

# Aruba Networks and AirWave 7.7



Switch Configuration

## Copyright

© 2013 Aruba Networks, Inc. Aruba Networks trademarks include  , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

## Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site:

[http://www.arubanetworks.com/open\\_source](http://www.arubanetworks.com/open_source)

## Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

## Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

<b>Chapter 1 Switch Configuration in AirWave</b>	<b>7</b>
Requirements, Restrictions, and ArubaOS Support in AirWave	7
Requirements	7
Restrictions	7
ArubaOS Support in AirWave	8
Overview of Switch Configuration in AirWave	8
Groups > Switch Config when Global Configuration is Disabled	8
APs/Devices > List Page	9
APs/Devices > Manage Page	9
APs/Devices > Monitor Page	10
APs/Devices > Audit Page	10
Additional Concepts and Components	10
Save, Save and Apply, and Revert Buttons	10
Additional Concepts and Benefits	11
Scheduling Configuration Changes	11
Auditing and Reviewing Configurations	11
Licensing and Dependencies in Aruba Configuration	11
Preparing AMP for Switch Config	11
Minimum Configuration	12
Keeping Controllers and Switches in Separate Groups	12
Importing Profiles for Switch Config	13
<b>Chapter 2 Switch Configuration in Daily Operations</b>	<b>15</b>
Pushing Device Configurations to Switches	15
Supporting APs with Switch Configuration	15
AP Overrides Guidelines	15
Visibility in Switch Configuration	16
Visibility Overview	16
Using AMP to Deploy Aruba APs	16
Defining Visibility for Aruba Configuration	17
<b>Appendix A Switch Configuration Reference</b>	<b>21</b>
Overview	21
Security and Authentication	21
Security and Authentication > AAA Profile	22
Security and Authentication > 802.1X Auth	22
Security and Authentication > MAC	23
Security and Authentication > Captive Portal	24
Security and Authentication > Wired Auth	24
Security and Authentication > Management	24
Security and Authentication > Policy/ACL	25

Security and Authentication > ACL > Time Range .....	25
Security and Authentication > Network Aliases > Destinations .....	26
Security and Authentication > Network Aliases > Services .....	26
Security and Authentication > Server Groups .....	26
Server Groups Page Overview .....	26
Supported Servers .....	27
Adding a New Server Group .....	27
Security and Authentication > Server Groups > Internal .....	28
Security and Authentication > Server Groups > LDAP .....	28
Security and Authentication > Server Groups > RADIUS .....	28
Security > Server Groups > RFC 3576 .....	28
Security and Authentication > Server Groups > TACACS .....	29
Security and Authentication > Server Groups > XML API .....	29
Security > TACACS Accounting .....	29
Security and Authentication > User Roles .....	29
Security and Authentication > User Derivation Rules .....	30
Security and Authentication > Advanced Authentication .....	31
Security and Authentication > Management Password Policy .....	32
Interfaces .....	32
Gigabit Ethernet Interface .....	32
Gigabit Ethernet Group .....	33
Loopback .....	34
Management Interface .....	34
LACP System Profile .....	34
LACP Profile .....	34
Tunneled Node Profiles .....	35
Routed VLAN Interfaces .....	35
Important Points to Remember .....	35
Configuring Routed VLAN Interfaces .....	36
Ethernet Link Profiles .....	36
Ethernet Flow of Control .....	36
Configuring Ethernet Link Profiles .....	36
POE Management Profile .....	37
Power Management Modes .....	37
PoE Guard Band .....	37
Configuring a PoE Management Profile .....	37
PoE Profile Configuration .....	37
PoE Time Range Profile .....	38
Layer 2 Features .....	38
Global GVRP Configuration .....	39
Interface GVRP Profiles .....	39
LLDP Profiles .....	40
Port Security Profiles .....	40

Router Advertisement Guard .....	40
DHCP Trust .....	40
Loop Protect .....	40
MAC Limit .....	41
Configuring a Port Security Profile .....	41
Port Switching Profiles .....	41
Spanning Tree Global Config .....	41
MSTP Overview .....	41
Interface MSTP Profiles .....	42
Global MSTP Profiles .....	42
Configuring an Interface MSTP Profile .....	42
Rapid PVST+ .....	43
Important Notes .....	43
Interface PVST Bridge Profiles .....	43
Configuring a Rapid PVST+ Profile .....	44
Configuring an Interface PVST Bridge Profile .....	44
VLAN Profiles .....	44
VoIP Profiles .....	45
Layer 3 Features .....	45
IP Profile .....	45
Important Points to Remember .....	46
Default Gateways .....	46
IPv6 Profile .....	46
OSPFv2 .....	46
Key Features Supported by MAS .....	46
LSAs Originated by MAS .....	47
OSPFv2 Global Config .....	47
Interface OSPF Profiles .....	47
Quality of Service Profile .....	47
Trusted Mode .....	48
Drop Precedence .....	48
Untrusted Mode .....	48
Profile .....	48
Policing .....	49
Configuring QoS .....	49
Configuring Policer .....	49
Multicast Features .....	49
Interface IGMP Profiles .....	49
IGMP Snooping .....	50
MLDv1 Snooping .....	50
Configuring an MLDv1 Snooping Profile .....	51
Protocol Independent Multicast .....	51
Configuring a Global PIM Rendezvous Point .....	51

Configuring an Interface PIM Profile .....	51
System Features .....	52
General Config .....	52
DHCP Relay Profile .....	52
Configuring a DHCP Relay Profile .....	53
DHCP Server Profile .....	53
Configuring a DHCP Server Profile .....	53
Monitoring and Diagnostics .....	54
Mirroring Profiles .....	54
802.3ah OAM Profiles .....	54
Remote Monitoring (RMON) .....	55
Enabling RMON .....	55
Configuring an Alarm .....	55
Alarm Profile .....	56
Ethernet Statistics Index .....	56
Event Index .....	56
History Index .....	57
SNMP Management Profile .....	57
SNMPv3 User .....	57
ArubaStack .....	57

ArubaOS is the operating system, software suite, and application engine that operates Aruba Mobility Access Switch (MAS) and centralizes control over the entire mobile environment.

Aruba Mobility Access Switches can apply role-based policies to wired users and devices. User roles can represent specific users or groups of users with defined names such as employees or guests. They can be defined with VLAN-IDs, QoS policies, VoIP policies or even ACLs

The ArubaOS wizards, command-line interface (CLI), and the ArubaOS Web UI are the primary means used to configure and deploy ArubaOS. For a complete description of ArubaOS, refer to the *ArubaOS User Guide* for your Mobility Access Switch release.

The Aruba Configuration feature in AirWave consolidates ArubaOS configuration and pushes global Aruba switch configurations from one utility.



---

When configuring the switch profiles through AirWave, we recommend that you have access to the *ArubaOS User Guide* and the *ArubaOS CLI Guide* to use as a reference.

---

This chapter introduces the components and initial setup of Aruba Switch Configuration with the following topics:

- ["Requirements, Restrictions, and ArubaOS Support in AirWave" on page 7](#)
- ["Additional Concepts and Components" on page 10](#)
- ["Preparing AMP for Switch Config " on page 11](#)



---

AMP supports *Aruba AP Groups*, which should not be confused with standard *Aruba Device Groups*. This document provides information about the configuration and use of Aruba AP Groups and describes how Aruba AP Groups inter-operate with standard Aruba Device Groups.

---

## Requirements, Restrictions, and ArubaOS Support in AirWave

### Requirements

Your system must meet the following requirements in order for AirWave to support Switch Config. as the following requirements in AirWave:

- AirWave 7.7.0 or a later version must be installed and operational on the network.
- Aruba switches on the network must have ArubaOS 7.2.0.0 or greater installed and operational.
- For access to all monitoring features, you must provide Telnet/SSH credentials for a user with minimum access level of read only. In order to perform configuration, the credentials must be for a root level user. In either case, the enable password must be provided.

### Restrictions

Switch Configuration has the following restrictions in AMP:

- AMP supports a variety of Aruba firmware versions, so profiles/fields that are not supported by an older version will not be configured on switch running that version.
- Switch Configuration is not supported in either Global Groups or on the Master Console.

## ArubaOS Support in AirWave

AirWave provides the following options for configuring your switches:

- Group-level GUI configuration for organizations who have multiple configuration strategies
- Configuration changes are pushed to the controller via SSH with no reboot required.
- AirWave understands ArubaOS license dependencies.
- You can provision thin APs from the **APs/Devices > Manage** page. You can move APs into Aruba AP Groups from the **Modify Devices** option on the **APs/Devices > List** page.
- You can configure AP names as **AP Overrides**.
- Values for specific fields can be overwritten for individual switches on the switch's **APs/Devices > Manage** page.

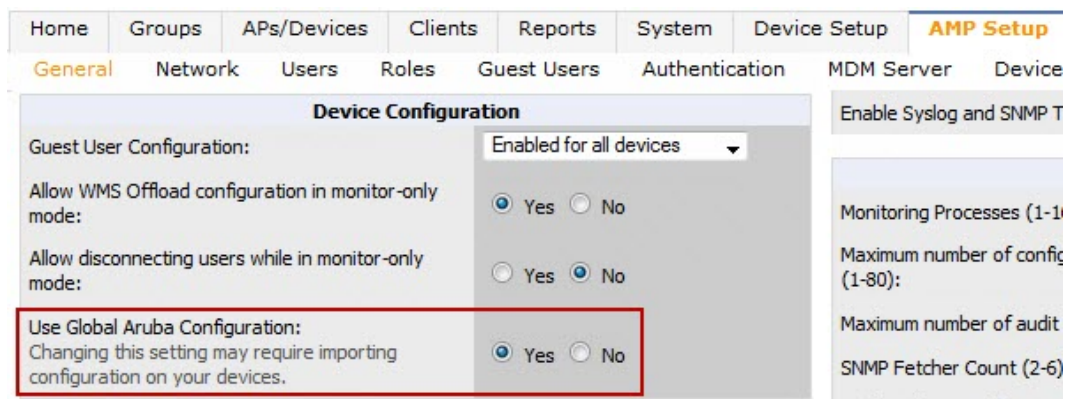
Changes to dependency between the AMP group and folders help customers who want to use the folder structure to manage configuration; however, users will be able to see (but not access) group and folder paths for which they do not have permissions.

For more detailed information about this feature, as well as steps to transition from template-based configuration to web-based configuration, refer to additional chapters in this user guide. For known issues and details on the ArubaOS version supported by each release, refer to the AirWave Release Notes .

## Overview of Switch Configuration in AirWave

AMP can be set up on **AMP Setup > General > Device Configuration** to configure Aruba switches by Device Group on the **Groups > Switch Config** page. Global Configuration is enabled by default, as shown in the following image.

