one or more SSIDs in local bridging mode, while supporting open association or encryption with PSKs. You can also use the backup configuration if you experience network connectivity issues, such as the WAN link or the central data center becoming unavailable. With the backup configuration, the remote site does not go down if the WAN link fails or the data center is unavailable.

You define the backup configuration in the virtual AP profile on the Managed Device. The remote AP checks for configuration updates each time it establishes a connection with the Managed Device. If the remote AP detects a change, it downloads the configuration changes.

The following remote AP backup configuration options define when the SSID is advertised (refer to for more information):

- Always - Permanently enables the virtual AP. Recommended for bridge SSIDs.
- Backup - Enables the virtual AP if the remote AP cannot connect to the Managed Device. This SSID is advertised until the Managed Device is reachable. Recommended for bridge SSIDs.
- Persistent - Permanently enables the virtual AP after the remote AP initially connects to the Managed Device. Recommended for 802.1X SSIDs.
- Standard - Enables the virtual AP when the remote AP connects to the Managed Device. Recommended for 802.1X, tunneled, and split-tunneled SSIDs. This is the default behavior.

While using the backup configuration, the remote AP periodically retries its IPsec tunnel to the Managed Device. If you configure the remote AP in backup mode, and a connection to the Managed Device is re-established, the remote AP stops using the backup configuration and immediately brings up the standard remote AP configuration. If you configure the remote AP in always or persistent mode, the backup configuration remains active after the IPsec tunnel to the Managed Device has been re-established.

Configuring Fallback Mode

To configure the fallback mode, you must:

- Configure the AAA profile
- Configure the virtual AP profile

Configuring the AAA Profile for Fallback Mode

The following procedure describes how to configure the AAA profile for fallback mode:

The AAA profile defines the authentication method and the default user role for unauthenticated users:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** tab.
2. Select **Wireless LAN > AAA** under **All Profiles**.
3. In the **AAA Profile: New Profile** table, click **+** in **AAA Profile**.
4. Enter the **Profile name**.
5. For **Initial role**, select the appropriate role (for example, logon) from the drop-down list.
6. For **802.1X Authentication Default Role**, select the appropriate role (for example, default) from the drop-down list.
7. Click **Save**.
8. Select the AAA profile that you just created:
   a. Click **802.1X Authentication Server Group**, and select the **Server Group** to be used (for example, default) from the drop-down list.
   b. Click **Save**.

   > If you need to create an 802.1X Authentication Server Group, select **new** from the **802.1X Authentication Server Group** drop-down list, and enter the appropriate parameters.

   c. Click **802.1X Authentication**, and select the **802.1X Authentication Profile** to be used (for example, default) from the drop-down list.
   d. Click **Save**.
9. Click **Pending Changes**.
10. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands configure the AAA profile for fallback mode:

```
(host) [md] (config) #aaa profile default
 (host) [md] (AAA Profile "default") #initial-role <role>
 (host) [md] (AAA Profile "default") #authentication-dot1x <dot1x-profile>
 (host) [md] (AAA Profile "default") #dot1x-default-role <role>
 (host) [md] (AAA Profile "default") #dot1x-server-group <group>
```

Configuring the DHCP Server on the Remote AP

You can configure the internal DHCP server on the remote AP to provide an IP address for the backup SSID if the Managed Device is unreachable. If configured, the remote AP DHCP server intercepts all DHCP requests and assigns an IP address from the configured DHCP pool.

To configure the remote AP DHCP server:

1. Enter the VLAN ID for the remote AP DHCP VLAN in the AP system profile. This VLAN enables the DHCP server on the AP (also known as the remote AP DHCP server VLAN). If you enter the native VLAN ID, the DHCP server is not configured and is unavailable.
2. Specify the DHCP IP address pool and netmask. The AP assigns IP addresses from the DHCP pool 192.168.11.0/24 by default, with an IP address range from 192.168.11.2 through 192.168.11.254. You can manually define the DHCP IP address pool and netmask based on your network design and IP address scheme.
3. Specify the IP address of the DHCP server, DHCP router, and the DHCP DNS server. The AP uses IP address 192.168.11.1 for the DHCP server, the DHCP router, and the DHCP DNS server by default.
4. Enter the amount of days the assigned IP address is valid (also known as the remote AP DHCP lease). The lease does not expire by default, which means the IP address is always valid.
5. Assign the VLAN ID for the remote AP DHCP VLAN to a virtual AP profile. When a client connects to that virtual AP profile, the AP assigns the IP address from the DHCP pool.

> The following is a high-level description of the steps required to configure the DHCP server on the remote AP. The steps assume you have already created the virtual AP profile, AAA profile, SSID profile, and other settings for your remote AP operation (for information about the backup configuration, see ArubaOS 8.6.0.0 Help Center).

The following procedure describes how to configure the DHCP Server on the Remote AP:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > AP Groups** menu option.
2. Select an **AP Group**.
3. Click **More** tab and add the appropriate value in the following fields:
   a. Enter the LMS IP address in the **LMS IP address** field and the Bakcup LMS IP address in the **Backup LMS IP address** field.
   b. Enter the LMS IPv6 address in the **LMS IPv6 address** field and the Bakcup LMS IPv6 address in the **Backup LMS IPv6 address** field.
   c. Click **Submit**.
4. In the **Managed Network** node hierarchy, navigate to **Configuration > System > Profiles** tab.
   a. Select **AP> AP System** under **All Profiles**, and select an AP system profile.
   b. Click **Remote AP** accordion.
   c. Enter the VLAN ID of the backup configuration virtual AP VLAN in the **Remote-AP DHCP Server VLAN** field .
   d. Enter the IP address of the DHCP server in the **Remote-AP DHCP Server ID** field.
   e. Enter the IP address of the default DHCP router in the **Remote-AP DHCP Default Router** field.
   f. Specify the DHCP IP address pool. This configures the pool of IP addresses from which the remote AP uses to assign IP addresses.
   - Enter the first IP address of the pool, in the **Remote-AP DHCP Pool Start** field.
   - Enter the last IP address of the pool, in the **Remote-AP-DHCP Pool End** field.
   - Enter the netmask, in the **Remote-AP-DHCP Pool Netmask** field.
   g. Specify the number of days for which the IP address is valid, in the **Remote-AP DHCP Lease Time** field.
   h. Click **Save**.
   i. Select **Wireless LAN > Virtual AP** under **All Profiles**, and the select virtual AP profile you want to configure.
   j. Click **Save**.
5. Click **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy changes**.

Configuring Advanced Backup Options

You can also use the backup configuration (fallback mode) to allow the remote AP to pass through a captive portal, such as network access in a hotel, airport, or other public network, to access the corporate network. For this scenario:

- Define a session ACL for the bridge SSID to source NAT all user traffic, except DHCP. For example, use **any any svc-dhcp permit** followed by **any any any route src-nat**. Apply the session ACL to a remote AP user role.
- Configure the AAA profile. Make sure the initial role contains the session ACL previously configured.

  The AAA profile defines the authentication method and the default user role.

  > 802.1X and PSK authentication is supported when configuring bridge or split tunnel modes.

- Configure the virtual AP profile for the backup configuration:
  - Set the remote AP operation to **always** or **backup**.
  - Create and apply the applicable SSID profile.
  - Configure a bridge SSID for the backup configuration. In the virtual AP profile, specify forward mode as **bridge**.

  For more information about the backup configuration, see Configuring Fallback Mode.
- Enter the remote AP DHCP server parameters in the AP system profile. For more information about the parameters, see Configuring the DHCP Server on the Remote AP .

  If you use a local DHCP server to obtain IP addresses, you must define one additional ACL to permit traffic between clients without using source NAT to route the traffic. Using the previously configured ACL, add **user alias internal-network any permit** before **any any any route src-nat**.
- Connect the remote AP to the available public network (for example, a hotel or airport network).

  The remote AP advertises the backup SSID so the wireless client can connect and obtain an IP address from the available DHCP server.

  > The client can obtain an IP address from the public network, for example a hotel or airport, or from the DHCP server on the remote AP.

  After obtaining an IP address, the wireless client can connect and access the corporate network and bring up the configured corporate SSIDs.

The following is a high-level description of what is needed to configure the remote AP to pass through a captive portal and access the corporate Managed Device. This information assumes you are familiar with configuring session ACLs, AAA profiles, virtual APs, and AP system profiles and highlights the modified parameters.

Specifying the DNS Managed Device Setting

In addition to specifying IP addresses for Managed Device, you can also specify the master DNS name for the Managed Device when provisioning the remote AP. The name must be resolved to an IP address when attempting to set up the IPsec tunnel. For information on how to configure a host name entry on the DNS server, refer to the vendor documentation for your server. It is recommended to use a maximum of 8 IP addresses to resolve a Managed Device name.

If the remote AP gets multiple IP addresses responding to a host name lookup, the remote AP can use one of them to establish a connection to the Managed Device. For more detailed information, see the next section ArubaOS 8.6.0.0 Help Center.

Specifying the name also lets you move or change remote AP concentrators without reprovisioning your APs. For example, in a DNS load-balancing model, the host name resolves to a different IP address depending on the location of the user. This allows the remote AP to contact the Managed Device to which it is geographically closest.

The DNS setting is part of provisioning the AP. The easiest way to provision an AP is to use the Provisioning page in the WebUI. These instructions assume you are only modifying the Managed Device information in the Master Discovery section of the Provision page.

> Reprovisioning the AP causes it to automatically reboot.

The following procedure describes how to specify the DNS managed device setting:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Access Points > Remote APs** tab.
2. Select the remote AP and click **Provision**.
3. In the **General** tab, enter master DNS name in the **Controller IP/DNS name** field.
4. Click **Submit**.
5. Click **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy changes**.

For more information, see Configuring the Secure Remote Access Point Service.

Backup Managed Device List

Using DNS, the remote AP receives multiple IP addresses in response to a host name lookup. Known as the backup managed device list, remote APs go through this list to associate with a managed device. If the primary managed device is unavailable or does not respond, the remote AP continues through the list until it finds an available managed device. This provides redundancy and failover protection.

The remote AP loses the IP address information received through DNS when it terminates and receives the system profile configuration from the managed device. If the remote AP loses connectivity on the IPsec tunnel to the managed device, the Remote AP fails over from the primary managed device to the backup managed device. For this scenario, add the IP address of the backup managed device in the backup LMS and the IP address of the primary managed device in the LMS field of the ap-system profile. Network connectivity is lost during this time. As described in the section ArubaOS 8.6.0.0 Help Center, you can also configure a remote AP to revert back to the primary managed device when it becomes available. To complete this scenario, you must also configure the LMS IP address and the backup LMS IP address.

For example, assume you have two data centers, data center 1 and data center 2, and each data center has one master managed device in the DMZ. You can provision the remote APs to use the managed device in data center 1 as the primary managed device, and the managed device in data center 2 as the backup managed device. If the remote AP loses connectivity to the primary, it will attempt to establish connectivity to the backup. You define the LMS parameters in the AP system profile.

Figure 1 Sample Backup Scenario

Configuring Remote AP Failback

In conjunction with the backup managed device list, you can configure remote APs to revert back (failback) to the primary managed device if it becomes available. If you do not explicitly configure this behavior, the remote AP will keep its connection with the backup managed device until the remote AP, managed device, or both have rebooted or some type of network failure occurs. If any of these events occur, the remote AP will go through the backup managed device list and attempt to connect with the primary managed device.

The following procedure describes how to configure Remote AP failback:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** tab.
2. Select **AP > AP system** under **All Profiles**.
3. Select the AP system profile you want to modify.
4. Enter the following details in the **LMS Settings** accordion:
   a. Select the **LMS Preemption** check box. This is disabled by default.
   b. Enter the duration (in seconds) for which the remote AP must wait before moving back to the primary managed device, in the **LMS Hold-down period** field.
5. Click **Save**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI command configures Remote AP failback:

```
(host) [md] (config) #ap system-profile <profile>
lms-preemption
lms-hold-down period <seconds>
```

Enabling Remote AP Local Network Access

You can enable local network access between the clients (from same or different subnets and VLANs) connected to a Remote AP through wired or wireless interfaces in split-tunnel or bridge forwarding modes. This allows the clients to effectively communicate with each other without routing the traffic via the managed device. You can use WebUI or CLI to enable the local network access.

The following procedure describes how to enable Remote AP local network access:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** tab.
2. Select **AP > AP system** under **All Profiles**.
3. Select the AP system profile you want to modify.
4. To enable remote network access, select the **Remote-AP Local Network Access** check box under the **Remote AP** accordion.
5. Click **Save**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy changes**.

- The following CLI commands enable Remote AP local network access:

```
(host) [md] (config) #ap system-profile <ap-profile> rap-local-network-access
```

- To disable, enter the following command:

```
(host) [md] (config) #ap system-profile <ap-profile> no rap-local-network-access
```

See the *ArubaOS CLI Reference Guide* for detailed information on the command options.

Configuring Remote AP Authorization Profiles

Remote AP configurations include an authorization profile that specifies which profile settings should be assigned to a remote AP that has been provisioned but not yet authenticated at the remote site. These yet-unauthorized APs are put into the temporary AP group **authorization-group** by default and assigned the predefined profile **NoAuthApGroup**. This configuration allows the user to connect to an unauthorized remote AP via a wired port, then enter a corporate username and password. Once a valid user has authorized the AP, and it will be marked as authorized on the network. The remote AP will then download the configuration assigned to that AP by its permanent AP group.

Adding or Editing a Remote AP Authorization Profile

The following procedure describes how to create a new authorization profile or edit an existing authorization profile:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** tab.
2. Select **AP > AP Authorization** under **All Profiles**.
   a. To edit an existing profile, select a profile listed under **AP Authorization** profile and select a new AP authorization group from the **AP authorization group** drop-down list.
   b. To create a new authorization profile, click **+** next to the **AP Authorization profile** field.
   - Enter the name in the **Profile name** field.
   - Select a group from the **AP authorization group** drop-down list.
3. Click **Save**.
4. Click **Pending Changes**.
5. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands create a new authorization profile or edit an existing authorization profile:

```
(host) [md] (config) #ap authorization-profile <profile>
authorization-group <ap-group>
```

Working with ACL and Firewall Policies

Remote APs support the following ACL; unless otherwise noted, you apply these ACLS to user roles:

- Standard ACLs—Permit or deny traffic based on the source IP address of the packet.
- Ethertype ACLs—Filter traffic based on the Ethertype field in the frame header.
- MAC ACLs—Filter traffic on a specific source MAC address or range of MAC addresses.
- Firewall policies (session ACLs)—Identifies specific characteristics about a data packet passing through the Aruba Managed Device and takes some action based on that identification. You apply these ACLs to user roles or uplink ports.

> To configure firewall policies, you must install the PEFNG license.

For more information about ACLs and firewall policies, see ArubaOS 8.6.0.0 Help Center.

Understanding Split Tunneling

The split tunneling feature allows you to optimize traffic flow by directing only corporate traffic back to the Managed Device, while local application traffic remains local. This ensures that local traffic does not incur the overhead of the round trip to the Managed Device, which decreases traffic on the WAN link and minimizes latency for local application traffic. This is useful for sites that have local servers and printers. With split tunneling, a remote user associates with a single SSID, not multiple SSIDs, to access corporate resources (for example, a mail server) and local resources (for example, a local printer). The remote AP examines session ACLs to distinguish between corporate traffic destined for the Managed Device and local traffic.

Figure 1 Sample Split Tunnel Environment

Figure 1 displays corporate traffic which is GRE tunneled to the Managed Device through a trusted tunnel and local traffic is sent through the source NAT and bridged on the wired interface based on the configured user role and session ACL.

Configuring Split Tunneling

The procedure to cconfigure split tunneling requires the following steps. Each step is described in detail later in this chapter.

> The split tunneling feature requires the PEFNG license. If you do not have the PEFNG license on your Managed Device, you must install it before you configure split tunneling. For details on installing licenses, refer to the *Aruba Managed Device Licensing Guide*.

1. Define a session ACL that forwards only corporate traffic to the Managed Device.
   a. Configure a net destination for the corporate subnets.
   b. Create rules to permit DHCP and corporate traffic to the corporate Managed Device.
   c. Apply the session ACL to a user role.
2. (Optional) Configure an ACL that restricts remote AP users from accessing the remote AP local debugging homepage.
3. Configure the remote AP's AAA profile.
   a. Specify the authentication method (**802.1X** or **PSK**) and the default user role for authenticated users. The user role specified in the AAA profile must contain the session ACL defined in the previous step.
   b. (Optional) Use the remote AP's AAA profile to enable RADIUS accounting.
4. Configure the virtual AP profile:
   a. Specify which AP group or AP to which the virtual AP profile applies.
   b. Set the VLAN used for split tunneling. Only one VLAN can be configured for split tunneling; VLAN pooling is not allowed.
   c. When specifying the use of a split tunnel configuration, use "split-tunnel" forward mode.
   d. Create and apply the applicable SSID profile.

   > When creating a new virtual AP profile in the WebUI, you can also configure the SSID at the same time. For information about AP profiles, see AP Configuration Profiles.

5. (Optional) Create a list of network names resolved by corporate DNS servers.

Configuring the Session ACL Allowing Tunneling

First you need to configure a session ACL that “permits” corporate traffic to be forwarded (tunneled) to the Mobility Master, and that routes, or locally bridges, local traffic.

The following procedure describes how to configure the session ACL allowing tunneling:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration** > **Roles and Policies** > **Policies** tab.
2. Click **+** to create a new policy.

The **New Policy** window is displayed.

3. Select **Session** from the **Policy Type** drop-down list.
4. Enter the policy name in the **Policy Name** field.
5. Click **Submit**.
6. To create the first rule:
   a. Click the policy created in the previous steps.
   b. Click **+**in the **Policy > <policy name> Rules** table.

   The **New Rule for <policy name>** window is displayed.
   c. Select **Access control** or **Application** in the **Rule Type**field.
   d. Click **OK**.
7. In the **New Policy > New Forwarding Rule** table, configure the following parameters:
   - **IP version**—Select **IPv4** or **IPv6** from the drop-down list.
   - **Source**—Select **Any** from the drop-down list.
   - **Destination**—Select **Any** from the drop-down list.
   - **Service/app**—Select **Service** from the drop-down list.
   - **Service alias**—Select **svc-dhcp** from the drop-down list.
   - **Action**—Select **Permit** from the drop-down list.
8. Click **Submit**.
9. Click **Pending Changes**.
10. In the **Pending Changes** window, select the check box and click **Deploy changes**.

    The following steps define an alias representing the corporate network. Once defined, you can use the alias for other rules and policies. You can also create multiple destinations the same way.
11. In the **Managed Network** node hierarchy, navigate to the **Configuration** > **Roles and Policies** > **Aliases** tab.
12. Click **+** In the **Network Aliases** pane.
13. In the **Destination** pane, configure the following parameters:
    - **IP version**—Select **IPv4** or **IPv6** from the drop-down list.
    - **Destination name**—Enter a name.
    - **Description**—Enter a description of the destination within 128 characters.
    - **Invert**—Select the check box to specify that the inverse of the network addresses configured are used.
14. Under **Items**, click **+**.

    The **Add New Destination** window is displayed.
15. Configure the following parameters:
    - **Rule Type**—Select **Network** from the drop-down list.
    - **IP address**—Enter the public IP address of the managed device.
    - **Network mask**—Enter the network mask or range.