**Figure 1** AMP Setup > General Setting for Global for Group Configuration



AMP supports Aruba Configuration with the following pages:

- "[Groups > Switch Config when Global Configuration is Disabled](#)" on [page 8](#)— this page modifies or reboots all devices when Global Aruba Configuration is disabled.
- "[APs/Devices > Manage Page](#)" on [page 9](#)—supports device-level settings and changes in AMP.
- "[APs/Devices > Monitor Page](#)" on [page 10](#)—supports device-level monitoring in AMP.
- "[APs/Devices > Audit Page](#)" on [page 10](#)—supports device level configuration importing in AMP.

## Groups > Switch Config when Global Configuration is Disabled

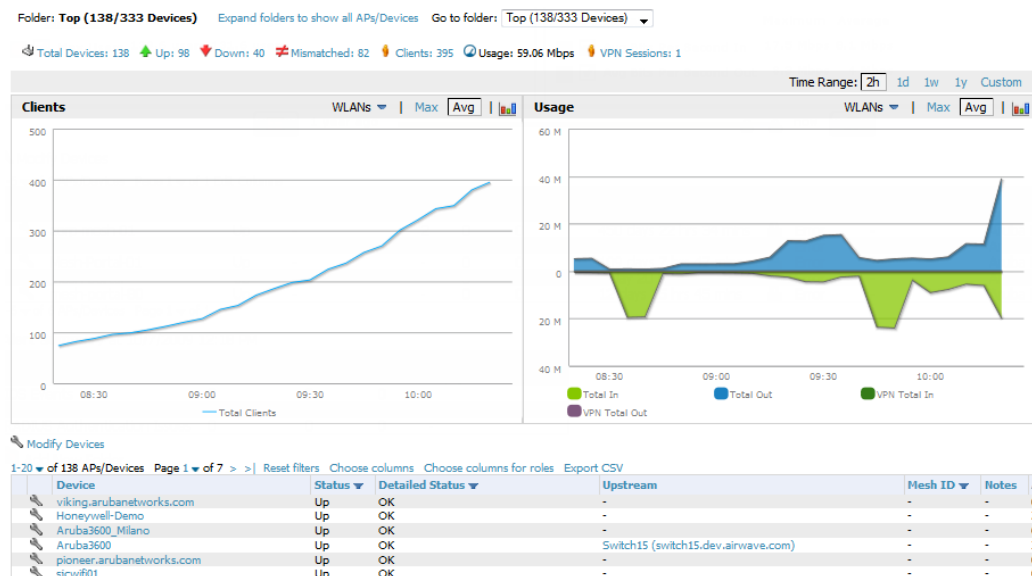
If **Use Global Aruba Configuration** in **AMP Setup > General** is set to **No**, the **Groups > Switch Config** page can be used to manage two or more distinctive configuration strategies. Each of the sections is explained in "[Switch Configuration Reference](#)" on [page 21](#).



## APs/Devices > List Page

This page supports devices in all of AMP. This page supports switch reboot, re-provisioning, changing Aruba AP groups, and updating thin AP settings. Select **Modify Devices** below the graphs to perform these tasks and more.

**Figure 2** APs/Devices List page illustration (Partial Display)



## APs/Devices > Manage Page

This page configures device-level settings, including **Manage** mode, that enable pushing configurations to switches. For additional information, refer to "Pushing Device Configurations to Switches" on page 15.

You can create switch overrides for entire profiles or a specific profile setting per profile. This allows you to avoid creating new profiles or Aruba AP Groups that differ by one more settings. Switch overrides can be added from the switch's **APs/Devices > Manage** page. Figure 3 illustrates an **APs/Devices > Manage** page with switch overrides.

**Figure 3** APs/Devices > Manage page illustration (partial display)

The screenshot shows the 'APs/Devices > Manage' page for a device named 'alpo.arubanetworks.com'. The page is divided into several sections: 'General', 'Settings', 'Notes', and 'Device Communication'. The 'General' section includes fields for Name, Status (Up (OK)), Configuration (Mismatched), Last Contacted (6/17/2013 10:26 AM), Type (Aruba 3500), Firmware (6.3.0.0), Group (Aruba HQ), Folder (Top), and Management Mode (Monitor Only + Firmware Upgrades). The 'Settings' section includes fields for Name (10.11.1.10), Location (1344-1 Rack 28), Contact, Latitude, Longitude, Altitude (m), Group (Aruba HQ), Folder (Top), Auto Detect Upstream Device (Yes), and Upstream device will automatically be updated when the device is polled. The 'Notes' section is empty. The 'Device Communication' section includes fields for IP Address (10.11.0.10), SNMP Port (1-65535) (161), and SSH Port (1-65535) (22). A red box highlights the 'Aruba Overrides' section, which contains a table for switch overrides. The table has columns for Profile, Instance, Field, and Value. The first row shows '802.1X Authentication Profile' with Instance 'voip', Field 'Dynamic WEP Key Size', and Value '40'.

Profile	Instance	Field	Value
802.1X Authentication Profile	voip	Dynamic WEP Key Size	40

## APs/Devices > Monitor Page

Used in conjunction with the **Manage** page, the **Monitor** page enables review of device-level settings. This page is large and often contains a great amount of information, including the following sections:

- Status information
- Switch's License link
- Radio Statistics of some Aruba thin APs
- User and Bandwidth interactive graphs
- CPU Utilization and Memory Utilization interactive graphs
- APs Managed by this switch list (when viewing a switch)
- Alert Summary
- Recent Events
- Audit Log

For additional information, refer to ["Pushing Device Configurations to Switches" on page 15](#).

## APs/Devices > Audit Page

The **APs/Devices > Audit** page is used to view the configuration status of a device. You can also perform the following tasks:

- Audit a device's current configuration
- Update group settings based on the device's current configuration using the **Import** button
- Customize settings to include/ignore during configuration audits
- View any mismatches

## Additional Concepts and Components

Aruba Configuration emphasizes the following components and network management concepts.

- ["Save, Save and Apply, and Revert Buttons" on page 10](#)
- ["Additional Concepts and Benefits" on page 11](#)

### Save, Save and Apply, and Revert Buttons

Several **Add** or **Detail** pages in Aruba Configuration include the **Save**, **Save and Apply**, and **Revert** buttons. These buttons function as follows:

- **Save** —This button saves a configuration but does not apply it, allowing you to return to complete or apply the configuration at a later time. If you use this button, you may see the following alert on other Aruba Configuration pages. You can apply the configuration when all changes are complete at a later time.

**Figure 4** *Unapplied Configuration Changes Message*

Note: You have unapplied Aruba Configuration changes. You must click 'Save and Apply' to make them take effect.

- **Save and Apply** —This button saves and applies the configuration with reference to Manage and Monitor modes. For example, you must click **Save and Apply** for a configuration profile to propagate to all switches in **Manage** mode. If you have switches in **Monitor Only** mode, AMP audits them, comparing their current configuration with the new desired configuration. For additional information and instructions about using **Manage** and **Monitor Only** modes, refer to ["Pushing Device Configurations to Switches" on page 15](#).
- **Revert**—This button cancels out of a new configuration or reverts back to the last saved configuration.

## Additional Concepts and Benefits

### Scheduling Configuration Changes

You can schedule deployment of Aruba Configuration to minimize impact on network performance.

For example, configuration changes can be accumulated over time by using **Save and Apply** for devices in **Monitor Only** mode, then pushing all configuration changes at one time by putting devices in **Manage** mode. Refer to "[Pushing Device Configurations to Switches](#)" on page 15.



---

If your controllers are already in Manage mode, you can also schedule the application of a single set of changes when clicking **Save and Apply**; just enter the date/time under **Scheduling Options** and click **Schedule**.

---

AMP pushes configuration settings that are defined in the GUI to the Aruba controllers as a set of CLI commands using Secure Shell (SSH). No controller reboot is required.

### Auditing and Reviewing Configurations

AMP supports auditing or reviewing in these ways:

1. You can review the ArubaOS running configuration file. This is configuration information that AMP reads from the device. In template-based configuration, you can review the running configuration file when working on a related template.
2. You can use the **APs/Devices > Audit** page for device-specific auditing.
3. Once you audit your controller, you can click **Import** from the **APs/Devices > Audit** page to import the controller's current settings into its AMP Group's desired settings.

### Licensing and Dependencies in Aruba Configuration

You can review your current licensing status with the **Licenses** link on the **APs/Devices > Monitor** page.

AMP requires that you have a policy enforcement firewall license always installed on all Aruba controllers. If you push a policy to a controller without this license, a **Good** configuration will not result, and the controller will show as **Mismatched** on AMP pages that reflect device configuration status.

Aruba Configuration includes several settings or functions that are dependent on special licenses. The user interface conveys that a special license is required for any such setting, function, or profile. AMP does not push such configurations when a license related to those configurations is unavailable. For details on the licenses required by a specific version of ArubaOS, refer to the *ArubaOS User Guide* for that release.

## Preparing AMP for Switch Config

The **Switch Config** tab is available for groups that include a Mobility Access Switch (MAS) running 7.2.0.0 or newer firmware. On the **AMP Setup > General** page, disable the **Use Global Aruba Configuration** option. Global configuration for switches is not available, so the **Groups > Switch Config** page will display only if this option is disabled.

**Figure 5** *Groups > Switch Config*

The screenshot shows the AirWave 7.7 web interface. The top navigation bar includes tabs for Home, Groups (selected), APs/Devices, Clients, Reports, System, Device Setup, AMP Setup, RAPIDS, and VisualRF. Below this is a sub-navigation bar with List, Monitor, Basic, Controller Config, Switch Config (selected), and Firmware.

The left sidebar shows a tree view under 'Security & Authentication' with options like AAA Profile, 802.1x, MAC, Captive Portal, Wired, Management, ACL, Network Aliases, Server Groups, TACACS Accounting, User Roles, User Derivation Rules, Advanced, and Management Password Policy.

The main content area is titled 'Group: Aruba S2500'. It features an 'Add' button for 'New AAA Profile'. Below this is a table of AAA profiles:

1-3 of 3 AAA Profiles Page 1 of 1 Choose columns Export CSV							
	Name	Gigabitethernet	VLAN	Wired Auth	Used By Interface	User Rules	Controller
<input type="checkbox"/>	default	-	-	-	-	-	-
<input type="checkbox"/>	default-dot1x	-	-	-	-	-	-
<input type="checkbox"/>	default-mac-auth	-	-	-	-	-	-

Below the table, it says '1-3 of 3 AAA Profiles Page 1 of 1' and 'Select All - Unselect All'. There is also a 'Delete' button.

## Minimum Configuration

AMP will be able to communicate with your MAS device if you configure the switch using the QuickStart Wizard from the CLI. (Refer to the *ArubaOS User Guide* for more information.)

Refer to the *AirWave 7.7 Quick Start Guide* for instructions on how to configure your device manually. At a minimum, you must set the following options before AMP can be used to monitor your switch:

- System Name
- Management VLAN
- Interface IP
- Management Interface VLAN Subnet Mask
- Management Interface Subnet Mask
- IP Default Gateway
- Country Code
- Time Zone
- Time
- Date
- Admin login and password
- Enable password

## Keeping Controllers and Switches in Separate Groups

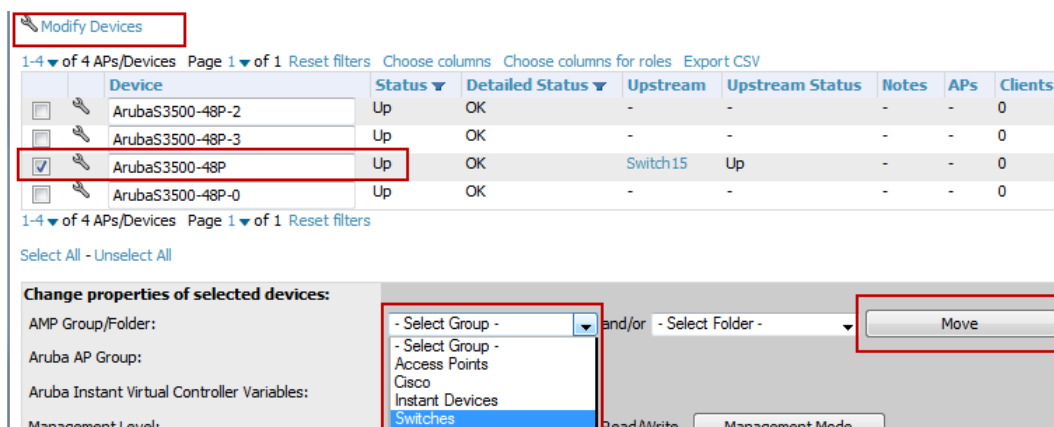
Although it is possible for switches and controllers to reside in the same group, a best practice to keep these separated. With switches and controllers residing under separate groups, users will not mismatches on their switches that are the direct result of controller configurations.

Perform the following steps if you currently keep controllers and switches in the same group.

1. Back up your AMP. Information about backing up AMP is available in the *AirWave 7.7 User Guide* in the "Performing Daily Operations in AMP" chapter.
2. Navigate to the **Groups** page and click **Add New Group**.

3. Provide an appropriate name for the new group. For example, if you are going to move switches from a "Building1" folder, then consider naming this group "Building1 Switches."
4. Review the settings on the **Basic** tab and change any options/setting if necessary. In most cases, the default settings are appropriate. (Refer to the "Configuring and Using Device Groups" section in the *AirWave 7.7 User Guide* for more information.)
5. Navigate back to the **Groups** page, and select the group that currently includes both controllers and switches.
6. Click **Modify Devices**.
7. Select the check box beside each of your switches.
8. Scroll down to the edit form. In the **AMP Group/Folder** section, click on the **Select Group** drop down menu. Select your newly created switch group, and click **Move**.

**Figure 6** Moving switches to a new group



9. On the Confirm Changes page, click **Apply Changes Now** to make the move immediately, or schedule a time to apply the changes.



If the **Switch Config** page does not display, and the **Controller Config** page is still an available navigation item, perform an audit of your switches and then import the settings. The **Switch Config** page will be available after a switch is added to the group, and its configuration is successfully imported.

10. Repeat the above steps for all groups that include both controllers and switches.

## Importing Profiles for Switch Config

The Controller Config page is available by default for existing AMP customers who upgrade to 7.7, Please perform the following steps to import switching profiles.

1. Navigate to the **Groups** page and select the group that includes your switches. Be sure that this group does not also include controllers. If it does, then the switches must first be moved to a separate group.
2. On the **Monitor** page, click on **Modify Devices**.
3. Select your existing switches. Be sure that the configuration status is not "Mismatched." Refer to the *AirWave 7.7 Quick Start Guide* for information on how to resolve mismatches.
4. Click the **Import Settings** button. This import will enable the Switch Config page and populates the page with existing profiles.



This section presents common tasks or concepts after initial setup of Aruba Configuration is complete, as described in the section ["Preparing AMP for Switch Config " on page 11](#). This chapter emphasizes frequent procedures as follows:

- ["Pushing Device Configurations to Switches" on page 15](#)
- ["Supporting APs with Switch Configuration" on page 15](#)
- ["Visibility in Switch Configuration" on page 16](#)
- ["Using AMP to Deploy Aruba APs" on page 16](#)



---

For a complete reference on all Configuration pages, field descriptions, and certain additional procedures that are more specialized, refer to ["Switch Configuration Reference" on page 21](#).

---

## Pushing Device Configurations to Switches

When you add or edit device configurations, you can push device configurations to switches as follows:

- Make device changes on the **Switch Config** page and click **Save and Apply**.

A device must be in Manage mode to push configurations in this way.



---

If you click **Save and Apply** when a device is in Monitor mode, this initiates a verification process in which AMP advises you of the latest mismatches. Mismatches are viewable from the **APs/Devices > Mismatched** page. Additional **Audit** and **Group** pages list mismatched statuses for devices.

---

Normally, devices are in Monitor mode. It may be advisable in some circumstances to accumulate several configuration changes in Monitor mode prior to pushing an entire set of changes to switches. Follow these general steps when implementing configuration changes for devices in Monitor mode:

1. Make all device changes using the **Switch Config** pages. Click **Save and Apply** as you complete device-level changes. This builds an inventory of pending configuration changes that have not been pushed to the controller and APs.
2. Review the entire set of newly mismatched devices on the **APs/Devices > Mismatched** page.
3. For each mismatched device, navigate to the **APs/Devices > Audit** page to audit recent configuration changes as desired.
4. Once all mismatched device configurations are verified to be correct from the **APs/Devices > Audit** page, use the **Modify Devices** link on the **Groups > Monitor** page to place these devices into Manage mode. This instructs AMP to push the device configurations to the switch.
5. As desired, return devices to Monitor mode until the next set of configuration changes is ready to push to switches.

## Supporting APs with Switch Configuration

### AP Overrides Guidelines

The **AP Override** component of Switch Configuration operates with the following principles:

- AP devices function within groups that define operational parameters for groups of APs. This is standard across all of AMP.

- **AP Overrides** allow you to change some parameters of any given AP without having to remove that AP from the configuration group in which it operates.
- The name of any **AP Override** that you create should be the same as the name of the AP device to which it applies. This establishes the basis of all linking to that AP device.
- Once you have created an **AP Override**, you select the devices to which it applies.
- You can also exclude mesh clusters from the **AP Override**.

In summary, the **AP Override** feature prevents you from having to create a new AP group for customized APs that otherwise share parameters with other APs in a group. **AP Override** allows you to have less total AP groups than you might otherwise require.

## Visibility in Switch Configuration

### Visibility Overview

Switch Configuration supports device configuration and user information in the following ways:

- User roles
- AP/Device access level
- Folders (in *global* configuration)

Additional factors for visibility are as follows:

- Administrative and Management users in AMP can view the **Switch Config** page and the **APs/Devices > Manage** pages.
  - Administrative users are enabled to view all configurations.
  - Management users have access to all profiles for their respective folders.
- Switch Configuration entails specific user role and security profiles that define some components of visibility, as follows:
  - ["Security and Authentication" on page 21](#)
  - ["Security and Authentication > User Roles" on page 29](#)
- AMP continues to support the standard operation of folders, users, and user roles as described in the *AirWave 7.7 User Guide*.

### Using AMP to Deploy Aruba APs

In addition to migrating Aruba access points (APs) from ArubaOS-oriented administration to AMP administration, you can use AMP to deploy Aruba APs for the first time without separate ArubaOS configuration. Be aware of the following dynamics in this scenario:

- AMP can manage all network management functions, including:
  - the first-time provisioning of Aruba APs
  - managing Aruba switches with AMP
- In this scenario, when a new Aruba AP boots up, AMP may discover the AP before you have a chance to configure and launch it through ArubaOS configuration on the switch. In this case, the AP appears in AMP with a device name based on the MAC address.
- When you provision the AP through the Aruba switch and then rename the AP, the new AP name is *not* updated in AMP.

An efficient and robust approach to update an Aruba AP device name is to deploy Aruba APs in AMP with the following steps:



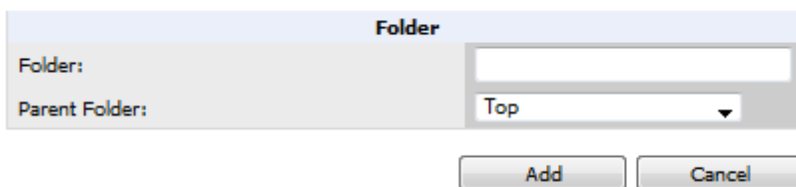
1. Define communication settings for Aruba APs pending discovery in the **Device Setup > Communication** page. This assigns communication settings to multiple devices at the time of discovery, and prevents having to define such settings manually for each device after discovery.
2. Discover new APs with AMP. You can do so with the **Device Setup > Discover** page.
3. Click **New Devices** In the **Status** section at the top of any AMP page, or navigate to the **APs/Devices > New** page.
4. Select (check) the box next to any AP you want to provision.
5. Rename all new APs. Type in the new device name in the **Device** column.
6. Scroll to the bottom of the page and put APs in the appropriate AMP group and folder. Set the devices to **Manage Read/Write** mode.
7. Click **Add**. Wait approximately five to 10 minutes. You can observe that the APs have been renamed not only in AMP but also on the switch.