Configuring an ACL to Restrict Local Debug Homepage Access

A user in split or bridge role using a Remote AP can log on to the local debug (LD) homepage (for example, (http://rapconsole.arubanetworks.com) and perform a reboot or reset operations. The LD homepage provides various information about the Remote AP and also has a button to reboot the Remote AP. You can now restrict a Remote AP user from resetting or rebooting a Remote AP by using the **localip** keyword in the in the user role ACL.

> You will require the PEFNG license to use this feature. For complete information on the centralized licensing requirements, refer to the *Aruba Mobility Master Licensing Guide*.

Any user associated to that role can be allowed or denied access to the LD homepage. You can use the `localip` keyword in the ACL rule to identify the local IP address on the Remote AP. The `localip` keyword identifies the set of all local IP addresses on the system to which the ACL is applied. The existing keywords Managed Device and `mswitch` indicate only the primary IP address on the Managed Device.

> This release of ArubaOS provides localip keyword support only for Remote AP and not for Managed Device.

The following procedure describes how to configure an ACL to restrict local debug homepage access:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration** > **Roles and Policies** > **Policies** tab.
2. Click **+** to create a new policy.
3. Enter the policy name in the **Policy Name** field.
4. From the **Policy Type** drop-down list, select **Session**.
5. Click **Submit**.
6. To create the first rule:
   a. Select the policy created.
   b. Click **+**in the **Policies** > **<policy name>** table .
   c. Select the **Rule Type** in the **New Rule for <policy name>** dialog box.
   d. Click **OK**.
7. Enter the following details in the **Roles** > **<policy name>** > **<rule name>** table:
   e. From the **IP version** drop-down list, select **IPv4** or **IPv6**.
   f. Select **Any** from the **Source** drop-down list.
   g. Select **Any** from the **Destination** drop-down list.
   h. Select **Service** from the **Service/app** drop-down list.
   i. Select **svc-dhcp** from the **Service alias** drop-down list.
   j. Select **Permit** from the **Action** drop-down list.
   k. Click **Submit**.
8. Click **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands configure an ACL to restrict local debug homepage access:

Use the `localip` keyword in the user role ACL.

All users have an ACL entry of type `any any deny` by default. This rule restricts access to all users. When the ACL is configured for a user role, if a `user any permit` ACL rule is configured, add a deny ACL before that for `localip` for restricting the user from accessing the LD homepage.

Example:

```
(host) [md] (config) #ip access-list session logon-control
```

Configuring the AAA Profile for Tunneling

After you configure the session ACL, you define the AAA profile used for split tunneling. When defining the AAA parameters, specify the previously configured user role that contains the session ACL used for split tunneling.

If you enable RADIUS accounting in the AAA profile, the Managed Device sends a RADIUS accounting start record to the RADIUS server when a user associates with the remote AP, and sends a stop record when the user logs out or is deleted from the user database. If you enable interim accounting, the Managed Device sends updates at regular intervals. Each interim record includes cumulative user statistics, including received bytes and packets counters. For more information on RADIUS accounting, see

The following procedure describes how to configure the AAA profile for tunneling:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** tab.
2. Select **Wireless LAN >AAA** under **All Profiles**.
3. Click **+** in **AAA Profile** and enter the following details:
   a. Enter the **Profile name**.
   b. For **Initial role**, select the appropriate role (for example, logon) from the drop-down list.
   c. For **802.1X Authentication Default Role**, select the appropriate role (for example, “default”) from the drop-down list.
   d. Click **Save**.
   e. Under the AAA profile that you created, locate **802.1X Authentication Server Group**, and select the Server Group to be used (for example “default”) from the drop-down list.
   f. Click **Save**.
4. (Optional) To enable RADIUS accounting:
   a. Select the AAA profile from the profile list to display the list of authentication and accounting profiles associated with the AAA profile.
   b. Select the **Radius Accounting Server Group** profile associated with the AAA profile. Click the **Server Group** drop-down list to select a RADIUS server group. (For more information on configuring a RADIUS server or server group, see Configuring Authentication Servers.)
5. Click **Save**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands configures the AAA profile for tunneling:

```
(host) [md] (config) #aaa profile <name>
  authentication-dot1x <dot1x-profile>
  dot1x-default-role <role>
  dot1x-server-group <group>
  radius-accounting <group>
  radius-interim-accounting
```

Configuring the Virtual AP Profile

The following procedure describes how to configure the virtual AP profile:

1. In the **Managed Network** node hierarchy, navigate to **Configuration > System > Profiles** tab.
2. Select **Wireless LAN > Virtual AP** under **All Profiles.**
3. To create a new virtual AP profile, click **+** in **Virtual AP profile**. Enter the name for the virtual AP profile, and click **Save**.

   Whenever you create a new virtual AP profile in the WebUI, the profile automatically contains the default SSID profile with the default ESSID. You must configure a new ESSID and SSID profile for the virtual AP profile before you apply the profile.

   a. Select **Wireless LAN > SSID** under **All Profiles.**
   b. Click **+** in **SSID Profile** and enter the following details:
   - Enter the name of the profile in the **Profile name** field.
   - To enable SSID, select the **SSID enable** check box.
   - Select the appropriate check box under the **Encryption** field, to choose the network authentication and encryption method.
   c. Click **Save**.
4. Select the new virtual AP name listed under **Wireless LAN > Virtual AP**, to view the configuration parameters.
5. In the **General** accordion under **Virtual AP profile: name**, execute the following:
   a. Ensure that the **Virtual AP enable** is selected.
   b. Enter the VLAN ID to be used for the Virtual AP profile in the **VLAN** field.
   c. Select **split-tunnel** from the **Forward mode** drop-down list.
   d. Click **Save**.
6. Under **All Profiles**, select **AP > AP system** profile.
7. Select the AP system profile that you want to edit.
   a. Under the **LMS Settings** accordion, enter the LMS IP address in the **LMS IP** field.
   b. Under the **Remote AP** accordion, click + under **Remote-AP DHCP DNS Server** and enter the Remote -AP DHCP DNS server in the **Remote-AP DHCP DNS Server** field.
   c. Click **OK**.
   d. Click **Save**.
8. Click **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands configure the virtual AP profile:

```
(host) [md] (config) #wlan ssid-profile <profile>
essid <name>
opmode <method>

(host) [md] (config) #wlan virtual-ap <profile>
ssid-profile <name>
forward-mode <mode>
(host) [md] (config) # vlan <vlan id>
aaa-profile <profile>

(host) [md] (config) #ap-group <name>
virtual-ap <profile>
```

or

Defining Corporate DNS Servers

Clients send DNS requests to the corporate DNS server address that it learned from DHCP. If configured for split tunneling, corporate domains and traffic destined for corporate use the corporate DNS server. For non-corporate domains and local traffic, other DNS servers can be used.

The following procedure describes how to define corporate DNS servers:

1. In the **Managed Network** node hierarchy, navigate to **Configuration > System > Profiles** tab.
2. Select **AP > AP system** under **All Profiles**.
3. Select an AP System Profile.
4. Click **+** under **Corporate DNS Domain** table and enter the **Corporate DNS Domain**.
5. Click **OK**. The DNS name appears in **Corporate DNS Domain** table. You can add multiple names the same way.
6. Click **Save**.
7. Click **Pending Changes**.
8. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands define corporate DNS servers:

```
(host) [md] (config) #ap system-profile <profile>
dns-domain <domain name>
```

Understanding Bridge

The bridge feature allows you to route the traffic flow only to the internet and not to the corporate network. Only the 802.1X authentication request is sent to the corporate network. This feature is useful for guest users.

> ArubaOS does not support Wired 802.1X authentication in bridge mode for a s. 802.1X authentication is supported only in tunnel and split modes.

Figure 1 Sample Bridge Environment

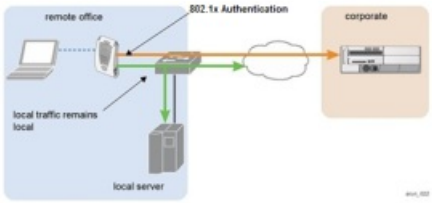


Figure 1 displays the local traffic being routed to the internet and the 802.1X authentication request sent to the corporate network.

Configuring Bridge

The following procedure describes how to configure a bridge. Each step is described in detail later in this chapter.

> The bridge feature requires the PEFNG license. If you do not have the PEFNG license on your managed device, you must install it before you configure bridge. For details on installing licenses, refer to the *Aruba Mobility Master Licensing Guide.*

1. Define a session ACL that routes the traffic.
   a. Create rules to permit DHCP and local data traffic.
   b. Apply the session ACL to a user role. For information about user roles and policies, see Roles and Policies.
2. Configure the remote AP's AAA profile. Specify the authentication method (**802.1X** or **PSK**) and the default user role for authenticated users. The user role specified in the AAA profile must contain the session ACL defined in the previous step. Optionally, use the remote AP's AAA profile to enable RADIUS accounting.
3. Configure the virtual AP profile:
   a. Specify the AP group or ap-name to which the virtual AP profile applies.
   b. Set the VLAN in the virtual AP.
   c. When specifying the use of a bridge configuration, use bridge forward mode.
   d. Create and apply the applicable SSID profile. Optionally under AP system profile, configure the Remote AP DHCP pool. Remote AP DHCP VLAN must be same as virtual AP's VLAN. If the client needs to obtain from the Remote AP DHCP Server.

> When creating a new virtual AP profile In the WebUI, you can simultaneously configure the SSID. For information about AP profiles, see AP Configuration Profiles.

Configuring the Session ACL

First you need to configure a session ACL that “permits” corporate traffic to be forwarded to the managed device and that routes, or locally bridges, local traffic.

The following procedure describes how to configure session ACL:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Roles and Policies > Policies** tab.
2. Click **+** to create a new policy.
3. Enter the name in the **Policy name** field.
4. Select **Session** from the **Policy type** drop-down list.
5. Click **Submit**.
6. Select the policy created and click **+** under **Policies<policy name>** table.
7. Select **Access Control** option in the **Rule Type** field.
8. Click **OK**.
9. To complete creating the rule:
   a. Select **IPv4** or **IPv6** from the **IP version** drop-down list.
   b. Select **Any** from the **Source** drop-down list.
   c. Select **Any** from the **Destination** drop-down list.
   d. Select **Service** from the **Service/app** drop-down list.
   e. Select **svc-dhcp** from the **Service alias** drop-down list.
   f. Select **Permit** for IPv4 or **Captive** for IPv6 from the **Action** drop-down list.
   g. Click **Submit**.
10. To create a new forwarding rule:
    a. Select policy created and click **+** in the **Policies <policy name>** table.
    b. Select **Access Control** option in the **Rule Type** field.
    c. Click **OK**.
    d. Select **IPv4** or **IPv6** from the **IP version** drop-down list.
    e. Select **any** from the **Source** drop-down list.
    f. Select **alias** from the **Destination** drop-down list.
    g. Click **+** in the **Destinationalias** drop-down list.
    h. In the **Add New Destination** window, click **+** in the **Rule** table.
    i. Select **Network** from the **Rule type** drop-down list.
    j. Enter the public IP address of the managed device in the **IP address** field.
    k. Enter the netmask or range in the **Network mask** field.
    l. Click **OK**. The new alias appears in the **Destination alias** drop-down list.
    m. Click **Submit**.
11. Navigate to the **Configuration** >**Roles and Policies** >**Roles** tab.

    Roles can be created only in the managed device.

    a. Click **+** to create a new role.
    b. Enter the role name in the **Name** field.
    c. Click **Submit**.

Configuring the AAA Profile for Bridge

After you configure the session ACL, define the AAA profile used for bridge. When defining the AAA parameters, specify the previously configured user role that contains the session ACL used for bridge.

If you enable RADIUS accounting in the AAA profile, the Mobility Master sends a RADIUS accounting start record to the RADIUS server when a user associates with the remote AP, and sends a stop record when the user logs out or is deleted from the user database. If you enable interim accounting, the Mobility Master sends updates at regular intervals. Each interim record includes cumulative user statistics, including received bytes and packets counters. For more information on RADIUS accounting, see .

The following procedure describes how to configure the AAA profile for bridge:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** tab.
2. Select **Wireless LAN > AAA** under **All Profiles**.
3. Click **+** in **AAA Profile**.
4. Enter the **Profile name**.
5. Select the appropriate role (for example, “logon”) from the **Initial role** drop-down list.
6. Select the user role you previously configured for split tunneling or bridge from the **802.1X Authentication Default Role** drop-down list.
7. Click **Save**.
8. Select the AAA profile created and locate the **802.1X Authentication Server Group**, and select the **Server Group** to be used (for example “default”) from the drop-down list.
9. Click **Save**.
10. Click **Pending Changes**.
11. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands configures the AAA profile for bridge:

```
(host) [mynode] (config) #aaa profile <name>
(host) [mynode] (config) #authentication-dot1x <dot1x-profile>
(host) [mynode] (config) #dot1x-default-role <role>
(host) [mynode] (config) #dot1x-server-group <group>
(host) [mynode] (config) #radius-accounting <group>
(host) [mynode] (config) #radius-interim-accounting
```

Configuring the Virtual AP Profile

The following procedure describes how to configure the virtual AP profile:

1. In the **Managed Network** node hierarchy, navigate to **Configuration > System > Profiles** tab.
2. Select **Wireless LAN > Virtual AP** under **All Profiles.**
3. To create a new virtual AP profile, click **+** in **Virtual AP profile**. Enter the name for the virtual AP profile, and click **Save**.

   > Whenever you create a new virtual AP profile in the WebUI, the profile automatically contains the default SSID profile with the default ESSID. You must configure a new ESSID and SSID profile for the virtual AP profile before you apply the profile.

   a. Select **Wireless LAN > SSID** under **All Profiles.**
   b. Click **+** in **SSID Profile** and enter the following details:
   - Enter the name of the profile in the **Profile name** field.
   - To enable SSID, select the **SSID enable** check box.
   - Select the appropriate check box under the **Encryption** field, to choose the network authentication and encryption method.
   c. Click **Save**.
4. Select the new virtual AP name listed under **Wireless LAN > Virtual AP**, to view the configuration parameters.
5. In the **General** accordion under **Virtual AP profile: name**, execute the following:
   a. Ensure that the **Virtual AP enable** is selected.
   b. Enter the VLAN ID to be used for the Virtual AP profile in the **VLAN** field.
   c. Select **split-tunnel** from the **Forward mode** drop-down list.
   d. Click **Save**.
6. Under **All Profiles**, select **AP > AP system** profile.
7. Select the AP system profile that you want to edit.
   a. Under the **LMS Settings** accordion, enter the LMS IP address in the **LMS IP** field.
   b. Under the **Remote AP** accordion, click + under **Remote-AP DHCP DNS Server** and enter the Remote -AP DHCP DNS server in the **Remote-AP DHCP DNS Server** field.
   c. Click **OK**.
   d. Click **Save**.
8. Click **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands configure the virtual AP profile:

```
(host) [md] (config) #wlan ssid-profile <profile>
essid <name>
opmode <method>

(host) [md] (config) #wlan virtual-ap <profile>
ssid-profile <name>
forward-mode <mode>
(host) [md] (config) # vlan <vlan id>
aaa-profile <profile>

(host) [md] (config) #ap-group <name>
virtual-ap <profile>
```

or

Provisioning Wi-Fi Multimedia

WMM is a WFA specification based on the IEEE 802.11e wireless QoS standard. WMM works with 802.11a, b, g, and n physical layer standards. The IEEE 802.11e standard also defines the mapping between WMM access categories and DSCP tags. Remote APs support WMM.

WMM supports four access categories: voice, video, best effort, and background. You apply and configure WMM in the SSID profile.

When planning your configuration, make sure that immediate switches or routers do not have conflicting 802.1p or DSCP configurations or mappings. If this happens, your traffic may not be prioritized correctly.

Reserving Uplink Bandwidth

You can reserve and prioritize uplink bandwidth traffic to provide higher QoS for specific applications, traffic, or ports. This is done by applying bandwidth reservation on existing session ACLs. Typically, the bandwidth reservation is applied for uplink voice traffic.

Note the following before you configure bandwidth reservation:

- You must know the total bandwidth available.
- Bandwidth reservation is applicable only on session ACLs.
- Bandwidth reservation on voice traffic ACLs receives higher priority over other reserved traffic.
- You can configure up to three unique priority for bandwidth reservation.
- The bandwidth reservation must be specified in absolute value (Kbps).
- Priorities for bandwidth reservation are optional, and bandwidth reservations without priorities are treated equal.

Understanding Bandwidth Reservation for Uplink Voice Traffic

Voice ACLs are applicable on the voice signaling traffic used to establish a voice call through a firewall. When a voice ACL is executed, a dynamic session is introduced to allow voice traffic through the firewall. This prevents the re-use of voice ACLs for bandwidth reservation. However, you can create bandwidth reservation rules that can be applied on voice signaling traffic and ports used for voice data traffic. This mechanism filters traffic as per the security requirements.

Configuring Bandwidth Reservation

You can configure bandwidth reservation ACLs using the WebUI or the CLI.

The following procedure describes how to configure bandwidth reservation:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** tab.
2. Click **AP** and select **AP system**.
3. Click **Remote AP** accordion. You can create a new AP system profile to configure bandwidth reservation or edit an existing AP system profile. In **Remote-AP bw reservation 1**, **Remote-AP bw reservation 2** and **Remote-AP bw reservation 3** fields, specify bandwidth reservation values.
4. Click **Save**.
5. Click **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy changes**.

The following CLI commands configure bandwidth reservation

```
(host) [mynode] (config)#ap system-profile remotebw
(host) [mynode] (AP system profile "remotebw") #rap-bw-total 1024
(host) [mynode] (AP system profile "remotebw") #rap-bw-resv-1 acl voice 128 priority 1
```

To view bandwidth reservations:

```
(host) [mynode] #show datapath rap-bw-resv ap-name remote-ap-1
```

Provisioning 4G USB Modems on Remote Access Points

ArubaOS provides support for 4G networks by allowing you to provision 4G USB modems on the Remote AP. You can also provision the Remote AP to support both 4G and 3G USB modems. This enables the Remote AP to choose the available network automatically. 4G takes precedence over 3G when the Remote AP tries to auto select the network. You can also configure the Remote AP to work exclusively on a 3G or 4G network. It is recommended that you provision the USB modems for the Remote AP based on your network requirements.

4G USB Modem Provisioning Best Practices and Exceptions

- Remote AP does not support dynamic plug-and-play for the 4G USB modems. You must provision a Remote AP with the 4G USB parameters on the managed device manually based on its type and family (4G-WiMAX or 4G-LTE).
- When a Remote AP connects to a 4G network, it appears as a Remote AP (R) and Cellular (C) on the managed device.
- For a 3G or 4G network switch, using the UML290 modem with the firmware version L0290VWB522F.242 or later is recommended. Using a lower version of the firmware auto-selects the network mode based on the network availability. The latest version allows the Remote AP to lock the modem in a particular network mode (for example, 3G only).

> The 4G-WiMAX family of modems do not support the 3G-4G network switch-over functionality.

A new method of provisioning multimode USB modems (such as a Verizon UML290, Verizon MC551L, AT&T 313u, Huawei K5150, AT &T ZTE MF861 and Inseego U730L) for a Remote AP has been introduced. These changes simplify modem provisioning for both 3G and 4G networks. Earlier the modem configuration procedure required that you define a driver for a 3G modem in the USB modem field under the AP provisioning profile, or define a driver for a 4G modem in the 4G USB type field. You can now configure drivers for both a 3G or a 4G modem using the USB field, and the 4G USB Type field is deprecated. The managed device can auto configure the USB modem when it is plugged into the associated Remote AP. Since most 4G-LTE modem support dynamic network-switching between 4G and 3G, by default (for zero touch) Remote AP is configured in 3G/4G mode. In such cases, the Remote AP selects the best available cellular network coverage in that specific region.