## Defining Visibility for Aruba Configuration

Perform these steps to define or adjust visibility for users to manage and support Aruba Configuration:

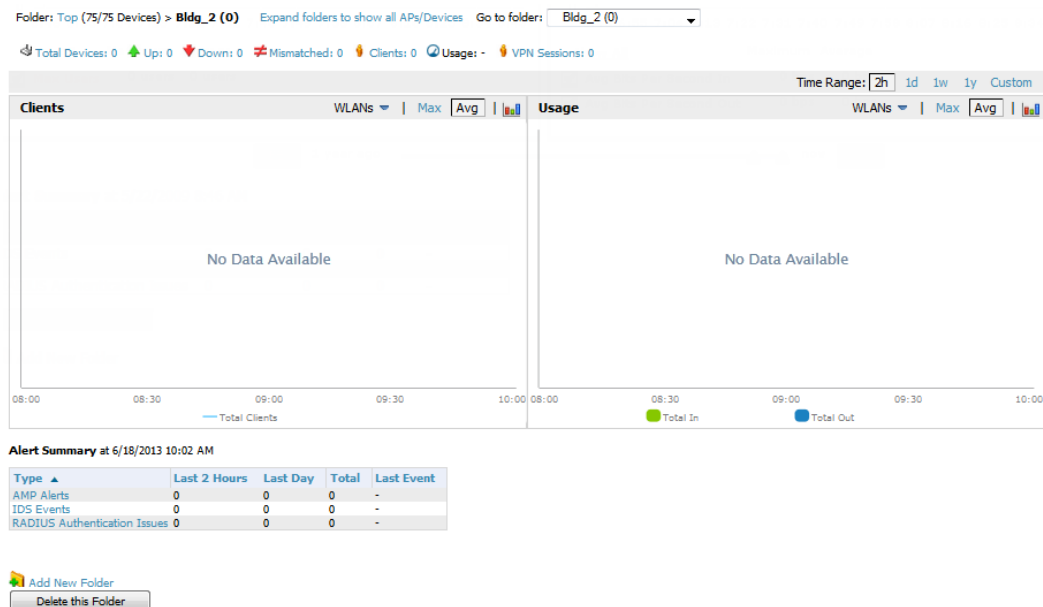
1. As required, create a new AMP device folder with management access.
  - a. Navigate to the **APs/Device > List** page, scroll to the bottom of the page. (An alternate page supporting new folders is **Users > Connected** page.)
  - b. Click the **Add New Folder** link. The **Folder** detail page appears, as illustrated in [Figure 7](#):

**Figure 7** *APs/Devices > Add New Folder > Folders page illustration*



- c. Click **Add**. The **APs/Devices > List** page reappears. You can view your new folder by selecting it from the **Go to folder** drop-down list at the top right of this page. [Figure 8](#) illustrates an unpopulated device page for an example folder.

**Figure 8** *APs/Devices > List Page with no devices*



2. Add Aruba controller devices to that folder as required. Use the **Device Setup > Add** page following instructions available in the *AirWave 7.7 User Guide*.
3. As required, create or edit a user role that is to have rights and manage privileges required to support their function in Aruba Configuration.
  - a. At least one user must have administrative privileges, but several additional users may be required with less rights and visibility to support Aruba Configuration without access to the most sensitive information, such as SSIDs or other security related data.
  - b. Navigate to the **AMP Setup > Roles** page, and click **Add New Role** to create a new role with appropriate rights, or click the **pencil** (manage) icon next to an existing role to adjust rights as required. The Role page appears, illustrated in [Figure 9](#).

**Figure 9** AMP Setup > Roles > Add/Edit Role Page Illustration

**Role**

Name:

Enabled: ☒ Yes ☐ No

Type:  ▼

AP/Device Access Level:  ▼

Top Folder:  ▼

RAPIDS:  ▼

VisualRF:  ▼

Aruba Controller Role:  ▼

Display client diagnostics screens by default: ☐ Yes ☒ No

Allow user to disable timeout: ☐ Yes ☒ No

**Guest User Preferences**

Allow creation of Guest Users: ☒ Yes ☐ No

Allow accounts with no expiration: ☒ Yes ☐ No

Allow sponsor to change sponsorship username: ☐ Yes ☒ No

Custom Message:

- c. As per standard AMP configuration, complete the settings on this page. The most important fields with regard to Aruba Configuration, device visibility and user rights are as follows:
  - **Type**—Specify the type of user. Important consideration should be given to whether the user is an administrative user with universal access, or an AP/Device manager to specialize in device administration, or additional users with differing rights and access.
  - **AP/Device Access Level**—Define the access level that this user is to have in support of Aruba controller, devices, and general Aruba Configuration operations.
  - **Top Folder**—Specify the folder created earlier in this procedure, or specify the Top folder for an administrative user.
- d. Click **Add** to complete the role creation, or click **Save** to retain changes to an existing role. The **AMP Setup** page now displays the new or revised role.
4. As required, add or edit one or more users to manage and support Aruba Configuration. This step creates or edits users to have rights appropriate to Aruba Configuration. This user inherits visibility to Aruba controllers and Aruba Configuration data based on the role and device folder created earlier in this procedure.
  - a. Navigate to the **AMP Setup> User** page.
  - b. Click **Add New User**, or click the **pencil** (manage) icon next to an existing user to edit that user.
  - c. Select the user role created with the prior step, and complete the remainder of this page as per standard AMP configuration. Refer to the *AirWave 7.7 User Guide* as required.
5. Observe visibility created or edited with this procedure.

The user, role, and device folder created with this procedure are now available to configure, manage, and support Aruba Configuration and associated devices according to the visibility defined in this procedure. Any component of this setup can be adjusted or revised by referring to the steps and AMP pages in this procedure.
6. Add or discover devices for the device folder defined during step 1 of this procedure. Information about devices is available in the *AirWave 7.7 User Guide*.

7. Continue to other elements of Switch Configuration described in the Reference section of this document.

## Overview

This section describes the pages and inter-dependencies of Switch Configuration profiles. This document should be used along side the Mobility Access Switch documentation. For architectural information about ArubaOS, refer to the *ArubaOS User Guide* for your Mobility Access Switch. For field-level information about the options within this page, refer to the *ArubaOS Command Line Interface Guide* for your Mobility Access Switch.



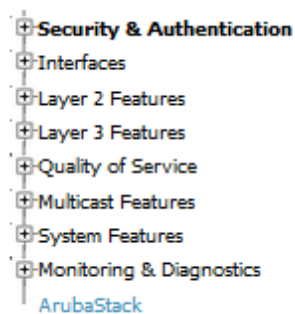
---

The default values of profile parameters or functions may differ slightly between ArubaOS releases.

---

To access the pages described in this section, select the appropriate Switch Group from the **Groups** page, and then navigate to the **Groups > Switch Config**.

**Figure 10** *Switch Configuration Components*



This section describes Switch Configuration components with the following organization and topics:

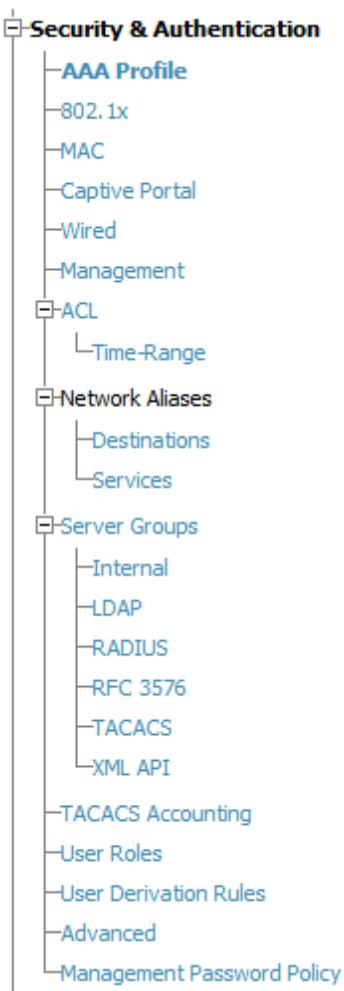
- "Security and Authentication" on page 21
- "Interfaces" on page 32
- "Layer 2 Features" on page 38
- "Layer 3 Features" on page 45
- "Quality of Service Profile" on page 47
- "Multicast Features" on page 49
- "System Features" on page 52
- "Monitoring and Diagnostics" on page 54
- "ArubaStack" on page 57

## Security and Authentication

Switch Configuration supports user roles, policies, server groups, and additional security parameters with profiles that define security and authentication settings for the WLAN users, including the role for unauthenticated users and the different roles that should be assigned to users authenticated via 802.1x, MAC, or SIP authentication.

To view and configure Security and Authentication profiles, click the **Security & Authentication** profile heading in the navigation pane. [Figure 11](#) illustrates this page.

**Figure 11** *Switch Config > Security & Authentication navigation*



## Security and Authentication > AAA Profile

Perform these steps to configure a AAA profile.

1. Select **Security & Authentication > AAA Profile** in the navigation pane.
2. Select the **Add** button to create a new AAA profile, or click the **pencil** icon next to an existing profile to edit.
3. Configure the settings for the AAA profile.
4. Select **Add** or **Save**. The added or edited **AAA** profile appears on the **AAA Profiles** page.

### Refer to

- Refer to the AAA Authentication chapter in the *ArubaOS User Guide* for more information about AAA profiles.
- Refer to the "aaa profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > 802.1X Auth

802.1X authentication consists of three components:

- The *supplicant*, or *client*, is the device attempting to gain access to the network. You can configure the Aruba user-centric network to support 802.1X authentication for wired users as well as wireless users.

- The *authenticator* is the gatekeeper to the network and permits or denies access to the supplicants. The Aruba controller acts as the authenticator, relaying information between the authentication server and supplicant. The EAP type must be consistent between the authentication server and supplicant and is transparent to the controller.
- The *authentication server* provides a database of information required for authentication and informs the authenticator to deny or permit access to the supplicant.

The 802.1X authentication server is typically an EAP-compliant Remote Access Dial-In User Service (RADIUS) server which can authenticate either users (through passwords or certificates) or the client computer.

An example of an 802.1X authentication server is the Internet Authentication Service (IAS) in Windows. (See <http://technet2.microsoft.com/windowsserver/en/technologies/ias.mspix>.)

In Aruba user-centric networks, you can terminate the 802.1X authentication on the controller. The controller passes user authentication to its internal database or to a backend non-802.1X server. This feature, also called AAA FastConnect, is useful for deployments where an 802.1X EAP-compliant RADIUS server is not available or required for authentication.

Perform these steps to configure an 802.1X Auth profile.

1. Select **Security & Authentication > 802.1X Auth** in the navigation pane. The details page summarizes the current profiles of this type.
2. Select the **Add** button to create a new 802.1X Auth profile, or click the **pencil** icon next to an existing profile to edit.
3. Configure the settings for 802.1X authentication.
4. Select **Add** or **Save**. The added or edited 802.1X Auth profile appears on the **802.1x** page.

#### Refer to

- Refer to the 802.1X Authentication chapter in the *ArubaOS User Guide* for more information about AAA profiles.
- Refer to the "aaa authentication dot1x" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > MAC

Before configuring MAC-based authentication, you must configure the following:

- The user role that will be assigned as the default role for the MAC-based authenticated clients. You configure the default user role for MAC-based authentication in the AAA profile. If derivation rules exist or if the client configuration in the internal database has a role assignment, these values take precedence over the default user role.
- Authentication server group that the controller uses to validate the clients. The internal database can be used to configure the clients for MAC-based authentication.

Perform these steps to configure a MAC authentication profile.

1. Select **Security & Authentication > MAC** in the navigation pane.
2. Select the **Add** button to create a new MAC authentication profile, or click the **pencil** icon next to an existing profile to edit.
3. Configure the settings for MAC authentication.
4. Select **Add** or **Save**. The added or edited MAC authentication profile appears on the **MAC** details page.

#### Refer to

- Refer to the MAC-Based Authentication chapter in the *ArubaOS User Guide* for more information about AAA profiles.
- Refer to the "aaa authentication mac" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > Captive Portal

You can configure captive portal for guest users where no authentication is required, or for registered users who must be authenticated against an external authentication server or the Mobility Access Switch's internal user database.

The captive portal authentication profile specifies the captive portal login page and other configurable parameters. The initial user role configuration must include the applicable captive portal authentication profile instance. Therefore, you need to modify the guest-logon user role configuration to include the guestnet captive portal authentication profile.

Perform these steps to configure a Captive Portal Authentication profile.

1. Select **Security & Authentication > Captive Portal** page.
2. Select the **Add** button to create a new Captive Portal authentication profile, or click the **pencil** icon next to an existing profile to edit.
3. Configure the settings for Captive Portal authentication.
4. Select **Add** or **Save**. The added or edited Captive Portal Auth profile appears on the **Captive Portal** page.

### Refer to

- Refer to the Captive Portal chapter in the *ArubaOS User Guide* for more information about Captive Portal profiles.
- Refer to the "aaa authentication captive-portal" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > Wired Auth

This profile type references a profile to be used for wired authentication. Navigate to the **Security & Authentication > Wired** page. Select an AAA profile from the drop-down box to change the profile to a currently available option, or select the plus symbol to create a new AAA profile.

### Refer to

- Refer to the AAA Authentication chapter in the *ArubaOS User Guide* for more information about wired authentication.
- Refer to the "aaa authentication wired" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > Management

Users who need to access the controller to monitor, manage, or configure the Aruba user-centric network can be authenticated with RADIUS, TACACS+, or LDAP servers or the internal database.

Perform these steps to configure a Management authentication profile.

1. Select **Security & Authentication > Management** in the Switch Config navigation pane.
2. Complete the settings as described in [Table 1](#):

**Table 1:** *Security & Authentication > Management Auth Profile Settings*

Field	Default	Description
Referenced Profiles		
Server Group		Select the AAA authentication server group. Select the pencil icon to edit an existing server group or click the add (+) icon to create a new server group.
Other Settings		



Field	Default	Description
Default Role	root	<p>The role to be associated with this authentication profile:</p> <ul style="list-style-type: none"> <li>• <b>guest-provisioning</b>: Allows the user to create guest accounts.</li> <li>• <b>location-api-mgmt</b>: Permits access to location API information. You can log in, however, you cannot use any commands.</li> <li>• <b>network-operations</b>: Permits access to Monitoring, Reports, and Events pages in the WebUI. You can log in; however, you can only use a subset of commands to monitor the controller.</li> <li>• <b>no-access</b>: Indicates that no access is available.</li> <li>• <b>read-only</b>: Permits access to monitoring pages only.</li> <li>• <b>root</b>: Permits access to all management functions on the controller.</li> </ul>
Enable	No	When enabled, this setting activates the authentication server.
Mschapv2	No	When enabled, MSCHAPv2 (Microsoft Challenge Authentication Protocol version 2) will be used for authentication. Refer to RFC 2759 for more information about MSCHAPv2.

3. Select **Save**.

## Security and Authentication > Policy/ACL

The **Security & Authentication > ACL** page under Switch Config displays all currently configured policies, including the policy name and the user role that use this policy.

Perform these steps to configure a new Policy/Access Control List.

1. Select **Security & Authentication > ACL** page.
2. Select the **Add** button to create a new policy, or click the **pencil** icon next to an existing policy to edit.
3. Configure the settings for the ACL.
4. Select **Add** or **Save**. The added or edited ACL appears on the **ACL** page.

### Refer to

- Refer to the Roles and Policies chapter in the *ArubaOS User Guide* for more information about Access Control Lists.
- Refer to the "ip access-list" commands in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > ACL > Time Range

A time range profile establishes the boundaries by which users and guest users are to be supported on the network. This is a security and access-related profile, and several time range profiles can be configured to enable absolute or periodic access.

The **Security & Authentication > ACL > Time Range** page displays all time ranges that are currently available configured, time range profile type, the policy that uses time range profiles, and the controller in which each profile is visible.

To create a new time range profile, click the **Add New Time Range** button, or click the pencil icon next to an existing time range profile to adjust settings.

### Refer to

- Refer to the Access Control List chapter in the *ArubaOS User Guide* for more information Time Ranges that are used with policy.
- Refer to the "time-range" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > Network Aliases > Destinations

The **Security & Authentication > Network Aliases > Destinations** page lists the destination name, protocol, and port currently configured, along with the policy and switch that use a configured destination.

To edit an existing destination, click the pencil icon. To create a new destination to be referenced by a security policy, click the **Add New Net Destination** button.

### Refer to

- Refer to the Roles and Policies chapter in the *ArubaOS User Guide* for more information about network destination aliases.
- Refer to the "netdestination" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > Network Aliases > Services

The **Security & Authentication > Network Aliases > Services** page displays all Netservice profiles that are available for reference by Security policies. This page displays Netservice profile names, the protocol associated with it, the policy that uses this Netservice profile, and the folder.

To edit an existing network service, click the pencil icon. To create a new network service to be referenced by a security policy, click the **Add New Netservice** button.

### Refer to

- Refer to the Roles and Policies chapter in the *ArubaOS User Guide* for more information about network aliases.
- Refer to the "netservice" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > Server Groups

### Server Groups Page Overview

The **Server > Server Groups** page displays all server groups currently configured along with the profiles and controllers that are used by each server group:

- AAA
- Captive Portal Auth
- Stateful Kerberos Auth
- Management Auth
- Stateful NTLM Auth
- Stateful 802.1X Auth
- TACACS Accounting
- VIA Auth
- VPN Auth
- WISPr Auth
- Controller

The list of servers in a server group is an ordered list. By default, the first server in the list is always used unless it is unavailable, in which case the next server in the list is used. You can configure the order of servers in the server group. In the Web UI, use the up or down arrows to order the servers (the top server is the first server in the list). In the CLI, use the position parameter to specify the relative order of servers in the list (the lowest value denotes the first server in the list).

The first available server in the list is used for authentication. If the server responds with an authentication failure, there is no further processing for the user or client for which the authentication request failed. You can optionally enable fail-through authentication for the server group so that if the first server in the list returns an authentication deny, the controller attempts authentication with the next server in the ordered list. The controller attempts authentication with each server in the list until either there is a successful authentication or the list of servers in the group is exhausted. This feature is useful in environments where there are multiple, independent authentication servers; users may fail authentication on one server but can be authenticated on another server.

Before enabling fail-through authentication, note the following:

- This feature is not supported for 802.1x authentication with a server group that consists of external EAP compliant RADIUS servers. You can, however, use fail-through authentication when the 802.1x authentication is terminated on the controller (AAA FastConnect).
- Enabling this feature for a large server group list may cause excess processing load on the controller. Best practices are to use server selection based on domain matching whenever possible.
- Certain servers, such as the RSA RADIUS server, lock out the controller if there are multiple authentication failures. Therefore you should not enable fail-through authentication with these servers.

When fail-through authentication is enabled, users that fail authentication on the first server in the server list should be authenticated with the second server.

## Supported Servers

ArubaOS supports the following external authentication servers:

- LDAP (Lightweight Directory Access Protocol)
- RADIUS (Remote Authentication Dial-In User Service)
- RFC 3576
- TACACS+ (Terminal Access Controller Access Control System)
- XML API

Additionally, you can use the controller's internal database to authenticate users. You create entries in the database for users and their passwords and default role.



---

The Switch Config **Security & Authentication > Server Groups** feature does not support Windows server groups.

---

You can create groups of servers for specific types of authentication. For example, you can specify one or more RADIUS servers to be used for 802.1x authentication. The list of servers in a server group is an ordered list. This means that the first server in the list is always used unless it is unavailable, in which case the next server in the list is used. You can configure servers of different types in one group — for example, you can include the internal database as a backup to a RADIUS server.

Server names are unique. You can configure the same server in multiple server groups. You must configure the server before you can add it to a server group.

## Adding a New Server Group

The server group is assigned to the server group for 802.1x authentication.

To create a new server group, click the **Add** button, or to edit an existing group, click the pencil icon next to that group. The **Add New Server Group** page appears.

### Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about server groups.

- Refer to the `"aaa server-group"` command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > Server Groups > Internal

An internal server group configures the internal database with the username, password, and role (student, faculty, or sysadmin) for each user. There is a default internal server group that includes the internal database. For the internal server group, configure a server derivation rule that assigns the role to the authenticated client.

### Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about internal server groups.
- Refer to the `"local-userdb add"` command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > Server Groups > LDAP

You can configure Lightweight Directory Access Protocol (LDAP) servers for use by a server group.

The **Security & Authentication > Server Groups > LDAP** page displays current LDAP servers available for inclusion in server groups. Click **Add** to create a new LDAP server, or click the pencil icon next to an existing LDAP server to edit the configuration.

### Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about LDAP servers.
- Refer to the `"aaa authentication-server ldap"` command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > Server Groups > RADIUS

You can configure RADIUS servers for use by a server group. The **Security & Authentication > Server Groups > RADIUS** page displays current RADIUS servers available for inclusion in server groups. Click **Add** to create a new RADIUS server, or click the pencil icon next to an existing RADIUS server to edit the configuration.

### Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about RADIUS servers.
- Refer to the `"aaa authentication-server radius"` command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security > Server Groups > RFC 3576

RFC 3576 servers support dynamic authorization extensions to Remote Authentication Dial-In User Service (RADIUS). Switch Configuration supports RFC 3576 servers that can be referenced by server groups.

To view currently configured RFC 3576 servers and where they are used, navigate to the **Security & Authentication > Server Groups > RFC 3576** page.

Click **Add** to create a new RFC3576 server, or click the pencil icon next to an existing RFC 3576 server to edit the configuration.

### Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about RFC 3576 servers.
- Refer to the `"aaa rfc-server"` command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > Server Groups > TACACS

You can configure TACACS+ servers for use by a server group. The **Security & Authentication > Server Groups > TACACS** page displays current TACACS servers available for inclusion in server groups. Click **Add** to create a new TACACS server, or click the pencil icon next to an existing TACACS server to edit the configuration.

### Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about TACACS servers.
- Refer to the "aaa authentication-server tacacs" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > Server Groups > XML API

Switch Configuration supports server groups that can include XML API servers. XML API servers send and accept requests for information. XML API servers process such requests and act on these requests by performing requested actions. Such a server also compiles necessary reporting data and sends it back to requesting source.

The **Security & Authentication > Server Groups > XMP API** page lists any XML API servers currently available for use by server groups. From this page, click **Add** to create a new XML API server, or click the pencil icon next to an existing XML API server to edit the configuration.

### Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about XML API servers.
- Refer to the "aaa authentication-server xml-api" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security > TACACS Accounting

TACACS+ accounting allows commands issued on the switch to be reported to TACACS+ servers. You can specify the types of commands that are reported, and these are action, configuration, or show commands. You can have all commands reported as desired. Aruba Configuration supports TACACS Accounting servers that can be referenced by server groups.

To view currently configured TACACS Accounting profiles and where they are used, navigate to the **Security > TACACS Accounting** page. Select **Add** to create a new TACACS Accounting profile, or click the pencil icon to edit an existing profile.

Select **Add** to complete the new TACACS Accounting profile, or click **Save** to complete the editing of an existing profile.

### Refer to

- Refer to the Authentication Servers chapter in the *ArubaOS User Guide* for more information about TACACS Accounting.
- Refer to the "aaa tacacs-accounting server-group" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > User Roles

A client is assigned a user role by one of several methods. A user role assigned by one method may take precedence over a user role assigned by a different method. The methods of assigning user roles are, from lowest to highest precedence:

1. The initial user role for unauthenticated clients is configured in the AAA profile for a virtual AP.
2. The user role can be derived from user attributes upon the client's association with an AP (this is known as a user-derived role). You can configure rules that assign a user role to clients that match a certain set of criteria. For

example, you can configure a rule to assign the role VoIP-Phone to any client that has a MAC address that starts with bytes xx:yy:zz. User-derivation rules are executed before client authentication.

3. The user role can be the default user role configured for an authentication method, such as 802.1x or VPN. For each authentication method, you can configure a default role for clients who are successfully authenticated using that method.
4. The user role can be derived from attributes returned by the authentication server and certain client attributes (this is known as a server-derived role). If the client is authenticated via an authentication server, the user role for the client can be based on one or more attributes returned by the server during authentication, or on client attributes such as SSID (even if the attribute is not returned by the server). Server-derivation rules are executed after client authentication.
5. The user role can be derived from Aruba Vendor-Specific Attributes (VSA) for RADIUS server authentication. A role derived from an Aruba VSA takes precedence over any other user roles.

In the Aruba user-centric network, the user role of a wireless client determines its privileges, including the priority that every type of traffic to or from the client receives in the wireless network. Thus, QoS for voice applications is configured when you configure firewall roles and policies.

In an Aruba system, you can configure roles for clients that use mostly data traffic, such as laptop computers, and roles for clients that use mostly voice traffic, such as VoIP phones. Although there are different ways for a client to derive a user role, in most cases the clients using data traffic will be assigned a role after they are authenticated through a method such as 802.1x, VPN, or captive portal. The user role for VoIP phones can be derived from the OUI of their MAC addresses or the SSID to which they associate. This user role will typically be configured to have access allowed only for the voice protocol being used (for example, SIP or SVP).



---

You must install the Policy Enforcement Firewall license in the switch.

---

This page displays the current user roles in Switch Config and where they are used.

Select **Add** to complete the configuration of the **User Role**, or click **Save** to complete the editing of an existing role. The new role appears on the **Security and Authentication > User Roles** page.

#### Refer to

- Refer to the Roles and Policies chapter in the *ArubaOS User Guide* for more information about Roles.
- Refer to the "user-role" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

### Security and Authentication > User Derivation Rules

The user role is a user derivation profile. User Rules can be derived from attributes from the client's association with an AP. For VoIP phones, you can configure the devices to be placed in their user role based on the SSID or the Organizational Unit Identifier (OUI) of the client's MAC address.

Navigate to the **Security & Authentication > User Derivation Rules** page in the Aruba Configuration navigation pane. This page displays user rules that are currently configured and the AAA profile that references these rules.

To add a new user rule, which is a derivation profile, click the **Add New User Derivation Profile** button. To edit an existing user rule, click the pencil icon next to an existing rule.

#### Refer to

- Refer to the Roles and Policies chapter in the *ArubaOS User Guide* for more information about User-Derived roles.
- Refer to the "aaa derivation-rules" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Security and Authentication > Advanced Authentication

In Advanced Authentication, you can apply timers and DNS query intervals. Follow these steps to configure an Advanced Authentication profile.

1. Select **Security & Authentication > Advanced** in the navigation pane. The details page summarizes the current profiles of this type.
2. Complete the settings as described in [Table 2](#):

**Table 2:** *Security & Authentication > Advanced Profile Settings*

Field	Default	Description
<b>Authentication Timers</b>		
User Idle Timeout (30-15300 sec)	300 seconds	Maximum period, in seconds, after which a client is considered idle if there is no user traffic from the client. The timeout period is reset if there is a user traffic. After this timeout period has elapsed, the controller sends probe packets to the client; if the client responds to the probe, it is considered active and the User Idle Timeout is reset (an active client that is not initiating new sessions is not removed). If the client does not respond to the probe, it is removed from the system. Range: 30 to 15300 seconds
User Stats Timeout (300-600 sec)	600 sec	Set the timeout value for user stats reporting in seconds. The supported range is 300-600 seconds, or 5-10 minutes, and the default value is 600 seconds. Requires a minimum version of 6.1.0.0.
Poll user stats (60-600)		Specify a the frequency with which user stats are polled. An empty value indicates that polling will not occur.
Dead Time for down Authentication Server (0-60 min)	10 minutes	Maximum period, in minutes, that the controller considers an unresponsive authentication server to be out of service. This timer is only applicable if there are two or more authentication servers configured on the controller. If there is only one authentication server configured, the server is never considered out of service and all requests are sent to the server. If one or more backup servers are configured and a server is unresponsive, it is marked as out of service for the dead time; subsequent requests are sent to the next server on the priority list for the duration of the dead time. If the server is responsive after the dead time has elapsed, it can take over servicing requests from a lower-priority server; if the server continues to be unresponsive, it is marked as down for the dead time. Range: 0-60 minutes
Unauthenticated User Lifetime (0-255 min)	5 minutes	Maximum time, in minutes, unauthenticated clients are allowed to remain logged on. Range: 0-255 minutes
<b>RADIUS Attributes</b>		
Attribute Name	blank	Specify the name for this new Radius attribute.
Attribute Value	blank	Enter an integer value for a the Radius attribute.
Attribute type	date	Specify one of the following types to be associated with this attribute: <ul style="list-style-type: none"><li>• date</li><li>• integer</li></ul>

Field	Default	Description
		<ul style="list-style-type: none"> <li>• ipaddr</li> <li>• string</li> </ul>
Vendor Name	blank	Enter the name of the vendor associated with this attribute.
Vendor Id	blank	Enter an integer value for the vendor ID associated with this attribute.

3. Select **Add** or **Save**. The added or edited profile appears on the **Advanced** page.

## Security and Authentication > Management Password Policy

On Aruba Mobility Access Switches, the password for a new management user by default has no requirements other than a minimum length of 6 alphanumeric or special characters. Using the **Security & Authentication > Management Password Policy** page, you can configure a password policy that sets requirements for management user passwords.

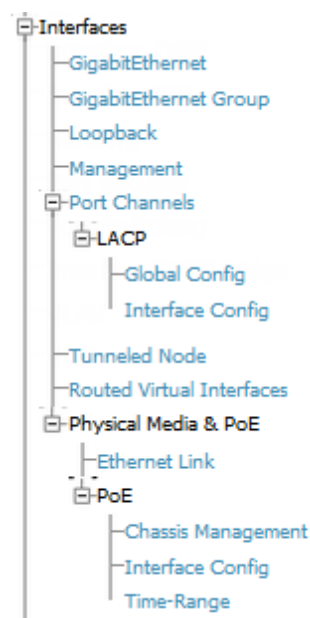
### Refer to

- Refer to the Management Access chapter in the *ArubaOS User Guide* for more information.
- Refer to the "aaa password-policy mgmt" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Interfaces

Switch Configuration supports a variety of profiles that can be associated with Interfaces. Refer to the **Interfaces** portion of the navigation pane on the **Switch Config** page, as illustrated in [Figure 12](#):

**Figure 12** *Interfaces Components in Switch Config*



This sections that follow describes the profiles for all Interface components in **Switch Config**.

### Gigabit Ethernet Interface

The Mobility Access Switch supports 24 or 48 port gigabit Ethernet interfaces of 10/100/1000 Mbps speeds.



A network gigabit Ethernet interface is referred by its <slot>/<module>/<port>.

- Slot—The member ID of the stack.
- Module—There are two modules where the first one is the front-panel network module (0), while the other one is the uplink network module (1).
- Port—The individual port number.

For example, interface gigabitethernet 0/0/20 refers to the first stack member (0) on the front-panel network module (0) at port number (20).



---

Mobility Access Switch also supports four 10-Gigabit Ethernet interfaces for stacking and uplink purposes. Refer to the Hardware Installation Guide for more information on the 10-Gigabit Ethernet uplink module.

---

1. To configure a Gigabit Ethernet interface, navigate to the **Interfaces > GigabitEthernet** page and click **Add New GigabitEthernet Interface**.
2. Specify your settings for the interface.
3. Click **Add** to save the new interface. Additional Gigabit Ethernet Interfaces can then be added and edited from this page.

#### Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information.
- Refer to the "interface gigabitethernet" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Gigabit Ethernet Group

The Mobility Access Switch can group the interfaces together so that any interface within the group has the same configuration. When you configure an interface that is a member of an interface-group, applying a non-default profile or a parameter to the interface takes precedence over the interface-group configuration. By default, all the interfaces belong to a default interface-group.

When you create non-default interface-groups, the excluded interfaces continue to belong to the default interface-group.



---

Interface groups and port channels are not the same. Interface groups assign the configuration to individual interfaces, whereas the port channel makes a group of interfaces to work as a single logical interface.

---

1. To configure a Gigabit Ethernet interface, navigate to the **Interfaces > GigabitEthernet Group** page and click **Add New GigabitEthernet Group**.
2. Specify your settings for the group.
3. Click **Add** to save the new group. Additional Gigabit Ethernet groups can then be added and edited from this page.



---

You cannot have overlapping ranges of interfaces when you have multiple interface groups. For more information about the scope of an interface and interface group profiles, see the "Scope of the Profiles and Parameters" in the *ArubaOS User Guide*.

---

#### Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information.
- Refer to the "interface-group gigabitethernet" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Loopback

The Mobility Access Switch supports a maximum of 64 (0-63) loopback interfaces. You can also assign a secondary IP address to a loopback interface.

1. To configure a Loopback interface, navigate to the **Interfaces > Loopback** page and click **Add New Loopback**.
2. Specify your settings for the loopback interface.
3. Click **Add** to save the new Loopback Interface. Additional Loopback Interfaces can then be added and edited from this page.

### Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information.
- Refer to the "interface loopback" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Management Interface

The management interface is located above the console port on the rear panel of the Mobility Access Switch. It is labeled as mgmt. The management port is a dedicated interface for out-of-band management purpose. This interface is specifically available for the management of the system and cannot be used as a switching interface. You can configure only the IP address and description for this interface. The management port can be used to access the Mobility Access Switch from any location and configure the system.