Provisioning Remote AP for USB Modems

To enable 3G or 4G network support, you must provision the Remote AP with the USB parameters on the managed device. You can use the WebUI or CLI to provision the USB parameters.

The following procedure describes how to provision Remote AP for USB modems:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Access Points > Remote APs** tab.
2. Select the remote AP and click **Provision**.
3. Select **Uplink** tab. This tab is displayed only when a Remote AP is selected.
4. Select a profile from the **USB Profile** drop-down list. This field is displayed only when the device is USB enabled.
5. Click **Submit**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy changes**.

Table 1: *Cellular Network Preference Parameters*

Parameter	Description
auto (default)	In this mode, the modem firmware will control the cellular network service selection; so the cellular network service failover and fallback is not interrupted by the Remote AP.
3g_only	Locks the modem to operate only in 3G.
4g_only	Locks the modem to operate only in 4G.
advanced	The Remote AP controls the cellular network service selection based on an RSSI threshold-based approach. ▪ Initially the modem is set to the default auto mode. This allows the modem firmware to select the available network. ▪ The Remote AP determines the RSSI value for the available network type (for example 4G), checks whether the RSSI is within required range, and if so, connects to that network. ▪ If the RSSI for the modem's selected network is not within the required range, the Remote AP will then check the RSSI limit of an alternate network (for example, 3G), and reconnect to that alternate network. The Remote AP will repeat the above steps each time it tries to connect using a 4G multimode modem in this mode.

The following CLI commands provision Remote AP for USB modems:

To enable 4G-exclusive network support on the Remote AP, execute the following commands:

```
(host) [md] (config) #ap provisioning-profile <profile-name>
(host) [md] (Provisioning profile "<profile-name>") usb-type <USB modem type>
(host) [md] (Provisioning profile "<profile-name>") #usb-type none
(host) [md] (Provisioning profile "<profile-name>") #cellular_nw_preference 4g_only
```

To enable 3G-exclusive network support on the Remote AP, execute the following commands:

```
(host) [md] (config) #ap provisioning-profile <profile-name>
(host) [md] (Provisioning profile "<profile-name>") usb-type <USB modem type>
(host) [md] (Provisioning profile "<profile-name>") #usb-type none
(host) [md] (Provisioning profile "<profile-name>") #cellular_nw_preference 3g_only
```

To enable 3G or 4G network switch support, execute the following commands:

```
(host) [md] (config) #ap provisioning-profile <profile-name>
(host) [md] (Provisioning profile "<profile-name>") usb-type <USB modem type>
```

Remote AP 3G or 4G Backhaul Link Quality Monitoring

The Remote AP is enhanced to support link monitoring on 2G, 3G, and 4G modems to provide information about the state of the USB modem and cellular network.

The USB modem has the following four states:

- **Active** - The USB modem is used as the primary path for connecting VPN to the managed device
- **Standby** or **Backup** - The network is available but the USB modem is not used for connecting VPN to the managed device
- **Error** - The USB modem is available but the modem is faulty
- **Not Plugged** - The USB modem is unavailable

To view the USB modem details on the Remote AP, execute the following command:

```
(host) [md] #show ap debug usb ap-name <ap-name>
```

Provisioning Remote AP at Home

The following section provides information on provisioning your Remote Ap at home using a static IP address, PPPoE connection, or USB modem.

Prerequisites

Follow the steps below to acquire a static IP address before provisioning the Remote AP at home:

1. Connect the Remote AP at the site of deployment and ensure that it has connectivity to the Internet to reach the managed device.
2. Connect a laptop to Port 1 of the Remote AP to get an IP address from the Remote AP's internal DHCP pool.

Provisioning Remote AP Using ZTP

You provision the Remote AP using provisioning wizard:

1. Navigate to the Remote AP configuration URL: http://rapconsole.arubanetworks.com.
2. Enter the IP address or hostname of the managed device.
3. Click the **Show Advanced Settings** link, shown in Figure 1.

Figure 1 *Show Advanced Settings*

4. In the **Advanced Settings** wizard, you can select one of the following:
   a. **Static IP**—Select this tab to provision your Remote AP using a static IP address.
   b. **PPPoE**—Select this tab to provision your Remote AP on a PPPoE connection.
   c. **USB**—Select this tab to provision your Remote AP using 3G/EVDO USB modem.

Provisioning the Remote AP using a Static IP Address

Select the **Static IP** tab and enter the required details. See Table 1 for information on parameters.

Figure 2 *Provision Remote AP using Static IP*

Table 1: *Provision using Static IP*

Parameter	Description
IP Address	Enter the static IP address that you want to configure for your remote access point.
Netmask	Enter the network mask.
Gateway	Enter the default gateway IP address of your network.
Primary DNS	Enter the IP address of your primary DNS server. This is an optional parameter.
Domain	Enter your domain name. This is an optional parameter.

Click **Save** after you have entered all the details.

Converting an Instant AP to Remote AP or Campus AP

For Instant AP to Remote AP or Campus AP conversion, the virtual controller sends the convert command to all the other Instant APs. The virtual controller along with the other slave Instant APs then set up a VPN tunnel to the remote controller, and download the firmware by FTP. The virtual controller uses IPsec to communicate to the controller over the Internet.

> A mesh point cannot be converted to a Remote AP because mesh does not support VPN connection.

Important

- Converting an AP to Instant AP is only supported on UAP models.
- Converting non-UAP models is not supported on the Web UI and can only be done through CLI.

Converting Instant AP to Remote AP

To convert an Instant AP to Remote AP, follow the instructions below:

1. Navigate to the **Maintenance** tab in the top right corner of the Instant UI.
2. Click the **Convert** tab.
3. Select **Remote APs managed by a Mobility Controller** from the drop-down list.
4. Enter the hostname FQDN or the IP address of the managed device in the **Hostname or IP Address of Mobility Controller** text box. This information is provided by your network administrator.

> Ensure the controller IP Address is reachable by the IAPs.

5. Click **Convert Now** to complete the conversion.
6. The Instant AP reboots and begins operating in Remote AP mode.
7. After conversion, the Instant AP is managed by the Aruba controller which has been specified in the Instant UI.

> In order for the Remote AP conversion to work, ensure that you configure the Instant AP in the Remote AP white-list and enable the FTP service on the controller.

> If the VPN setup fails and an error message pops up, please click OK, copy the error logs and share them with your Aruba support engineer.

Converting an Instant AP to Campus AP

To convert an Instant AP to a Campus AP, do the following:

1. Navigate to the **Maintenance** tab in the top right corner of the Instant UI.
2. Click the **Convert** tab.
3. Select **Campus APs managed by a Mobility Controller** from the drop-down list.
4. Enter the hostname FQDN or the IP address of the controller in the **Hostname or IP Address of Mobility Controller** text box. This is provided by your network administrator.

> Ensure that the controller IP Address is reachable by the APs.

5. Click **Convert Now** to complete the conversion.

Enabling Bandwidth Contract Support for Remote APs

Bandwidth Contract support on Remote APs is achieved by extending the Bandwidth Contract support on split-tunnel and bridge modes. You can apply Bandwidth Contract for a Remote AP on a per-user or per-role basis. Bandwidth Contract is applied on a per-role basis by default. This implies that all the users belonging to the same role will share the bandwidth pool. When Bandwidth Contract configured on the managed device is attached to a user-role, it automatically gets pushed to the Remote APs terminating on it.

The following show commands have been enhanced to retrieve the Bandwidth Contract information from the Remote AP:

```
(host) [md] #show datapath user ap-name <ap-name>
(host) [md] #show datapath bwm ap-name <ap-name>
```

Configuring Bandwidth Contracts for Remote AP

The following examples illustrate how to configure, apply, and verify the Bandwidth Contracts on the RAPs.

Defining Bandwidth Contracts

Use the following command to define a 256 Kbps contract:

```
(host) [md] (config) #aaa bandwidth-contract 256k kbits 256
```

Use the following command to define a 512 Kbps contract

```
(host) [md] (config) #aaa bandwidth-contract 512k kbits 512
```

Applying Contracts

You can apply the contract on a per-role or per-user basis.

Applying Contracts Per-Role

Use the following commands to apply the contracts on a per-role basis for upstream and downstream:

For upstream contract of 512 Kbps:

```
(host) [md] (config) #user-role authenticated bw-contract 512k upstream
```

For downstream contract of 256 Kbps:

```
(host) [md] (config) #user-role authenticated bw-contract 256k downstream
```

Applying Contracts Per-User

Use the following commands to apply the contracts on a per-user basis for upstream and downstream:

For upstream contract of 512 Kbps:

```
(host) [md] (config) #user-role authenticated bw-contract 512k per-user upstream
```

For downstream contract of 256 Kbps:

```
(host) [md] (config) #user-role authenticated bw-contract 256k per-user downstream
```

Verifying Contracts on AP

The following example displays the bandwidth contracts on an AP for per-role configuration:

```
(host) [md] #show datapath bwm ap-name rap5-2
Datapath Bandwidth Management Table Entries
-------------------------------------------
Contract Types :
0 - CP Dos 1 - Configured contracts 2 - Internal contracts
-----------------------------------------------
Flags: Q - No drop, P - No shape(Only Policed),
T - Auto tuned
---  --------  ---------  ----------  -----------  -----------------
Cont                      Avail   Queued/Pkts
Type  Id   Bits/sec  Policed    Bytes    Bytes      Flags
---- ---- --------- ---------- ------- ------------ -----
1    1      512000          0   16000       0/0    P
1    2      256000          0    8000       0/0    P
```

The following example displays the bandwidth contracts on AP for per-user configuration (contract IDs 3 and 4 are per-user contracts):

```
(host) [md] #show datapath bwm ap-name rap5-2
Datapath Bandwidth Management Table Entries
-------------------------------------------
Contract Types :
0 - CP Dos 1 - Configured contracts 2 - Internal contracts
-----------------------------------------------
Flags: Q - No drop, P - No shape(Only Policed),
T - Auto tuned
---  --------  ---------  ----------  -----------  -----------------
Cont                      Avail   Queued/Pkts
Type  Id   Bits/sec  Policed    Bytes    Bytes      Flags
---- ---- --------- ---------- ------- ------------ -----
1    1       512000        300   16000       0/0    P
1    2       256000        277    8000       0/0    P
1    3       512000          0   16000       0/0    P
1    4       256000          0    8000       0/0    P
```

Verifying Contracts Applied to Users

You can verify if the contracts are applied to the user after the user connects to the AP using CLI.

The following is a sample output for a per-role configuration:

```
(host) [md] #show datapath user ap-name rap5-2
Datapath User Table Entries
---------------------------
Flags: P - Permanent, W - WEP, T- TKIP, A - AESCCM, G - AESGCM, V - ProxyArp to/for MN(Visitor),
N - VPN, L - local, Y - Any IP user, R - Routed user, M - Media Capable,
S - Src NAT with VLAN IP, E - L2 Enforced, F - IPIP Force Delete, O - VOIP user
FM(Forward Mode): S - Split, B - Bridge, N - N/A
IP              MAC           ACLs    Contract   Location  Age  Sessions   Flags   Vlan   FM
--------------  ------------  ------  ---------  --------  ---  ---------  -----   ----   --
10.15.72.50     00:0B:86:61:12:AC  2703/0     0/0    0         16       1/65535     P      0   N
10.15.72.253    00:18:8B:A9:A8:DF    52/0     1/2    0         1        0/65535             1   S
192.168.11.1    00:0B:86:66:03:3F  2700/0     0/0    0         20024    0/65535     P    177   N
10.15.196.249   00:0B:86:66:03:3F  2700/0     0/0    0         3        1/65535     P      1   N
```

The following is a sample output for a per-user configuration:

```
(host) [mynode] #show datapath user ap-name rap5-2
Datapath User Table Entries
---------------------------
Flags: P - Permanent, W - WEP, T- TKIP, A - AESCCM, G - AESGCM, V - ProxyArp to/for MN(Visitor),
N - VPN, L - local, Y - Any IP user, R - Routed user, M - Media Capable,
S - Src NAT with VLAN IP, E - L2 Enforced, F - IPIP Force Delete, O - VOIP user
FM(Forward Mode): S - Split, B - Bridge, N - N/A
IP              MAC           ACLs    Contract   Location  Age  Sessions   Flags   Vlan   FM
--------------  ------------  ------  ---------  --------  ---  ---------  -----   ----   --
10.15.72.50     00:0B:86:61:12:AC  2703/0     0/0    0         11       0/65535  P          0    N
10.15.72.253    00:18:8B:A9:A8:DF    52/0     3/4    0         46       0/65535             1    S
192.168.11.1    00:0B:86:66:03:3F  2700/0     0/0    0         20883    0/65535  P        177    N
10.15.196.249   00:0B:86:66:03:3F  2700/0     0/0    0         15       1/65535  P          1    N
```

Verifying Bandwidth Contracts During Data Transfer

You can verify the Bandwidth Contracts that are in use during data transfer using CLI.

The following is a sample output for a per-role configuration:

```
(host) [md] #show datapath session ap-name rap5-2 table 10.15.72.99
Datapath Session Table Entries
------------------------------
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
Q - Real-Time Quality analysis
I - Deep inspect, U - Locally destined
E - Media Deep Inspect, G - media signal
RAP Flags: 1 - Class 1, 2 - Class 2, 3 - Class 3
Source IP     Destination IP  Prot SPort DPort  Cntr Prio ToS Age Destination TAge Flags
--------------  --------------  ---- ----- -----  ---- ---- --- --- ------------ ---- -----
10.15.72.253    10.15.72.99     6    5001  36092  1/1     0 0   0   dev12        6
10.15.72.253    10.15.72.99     6    3488  5001   1/1     0 0   0   dev5         6    C
10.15.72.99     10.15.72.253    6    5001  3488   1/2     0 0   0   dev5         6
10.15.72.99     10.15.72.253    6    36092 5001   1/2     0 0   0   dev12        6    C
```

The following is a sample output for a per-user configuration:

```
(host) [md] #show datapath session ap-name rap5-2 table 10.15.72.99

Datapath Session Table Entries
------------------------------
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
Q - Real-Time Quality analysis
I - Deep inspect, U - Locally destined
E - Media Deep Inspect, G - media signal
RAP Flags: 1 - Class 1, 2 - Class 2, 3 - Class 3
Source IP     Destination IP  Prot SPort DPort  Cntr Prio ToS Age Destination TAge Flags
--------------  --------------  ---- ----- -----  ---- ---- --- --- ------------ ---- -----
10.15.72.253    10.15.72.99     6    3489  5001   1/3     0 0   0   dev5         37   FC
10.15.72.99     10.15.72.253    6    5001  3489   1/4     0 0   0   dev5         37   F
10.15.72.99     10.15.72.253    6    36096 5001   1/4     0 0   0   dev12        37   C
10.15.72.253    10.15.72.99     6    5001  36096  1/3     0 0   0   dev12        37
```

Control Plane Security

ArubaOS supports secure IPsec communications between a managed device and campus APs or remote APs using public-key self-signed certificates created by each Mobility Master. The managed device certifies its APs by issuing them certificates.

If the Mobility Master has any associated managed device, the Mobility Master sends a certificate to each managed device, which in turn sends certificates to their own associated APs. If a managed device is unable to contact the Mobility Master to obtain it's own certificate, it will not be able to certify the APs, and those APs can not communicate with their managed device until Mobility Master-managed device communication has been re-established. You create an initial CPsec configuration when you first configure the managed device using the initial setup wizard. The ArubaOS initial setup wizard enables CPsec by default, so it is very important that the managed device be able to communicate with the Mobility Master when it is first provisioned.

Some AP model types have factory-installed digital certificates. These AP models use their factory-installed certificates for IPsec, and do not need a certificate from the managed device. Once a campus AP or remote AP is certified, either through a factory-installed certificate or a certificate from the managed device, the AP can failover between managed devices and still stay connected to the secure network, because each AP has the same Mobility Master as a common trust anchor.

The managed device maintains two separate AP whitelists; one for campus APs and one for remote APs. These whitelists contain records of all campus APs or remote APs connected to the network. You can use a campus AP or remote AP whitelist at any time to add a new valid campus AP or remote AP to the secure network, or revoke network access to any suspected rogue or unauthorized APs.

When the managed device sends a certificate to the AP, that AP must reboot before it can connect to the managed device over a secure channel. If you are enabling CPsec for the first time on a large network, you may experience several minutes of interrupted connectivity while each AP receives its certificate and establishes its secure connection.

Topics in this section include:

Control Plane Security Overview

Controllers using CPsec send certificates to APs that you have identified as valid APs on the network. If you want closer control over each AP that is certified, you can manually add individual campus and remote APs to the secure network by adding each AP's information to the whitelists when you first run the initial setup wizard. If you are confident that all APs currently on your network are valid APs, then you can use the initial setup wizard to configure automatic certificate provisioning to send certificates from the controller to each campus or remote AP, or to all campus and remote APs within specific ranges of IP addresses.

The default automatic certificate provisioning setting requires that you manually enter each campus AP's information into the campus AP whitelist, and each remote AP's information into the remote AP whitelist. If you change the default automatic certificate provisioning values to let the controller send certificates to all APs on the network, all valid APs will receive certificate, but this also increases the chance that you will certify a rogue or unwanted AP. If you configure the controller to send certificates to only those APs within a range of IP addresses, there is a smaller chance that a rogue AP receives a certificate, but any valid AP with an IP address outside the specified address ranges will not receive a certificate, and cannot communicate with the controller (except to obtain a certificate). Consider both options carefully before you complete the CPsec portion of the initial setup wizard. If your controller has a publicly accessible interface, you should identify the APs on the network by the IP address range. This prevents the controller from sending certificates to external or rogue campus APs that may attempt to access your controller through that publicly accessible interface.

Configuring Control Plane Security

When you initially deploy the controller, you create your initial CPsec configuration using the initial setup wizard. These settings can be changed at any time using the WebUI or CLI. The following procedure describes how to create the initial CPsec configuration.

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > CPSec** tab.
2. Select the **Control Plane Security** accordion.
3. Click the **Enable CPSEC** toggle switch to enable this setting.
4. Click **Submit**.
5. Click **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy changes**.

To enable auto cert provisioning:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > CPSEC** tab.
2. Select the **Control Plane Security** accordion.
3. Click the **Enable CPSEC** toggle switch to enable this setting.
4. Click the **Enable auto cert provisioning** toggle switch to allow AP's from specified ranges.
5. Click the **Only accept APs from specified ranges** toggle switch to enable this setting.
   a. Click **+** in **Address ranges for Auto Cert Provisioning** table. The **New Address Range** window is displayed.
   b. Enter the IPv4 or IPv6 address in the **Start address IPv4 or v6** and **End address IPv4 or v6** fields.
   c. Click **OK**.
6. Click **Submit**.
7. Click **Pending Changes**.
8. In the **Pending Changes** window, select the check box and click **Deploy changes.**

The Mobility Master generates its self-signed certificate and begins distributing certificates to campus APs and any managed devices on the network over a clear channel. After all APs have received a certificate and have connected to the network using a secure channel, access the **Control Plane Security** window and turn off auto certificate provisioning if that feature was enabled. This prevents the controller from issuing a certificate to any rogue APs that may appear on your network at a later time.