1. To configure a Gigabit Ethernet interface, navigate to the **Interfaces > Management** page.
2. Specify your settings for the interface.
3. Click **Save** to save the new interface.

### Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information.
- Refer to the "interface mgmt" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## LACP System Profile

The Link Aggregation Control Protocol (LACP), based on the IEEE 802.3ad standard, provides a standardized means for exchanging information with partner systems to form a dynamic link aggregation group.

After a system profile is configured, this profile can be used for configuring interface-level LACP options, including the port mode. Refer to the ["LACP Profile" on page 34](#) section for more information.

1. To configure an LACP System Profile, navigate to the **Interfaces > Port Channels > LACP > Global Config** page.
2. Enter the LACP Priority value.
3. Select **Save** to save the LACP system profile.

### Refer to

- Refer to the Port Channels chapter in the *ArubaOS User Guide* for more information.
- Refer to the "lACP" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## LACP Profile

LACP profiles can be defined at the Interface level as well as at the Global level. (Refer to ["LACP System Profile" on page 34](#) for information on configuring LACP at the global level.) When configuring an interface LACP profile, you can specify port mode, timeout settings, and priority values.

1. To configure an Interface LACP profile, navigate to the **Interfaces > Port Channels > LACP > Interface Config** page and click **Add New LACP Profile**.
2. Specify values for the profile
3. Click **Add** to save the new profile. Additional LACP profiles can then be added and edited from this page.

#### Refer to

- Refer to the Port Channels chapter in the *ArubaOS User Guide* for more information about LACP.
- Refer to the "interface-profile lacp-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Tunneled Node Profiles

Tunneled Node (previously known as Mux) provides the ability to tunnel the ingress packets (via GRE) from an interface on the Mobility Access Switch (Tunneled Node port) to an Mobility Controller (Tunneled Node server). You can use the Tunneled Nodes to allow the Mobility Controller to provide centralized security policy, authentication, and access-control.

Refer to the *ArubaOS User Guide* for important information regarding Tunneled Node support, including minimum version requirements, devices that support Tunneled Node, support for backup servers, and more.

1. To configure a Tunneled Node Server profile, navigate to the **Interfaces > Tunneled Node Server** page and click **Add New Tunneled Node Server Profile**. describes the fields that appear on this page.
2. Enter values for the tunneled node.
3. Click **Add** to save the new profile. Additional Tunneled Node Server profiles can then be added and edited from this page.

#### Refer to

- Refer to the Tunneled Nodes chapter in the *ArubaOS User Guide* for more information about tunneled nodes.
- Refer to the "interface-profile tunneled-node-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Routed VLAN Interfaces

Routed VLAN Interfaces (RVI) are logical interfaces that enable routing and bridging between VLANs. You can route and bridge a protocol on the same interface. The traffic that remains in the bridge group (the bridged traffic) will be bridged among the bridged interfaces, and the traffic that needs to go out to another network (the routed traffic) will be routed internally to the appropriate output routed interface.

There can be an IPv4 address for each VLAN interface. You can also configure IGMP and PIM interface profiles to the VLAN interfaces. A total of 4094 routed VLAN interfaces can be configured in this release. VLAN interface 1 is configured by default.

### Important Points to Remember

- The maximum number of VLAN interfaces supported are 4094.
- The Layer 2 VLAN must be configured before configuring the corresponding RVIs.
- The protocol status of a RVI is in up state only when the protocol status of at least one member port in the corresponding VLAN is in up state.

To assign member ports to a VLAN, create a switching profile with the corresponding VLAN, and assign the switching profile to the member interfaces.

## Configuring Routed VLAN Interfaces

1. To configure a Routed VLAN interface, navigate to the **Interfaces > Routed Virtual Interfaces** page and click **Add New Routed Virtual Interface**.
2. Specify your settings for the interface.
3. Click **Add** to save the new interface. Additional Routed VLAN Interfaces can then be added and edited from this page.

### Refer to

- Refer to the Layer 3 Routing chapter in the *ArubaOS User Guide* for more information.
- Refer to the "interface vlan" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Ethernet Link Profiles

You can use the Ethernet link profile to configure gigabit Ethernet switching and uplink ports. The Ethernet interfaces support auto negotiation from 10BaseT to 1000BaseT as per the IEEE 802.3u/z standards. When you enable auto negotiation, the device that is connected to the port is automatically configured to the highest speed supported by the device in the following order (highest to lowest):

- 10000 Mbps full duplex (supported only on the uplink interfaces)
- 1000 Mbps full duplex
- 100 Mbps full duplex
- 100 Mbps half duplex
- 10 Mbps full duplex
- 10 Mbps half duplex



---

The 1000 Mbps ports (10 gigabit uplink interfaces) cannot scale down to less than 1000 Mbps (1 gigabit speed).

---

Auto negotiation also supports the pause capabilities, automatic Media Detection Interface (MDI), and Media Detection Interface Crossover (MDIX) cable detection. The devices exchange information using the Fast link Pulse (FLP) bursts. The auto negotiation on the link is performed when you perform any of the following activities:

- Connect the device.
- Power on or reset the device at either end of the link.
- Make a negotiation request.

## Ethernet Flow of Control

Ethernet flow control prevents loss of frames by providing a back pressure. When an Ethernet port receives frames faster than it can handle, it sends a PAUSE frame to stop the transmission from the sender for a specific period of time. The PAUSE frame has a destination group address of 01-80-c2-00-00-01.



---

When flow control frames are received, only pausing the transmit is supported. Sending flow control frames are not supported. This means that the system can only respond to PAUSE frames and cannot generate them. The flow control can be enabled or disabled to respond to incoming PAUSE frames.

---

## Configuring Ethernet Link Profiles

1. To configure an Ethernet Link profile, navigate to the **Interfaces > Physical Media & PoE > Ethernet Link** page and click **Add New Ethernet Link Profile**.
2. Specify values for the profile.

3. Click **Add** to save the new profile. Additional Ethernet Link Profiles can then be added and edited from this page.

#### Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information about Ethernet link profiles.
- Refer to the "interface-profile enet-link-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## POE Management Profile

Power over Ethernet (PoE) as per IEEE 802.3at is a technology for wired Ethernet LANs to carry the electric-power required for the device in the data cables. The IEEE standard defined in IEEE 802.3af allows network equipment (power sourcing equipment) to provide up to 15.4 Watts of power at the output for powered devices (PDs). In addition, the IEEE 802.3at (PoE+) standard provides more power to PDs where up to 30.0 Watts of power on output is delivered on the standard copper cable. The Aruba Mobility Access Switch supports both PoE standards.

### Power Management Modes

The Aruba Mobility Access Switch supports three PoE power management modes:

- **Static Mode**—The power deducted from the total power pool is the maximum power for that interface. This mode ensures that the maximum power specified by you for the interface is always reserved and cannot be shared by other PDs.
- **Dynamic Mode**—The power allocated from the total power pool for each port is the actual power consumed at that port. You can allocate any unused portion of power to the other PDs. This is the default mode.
- **Class-based Mode**—The power allocated for each port from the total power pool is the maximum power available for the class of PD connected to that port.

### PoE Guard Band

The PoE guard-band can provide protection when there is a sudden spike in the consumed power of powered devices that could potentially impact other PoE enabled ports. When the guard-band is configured, the Aruba Mobility Access Switch reserves a specified amount of power to prevent other PoE enabled ports from powering off and then powering back on again. The default value for guard-band is 11,000 milliwatts (mW). You can specify the guard-band value in increments of 1000 beginning with 1000mW. The maximum guard-band value that you can configure is 30,000mW.

### Configuring a PoE Management Profile

1. To configure a PoE Management Profile, navigate to the **Interfaces > Physical Media & PoE > PoE > Chassis Management** page and click **Add New Poe Management Profile**.
2. Specify values for the profile.
3. Click **Add** to save the route. Additional Poe Management Profiles can then be added and edited from this page.

#### Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information about PoE profiles.
- Refer to the "poe-management-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

### PoE Profile Configuration

PoE Profiles can configured and then applied to interfaces. Perform the following steps.

1. To configure a PoE Profile, navigate to the **Interfaces > PoE > Interface Config** page and click **Add New PoE Profile**.

2. Specify your settings for the profile.
3. Click **Add** to save the new profile. Additional PoE profiles can then be added and edited from this page.

#### Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information.
- Refer to the "interface-profile poe-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## PoE Time Range Profile

The Mobility Access Switch supports time range for controlling the mode of the PoE power (enable/disable) to the PoE port.



---

The time range profile is disabled by default in the PoE profile.

---

The PoE time range can be configured in two modes: absolute and periodic. In absolute mode, the time parameters correspond to a specific time range: start date, start time, end date, and the end time. The PoE port is enabled if the current system time is within this range. In periodic mode, the user can specify start day, start time, end day, and end time. The start day or end day can be daily, weekend, weekday, or any day of the week. The PoE port is enabled if the current day and time falls within the range.

The following are the invalid combinations for start and end values for the time range parameters in the periodic mode:

- start-day: daily, end-day: any other day other than daily
- start-day: weekend, end-day: any other day other than weekend. (Here weekend refers to Saturday or Sunday)
- start-day: weekday, end-day: any other day other than weekday



---

Avoid configuring the PoE time-of-day when the connected devices are in the process of being upgraded or when a power loss has rendered the connected device inoperable. In the case of an Aruba wireless Access Point, the PoE time-of-day should not be configured when an AP flash memory upgrade is in progress, as it may result in potential corruption of the flash.

---

1. To configure a PoE time range, navigate to the **Interfaces > PoE > Time-Range** page and click **Add New PoE Time-Range**.
2. Specify your settings for the time range.
3. Click **Add** to save the new time range. Additional time ranges can then be added and edited from this page.

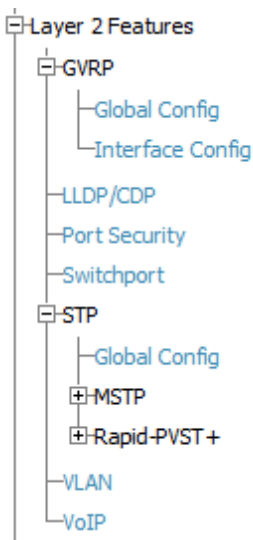
#### Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information.
- Refer to the "time-range-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Layer 2 Features

Switch Configuration supports a variety of profiles that can be associated with Layer 2 protocols. Refer to the **Layer 2 Features** portion of the navigation pane on the **Switch Config** page, as illustrated in [Figure 13](#):

**Figure 13** *Layer 2 Components in Switch Config*



This sections that follow describes the profiles for all Layer 2 components in **Switch Config**.