Table 1: *Control Plane Security Parameter*

Parameter	Description
Enable CPSEC	Select **enable** or **disable** to turn the control plane security feature on or off. This feature is enabled by default.
Enable auto cert provisioning	When you enable the control plane security feature, you can toggle this switch to turn on automatic certificate provisioning. When you enable this feature, the controller attempts to send certificates to all associated campus APs. Auto certificate provisioning is disabled by default. **NOTE:** If you do not want to enable automatic certificate provisioning the first time you enable control plane security on the controller, you must identify the valid APs on your network by adding those to the campus AP whitelist. For details, see Managing AP Whitelists. After you have enabled automatic certificate provisioning, you must select **Only accept APs from specified ranges.**
Only accept APs from specified ranges	Enabling this option will let you automatically certify APs within a select range of IP addresses.
Address ranges for Auto Cert	The **Address ranges for Auto Cert Provisioning** section allows you to send certificates to a group of campus or remote APs within a range of IP addresses. Click + to specify the start and end IP address of the range. Repeat this procedure to add additional IP ranges to the list of allowed addresses. If you enable both control plane security and auto certificate provisioning, all APs in the address list receives automatic certificate provisioning.

Managing AP Whitelists

Campus or Remote APs appear as valid APs in the Campus AP or Remote AP whitelists when you manually enter their information into the Campus AP or Remote AP whitelists using the WebUI or CLI of a controller. Also, the Campus APs or Remote APs appear as valid APs after a controller sends a certificate to an AP as part of automatic certificate provisioning and the AP connects to the controller over a secure tunnel. APs that are not approved or certified on the network are included in the Campus AP whitelists, but these APs appear in an unapproved state.

Use the AP whitelists to grant valid APs secure access to the network or to revoke access from suspected rogue APs. When you revoke or remove an AP from the Campus AP or Remote AP whitelists on a controller that uses CPsec, that AP will not able to communicate with the controller again, unless the AP obtains a new certificate.

The following sections discuss the procedures to manage AP whitelists:

Adding an AP to the Campus or Remote AP Whitelists

You can add an AP to the Campus AP or Remote AP whitelists using the WebUI or CLI. The following procedure describes the steps to add an AP to the Campus AP or Remote AP whitelist:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Access Points > Whitelist** tab.
2. Click **Campus AP Whitelist** or **Remote AP Whitelist** tab.
3. Click **+**.
4. Define the following parameters for each AP you want to add to the AP whitelist:

Table 1: *AP Whitelist Parameters*

Parameter	Description
Campus AP whitelist configuration parameters	
MAC address	MAC address of campus AP that supports secure communications to and from its controller.
AP name	Name of the campus AP. If you do not specify a name, the AP uses its MAC address as AP name.
AP group	Name of the AP group to which the campus AP is assigned. If you do not specify an AP group, the AP uses default as its AP group.
Description	Brief description of the campus AP.
Remote AP whitelist configuration parameters	
MAC address	MAC address of the remote AP, in colon-separated octets.
AP name	Name of the Remote AP. If you do not specify a name, the AP uses its MAC address as AP name.
AP group	Name of the AP group to which the Remote AP is assigned.
Description	Brief description of the Remote AP.
IPv4 address	IPv4 address of the Remote AP.
IPv6 address	IPv6 address of the Remote AP.

5. Click **Submit**.

Whitelist DB Optimization

In addition to the existing push-based model that syncs whitelist entries to managed devices when they are updated, deleted, or revoked from Mobility Master. The Mobility Master introduces a pull-based sync mechanism for the whitelist database, in which AP whitelist entries are only synced to the managed devices that require the entry. The pull-based sync mechanism is used when a Remote AP or CPsec AP terminates on a managed device or if a network is down during a whitelist push, which can prevent messages from going through to the managed devices. The managed device can use this as a fallback mechanism to periodically check if it is in sync with the Mobility Master. If a mismatch is detected, the managed device pulls the new entry from Mobility Master. All whitelist entries are configured from a centralized location on the Mobility Master and synced to appropriate managed devices. Entries can also be configured directly on a managed device for debugging purposes. However, these changes are not synced back to the Mobility Master or any other managed device.

This whitelist-DB optimization provides the following enhancements on Mobility Master:

- Reduced memory footprint.
- Increased performance on the Mobility Master and managed devices.
- Scalability and support for over 1000 managed devices and 10,000 APs on a Mobility Master.
- Scalability and support for managed devices with varying AP capacities.
- Simplified debugging process, as corrupt entries are no longer synced to every managed device on a given Mobility Master.

> Changes made to the whitelist-DB can only be applied to the postgres database and are not backwards-compatible.

You can view a controller's current sequence number using the CLI:

```
(host) #show whitelist-db seq-pendlist
```

> In a Mobility Master, only a global list of whitelist entries are available. To view the entries specific to a managed device, login into the particular device to view the whitelist specific to the device.

Configuring Networks with a Backup Mobility Master

This section describes the configuration with a backup Mobility Master.

If your network includes a redundant backup Mobility Master, *you must synchronize the database from the primary Mobility Master to the backup Mobility Master at least once* after all APs are communicating with the controllers over a secure channel. This ensures that all certificates, IPsec keys, and campus AP whitelist entries are synchronized to the backup controller. You should also synchronize the database any time the campus AP whitelist changes (APs are added or removed to ensure that the backup controller has the latest settings).

Mobility Master and backup Mobility Masters can be synchronized using either of the following methods:

- **Manual Synchronization**: Issue the **database synchronize** command to manually synchronize databases from your primary Mobility Master to the backup Mobility Master.
- **Automatic Synchronization**: Schedule automatic database backups using the **database synchronize period** command in configuration mode.

> If you add a new backup Mobility Master to an existing Mobility Master, you must add the backup Mobility Master as the **lower priority** controller. If you do not add the backup Mobility Master as a lower priority controller, your CPsec security keys and certificates may be lost. If you want the new backup Mobility Master to become your primary controller, increase the priority of that controller to a primary controller *after* you have synchronized your data.

Replacing a Controller on a Multi-Controller Network

The procedure to replace a controller within a multi-controller network varies, depending upon the role of that controller, whether the network has a single Mobility Master or a cluster of Mobility Masters, and whether or not the controller has a backup.

Replacing Controllers in a Single Mobility Master Network

Use the procedures in this section to replace a Mobility Master or managed device in a network environment with a single Mobility Master.

Replacing a Managed Device

Follow the steps below to replace a managed device in a single Mobility Master network:

1. Disconnect the managed device from the network.
2. If you plan on moving the managed device to another location on the network, purge the campus AP whitelist on the managed device.

   Access the CLI on the old managed device and issue the **whitelist-db cpsec purge** command.
3. Install the new managed device, but do not connect it to the network. If the managed device has been previously installed on the network, you must ensure that the new managed device has a clean whitelist.
4. Purge the managed device whitelist by executing the **whitelist-db cpsec purge** command on the new managed device.
5. Once the managed device has a valid CPsec certificate and configuration, the managed device receives the campus AP whitelist from the Mobility Master and starts certifying approved APs.
6. APs associated with the new managed device reboots and creates new IPsec tunnels to the controller using the new certificate keys.

Replacing a Redundant Mobility Master

The CPsec feature requires you to synchronize databases from the primary Mobility Master to the backup Mobility Master at least once after the network is up and running. This ensures that all certificates, keys, and whitelist entries are synchronized to the backup Mobility Master. Because the AP whitelist may change periodically, you should regularly synchronize these settings to the backup Mobility Master. For details, see Configuring Networks with a Backup Mobility Master.

When you install a new backup Mobility Master, *you must add it as a lower priority* controller than the existing primary Mobility Master. After you install the backup Mobility Master on the network, synchronize the database from the existing primary Mobility Master to the new backup Mobility Master to ensure that all certificates, keys, and whitelist entries required for CPsec are added to the new backup Mobility Master configuration. If you want the new Mobility Master to act as the primary Mobility Master, you can increase that Mobility Master's priority *after* the settings have been synchronized.

> The CPsec settings of a controller does not change if you upgrade the controller running ArubaOS 6.x to ArubaOS 8.0.0.0. If CPsec was already enabled, then it remains enabled after the upgrade, however if CPsec was not enabled previously and you want to use this feature after upgrading, then you must manually enable CPsec.

Troubleshooting Control Plane Security

Follow the procedures below to identify and troubleshoot CPsec issues:

Identifying Certificate Problems

If an AP has a problem with its certificate, check the state of the AP in the campus AP whitelist. If the AP is in either the certified-hold-factory-cert or certified-hold-switch-cert states, you may need to manually change the status of that AP before it can be certified.

- **certified-hold-factory-cert**: An AP is put in this state when the controller thinks the AP has been certified with a factory certificate, but the AP requests to be certified again. Because this is not a normal condition, the AP is not approved as a secure AP until you manually change the status of the AP to verify that it is not compromised. If an AP is in this state due to connectivity problems, then the AP recovers and is taken out of this hold state as soon as connectivity is restored.
- **certified-hold-switch-cert**: An AP is put in this state when the controller thinks the AP has been certified with a controller certificate yet the AP requests to be certified again. Because this is not a normal condition, the AP is not be approved as a secure AP until a network administrator manually changes the status of the AP to verify that it is not compromised. If an AP is in this state due to connectivity problems, then the AP recovers and is taken out of this hold state as soon as connectivity is restored.

Verifying Certificates

If you are unable to configure the CPsec security feature, verify that its TPM and factory-installed certificates are present and valid by accessing the controller's CLI and issuing the **show tpm cert-info** command. If the controller has a valid certificate, the output of the command appears similar to the output in the example below.

> This command works only on hardware controllers.

```
(host) #show tpm cert-info
====================================
TPM manufacturing factory certificate
====================================
subject= /CN=BA0003137::00:1a:1e:00:89:b8
issuer= /DC=com/DC=arubanetworks/DC=ca/CN=DEVICE-CA1
serial=2E1DF0D10000004C8EE7
notBefore=Aug  6 22:50:04 2013 GMT
notAfter=Sep 14 03:21:14 2032 GMT
====================================
Generated Factory certificate
====================================
subject= /CN=BA0003137::00:1a:1e:00:89:b8/L=SW
issuer= /CN=BA0003137::00:1a:1e:00:89:b8
serial=2E1DF0D10000004C8EE7
notBefore=Aug  6 22:50:04 2013 GMT
notAfter=Sep 14 03:21:14 2032 GMT
```

If the controller displays the following output, it may have a corrupted or missing TPM and factory certificates. Contact Aruba support.

```
(host) #show tpm cert-info
Cannot get TPM and Factory Certificate Info.
```

Disabling Control Plane Security

If you disable CPsec on a Mobility Master or managed device, all APs connected to that controller reboot then reconnect to the controller over a clear channel.

If you disable CPsec for a managed device, APs directly connected to the managed device reboot and reconnect to the managed device over a clear channel.

MultiZone

The MultiZone feature allows organizations to have multiple and separate secure networks while using the same access point. It also allows AP to terminate to multiple managed devices that reside in different zones. A zone is a collection of managed devices under a single administration domain. The zone can have a single managed device or a cluster setup.

Traditionally, one AP was managed by a single zone where the configuration was generated on a master controller and synchronized across all other local controllers. Starting from ArubaOS 8.0.0.0, MultiZone AP is supported and an AP can be managed by multiple zones. Different zones can have different configurations. The managed devices in different zones do not communicate with one another.

Initially, when the AP is booted up, the first zone it contacts is called the Primary Zone. When the AP boots up on a managed device, and the primary zone managed device configures the AP including the BSS, radio channel, radio power, and other features. The primary zone can configure MultiZone profiles to enable the MultiZone feature.

Data zone is the secondary zone that an AP connects to after receiving the MultiZone configuration from the primary zone. If there are MultiZone profiles configured and associated in the AP group or AP name profile of the primary zone, then the AP enters MultiZone state and starts connecting with the specified data zones. Only one MultiZone profile per ap-group or ap-name can be attached. The data zone managed device must be configured with the same AP group or AP name profile as the primary zone. When the AP connects to the data zone managed devices, there is a flag in the HELLO message indicating that the AP is connecting to the zone as a data zone. The data zone managed device then can configure additional BSSs.

The AP virtually connects to each data zone independently. Each data zone's network change or failure does not affect the management of an AP from other data zones. The data zone can configure the AP separately and the AP will apply each configuration. However, if the primary zone goes down, then all the data zones will be affected including the traffic on the data zone.

For example, the first zone has SSID-1, SSID-2 configured and has stand-alone setup, while the second zone has SSID-3, SSID-4 configured and has cluster setup. Then, the MultiZone AP receives both configurations and provides service for all the four SSIDs with no communication between the managed devices.

The MultiZone feature allows the client traffic of different ESS to go to different managed devices into various zones without cross-contamination. The client traffic of the specific ESS is encrypted and tunneled directly from AP to the managed devices using the tunnel mode. All devices in the path including the primary managed device managing the AP are automatically secured. Client wireless frames are encrypted or decrypted for the corresponding SSID data zone managed device in the secure zone.

All the zones can have a maximum of 12 managed devices and 16 VAPs per radio and a maximum of 5 zones are supported including the primary zone.

Starting from ArubaOS 8.3.0.0, MultiZone supports Decrypt Tunnel forwarding mode on the data zone Virtual APs.

Following sections describe the functional flow, licenses, and features of MultiZone:

Functional Flow of a MultiZone AP

The functional flow of a MultiZone AP is as follows:

- AP boots up and terminates on primary zone.
- Receives configuration from primary zone and apply.
- Simultaneously, it connects to each IP address of data zone configured in the MultiZone profile.
- Receives VAP configuration from data zone and apply.
- If common configuration like radio or channel is changed on primary zone, data zone needs to rebootstrap to update.
- If the CPsec is enabled, each data zone managed device should have the AP appropriately white-listed.

Important Points

- CPsec is not mandatory for MultiZone.
- If High Availability is enabled, MultiZone cannot be configured.

Configuring MultiZone

The primary zone can configure MultiZone profiles to enable the MultiZone feature. The data zone APs are referred to as zone APs. In the data zone, the APs cannot be rebooted, provisioned, or upgraded.

Starting from ArubaOS 8.4.0.0, you can configure either or both IPv4 and IPv6 addresses in one data zone of an AP MultiZone profile. The AP selects either IPv4 or IPv6 address from the data zone configuration.

> The **AP-SYSTEM** profile configured in the data zone is ignored except for the LMS redirect option.

The following procedure describes how to configure MultiZone:

To create a MultiZone:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > AP Groups > AP Groups**.
2. Click on the **AP group name** for which you want to create a MultiZone.
3. In the **AP Groups > <AP Group Name>** tab, Click **MultiZone**.
4. Click **Enable multizone** toggle switch to enable MultiZone in an AP.
5. To add a new MultiZone profile, click + in the **MultiZone Profiles** field.
6. Enter the MultiZone name and click **OK**.
7. To add the primary zone and data zone details, click on the MultiZone profile. The parameters are listed in the following table:

Table 1: *MultiZone profile Parameters*

Parameter	Description
IPV4ADDRESS	Specify the IPv4 address of the AP.
IPV6ADDRESS	Specify the IPv6 address of the AP.
No. of WLANs	Specify the number of WLAN SSIDs. The maximum number of WLANs that can be configured are 16.
No. of CONTROLLERS	Specify the number of managed devices. The maximum number of controllers that can be configured are 12.

8. For primary zone, enter the **No. of WLANs** and **No. of Controllers** in their respective field.
9. For data zone, click + and enter the **IPv4 address**, **IPv6 address**, **No. of WLANs**, and **No. of Controllers**.
10. Click **Submit**.
11. Click **Pending Changes**.
12. In the **Pending Changes** window, select the check box and click **Deploy changes**.

To create a MultiZone profile :

1. In the **Managed Network** node hierarchy, navigate to **Configuration > System > Profiles > AP**.
2. Click **AP MultiZone**. **AP MultiZone profile: New Profile** is displayed.
3. Click **+** in **AP MultiZone profile** to add a new profile.
4. Enter the name of the profile in the **Profile Name** field.

> The data zone managed device configuration should only include the VAP profile and AAA profile for the MultiZone AP Group.

Spectrum Analysis

Wireless networks operate in environments with electrical and radio frequency devices that can interfere with network communications. Microwave ovens, cordless phones, and even adjacent Wi-Fi networks are all potential sources of continuous or intermittent interference. The HTML-based spectrum analysis software modules on APs that support this feature examine the RF environment in which the Wi-Fi network is operating, identify interference and classify its sources. An analysis of the results quickly isolate issues with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel.

AP radios that gather spectrum data but do not service clients are called Spectrum Monitor (SM). Each SM scans and analyzes the spectrum band used by the radio (2.4 GHz or 5 GHz) of the SM. An AP radio in *hybrid AP* mode continues to serve clients as an access point while analyzing spectrum analysis data for the channel the radio uses to serve clients. You can record data for both types of spectrum analysis devices, save that data, and then play it back for later analysis.

Topics in this section include:

Understanding Spectrum Analysis

Single-radio mesh APs do not support the spectrum analysis feature; if an AP radio has a virtual AP carrying mesh backhaul traffic, no other virtual AP on that radio can be configured as a spectrum monitor. However, dual-radio mesh APs can have the client access radio configured as a Spectrum monitor or hybrid AP while the other radio supports mesh backhaul traffic.

This section describes the following topics:

Device Support for Spectrum Analysis

The table below lists the AP models that support the spectrum analysis feature.

Table 1: *Device Support for Spectrum Analysis*

Device	Configurable as a Spectrum Monitor	Configurable as a Hybrid AP
550 Series	Yes	Yes
530 Series	Yes	Yes
320 Series	Yes	Yes
270 Series	Yes	Yes
220 Series	Yes	Yes
210 Series	Yes	Yes
200 Series	Yes	Yes
AP-115	Yes	Yes
170 Series	Yes	No
130 Series	Yes	Yes
AP-114	Yes	Yes
AP-105	Yes	Yes
AP-104	Yes	Yes
RAP-3WN Series	Yes	No

Viewing Spectrum Analysis

The radios on groups of APs can be converted to dedicated spectrum monitors or hybrid APs via the 802.11A and 802.11G radio profiles of the AP group. Individual APs can also be converted to spectrum monitors through the spectrum override profile of the AP.

> The spectrum analysis feature requires the RF Protect license. To convert an AP to a spectrum monitor or hybrid AP, you must have an AP license *and* an RFProtect license for each AP on that managed device.

The **Spectrum Analysis** tab of the **Diagnostics** > **Tools** in the WebUI includes the **Spectrum Dashboards** , **Spectrum Monitors**, and **Session Log** windows.

- **Spectrum Monitors**: this window displays a list of active spectrum monitors and hybrid APs streaming data to your client, the radio band the device is monitoring, and the date and time the SM or hybrid AP was connected to your client. This window allows you to select the spectrum monitors or hybrid APs for which you want to view information, and release the connection between your client and any device you no longer want to view.
- **Session Log**: this tab displays activity for spectrum monitors and hybrid APs during the current browser session, including timestamps showing when the devices were connected to and disconnected from the client, and any changes to a hybrid APs monitored channel.
- **Spectrum Dashboards**: this window shows different user-customizable data charts for 2.4 GHz and 5 GHz spectrum monitor or hybrid AP radios. Table 1 below gives a basic description of each of the spectrum analysis graphs that can appear on the spectrum dashboard.

> For more detailed information on these graphs, refer to Customizing Spectrum Analysis Graphs.

Table 1: *Spectrum Analysis Graphs*

Graph Title	Description	Update Interval
Active Devices	A pie chart showing the percentages and total numbers of each device type for all active devices. This graph has no set update interval; the graph automatically updates when values change. For details, see Active Devices.	-
Active Devices Trend	A line chart showing the numbers of up to five different types of Wi-Fi and non-Wi-Fi devices seen on selected channels during a specified time interval. This chart can show devices on multiple channels for a spectrum monitor, or the single monitored channel for a hybrid AP. For details, see Active Devices Trend.	5 seconds
Channel Metrics	This stacked bar chart shows the current relative quality, availability or utilization of selected channels in the 2.4 GHz or 5 GHz radio bands. This chart can show multiple channels for a spectrum monitor, or the single monitored channel for a hybrid AP. For details, see Channel Metrics.	5 seconds
Channel Metrics Trend	A line chart showing the relative quality or availability of selected channels in the 2.4 GHz or 5 GHz radio bands over a specified time interval. Spectrum monitors can show channel data for multiple channels, while a hybrid AP shows information only for its one monitored channel. For details, see	5 seconds

Spectrum Analysis Clients

The maximum number of spectrum monitor radios and hybrid AP radios on a stand-alone controller is limited only by the number of APs on that stand-alone controller. If desired, you can configure every radio on an AP that supports the Spectrum Analysis feature as a spectrum device. A dual-radio AP can operate as two spectrum devices, because each radio can be individually configured as a spectrum monitor or hybrid AP.

A spectrum analysis client can simultaneously access data from up to four individual spectrum device radios. Each spectrum device radio, however, can only be connected to a single client WebUI.

When you select a specific spectrum monitor or hybrid AP radio to stream data to your client, the stand-alone controller first verifies the device is not subscribed to some other client. Once the SM or hybrid AP radio has been verified as available, the SM or hybrid AP establishes a connection to the client and begins sending spectrum analysis data either every second or every five seconds, depending on the type of data being requested. Each client may select up to twelve different spectrum analysis charts and graphs to appear in the spectrum dashboard.

A stand-alone controller can support up to 22 active WebUI connections. If spectrum analysis clients are simultaneously viewing data for more than 22 WebUI connections, any additional WebUI requests are refused until some clients close their WebUI browser sessions.

When you finish reviewing data from an SM or hybrid AP, you should disconnect the device from your spectrum client. Do not forget this important step—no other user can access data from that spectrum monitor or hybrid AP until you release your subscription. Note, however, that when you disconnect a spectrum monitor from your client, *the AP continues to operate as a spectrum monitor* until you return it to AP mode by removing the local spectrum override, or by changing the mode parameter in the 802.11A or 802.11G radio profile from spectrum-mode back to AP-mode.

> A spectrum monitor or hybrid AP automatically disconnects from a client when you close the browser window you used to connect the spectrum monitor to your client. However, if you use Internet Explorer and have multiple instances of an Internet Explorer browser open, the data-streaming connection to the spectrum monitor or hybrid AP is not released until 60 seconds after you close the spectrum client browser window. During this 60-second period, the spectrum monitor is still connected to the client.

When a spectrum monitor or hybrid AP is not subscribed to any client, it still performs all classification tasks and collect all necessary channel lists and device information. You can view classification, device, and channel information for any active spectrum monitor or hybrid AP via the command-line interface of the stand-alone controller, regardless of whether or not that device is sending real-time spectrum data to another client WebUI.

Individual spectrum analysis graphs and charts are explained in detail in Customizing Spectrum Analysis Graphs.

Hybrid AP Channel Changes

By default, a hybrid AP only monitors the channel specified in its 802.11A or 802.11G radio profile for spectrum interference. If you want to change the channel monitored by a hybrid AP, you must edit the channel setting in those profiles. However, there are other ArubaOS features that may automatically change the channels on hybrid APs. APs using DFS perform off-channel scanning to detect the presence of satellite and radar transmissions, and switch to a different channel if it detects that satellite or radar transmissions are present. APs using the ARM feature constantly monitor the network and automatically select the best channel and transmission power settings for that AP. If you manually change a channel monitored by a hybrid AP, best practices are to temporarily disable ARM, as ARM may automatically return the channel to its previous setting.

If a hybrid AP is using ARM or DFS, that hybrid AP may automatically move to a different channel in response to changes in the network environment. If a hybrid AP changes channels while it is connected to a spectrum analysis client, the hybrid AP updates the graphs in the spectrum dashboard to start displaying spectrum data for the new channel, and sends a log message to the session log. For details on changing the channel monitored by a hybrid AP, see 2.4 GHz and 5 GHz Radio RF Management.

Hybrid APs Using Mode-Aware ARM

If a radio is configured as a hybrid AP and that AP is enabled with mode-aware ARM, the hybrid AP can change to an AM if too many APs are detected in the area. If ARM changes a hybrid AP to an Air Monitor, that AM does not provide spectrum data after the mode change. The AM unsubscribes from any connected spectrum analysis client, and sends a log message warning about the change. If mode-aware ARM changes the AM back to an AP, the hybrid AP does not automatically resubscribe back to the spectrum analysis client. The hybrid AP must manually resubscribed before it can appear in the **spectrum monitors** page of the client.

Creating Spectrum Monitors and Hybrid APs

Each stand-alone controller can support up to 22 active WebUI connections to spectrum monitor or hybrid AP radios. If you plan on using spectrum monitors or hybrid APs as a permanent overlay to constantly monitor your network, you should create a separate AP group for these devices. If you plan on temporarily converting campus APs to spectrum monitors, best practices are to use the spectrum local override profile to convert an AP to a spectrum monitor.

This section describes the following tasks for converting regular APs into hybrid APs or spectrum monitors.

- Converting APs to Hybrid APs
- Converting AP to Spectrum Monitor
- Converting Group of APs to Spectrum Monitors

Converting APs to Hybrid APs

You can convert a group of regular APs into a group of hybrid APs by selecting the **spectrum monitor** option in the 802.11A and 802.11G radio profiles of the AP group. Once you have enabled the spectrum monitor option, all APs in the group that support the spectrum monitoring feature start to function as hybrid APs. If any AP in the group does *not* support the spectrum monitoring feature, that AP continues to function as a standard AP, rather than a hybrid AP.

> The spectrum monitoring option in the 802.11A and 802.11G radio profiles only affects APs in ap-mode. Devices in am-mode (Air Monitors) or sm-mode (Spectrum Monitors) are not affected by enabling this option.

If you want to convert a individual AP (and not an entire AP group) to a hybrid AP, you must create a new 802.11A or 802.11G radio profile, enable the **spectrum monitor** option, then reassign that AP to the new profile. For additional information see Creating and Editing Mesh High-Throughput SSID Profiles for details on how to create a new 802.11A or 802.11G radio profile, then assign an individual AP to that profile.

> If the spectrum local-override profile on the stand-alone controller that terminates the AP contains an entry for a hybrid AP radio, that entry overrides the mode selection in the 802.11A or 802.11G radio profile, and the AP operates as a spectrum monitor, not as a hybrid AP. You must remove any spectrum local override for an AP to allow the device to operate as a hybrid AP. For further details on editing a spectrum local override, see Converting AP to Spectrum Monitor.

The following procedure converts an AP group into hybrid APs:

1. In the **Mobility Master** node hierarchy, navigate to **Configuration** > **AP Groups**.
2. Select an **AP Group**.
3. Click **Radio** tab for the selected AP group.
4. Under **Basic** > **Radio mode**, select **spectrum-mode** under either 2.4 GHz or 5 GHz.
5. Click **Submit**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the required check box and click **Deploy changes**.

To convert a group of APs via the command-line interface, access the CLI in config mode and issue the following commands, where profile is the name of the 802.11A or 802.11G radio profile used by the group of APs you want to convert to hybrid APs:

```
rf dot11a-radio-profile <profile> spectrum-monitoring
rf dot11g-radio-profile <profile> spectrum-monitoring
```

Converting AP to Spectrum Monitor

There are two ways to change a radio on an individual AP or AM into a spectrum monitor. You can assign that AP to a different 802.11A and 802.11G radio profile that is already set to spectrum mode, or you can temporarily change the AP into a spectrum monitor using a local spectrum override profile. When you use a local spectrum override profile to override the mode setting of an AP, that AP begins to operate as a spectrum monitor, but remains associated with its previous 802.11A and 802.11G radio profiles. If you change any parameter (other than the overridden **mode** parameter) in the 802.11A or 802.11G radio profiles of the spectrum monitor, the spectrum monitor immediately updates with the change. When you remove the local spectrum override, the spectrum monitor reverts back to its previous mode, and remains assigned to the same 802.11A and 802.11G radio profiles as before.

The spectrum local override profile overrides the **mode** parameter in the 802.11A or 802.11G radio profile, changing it from ap-mode or am-mode to spectrum-mode, while allowing the spectrum monitor to continue to inherit all other settings from its 802.11A or 802.11G radio profiles. When the spectrum local override is removed, the AP automatically reverts to its previous mode as defined it its 802.11A or 802.11G radio profile settings. If you use the local override profile to change an AP radio to a spectrum monitor, you must do so by accessing the WebUI or CLI of the stand-alone controller that terminates the AP.

The following procedure converts an individual AP using the spectrum local override profile:

1. In the **Mobility Master** node hierarchy, navigate to **Configuration** > **System**.
2. Select **Profiles** tab.
3. Select **Spectrum Local Override**.
4. In the **Spectrum Local Override Profile**, click **+**.
5. In the **ap_name**, enter the name of an AP whose radio you want to configure as a spectrum monitor. The AP names are case-sensitive. Any extra spaces before or after the AP name prevents the AP from being correctly added to the override list.
6. If your AP has multiple radios or a single dual-band radio, click the **spectrum_band** drop-down list and select the spectrum band you want that radio to monitor: **2.4 GHz** or **5 GHz**.
7. Click **OK** to add that radio to the **Override Entry** list.
8. Repeat steps 4 through 7 to convert other AP radios to spectrum monitors, if required.
9. To remove spectrum monitor from the override entry list, select that radio name in the override entry list, then click **Delete**.
10. Click **Submit**.
11. Click **Pending Changes**.
12. In the **Pending Changes** window, select the required check box and click **Deploy changes**.

Access the CLI in config mode and issue the following command to convert an individual AP using the spectrum local override profile:

```
ap spectrum local-override override ap-name <ap-name> spectrum-band 2ghz|5ghz
```

Converting Group of APs to Spectrum Monitors

When you convert a group of APs to spectrum monitors using their 802.11A or 802.11G radio profiles, all AP radios associated with that profile stop serving clients and act as spectrum monitors only. Therefore, before you convert an entire group of APs to spectrum monitors, be sure that none of the APs are currently serving clients, as that may temporarily interrupt service to those clients.

> If you use an 802.11A or 802.11G radio profile to create a group of spectrum monitors, all APs in any AP group referencing that radio profile are set to spectrum mode. Therefore, best practices are to create a new 802.11A or 802.11G radio profile just for spectrum monitors, using the following CLI commands:
> `ap-name <ap name> dot11a-radio-profile <profile-name>ap-name <ap name> dot11g-radio-profile <profile-name>`
>
> If you want to set an existing 802.11A or 802.11G radio profile to spectrum mode, verify that no other AP group references that radio profile, using the following CLI commands:
> `show references rf dot11a-radio-profile <profile-name>show references rf dot11g-radio-profile <profile-name>`

The following procedures convert an AP group into Spectrum mode:

1. In the **Mobility Master** node hierarchy, navigate to **Configuration** > **AP Groups**.
2. Select an **AP Group**.
3. Click **Radio** tab for the selected AP group.
4. Under **Basic** > **Radio mode**, select **spectrum-mode** under either 2.4 GHz or 5 GHz.
5. Click **Submit**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the required check box and click **Deploy changes**.

Access the CLI in config mode and issue the following commands, where **<profile>** is the 802.11A or 802.11G radio profile used by the AP group.

```
rf dot11a-radio-profile <profile> mode spectrum-mode
rf dot11g-radio-profile <profile> mode spectrum-mode
```

Spectrum Analysis Tasks

A spectrum analysis client is any laptop or desktop computer that can access a stand-alone controller WebUI and receive streaming data from individual spectrum monitors or hybrid APs. Once you have configured one or more APs to operate as a spectrum monitor or hybrid AP, navigate to the **Managed Network** node hierarchy from the Mobility Master WebUI, and use the **Spectrum Monitors** window to identify the spectrum devices you want to actively connect to the spectrum analysis client.

> The Spectrum Analysis option is not available if the license is not enabled or present.

The following sections explain the various tasks related to spectrum analysis as per the needs of your individual network:

Obtaining Managed Device Node Details

Before you log in to the Spectrum Analysis window, you must obtain the managed device node where the AP or spectrum monitor is terminated by using one of the following methods:

- In the **Managed Network** node hierarchy, navigate to **Configuration** > **Access Points** > **Campus APs** tab to obtain the managed device node details from the **Switch IP** column.
- In the **Managed Network** node hierarchy, navigate to **Dashboard** > **Infrastructure** > **Access Devices** tab to obtain the managed device node details from the **Active Controller** column.

Connecting Spectrum Devices to Spectrum Analysis Client

To connect one or more spectrum devices to your client, log in to the managed device obtained from the **Managed Network** node hierarchy (as described in Obtaining Managed Device Node Details):

1. In the **Managed Device** node hierarchy, navigate to **Diagnostics** > **Tools** > **Spectrum Analysis**.
2. Click **Launch** to launch the Spectrum Analysis tool.
3. Click the **Spectrum Monitors** tab in the new window.
4. Click **Add**. A table appears, displaying a list of spectrum analysis devices, sorted by name. Single-radio spectrum devices have a single entry in this table, and dual-radio spectrum devices have two entries: one for each radio. This table displays the following data for each radio.

Table 1: *Spectrum Device Selection Information*

Table Column	Description
AP	Name of the AP whose radio you want to convert to a spectrum monitor. AP names are case sensitive. This column includes the following icons: Radio is operating as a spectrum monitor. Radio is operating as a hybrid AP with spectrum enabled.
Band	The frequency band currently used by the radio. This value can be either **2.4 GHz** or **5 GHz**.
Model	AP model type.
AP Group	Name of the AP group to which the spectrum monitor is currently associated.
Mode	This column indicates the type of spectrum analysis device: ▪ **Spectrum Monitor**: AP is in spectrum monitor mode. ▪ **Access Point**: AP is configured as an access point but with spectrum monitoring enabled Hybrid AP.

Configuring Spectrum Analysis Dashboards

Once you have connected spectrum monitors to your spectrum analysis client, you can begin to monitor spectrum data in the spectrum analysis dashboards. There are three predefined sets of dashboard views, **View 1**, **View 2** and **View 3**. View 1 displays the Real-Time FFT, FFT Duty-Cycle and Swept Spectrogram graphs by default, and Views 2 and 3 display the Swept Spectrogram and Quality Spectrogram charts, and the Channel Summary and Active Devices tables.

> Spectrum Analysis dashboards are available only on stand-alone controllers.

Each chart in the dashboard can be replaced with other chart types, or reconfigured to show data for a different spectrum monitor. Once you have configured a dashboard view with different settings, you can rename that dashboard view to better reflect its new content.

The following sections explain how to customize your Spectrum Analysis dashboard to best suit the needs of your individual network:

Selecting Spectrum Monitor

When you first log in to the **Spectrum Analysis** dashboard from the Managed Device WebUI, it displays blank charts. You must identify the spectrum monitor whose information you want to view before the graphs display any data.

To identify the spectrum monitor radio whose data you want to display in the **Spectrum Analysis** dashboard, log in to the managed device obtained from the **Managed Network** node hierarchy (as described in **Obtaining Managed Device Node Details** section of Spectrum Analysis Tasks):

1. In the **Managed Device** node hierarchy, navigate to **Diagnostics** > **Tools** > **Spectrum Analysis**.
2. Click **Launch** to launch the Spectrum Analysis tool.
3. Click the **Spectrum Monitors** tab in the new window.
4. Click **Add**.
5. Select a spectrum monitor from the list and click **Connect**.

After you have selected the initial spectrum monitor or hybrid AP for a graph, you can display data for a different spectrum device at any time by clicking the down arrow by the device name in the chart titlebar and selecting a different connected spectrum monitor or hybrid AP.

Changing Graphs within Spectrum View

To replace an existing graph with any other type of graph or chart, log in to the managed device obtained from the **Managed Network** node hierarchy (as described in **Obtaining Managed Device Node Details** section of Spectrum Analysis Tasks):

1. In the **Managed Device** node hierarchy, navigate to **Diagnostics** > **Tools** > **Spectrum Analysis**.
2. Click **Launch** to launch the Spectrum Analysis tool.
3. Click the **Spectrum Dashboards** tab.
4. From **Spectrum Dashboards** window, click one of the view names at the top of the window to select the dashboard layout with the graph you want to change.
5. Click the down arrow at the far right end of the graph title bar to display a drop-down list of chart options.
6. Click **Replace With** to display a list of available graphs.
7. Click the name of the new graph you want to display.

Renaming Spectrum Analysis Dashboard View

You can rename any of the three spectrum analysis dashboard views at any time. However, renaming a view does not save its settings. (For details on saving a spectrum dashboard view, refer to Saving Dashboard View.)

To rename a Spectrum Analysis Dashboard view, log in to the managed device obtained from the **Managed Network** node hierarchy (as described in **Obtaining Managed Device Node Details** section of Spectrum Analysis Tasks):

Customizing Spectrum Analysis Graphs

Each Spectrum Analysis graph can be customized to display or hide selected data types. To view the available options for a graph type, log in to the managed device obtained from the **Managed Network** node hierarchy in the Mobility Master (as described in **Obtaining Managed Device Node Details** section of Spectrum Analysis Tasks):

1. In the **Managed Device** node hierarchy, navigate to **Diagnostics** > **Tools** > **Spectrum Analysis**.
2. Click **Launch** to launch the Spectrum Analysis tool.
3. Click the **Spectrum Dashboards** tab in the new window.
4. Click the down arrow at the end of the title bar for the graph you want to configure.
5. Select **Options**. The **Options** window appears to the right of the graph.
6. From the **Options** window, configure graph settings described in Spectrum Analysis Graph Configuration Options.
7. When you are done, click **Close** at the bottom of the **Options** window to hide the options window.
8. Click **Save Spectrum Views** at the top of the window to save your new settings.

Spectrum Analysis Graph Configuration Options

The following sections describe the customizable parameters and the default settings for each spectrum analysis graph.

This section contains the following topics:

Working with Non-Wi-Fi Interferers

The following table describes each type of non-Wi-Fi interferer detected by the spectrum analysis feature. These devices appear in the following charts:

- Active Devices
- Active Devices Table
- Active Devices Trend
- Device Duty Cycle
- Device vs Channel
- Interference Power

Table 1: *Non-Wi-Fi Interferer Types*

Non-Wi-Fi Interferer	Description
Bluetooth	Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a *Bluetooth* device. Bluetooth uses a frequency hopping protocol.
Fixed Frequency (Audio)	Some audio devices such as wireless speakers and microphones also use fixed frequency to continuously transmit audio. These devices are classified as *Fixed Frequency (Audio)*.
Fixed Frequency (Cordless Phones)	Some cordless phones use a fixed frequency to transmit data (much like the fixed frequency video devices). These devices are classified as *Fixed Frequency (Cordless Phones)*.
Fixed Frequency (Video)	Video transmitters that continuously transmit video on a single frequency are classified as *Fixed Frequency (Video)*. These devices typically have close to a 100% duty cycle. These types of devices may be used for video surveillance, TV or other video distribution, and similar applications.
Fixed Frequency (Other)	All other fixed frequency devices that do not fall into one of the above categories are classified as *Fixed Frequency (Other)*. Note that the RF signatures of the fixed frequency audio, video and cordless phone devices are very similar, and that some of these devices may be occasionally classified as Fixed Frequency (Other).
Frequency Hopper (Cordless Base)	Frequency hopping cordless phone base units transmit periodic beacon-like frames at all times. When the handsets are not transmitting (that is, no active phone calls), the cordless base is classified as *Frequency Hopper (Cordless Base)*.
Frequency Hopper (Cordless Network)	When there is an active phone call and one or more handsets are part of the phone conversation, the device is classified as *Frequency Hopper (Cordless Network)*. Cordless phones may operate in 2.4 GHz or 5 GHz bands. Some phones use both 2.4 GHz and 5 GHz bands (for example, 5 GHz for Base-to-handset and 2.4 GHz for Handset-to-base). These phones may be classified as unique Frequency Hopper devices on both bands.
Frequency Hopper (Xbox)	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as *Frequency Hopper (Xbox)*.
Frequency Hopper (Other)	When the classifier detects a frequency hopper that does not fall into one of the above categories, it is classified as *Frequency Hopper (Other)*. Some examples include IEEE 802.11 FHSS devices, game consoles, and cordless or hands-free devices that do not use one of the known cordless phone protocols.

Understanding Spectrum Analysis Session Log

The spectrum analysis **Session Log** tab displays times the spectrum monitors and hybrid APs connected to or disconnected from the spectrum client during the current browser session. This tab also shows changes in the scanning channel caused by changes to the 802.11A or 802.11G radio profile or automatic channel changes by the DFS or ARM features of the hybrid AP. The latest entry in the session log is also displayed in a footer at the bottom of the Spectrum Monitors and Spectrum Dashboard window. When you close the browser and end your spectrum analysis session, the session log is cleared.

Viewing Spectrum Analysis Data

You can use the command-line interface to view spectrum analysis data from any spectrum monitor, even if that spectrum monitor is currently sending data to the WebUI of the another spectrum monitor client.

Table 1 shows the commands that display spectrum analysis data in the CLI interface.

Table 1: *Spectrum Analysis CLI Commands*

Command	Description
show ap spectrum ap-list	Shows spectrum data seen by an access point that has been converted to a spectrum monitor.
show ap spectrum channel-metrics	Shows channel utilization information for a 802.11A or 802.11G radio band, as seen by a spectrum monitor
show ap spectrum channel-summary	Displays a summary of the 802.11A or 802.11G channels seen by a spectrum monitor.
show ap spectrum client-list	Shows details for Wi-Fi clients seen by a specified spectrum monitor.
show ap spectrum debug	Sub-commands under this command save spectrum analysis channel information to a file on the stand-alone controller.
show ap spectrum device-duty-cycle	Shows the current duty cycle for devices on all channels being monitored by the spectrum monitor radio.
show ap spectrum device-history	Displays spectrum analysis history for non-interfering devices.
show ap spectrum device-list	Shows summary table and channel information for non-Wi-Fi devices currently seen by the spectrum monitor.
show ap spectrum device-log	Shows a time log of add and delete events for non-Wi-Fi devices.
show ap spectrum device-summary	Shows the numbers of Wi-Fi and non-Wi-Fi device types on each channel monitored by a spectrum monitor.
show ap spectrum interference-power	Shows the interference power detected by a 802.11A or 802.11G radio on a spectrum monitor.
show ap spectrum monitors	Shows a list of APs currently configured as spectrum monitors.
show ap spectrum technical-support	Saves spectrum data for later analysis by your Aruba technical support representative.

Recording Spectrum Analysis Data

The spectrum analysis tool allows you to record up to 60 continuous minutes (or up to 10 Mb) of spectrum analysis data. By default, each spectrum analysis recording displays data for the Real-Time FFT, FFT Duty Cycle, Interference Power and Swept Spectrogram charts, however, you can view recorded device data for any the spectrum analysis charts supported by that spectrum monitor radio. Configurable recording settings allow you to start a recording session immediately, or schedule a recording to begin at a later date and time. Each recording can be scheduled to end after a selected amount of time has passed, or continue on until the recorded data file reaches a specified size. You can save the file to your spectrum monitor client, then play back that data at a later time.

The following sections provide information on creating, saving, and playing spectrum analysis data:

Creating a Spectrum Analysis Record

To record spectrum analysis data for later analysis, log in to the managed device obtained from the **Managed Network** node hierarchy in the Mobility Master (as described in **Obtaining Managed Device Node Details** section of Spectrum Analysis Tasks):

1. In the **Managed Device** node hierarchy, navigate to **Diagnostics** > **Tools** > **Spectrum Analysis**.
2. Click **Launch** to launch the Spectrum Analysis tool.
3. Click the **Spectrum Monitors** tab in the new window.
4. Click **Record** at the top of the window. The **New Recording** popup window appears.
5. Click the **Record From** link, and select the spectrum monitor whose data you want to record.
6. Next, decide whether you want the recording to start immediately, or at a later scheduled time. If you want the recording to start immediately, select **When the OK button is clicked**. To schedule a different starting time for the recording, click the date and time drop-down lists to select a starting month, day, year and time.
7. The recording continues until either the specified amount of time has passed, or until the recording files reaches a selected size. Click the **Length of recording reaches** drop-down list and select the amount of time the recording should last, or click the **Data file reaches** drop-down list and select the maximum file size for the recording.
8. Click **OK** to save your settings. If you selected the **When the OK button is clicked** in step 5, the recording begins.

While the recording is in progress, a round, red recording icon and recording status information appears at the top of the spectrum dashboard. You can view data for other spectrum monitors and charts while the recording is in progress. If you want to stop the recording before recording period has finished, click **Stop** by the recording status information. When you the **Stop**, a popup window appears and allows you to stop and delete the current recording, stop and save the recording in its current state (before it has completed), or continue recording again.

Saving Recording

After the recording has ended, either because the recording period has elapsed, the recording maximum file size has been reached, the **Spectrum Monitor Recording Complete** window appears and displays information for the current recording.

The following procedure saves the recording file:

1. From the **Spectrum Monitor Recording Complete** window, click **Continue**.
2. A **Save As** window appears and prompts you to select a file name for the recording and a location to save the file.
3. Click **Save**.

Playing Spectrum Analysis Recording

There are two ways to play back a spectrum recording. You can use the playback feature in the spectrum dashboard, or view recordings using the Aruba RFPlayback tool downloaded from the Aruba website.

Playing Recording in Spectrum Dashboard

The spectrum monitor does not have to be subscribed to your spectrum analysis client in order to play back a recording in the spectrum dashboard. However, you cannot play back an existing recording in the spectrum dashboard while another recording session is currently in progress.

Controller

Navigate to **Dashboard > Infrastructure** and click **CONTROLLERS** icon. The **Controllers** page lists all the managed devices in the network and provides its status and health related information. See Figure 1 for **Controllers** page.

Figure 1 *Controller Page*

Action Bar

The Action bar displays the total number of controllers depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the controllers in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand the controller from the **Controllers** table to view the detailed information of individual controller. See Figure 2 for Details page.

The **Controllers** table displays the following details:

- **Details** — Displays detailed information about the managed device.
- **Ports** — Displays the status of all the ports in the managed device.

Figure 2 *Details Page*

Access Devices

Navigate to **Dashboard > Infrastructure** and click **ACCESS DEVICES** icon. The **Access Points** page lists all the access points connected to managed devices in the network and provides its status and access point group related information. See Figure 1 for **Access Points** page.

Figure 1 *Access Points Page*

Action Bar

The Action bar displays the total number of APs depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the access points in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.
- **Sort**: Click a column header of the Access Points table to sort the complete list based on the entries on the active column. You can also use the sort icon that appears when you click on a column for sorting.
- **View client details**: Click on the number of clients associated with the AP to view the details of the clients on the **Clients** page.
- **View AP or radio summary**: Expand the access point from the **Access Points** table to view the summary of the individual APs. See Details for more information.
- **Capture and download packets:** Click Packet Capture icon of an access point from the Action column to start, pause, or stop capturing and downloading the AP packets.
- **Delete**: Select the check box for APs with **Down** status, and click the trash icon to remove the APs from the table. The APs with **Down** status are either unused or replaced when deployed.

> You can delete the APs with **Down** status only on Mobility Master or standalone controllers, and not on managed devices.

Details

Expand a access point from the **Access Points** table to view the detailed information of individual access point. See Figure 2 for Details page.

The **Access Points** table displays the following details:

Details — Displays detailed information about the selected access point.

Radio 2.4 GHz Channel — Displays the about channel utilization, noise floor, transmitted or received frames, and WLANs in the 2.4 GHz band.

You can view the following information using the **Show information about** drop-down list.

- **Channel Utilization** — Displays the percentage of the current channel utilization in the 2.4 GHz band. The channel utilization information is categorized as: **Tx time**, **Rx time**, **Interference**, and **Free**.

Click **Historical** icon in the top right corner of the window to display the percentage of the current channel utilization in the last 15 minutes.

- **Noise Floor** — Displays the information about noise floor (dBm) in the last 15 minutes.
- **Transferred Frames** — Displays the information about transmitted or received frames in the 2.4 GHz band. The transmitted or received frame information is categorized as: **Successful**, **Retried**, and **Dropped**.

Click **Historical** icon in the top right corner of the window to display the transmitted or received frames in the last 15 minutes.

- **WLANs** — Displays the throughput data (bps) in the 2.4 GHz band. Click the horizontal bar to navigate to the **Wireless clients** table and view the details of the wireless clients connected to this WLAN. For more information, see Details.

Radio 5 GHz Channel — Displays the detailed information about channel utilization, noise floor, transmitted or received frames, and WLANs in the 5 GHz band.

You can view the following information using the **Show information about** drop-down list

WAN

Navigate to **Dashboard > Infrastructure** and click **WAN** icon. The **Uplinks** page provides the status and health related information of uplinks in the network. See Figure 1 for **Uplinks** page.

Figure 1 *Uplinks Page*

Action Bar

The Action bar displays the total number of uplinks depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the uplinks in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand a uplink from the **Uplinks** table to view the detailed information of individual uplink. See Figure 2 for Details page.

The **Uplinks** table displays the following details:

- **HEALTH** — Displays detailed information about jitter, latency, and health score of the uplink in the network.

You can view the following information using the **Show** drop-down list.

  - **Jitter and Latency** — Displays the jitter and latency (Msec) in the last 15 minutes.
  - **Health Score** — Displays the percentage of health score in the last 15 minutes.

THROUGHPUT — Displays detailed information about transmitted or received data, and global compression on the uplink.

You can view the following information using the **Show** drop-down list.

  - **Tx and Rx** — Displays the transmitted or received data (bps) in the last 15 minutes.
  - **Global Compression** — Displays the aggregated compression saving on every uplink of the controller in the last 15 minutes.

Figure 2 *Details Page*

Cluster

The **Cluster** dashboard provides a visual overview on each cluster deployed on the network, displaying the following information:

- Total AP load per cluster
- Total Client load per cluster
- Status of each controller and access point in a cluster
- Health of each cluster

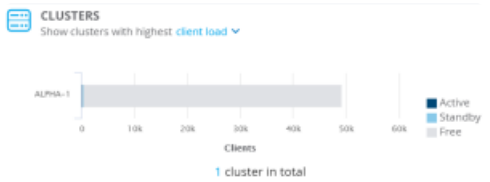
The **Cluster** dashboard can only be accessed from the root (Managed Network) node of the Mobility Master hierarchy. This information is not displayed on any stand-alone controllers, managed devices, or other nodes in the hierarchy. To view the **Cluster** dashboard, navigate to **Dashboard > Infrastructure > Clusters** in the WebUI. By default, the cluster dashboard displays the cluster with the highest AP load.

Following dashboard displays the cluster with the highest AP load. It also displays the number of active, standby and free APs for a given cluster.

Figure 1 *The Cluster Dashboard with Highest AP Load*

To view the client load, you can select client load to display the clusters with the highest client load from the drop-down menu.

Figure 2 *The Cluster Dashboard with Highest Client Load*



The **Cluster** dashboard consists of an **Cluster** section and **Cluster Member** section. Click on the AP load page or client load page to view more details.

- **Cluster > AP Load**: Displays the proportional distribution and number of active, standby, and free APs. Hover your mouse above a section of the chart to view the count for that AP type:
  - Free AP Load
  - Active AP Load
  - Standby AP Load
  - Total AP Load
- **Cluster > Client Load**: Displays the proportional distribution and number of active, standby, and free stations (clients). Hover your mouse above a section of the chart to view the count for that station type:
  - Free STA Load
  - Active STA Load
  - Standby STA Load
  - Total STA Load

To view in-depth information of each cluster member, click on the hyperlinked number under the **Controllers** column of the **Clusters** table. A **Cluster Members** pop-up window is displayed that contains a summary of each cluster member such as hostname, IP address, the cluster roles and so on.

Configuring WLANs

APs advertise WLANs to wireless clients by sending out beacons and probe responses that contain the WLAN's SSID and supported authentication and data rates. When a wireless client associates to an AP, it sends traffic to the AP's BSSID which is usually the AP's MAC address.

In the Aruba network, an AP uses a unique BSSID for each WLAN, so each individual AP or AP group can support multiple WLAN configurations.

Basic WLAN Configuration

The recommended method for creating a new WLAN configuration is through the new WLAN wizard, although advanced users may also configure a WLAN manually.

Creating a WLAN using the WLAN Wizard

To start the New WLAN wizard, in the **Managed Network** node hierarchy, navigate to **Configuration > Tasks** and select **Create a new WLAN**. The wizard opens and prompts you to enter the following information:

Configuration Setting	Description
General	
Name (SSID)	Name you assign to the new WLAN.
Primary usage	Select whether the WLAN will be primarily supporting employees or guest users.
Broadcast on	Choose whether the WLAN SSID should broadcast on all APs associated to the managed device or Mobility Master configuration, or whether the WLAN should broadcast on APs in a selected AP group. If you choose the **Select AP Groups** option, you are prompted to select one or more AP groups.
Forwarding mode	If the forwarding mode is set to **Tunnel**, data is tunneled to the managed device using GRE. When a WLAN is configured to use the **Decrypt-Tunnel** forwarding mode, that AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to the managed device, which then applies firewall policies to the user traffic. When the managed device sends traffic to a client, the managed device sends 802.3 traffic through the GRE tunnel to the AP, which then converts it to encrypted 802.11 and forwards to the client.
VLANs	
VLAN	The VLAN(s) into which users are placed in order to obtain an IP address. If you are creating a guest WLAN, remember that guest users must be separated from employee users by VLANs in the network.
Named VLANs	Click **Show VLAN Details** to view the list of named VLANs configured on the managed device or Mobility Master. To add a new VLAN, click + in the **Named VLANs** table, then enter appropriate values in the following fields: **VLAN name:** Name for the new VLAN **VLAN ID/Range:** Specify the beginning and ending VLAN IDs separated by a hyphen. For example, 55-58. To edit a named VLAN, select the VLAN from the table and click the pencil button. You can edit the **VLAN name** and **VLAN ID/Range** parameters.
VLAN IDs	Select a **VLAN** from the **Named VLANs** table to view the list of VLAN IDs configured on the managed device or Mobility Master. To add a new VLAN ID, click + in the **VLAN IDs** table, then enter/select appropriate values in the following fields: **VLAN ID:** Identification number for the VLAN **Admin state:** Enable or disable the VLAN interface. To edit a VLAN ID, select the VLAN from the **VLAN IDs** table and click the pencil button. You can edit the **VLAN ID** and **Admin state** settings.
Security*(for employee WLANs)*	
Enterprise	This option supports the following configuration parameters: **Key management**: Use this setting to select the layer-2 encryption type to be used on this WLAN SSID. Select either **WPA-3 Enterprise** (default), **WPA-2 Enterprise**, or **WPA Enterprise**. **Use CNSA suite**: Use Commercial National Security Algorithm (CNSA) for enterprise network. **Auth servers**: To add an existing server, Click + to open the **Add Existing Server** window and select a preconfigured server from the list of servers. To define a new server, click + on the Add Existing Server window and define a new **LDAP** or **RADIUS** server. For details, see Configuring Authentication Servers

WLAN Configuration Profiles

You can configure your WLANS to provide different network access or services to users on the same physical network. For example, you can configure a WLAN to provide access to guest users and another WLAN to provide access to employee users through the same APs. You can also configure a WLAN that offers open authentication and Captive Portal access with data rates of 1 and 2 Mbps, and another WLAN that requires WPA authentication with data rates of up to 11 Mbps. You can apply both virtual AP configurations to the same AP or an AP group.

When you define a WLAN using the New WLAN wizard on the **Configuration > Tasks** page of the Mobility Master or stand-alone controller WebUI, the wizard automatically creates a new virtual AP profile, AAA profile, 802.1X, Server group profile and SSID profile with the same name as the WLAN, and with the configuration settings and values defined via the wizard. These profiles also support additional advanced features that are not configurable via the WLAN wizard on the **Configuration > Tasks** page.

The following table describes the profiles that comprise the configuration settings for an ArubaOS WLAN, with links to the sections of this document that describe these profiles in more detail.

Table 1: *WLAN Profiles*

Profile	Description
Virtual AP Profile	This is the top-level WLAN configuration profile. A Virtual AP profile allows you to configure WLAN settings such as broadcast/multicast settings, forwarding modes and RF bands, but it also identifies the individual 802.11k, AAA, Anyspot, Hotspot 2.0, SSID and WWM Traffic management profiles to be used by that WLAN. Default profile name: <WLAN Name> When you create a WLAN using the WLAN wizard, ArubaOS automatically creates a new Virtual AP profile with the same name as the WLAN.
802.11k profile	The 802.11k protocol provides mechanisms for APs and clients to dynamically measure the available radio resources. Each 802.11k profile also references one instance of each the following additional profile types. ■ Beacon Report Request profile: Defines beacon report request settings. Beacon report requests are sent only to 802.11k-compliant clients that advertise Beacon Report Capability in their Radio Resource Management Enabled Capabilities IE. ■ Radio Resource Management IE profile: Defines Radio Resource Management Information Elements for WLANs with 802.11k support enabled. ■ Traffic Stream Measurement Report Request profile: Defines Traffic Stream Measurement report requests. These report requests are sent only to 802.11k- compliant clients that advertise a traffic stream report capability. Default profile name: default
AAA profile	The AAA profile defines the type of authentication used by clients associating to a WLAN. Each AAA profile also references one instance of each the following additional profile types: ■ 802.1X Authentication profile: Defines 802.1X authentication settings. ■ 802.1X Authentication Server Group profile: Defines fail through and load balancing settings for a group of servers used for 802.1X authentication. ■ MAC Authentication profile: Defines MAC authentication settings. ■ MAC Authentication Server Group profile: Defines fail through and load balancing settings for a group of servers used for MAC authentication. ■ RADIUS Accounting Server Group profile: Defines fail through and load balancing settings for a group of servers used for RADIUS accounting. ■ RFC 3576 Server profile: Defines a RADIUS server to send user disconnect, CoA, and session timeout messages as described in RFC 3576. ■ XML API Server profile: Define an authentication key for an XML API server, to perform customized external captive portal user management using an XML API interface. Default profile name: <WLAN Name> When you create a WLAN using the WLAN wizard, ArubaOS automatically creates a new AAA profile with the same name as the WLAN.
AnySpot Profile	The Anyspot client probe suppression feature decreases network traffic by suppressing probe requests from clients attempting to locate and connect to other known networks. By default, a virtual AP is not associated with an Anyspot profile, so an Anyspot profile must first be defined, and then manually associated to the virtual AP. Default profile name: N/A
Hotspot 2.0	Hotspot 2.0 is a WFA Passpoint specification based upon the 802.11u protocol that provides wireless clients with a streamlined

Configuring the Virtual AP Profile

The recommended method for creating a new WLAN configuration is through the new WLAN wizard, although advanced users may also configure a WLAN manually.

> For important information on changing the virtual AP forwarding mode for a WLAN serving active wired or wireless clients, see Changing a Virtual AP Forwarding Mode.

Manually Configuring the Virtual AP Profile

The following procedure describes how to configure Virtual AP profile.

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** tab.
2. From the **All Profiles** list, select **Wireless LAN >Virtual AP**.
3. To edit an existing Virtual AP profile, select the Virtual AP profile you want to edit. To create a new Virtual AP profile, click **+** and enter a name for the new Virtual AP profile in the **Profile name** field.
   The Virtual AP profile settings are divided into four sections, **General, RF, Advanced,** and **Broadcast/Multicast.**
4. Configure your Virtual AP settings, the profile parameters in each section are described in Virtual AP Profile Parameters.
5. Click **Submit**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Table 1: *Virtual AP Profile Parameters*

Parameter	Description
General	
Virtual AP enable	Select the **Virtual AP enable** check box to enable or disable the virtual AP.
VLAN	The VLAN(s) into which users are placed in order to obtain an IP address. **NOTE:** You must add an existing VLAN ID to the Virtual AP profile.
Forward mode	This parameter controls whether data is tunneled to the managed device using GRE, bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the managed device, and Internet access remains local). All forwarding modes support band steering, TSPEC/TCLAS enforcement, 802.11k and station blacklisting. Click the drop-down list to select one of the following forward modes: ▪ **Tunnel:** The AP handles all 802.11 association requests and responses, but sends all 802.11 data packets, action frames and EAPOL frames over a GRE tunnel to the managed device for processing. The managed device removes or adds the GRE headers, decrypts or encrypts 802.11 frames and applies firewall rules to the user traffic as usual. Both remote and campus APs can be configured in tunnel mode. ▪ **Bridge:** 802.11 frames are bridged into the local Ethernet LAN. When a remote AP or campus AP is in bridge mode, the AP (and not the managed device) handles all 802.11 association requests and responses, encryption/decryption processes, and firewall enforcement. The 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed. An AP in bridge mode does not support captive portal authentication. Both remote and campus APs can be configured in bridge mode. Note that you must enable the control plane security feature on the managed device before you configure campus APs in bridge mode. **NOTE:** In a bridge mode, the wired or wireless clients which have the same IP address as the Remote AP's local DHCP server cannot communicate with other devices even if the AP is deployed as a Campus AP. If you want to use the default Remote AP's IP address as the client IP address, you need to change the Remote AP's DHCP server IP address to a different IP address. To change Remote AP's DHCP server IP address, see Enabling Remote AP Advanced Configuration Options. ▪ **Split-Tunnel:** 802.11 frames are either tunneled or bridged, depending on the destination (corporate traffic goes to the managed device, and Internet access remains local)

Radio Resource (802.11k) and BSS Transition Management (802.11v)

The 802.11k protocol provides mechanisms for APs and clients to dynamically measure the available radio resources. In an 802.11k enabled network, APs and clients can send neighbor reports, beacon reports, and link measurement reports to each other. This allows the APs and clients to take appropriate connection actions.

The 802.11v BSS Transition capability can improve throughput, data rates and QoS for the voice clients in a network by shifting (via transition) the individual voice traffic loads to more appropriate points of association within the ESS.

Configuring the 802.11k Profile

The following procedure describes how to configure the 802.11k profile.

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** tab.
2. From the **All Profiles** list, select **Wireless LAN>802.11k**
3. To edit an existing 802.11k profile, select the 802.1k profile you want to edit. To create a new 802.11k profile, click **+** and enter a name for the new 802.11k profile in the **Profile name** field.
4. Configure your 802.11k radio settings. The configuration parameters are described in 802.11k Profile Parameters.
5. Click **Submit**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Table 1: *802.11k Profile Parameters*

Parameter	Description
Advertise 802.11k Capability	Select this option to allow Virtual APs using this profile to advertise 802.11k capability. Enabling this option also enables support for the 802.11v BSS transition management feature described in BSS Transition Management (802.11v). Default: Disabled
Forcefully disassociate on-hook voice clients	Select this option to allow the AP to forcefully disassociate *on-hook* voice clients (clients that are not on a call) after period of inactivity. Without the forced disassociation feature, if an AP has reached its call admission control limits and an on-hook voice client wants to start a new call, that client may be denied. If forced disassociation is enabled, those clients can associate to a neighboring AP that can fulfill their QoS requirements. Default: Disabled
Measurement Mode for Beacon Reports	Select any one of the following measurement modes from the drop down list: ▪ **active-all-ch**—Enables active beacon measurement mode. In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. ▪ **active-ch-rpt**—In this mode, the client and returns a report that contains a list of channels in a regulatory class where a client is likely to find an AP, including the AP transmitting the AP channel report. ▪ **beacon-table** (default)—Enables beacon-table beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. ▪ **passive**—Enables passive beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. **NOTE:** If a station does not support the selected measurement mode, it returns a Beacon Measurement Report with the incapable bit set in the Measurement Report Mode field.
Channel for Beacon	This value is sent in the 'Channel' field of the beacon requests on the 'A' radio. You can specify values in the range 34 to 165.

Fast BSS Transition (802.11r)

ArubaOS provides support for Fast BSS Transition as part of the 802.11r implementation. Fast BSS Transition mechanism minimizes the delay when a voice client transitions from one BSS to another within the same ESS. Fast BSS Transition establishes security and QoS states at the target AP before or during a re-association. This minimizes the time required to resume data connectivity when a BSS transition happens.

The following table provides the modes in which Fast BSS Transition is supported:

Table 1: *Supported VAP Forwarding Modes*

VAP Forwarding Mode	Support for 802.11r
Tunnel Mode	Yes
Decrypt-Tunnel Mode	Yes
Split-Tunnel Mode	No
Bridge Mode	Beta quality

Important Points to Remember

Fast BSS Transition is operational only if the wireless client has support for 802.11r standard. If the client does not have support for 802.11r standard, it falls back to normal WPA2 authentication method.

Configuring Fast BSS Transition

To enable and configure Fast BSS Transition on a configuration node, you must create and configure an 802.11r profile.

> Fast BSS transition is operational only with WPA2-Enterprise or WPA2-Personal.

The following procedure describes how to configure fast BSS transition.

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > System > Profiles** tab.
2. From the **All Profiles** list, select **Wireless LAN > 802.11r.**
3. To edit an existing 802.11r profile, select the 802.1r profile you want to edit. To create a new 802.11r profile, click **+** and enter a name for the new 802.11r profile in the **Profile name** field.
4. Configure your 802.11r radio settings:
   a. Select the **Advertise 802.11r Capability** option to allow Virtual APs using this profile to advertise 802.11r capability.
   b. Enter the mobility domain ID value (1-65535) in the **802.11r Mobility Domain ID** field. The default value is 1.
   c. Enter the R1 Key timeout value in seconds (60-86400) for decrypt-tunnel or bridge mode in the **802.11r R1 Key Duration** field. The default value is 3600.
5. Click **Submit**.

> Assign the edited 802.11r profile or the new 802.11r profile to an SSID profile, otherwise the 802.11r capability cannot be used.

WLAN SSID Profiles

An SSID is the network or WLAN that any client sees. A SSID profile defines the name of the network, authentication type for the network, basic rates, transmit rates, SSID cloaking, and certain WMM settings for the network.

SSID Profile Overview

ArubaOS supports different types of the AES, TKIP, and WEP encryption. AES is the most secure and recommended encryption method. Most modern devices are AES capable and AES should be the default encryption method. Use TKIP only when the network includes devices that do not support AES. In these situations, use a separate SSID for devices that are only capable of TKIP.

Suite-B Cryptography

The Suite-B (bSec) protocol is a pre-standard protocol that has been proposed to the IEEE 802.11 committee as an alternative to 802.11i. The main difference between bSec and standard 802.11i is that bSec implements Suite-B algorithms wherever possible. Notably, AES-CCM is replaced by AES-GCM, and the Key Derivation Function (KDF) of 802.11i is upgraded to support SHA-256 and SHA-384. In order to provide interoperability with standard Wi-Fi software drivers, bSec is implemented as a shim layer between standard 802.11 Wi-Fi and a Layer 3 protocol such as IP. A managed device configured to advertise a bSec SSID will advertise an open network, however only bSec frames will be permitted on the network.

> This feature requires the ACR license.

The bSec protocol requires that you use VIA 2.1.1 or greater on the client device. Consult VIA documentation for more information on configuring and installing VIA.

The bSec protocol is available in 128-bit mode and 256-bit mode. The number of bits specifies the length of the AES-GCM encryption key. Using United States Department of Defense classification terminology, bSec-128 is suitable for protection of information up to the SECRET level, while bSec-256 is suitable for protection of information up to the TOP SECRET level.

Suite-B AES-128-GCM and AES-256-GCM encryption is supported by the ArubaOS hardware.

Wi-Fi Multimedia Protection

Wi-Fi Multimedia™ (WMM®) is a Wi-Fi Alliance® certification program that is based on the IEEE 802.11e amendment. WMM ensures QoS for latency-sensitive traffic in the air. WMM divides the traffic into four queues or access categories:

- voice
- video
- best effort
- background

Management Frame Protection

ArubaOS supports the IEEE 802.11w standard, also known as Management Frame Protection (MFP). Management Frame Protection makes it difficult for an attacker to deny service by spoofing Deauth and Disassoc management frames. Management Frame Protection uses 802.11i (Robust Security Network) framework that establishes encryption keys between the client and AP.

Management Frame Protection is configured on a virtual AP as part of the wlan ssid-profile. SSIDs that support WPA2 opmode support MFP in all forwarding mode except tunnel mode. SSIDs that support WPA3 opmode support MFP in tunnel mode only. Two MFP related parameters, **mfp-capable** and **mfp-required**, cannot be configured through the CLI or WebUI. ArubaOS automatically configures these parameters based on the opmode.

> Management Frame Protection can only be enabled on SSIDs that support WPA2 or WPA3.

WLAN Authentication

The WLAN Wizard allows you to define the type of authentication used by clients associating to a WLAN. The WLAN wizard is the recommended method for defining WLAN settings, but advanced users can also define authentication settings manually via the AAA profile.

The following procedure describes how to configure WLAN authentication:

1. In the **Managed Network** node hierarchy, navigate to the **Configuration > Authentication > AAA Profiles** tab.
2. From the **AAA Profiles** list, select **AAA**.
3. To edit an existing AAA profile, select the AAA profile you want to edit. To create a new AAA profile, click **+** and enter a name for the new AAA profile in the **Profile name** field.
4. Configure the AAA profile parameters described in Table 1.
5. Click **Submit**.
6. Click **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Table 1: *AAA Profile Parameters*

Parameter	Description
Initial role	Click the **Initial Role** drop-down list and select a role for unauthenticated users. The default role for unauthenticated users is **logon**.
MAC Authentication Default Role	Click the MAC Authentication Default Role drop-down list and select the role assigned to the user when the device is MAC authenticated. The default role for MAC authentication is the **guest** user role. If derivation rules are present, the role assigned to the client through these rules take precedence over the default role. This feature requires the PEFNG license.
802.1X Authentication Default Role	Click the **802.1X Authentication Default Role** drop-down list and select the role assigned to the client after 802.1X authentication. The default role for 802.1X authentication is the **guest** user role. If derivation rules are present, the role assigned to the client through these rules take precedence over the default role. This feature requires the PEFNG license.
User idle timeout	Specify the idle timeout value for the client in seconds. A value of 0, deletes the user immediately after disassociation from the wireless network. Valid range is 30-15300 in multiples of 30 seconds.
RADIUS Interim Accounting	When this option is enabled, the RADIUS accounting feature allows the managed device to send Interim-Update messages with current user statistics to the server at regular intervals. This option is disabled by default, allowing the managed device to send only start and stop messages to the RADIUS accounting server.
User derivation rules	Click the drop-down list and specify a user attribute profile from which the user role or VLAN is derived.
Wired to Wireless Roaming	Enable this feature to keep users authenticated when they roam from the wired side of the network. This feature is enabled by default.
Reauthenticate wired user on VLAN change	When a wired user moves across VLANs, a trigger is created to reauthenticate this user. The default value is 'Enabled'.
Device Type Classification	When you select this option, the managed device will parse user-agent strings and attempt to identify the type of device connecting to the AP. When the device type classification is enabled, the Global client table shown in the **Monitoring>Network > All WLAN Clients** window shows each

The Basic User-Centric Networks

This section describes how to connect a managed device and an Aruba AP to your wired network. After completing the tasks described in this section, see Access Points for information on configuring APs.

This chapter describes the following topics:

Understanding Basic Deployment and Configuration Tasks

This section describes typical deployment scenarios and the tasks you must perform while connecting to a managed device and Aruba AP to your wired network.

Deployment Scenario #1: Managed Device and APs on Same Subnet

Figure 1 *Managed Device and APs on Same Subnet*

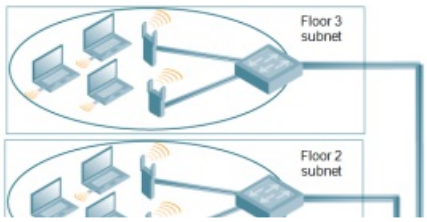
In this deployment scenario, the APs and managed device are on the same subnetwork and will use IP addresses assigned to the subnetwork. The router is the default gateway for the managed device and clients. There are no routers between the APs and the managed device. APs can be physically connected directly to the managed device. The uplink port on the managed device is connected to a layer-2 switch or router.

For this scenario, you must perform the following tasks:

1. Run the initial setup wizard.
   - Set the IP address of VLAN 1.
   - Set the default gateway to the IP address of the interface of the upstream router to which you will connect the managed device.
2. Connect the uplink port on the managed device to the switch or router interface. By default, all ports on the managed device are access ports and will carry traffic for a single VLAN.
3. Deploy APs. The APs will use the ADP to locate the managed device.
4. Configure the SSID(s) with VLAN 1 as the assigned VLAN for all users.

Deployment Scenario #2: APs All on One Subnet Different from Managed Device Subnet

Figure 2 *APs All on One Subnet Different from Managed Device Subnets*



In this deployment scenario, the APs and the managed device are on different subnetworks and the APs are on multiple subnetworks. The managed device acts as a router for the wireless subnetworks (the managed device is the default gateway for the wireless clients). The uplink port on the managed device is connected to a layer-2 switch or router; this port is an access port in VLAN 1.

For this scenario, you must perform the following tasks:

1. Run the initial setup wizard.
   - Set the IP address for VLAN 1.
   - Set the default gateway to the IP address of the interface of the upstream router to which you will connect the managed device.
2. Connect the uplink port on the managed device to the switch or router interface.
3. Deploy APs. The APs will use DNS or DHCP to locate the managed device.
4. Configure VLANs for the wireless subnetworks on the managed device.

Managed Devices Configuration Workflow

The tasks in deploying a basic user-centric network fall into two main areas:

- Configuring and connecting the managed device to the wired network (described in this section)
- Deploying APs (described later in this section)

The following workflow lists the tasks to configure a managed device. Click any of the links below for details on the configuration procedures for that task.

1. Connect the Managed Device to the Network.
2. Setting System Clock.
3. View current licenses and install new licenses.
4. For topologies similar to Deployment Scenario #3: APs on Multiple Different Subnets from Managed Devices), see Configuring VLANs to connect the managed device to your network. You do *not* need to perform this step if you are using VLAN 1 to connect the managed device to the wired network.
5. Configuring the Mobility Master IP Address. The managed device IP address is used by the managed device to communicate with external devices such as APs.
6. (Optional) Configuring the Loopback IP Address. You do *not* need to perform this step if you are using the VLAN 1 IP address as the managed device's IP address. Disable spanning tree on the managed device if necessary.
7. Configuring the Default Gateway for this managed device if you need to configure a trunk port between the managed device and another layer-2 switch (shown in Deployment Scenario #3: APs on Multiple Different Subnets from Managed Devices).
8. Trusted and Untrusted Ports and VLANs for this managed device.

Connect the Managed Device to the Network

To connect the managed device to the wired network, run the initial setup to configure administrative information for the managed device.

Initial setup can be done using the browser-based Setup Wizard or by accessing the initial setup dialog via a serial port connection. Both methods are described in the *ArubaOS 8.6.0.0 Quick Start Guide* and are referred to throughout this *section* as "initial setup."

This section describes the steps in detail.

Running the Initial Setup

When you connect to the managed device for the first time using either a serial console or a Web browser, the initial setup requires you to set the role (master, managed device, or stand-alone) for the managed device and passwords for administrator and configuration access.

> Do not connect the managed device to your network when running the initial setup. The factory-default managed device boots up with a default IP address and both DHCP server and spanning tree functions are disabled. You have completed the initial setup, you can use either the CLI or WebUI for further configuration before connecting the managed device to your network.

The initial setup might require that you specify the country code for the country in which the managed device will operate; this sets the regulatory domain for the radio frequencies that the APs use.

> You cannot change the country code for managed device designated for certain countries, such as the U.S. Improper country code assignment can disrupt wireless transmissions. Many countries impose penalties and sanctions for operators of wireless networks with devices set to improper country codes. If none of the channels supported by the AP you are provisioning have received regulatory approval by the country whose country code you selected, the AP will revert to Air Monitor mode.

7200 Series Controllers Port Behavior

The first two ports on the 7200 Series controllers, 0/0/0 and 0/0/1, are dual media ports and can be used for any purpose. Ports 0/0/2 through 0/0/5 are fiber-based ports that can be used for any purpose. If the fiber-based ports are connected with RJ45 or SFP transceivers, these ports can function as 1 Gbps ports. To access the controller, you can use port 0/0/0 to 0/0/5 when 0/0/2 through 0/0/5 are connected with RJ45 or SFP transceivers.

The following table describes the connector and speed supported for each physical interface of the 7200 Series controllers.

Table 1: *7200 Series Controllers Ports*

Port Type	Ports	Connector Type	Speed
10/100/1000 BASE-T Dual Media Ports	0/0/0–0/0/1	RJ45 or SFP	1 Gbps
10G BASE-X	0/0/2–0/0/5	SFP+	10 Gbps
		RJ45 or SFP	1 Gbps

Default Slot for USB Device

In 7000 Series and 7205 controllers, TRACES folder will not be automatically created when a USB device is connected to Slot 1. Ensure the USB device in Slot 0 as this is the default port where the TRACES folder is created.

Using the LCD Screen

Some managed devices are equipped with an LCD panel that displays a variety of information about the managed device's status and provides a menu that allows for basic operations such as initial setup and reboot. The LCD panel displays two lines of text with a maximum of 16 characters on each line. When using the LCD panel, the active line is indicated by an arrow next to the first letter.

Using the LCD Panel Mode

The LCD panel is operated using the two navigation buttons to the left of the screen.

- Menu: Allows you to navigate through the menus of the LCD panel.
- Enter: Confirms and executes the action currently displayed on the LCD panel.

The LCD has four modes:

- Boot: Displays the boot up status.
- LED Mode: Displays the mode that the STATUS LED is in.
- Status: Displays the status of different components of the managed device, including Power Supplies and ArubaOS version.
- Maintenance: Allows you to execute some basic operations of the managed device such as uploading an image or rebooting the system.

Table 1: *LCD Panel Mode: Boot*

Function or Menu Options	Display Output
Displays boot status	"Booting ArubaOS..."

Table 2: *LCD Panel Mode: LED Mode*

Function or Menu Options	Display Output
Administrative	LED MODE: ADM - displays whether the port is administratively enabled or disabled.
Duplex	LED MODE: DPX - displays the duplex mode of the port.
Speed	LED MODE: SPD - displays the speed of the port.
Exit Idle Mode	EXIT IDLE MENU

Table 3: *LCD Panel Mode: Status*

Function or Menu Options	Display Output
ArubaOS	Version ArubaOS X.X.X.X
PSU	Status Displays status of the power supply unit. **PSU 0: [OK | FAILED | MISSING]** **PSU 1: [OK | FAILED | MISSING]**
Fan Tray	Displays fan tray status. **FAN STATUS: [OK | ERROR | MISSING]** **FAN TEMP: [OK | HIGH | SHUTDOWN]**

Configuring a VLAN to Connect to the Network

You must follow the instructions in this section only if you need to configure a trunk port between the managed device and another Layer-2 switch (shown in Deployment Scenario #3: APs on Multiple Different Subnets from Managed Devices).

This section shows how to use both the WebUI and CLI for the following configurations (subsequent steps show how to use the WebUI only):

- Create a VLAN on the managed device and assign it an IP address.
- Optionally, create a VLAN pool. A VLAN pool consists of two more VLAN IDs which are grouped together to efficiently manage multi-managed device networks from a single location. For example, policies and virtual application configurations map users to different VLANs which may exist at a different managed device. This creates redundancy where one managed device has to back up many other managed devices. With the VLAN pool feature you can control your configuration globally.

> VLAN pooling should *not* be used with static IP addresses.

- Assign to the VLAN the ports that you will use to connect the managed device to the network. (For example, the uplink ports connected to a router are usually Gigabit ports.) In the example configurations shown in this section, a managed device is connected to the network through its Gigabit Ethernet port 1/25.
- Configure the port as a trunk port.
- Configure a default gateway for the managed device.

The following sections provides step-by-step instructions to configure a VLAN and connect to the network.

Creating, Updating, and Viewing VLANs and Associated IDs

You can create and update a single VLAN or bulk VLANs using the WebUI or the CLI. See Configuring VLANs.

> In the WebUI configuration windows, clicking the **Pending Changes** button saves configuration changes so that they are retained after the managed device is rebooted. Clicking the **Submit** or **Apply** button saves changes to the running configuration but the changes are not retained when the managed device is rebooted. A good practice is to use the **Submit** or **Apply** button to save changes to the running configuration and, after ensuring that the system operates as desired, click **Pending Changes**.

To view VLAN IDs in the CLI.

```
(host) [mynode] #show vlan
```

Creating, Updating, and Deleting VLAN Pools

> VLAN pooling should *not* be used with static IP addresses.

You can create, update, and delete a VLAN pool using the WebUI or the CLI. See Configuring VLANs.

Use the CLI to add existing VLAN IDs to a pool.

```
(host)[mynode](config) #vlan-name <name>
(host)[mynode](config) #vlan mygroup <vlan-ids>
```

To confirm the VLAN pool status and mappings assignments, use the **show vlan mapping** command:

```
(host)[mynode] #show vlan mapping
```

Configuring User-Centric Network

Configuring your managed device and AP is done through either the WebUI or the CLI.

- WebUI is accessible through a standard Web browser from a remote management console or workstation. The WebUI includes configuration tasks that walk you through easy-to-follow configuration steps. Each task has embedded online help. The tasks are:
  - Provision New APs—basic AP configurations including LAN, Remote, LAN Mesh, and Remote Mesh deployment scenarios.
  - Controller—applicable only the first time the managed device is brought UP; basic managed device configuration including system settings, Control Plane security, and cluster settings.
  - Create a New WLAN—creating and configuring new WLANs and LANs associated with the “default” ap-group. Includes campus-only and remote networking.

    Clicking **Cancel** from the tasks (wizards) return you to where you launched the tasks from. Any configuration changes you entered are not saved.

- The CLI allows you to configure and manage managed device. The CLI is accessible from a local console connected to the serial port on the managed device or through a Telnet or SSH session from a remote management console or workstation.

  By default, you can only access the CLI from the serial port or from an SSH session. To use the CLI in a Telnet session, you must explicitly enable Telnet on the managed device.

Replacing a Controller

The procedure below describes the steps to replace an existing stand-alone controller and/or a redundant controller. Best practice is to replace the backup controller first, and replace the active controller only after the new backup controller is operational on the network. When you remove the active controller from the network to replace it, the new backup controller takes over the active controller role. When you add a second controller to the network, the second controller automatically assumes the role of a backup controller.

For information on the Mobility Controller Virtual Appliance, refer to the *Aruba Virtual Appliance Installation Guide*.

Replacing an Returned Merchandise Authorization (RMA) Device

If the controller being replaced was returned to Aruba as an RMA device, the license keys on the RMA controller cannot be directly transferred to a new device, and must be regenerated.

To generate a new license key for a controller that is returned as an RMA:

1. Access the My Networking Portal at http://hpe.com/networking/mynetworking/.
2. Log in to the My Networking Portal using the HPE Passport.
3. Click **View licenses** or **Transfer licenses to new platform**. All available licenses are displayed.
4. Select the **>>** icon at the right end of the record to verify the license details before transferring it.
5. Click **Transfer License** at the bottom of the page.
6. Select a controller from the **AOS Controller Type** drop-down list.
7. Enter the serial number of the mobility controller in the **Serial number** text box; or enter the passphrase of the Mobility Master in the **PassPhrase** text box.
8. Select the license to be transferred.
9. Click **Transfer** at the bottom of the page. A new license key is generated, which you can apply to the controller.

Procedure Overview

The procedure to replace a backup or active controller consists of the following tasks:

> If your controller does not have any manually added licenses, skip steps 3, 4, and 6 of the following procedure.

Step 1: (Optional) Change the VRRP Priorities for a Redundant Master Pair

If your deployment uses VRRP to define the primary Mobility Master in a pair of redundant Mobility Masters and you are replacing only the primary Mobility Master, you must change the VRRP priority levels of the controllers so that the primary Mobility Master has a lower priority than the backup Mobility Master. This will allow the configuration from the backup Mobility Master to be copied to the new Mobility Master, and prevent an old or inaccurate configuration from being pushed to the managed devices.

For details on changing VRRP priorities, see Configuring a Primary and Backup Master for Failover Redundancy.

Step 2: Back Up the Flash File System

To start the migration process, access the backup controller or the Mobility Master being replaced and create a backup of the flash file system. You can create a backup file using the WebUI or command-line interfaces.

To create a flash backup from the command-line interface, access the active controller and issue the **backup flash** command.

To back up the flash from the WebUI, log in to the current backup controller or active controller and create a flash backup using the procedure below.

1. In the **Mobility Master** node hierarchy, select the device and navigate to the **Maintenance > Configuration Management > Backup** tab.
2. For the **Select what to backup** option, select **Flash**.
3. Click **Create Backup**. A confirmation message (**Backup saved successfully**) is displayed.

Controller

Navigate to **Dashboard > Infrastructure** and click **CONTROLLERS** icon. The **Controllers** page lists all the managed devices in the network and provides its status and health related information. See Figure 1 for **Controllers** page.

Figure 1 *Controller Page*

Action Bar

The Action bar displays the total number of controllers depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the controllers in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand the controller from the **Controllers** table to view the detailed information of individual controller. See Figure 2 for Details page.

The **Controllers** table displays the following details:

- **Details** — Displays detailed information about the managed device.
- **Ports** — Displays the status of all the ports in the managed device.

Figure 2 *Details Page*

Access Devices

Navigate to **Dashboard > Infrastructure** and click **ACCESS DEVICES** icon. The **Access Points** page lists all the access points connected to managed devices in the network and provides its status and access point group related information. See Figure 1 for **Access Points** page.

Figure 1 *Access Points Page*

Action Bar

The Action bar displays the total number of APs depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the access points in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.
- **Sort**: Click a column header of the Access Points table to sort the complete list based on the entries on the active column. You can also use the sort icon that appears when you click on a column for sorting.
- **View client details**: Click on the number of clients associated with the AP to view the details of the clients on the **Clients** page.
- **View AP or radio summary**: Expand the access point from the **Access Points** table to view the summary of the individual APs. See Details for more information.
- **Capture and download packets:** Click Packet Capture icon of an access point from the Action column to start, pause, or stop capturing and downloading the AP packets.
- **Delete**: Select the check box for APs with **Down** status, and click the trash icon to remove the APs from the table. The APs with **Down** status are either unused or replaced when deployed.

> You can delete the APs with **Down** status only on Mobility Master or standalone controllers, and not on managed devices.

Details

Expand a access point from the **Access Points** table to view the detailed information of individual access point. See Figure 2 for Details page.

The **Access Points** table displays the following details:

Details — Displays detailed information about the selected access point.

Radio 2.4 GHz Channel — Displays the about channel utilization, noise floor, transmitted or received frames, and WLANs in the 2.4 GHz band.

You can view the following information using the **Show information about** drop-down list.

- **Channel Utilization** — Displays the percentage of the current channel utilization in the 2.4 GHz band. The channel utilization information is categorized as: **Tx time**, **Rx time**, **Interference**, and **Free**.

Click **Historical** icon in the top right corner of the window to display the percentage of the current channel utilization in the last 15 minutes.

- **Noise Floor** — Displays the information about noise floor (dBm) in the last 15 minutes.
- **Transferred Frames** — Displays the information about transmitted or received frames in the 2.4 GHz band. The transmitted or received frame information is categorized as: **Successful**, **Retried**, and **Dropped**.

Click **Historical** icon in the top right corner of the window to display the transmitted or received frames in the last 15 minutes.

- **WLANs** — Displays the throughput data (bps) in the 2.4 GHz band. Click the horizontal bar to navigate to the **Wireless clients** table and view the details of the wireless clients connected to this WLAN. For more information, see Details.

Radio 5 GHz Channel — Displays the detailed information about channel utilization, noise floor, transmitted or received frames, and WLANs in the 5 GHz band.

You can view the following information using the **Show information about** drop-down list

WAN

Navigate to **Dashboard > Infrastructure** and click **WAN** icon. The **Uplinks** page provides the status and health related information of uplinks in the network. See Figure 1 for **Uplinks** page.

Figure 1 *Uplinks Page*

Action Bar

The Action bar displays the total number of uplinks depending on the filters applied. The Action bar includes action buttons namely, **Show/Hide table filters**, and **Customize columns**.

You can perform the following tasks on this page:

- **Show/Hide table filters** — Click **Show/Hide table filters** icon to filter and list the uplinks in the table that you want to view.
- **Customize columns** — Click **Customize columns** icon to select the table columns that you want to view.

Details

Expand a uplink from the **Uplinks** table to view the detailed information of individual uplink. See Figure 2 for Details page.

The **Uplinks** table displays the following details:

- **HEALTH** — Displays detailed information about jitter, latency, and health score of the uplink in the network.

You can view the following information using the **Show** drop-down list.

  - **Jitter and Latency** — Displays the jitter and latency (Msec) in the last 15 minutes.
  - **Health Score** — Displays the percentage of health score in the last 15 minutes.

THROUGHPUT — Displays detailed information about transmitted or received data, and global compression on the uplink.

You can view the following information using the **Show** drop-down list.

  - **Tx and Rx** — Displays the transmitted or received data (bps) in the last 15 minutes.
  - **Global Compression** — Displays the aggregated compression saving on every uplink of the controller in the last 15 minutes.

Figure 2 *Details Page*

Cluster

The **Cluster** dashboard provides a visual overview on each cluster deployed on the network, displaying the following information:

- Total AP load per cluster
- Total Client load per cluster
- Status of each controller and access point in a cluster
- Health of each cluster

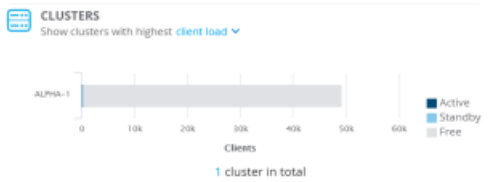
The **Cluster** dashboard can only be accessed from the root (Managed Network) node of the Mobility Master hierarchy. This information is not displayed on any stand-alone controllers, managed devices, or other nodes in the hierarchy. To view the **Cluster** dashboard, navigate to **Dashboard > Infrastructure > Clusters** in the WebUI. By default, the cluster dashboard displays the cluster with the highest AP load.

Following dashboard displays the cluster with the highest AP load. It also displays the number of active, standby and free APs for a given cluster.

Figure 1 *The Cluster Dashboard with Highest AP Load*

To view the client load, you can select client load to display the clusters with the highest client load from the drop-down menu.

Figure 2 *The Cluster Dashboard with Highest Client Load*



The **Cluster** dashboard consists of an **Cluster** section and **Cluster Member** section. Click on the AP load page or client load page to view more details.

- **Cluster > AP Load**: Displays the proportional distribution and number of active, standby, and free APs. Hover your mouse above a section of the chart to view the count for that AP type:
  - Free AP Load
  - Active AP Load
  - Standby AP Load
  - Total AP Load
- **Cluster > Client Load**: Displays the proportional distribution and number of active, standby, and free stations (clients). Hover your mouse above a section of the chart to view the count for that station type:
  - Free STA Load
  - Active STA Load
  - Standby STA Load
  - Total STA Load

To view in-depth information of each cluster member, click on the hyperlinked number under the **Controllers** column of the **Clusters** table. A **Cluster Members** pop-up window is displayed that contains a summary of each cluster member such as hostname, IP address, the cluster roles and so on.

DHCP with Vendor-Specific Options

This section describes how to configure several DHCP vendor-specific options.

Topics in this section include:

Configuring a Windows-Based DHCP Server

Configuring a Microsoft Windows-based DHCP server to send Option 43 to the DHCP client on an Aruba AP consists of the following two tasks:

- Configuring DHCP Response (Option 43)
- Configuring DHCP Vendor Class Request (Option 60)

DHCP servers are a popular way of configuring clients with basic networking information such as an IP address, a default gateway, network mask, DNS server, and so on. Most DHCP servers have the ability to also send a variety of optional information, including the Vendor-Specific Information (VSI), also called Option 43. When a client or an AP requests for Option 43 (VSI), the DHCP server responds with the IP address of the managed device configured by the administrator in the DHCP pool.

When a factory-default AP boots up and requests an IP address, the AP includes a Vendor Class Identifier (VCI) string by default in its DHCP request, also called Option 60. VCI is a text string that uniquely identifies a type of vendor device. Based on the VCI string, the DHCP server responds with the correct VSI included in Option 43.

Configuring DHCP Response (Option 43)

Configuring DHCP response (Option 43) returns the IP address of the Aruba managed device to an Aruba DHCP client. This information allows Aruba APs to auto-discover the Mobility Master and obtain their configuration.

Configuring Option 43 Using the Windows DHCP Server

The following procedure configures DHCP response (Option 43) using the Windows DHCP server:

1. On the DHCP server, navigate to **Start > Administration Tools > DHCP** to open the DHCP server administration tool.
2. Find your server and right-click on the scope to be configured under the server name.
3. Click on the **Scope Options** entry and select **Configure Options**.
4. In the **Scope Options** window, scroll down and select **043 Vendor Specific Info**.
5. In the **Data Entry** field, click anywhere in the area under the ASCII heading and enter ASCII : Loopback address of the managed device.
6. Click **OK** to save the configuration.

   Option 43 is configured for this DHCP scope.

> Though you entered the IP address of the managed device in ASCII text, the IP address is displayed in binary form.

Configuring DHCP Vendor Class Request (Option 60)

When an AP sends a DHCP request, the AP identifies itself to the DHCP server by setting its VCI to **ArubaAP** in the DHCP request. Configuring DHCP vendor class request (Option 60) consists of the following two tasks:

1. Creating a new vendor class—Configure a Vendor Class Identifier (VCI) on the DHCP server for each AP. This VCI must match the VCI (**ArubaAP**) defined in Option 60 on the AP.
2. Creating a new policy—Create a new policy and assign server values in Option 43 for the newly-created vendor class.

> You must configure the DHCP vendor class only when the other devices in the same DHCP scope use DHCP Option 43, or when you want to display the IP address of the managed device to APs only.

Creating a New Vendor Class

The following procedure configures a new vendor class on the Windows-based DHCP server:

1. On the DHCP server, navigate to **Start** > **Administration Tools** > **DHCP** to open the DHCP server administration tool.
2. Find your server and right-click on **IPv4**.

Enabling DHCP Relay Agent Information Option (Option 82)

Option-82 feature allows the DHCP Relay Agent to insert specific information into a client request that is being forwarded to a DHCP server. Option-82 can be customized to cater to the requirements of any ISP to make access control decisions using the Arubamanaged device.

The managed device, when acting as a DHCP relay agent can be configured with the following sub-type options,

- Type 1 – Circuit ID (AP, Port)
- Type 2 – Remote ID (Client SSID)
- Type 5 – Link Selection (Local VLAN Network)

Starting from ArubaOS 8.1.0.0, a XML definition file has been introduced to provide flexibility to configure multiple sub-type options. The XML file is used as the input from the user and is validated against an XSD file stored under flash on the managed device. The format in the XML file is parsed and stored by the DHCP relay agent module to ensure option-82 related values are inserted in the DHCP request packets from the client to the server.

Starting from ArubaOS 8.1.0.0, when IP Helper is enabled on L3 interface, DHCP discover broadcast is filtered at the datapath level and is unicast to the configured helper device. DHCP Option-82 on L2 VLAN can now be enabled without the helper address.

> DHCP Option-82 is supported only for wired and wireless IPv4 clients and applicable to wireless clients terminating in AP Tunnel and D-Tunnel modes.

Sample XML Format

The following is a sample XML file which specifies DHCP Option-82 circuit and remote IDs and link selection fields.

```
<?xml version="1.0" encoding="UTF-8"?>
   <dhcpopt82>
     <circuit_id>
       <param>
         <type>var</type>
           <val>apmac</val>
           <delim>-</delim>
       </param>
      </circuit_id>
      <remote_id>
       <param>
        <type>var</type>
          <val>cmac</val>
          <delim>:</delim>
        </param>
      </remote_id>
   <link_selection>
    <param>
     <type>var</type>
      <val>vlanip</val>
     </param>
   </link_selection>
</dhcpopt82>
```

The following table describes the fields to be configured for wired and wireless clients.

Type of client	Fields to be configured
Wired clients	link_selection field only

Enabling Linux DHCP Servers

The following is an example configuration for the Linux dhcpd.conf file. After you enter the configuration, you must restart the DHCP service.

```
option serverip code 43 = ip-address;
option serverip code 43 = ip-address;
class "vendor-class"
{
match option vendor-class-identifier;
}
subclass "vendor-class" "ArubaAP"
{
option vendor-class-identifier "ArubaAP";
}
subnet 10.200.10.0 netmask 255.255.255.0
{
default-lease-time 200;
max-lease-time 200;
option subnet-mask 255.255.255.0;
option routers 10.200.10.1;
option domain-name-servers 10.4.0.12;
option domain-name "vlan10.aa.mycorpnetworks.com";
#
#option serverip <loopback-IP-address-of-master-controller>
#
option serverip 10.200.10.10;
range 10.200.10.200 10.200.10.252;
}
```