## Global GVRP Configuration

Configuring GVRP in an Mobility Access Switch enables the switch to register/de-register the dynamic VLAN information received from a GVRP applicant such as an IAP in the network. GVRP support also enables the switch to propagate the registered VLAN information to the neighboring bridges in the network.

1. To configure a Global GVRP Management Profile, navigate to the **Layer 2 Features > GVRP > Global Config** page.



---

Additional GVRP profiles can be enabled on an interface. Refer to the ["Interface GVRP Profiles" on page 39](#) section for additional information.

---

2. Specify values for the global configuration.
3. Click **Save** to save the edited GVRP settings.

### Refer to

- Refer to the GVRP chapter in the *ArubaOS User Guide* for more information about GVRP.
- Refer to the "gvrp" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Interface GVRP Profiles

Switch Config allows you to configure an Interface GVRP profile, in which you can specify the GVRP registration mode. In normal registrar mode, the Mobility Access Switch registers and de-registers VLANs to or from its connected switches and IAPs. In forbidden registrar mode, the Mobility Access Switch cannot register nor de-register VLANs to or from its connected switches and IAPs.

1. To configure an Interface GVRP Profile, navigate to the **Layer 2 Features > GVRP > Interface Config** page.



---

A GVRP profile can also be enabled globally. Refer to the ["Global GVRP Configuration" on page 39](#) section for additional information.

---

2. Enable or disable GVRP on this interface profile and set the registration mode.

3. Click **Add** to save the new profile. Additional Interface GVRP Profiles can then be added and edited from this page.

#### Refer to

- Refer to the GVRP chapter in the *ArubaOS User Guide* for more information about GVRP.
- Refer to the "interface-profile gvrp-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## LLDP Profiles

Link Layer Discovery Protocol (LLDP), defined in the IEEE 802.1AB standard, is a Layer 2 protocol that allows network devices to advertise their identity and capabilities on a LAN. The Mobility Access Switch supports a simple one-way neighbor discovery protocol with periodic transmissions of LLDP PDU.

- LLDP frames are constrained to a local link.
  - LLDP frames are TLV (Type-Length-Value) form.
  - LLDP Multicast address is 01-80-C2-00-00-0E.
1. To configure an LLDP profile, navigate to the **Layer 2 Features > LLDP** page and click **Add New LLDP Profile**.
  2. Specify values for this profile.
  3. Click **Add** to save the new profile. Additional LLDP profiles can then be added and edited from this page.

#### Refer to

- Refer to the Link Layer Discovery Protocols chapter in the *ArubaOS User Guide* for more information about LLDP.
- Refer to the "interface-profile lldp-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Port Security Profiles

Port Security can be used to restrict the number of MACs allowed on an interface using Router Advertisement Guard, DHCP Trust, Loop Protect, and MAC limits.

### Router Advertisement Guard

The Router Advertisement (RA) Guard functionality analyzes the RAs and filters out RA packets sent by unauthorized devices. The RA guard feature is disabled by default. By enabling, the RA packets received on the interface are dropped and the port can be shutdown based on the interface configuration.

### DHCP Trust

The DHCP trust functionality provides support to filter the IPv4 DHCP packets from the unauthorized devices. The following IPv4 DHCP messages are filtered on an interface configured not to trust DHCP.

- DHCP offer messages
- DHCP Ack messages

By default the DHCP packets are trusted on the interface. When the DHCP Trust is disabled, the aforementioned DHCP messages that are received on the interface are dropped.

### Loop Protect

The Loop Protect functionality detects the unwanted physical loops in your network. A proprietary protocol data unit (PDU) is used to detect the physical loops in the network. When the system detects a loop, it disables the port that sends the PDU. You can re-enable the port automatically or manually



## MAC Limit

The MAC limit feature restricts the maximum number of MACs that can be learned on the interface. When the MAC limit is enabled, it provides support to log the excess MACs or drop the new MAC learning requests or shuts down the port.

## Configuring a Port Security Profile

1. To configure a Port Security profile, navigate to the **Layer 2 Features > Port Security** page and click **Add New Port Security Profile**.
2. Specify values for this profile.
3. Click **Add** to save the new profile. Additional Port Security profiles can then be added and edited from this page.

### Refer to

- Refer to the Port Security chapter in the *ArubaOS User Guide* for more information about Port Security.
- Refer to the "interface-profile port-security-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Port Switching Profiles

Port Switching profiles are used for assigning VLAN memberships to interfaces.

1. To configure a Port Switching profile, navigate to the **Layer 2 Features > Switchport** page and click **Add New Port Switching Profile**.
2. Enter settings for this profile.
3. Select **Add** to save the new profile. Additional Port Switching profiles can then be added and edited from this page.

### Refer to

- Refer to the VLANs chapter in the *ArubaOS User Guide* for more information switching profiles.
- Refer to the "interface-profile switching-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Spanning Tree Global Config

The spanning tree mode for Aruba Mobility Access Switches defaults to MSTP. Use the Global Config to enable spanning tree operations and to change the spanning tree mode.

1. To change the mode, navigate to the **Layer 2 Features > STP > Global Config** page.
2. Enable or disable STP for this profile, and select the Spanning Tree Operating Mode.
3. Click **Save** to save the setting.

### Refer to

- Refer to the MSTP and Rapids PVST chapters in the *ArubaOS User Guide* for more information about Spanning Tree.
- Refer to the "spanning-tree mode" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## MSTP Overview

MSTP maps a group of Virtual Local Area Networks (VLANs) to a reduced number of spanning tree instances. This allows VLAN bridges to use multiple spanning trees. This protocol enables network traffic from different VLANs to flow through different potential paths within a bridged VLAN. Because most networks do not need more than a few logical topologies, MSTP provides design flexibility as well as better overall network resource utilization.

Layer 2 networks typically use multiple paths and link redundancies to handle node and link failures. By definition, spanning tree uses a subset of the available physical links in its active logical topology to provide complete connectivity between any pair of end hosts.

## Interface MSTP Profiles

With the Interface MSTP profile, you can enable BPDUguard, Rootguard, Portfast, and Loopguard options.

### BPDUguard

The BPDU guard functionality prevents malicious attacks on edge ports. When the malicious attacker sends a BPDU on the edge port, it triggers unnecessary STP calculation. To avoid this attack, use the BPDU guard on that edge port. The BPDU guard enabled port shuts down as soon as a BPDU is received.

### Rootguard

Rootguard provides a way to enforce the root bridge placement in the network. The rootguard feature guarantees that a port will not be selected as Root Port for the CIST or any MSTI. If a bridge receives superior spanning tree BPDUs (Bridge Protocol Data Units) on a rootguard-enabled port, the port is selected as an Alternate Port instead of Root Port and no traffic is forwarded across this port.

By selecting the port as an Alternate Port, the rootguard configuration prevents bridges, external to the region, from becoming the root bridge and influencing the active spanning tree topology.

### Portfast

When the link on a bridge port goes up, MSTP runs its algorithm on that port. If the port is connected to a host that does not “speak” MSTP, it takes approximately 30 seconds for the port to transition to the forwarding state. During this time, no user data passes through this bridge port and some user applications may timeout.

### Loopguard

Loopguard provides additional protection against Layer 2 forwarding loops (spanning tree loops). A spanning tree loop is created when a spanning tree blocking port, in a redundant topology, erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the spanning tree blocking port) is no longer receiving spanning tree BPDUs.

If loopguard is enabled on a non-designated port receiving BPDUs, then that non-designated port is moved into the spanning tree loop-inconsistent blocking state.

Refer to the *ArubaOS User Guide* for important information regarding MSTP support.

## Global MSTP Profiles

1. To configure a Global MSTP profile, navigate to the **Layer 2 Features > STP > MSTP > Global Config** page.
2. Specify values for this profile.
3. Click **Save** to save the profile.

### Refer to

- Refer to the MSTP chapter in the *ArubaOS User Guide* for more information about MSTP.
- Refer to the "mstp" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Configuring an Interface MSTP Profile

1. To configure an Interface MSTP profile, navigate to the **Layer 2 Features > STP > MSTP > Interface Config** page and click **Add New MSTP Port Profile**.
2. Enter values for this profile.

3. Click **Add** to save the new profile. Additional Interface MSTP Profiles can then be added and edited from this page.

#### Refer to

- Refer to the MSTP chapter in the *ArubaOS User Guide* for more information about MSTP.
- Refer to the "interface-profile mstp-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Rapid PVST+

Rapid Per-VLAN Spanning Tree Plus (PVST+) provides for rapid recovery of connectivity following the failure of a device, a device port, or a LAN. It also provides rapid convergence for edge ports, new root ports, and ports connected through point-to-point links.

Rapid PVST+ runs a separate spanning tree instance for each Virtual Local Area Network (VLAN). This allows the port to forward some VLANs while blocking other VLANs. PVST+ provides for load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

Convergence occurs rapidly with Rapid PVST+. By default, each designated port in the spanning tree protocol sends out a BPDUs (Bridge Protocol Data Units) every 2 seconds. On a designated port in the topology, if hello messages are missed three consecutive times, or if the maximum age expires, the port immediately flushes all protocol information from the table. A port considers that it loses connectivity to its direct neighbor designated port when it misses three BPDUs or if the maximum age expires. This rapid aging of the protocol information allows for quick failure detection.

### Important Notes

- If your Mobility Access Switch is terminated on a router/switch spanning tree environment running PVST+, your Mobility Access Switch must be in PVST mode.
- Once in Rapid PVST+ mode, a predefined non-editable PVST profile automatically associates all configured VLANs (including default VLAN 1) and PVST+ starts running on all configured VLANs.
- Rapid PVST+ inter-operates seamlessly with IEEE and PVST bridges when the Mobility Access Switch is placed in a network.

### Interface PVST Bridge Profiles

Rapid Per-VLAN Spanning Tree Plus (PVST+) provides for rapid recovery of connectivity following the failure of a device, a device port, or a LAN. It provides rapid convergence for edge ports, new root ports, and ports connected through point-to-point links. Interface-based PVST+ Bridge profiles enable you to configure Rapid PVST+ port properties. With the Interface PVST Bridge profile, you can enable PBDUGuard, Rootguard, Portfast, and Loopguard options.

#### BPDUGuard

The BPDU guard functionality prevents malicious attacks on edge ports. When the malicious attacker sends a BPDU on the edge port, it triggers unnecessary STP calculation. To avoid this attack, use the BPDU guard on that edge port. The BPDU guard enabled port shuts down as soon as a BPDU is received.

#### Rootguard

Rootguard provides a way to enforce the root bridge placement in the network. The rootguard feature guarantees that a port will not be selected as Root Port for the CIST or any MSTI. If a bridge receives superior spanning tree BPDUs (Bridge Protocol Data Units) on a rootguard-enabled port, the port is selected as an Alternate Port instead of Root Port and no traffic is forwarded across this port.

By selecting the port as an Alternate Port, the rootguard configuration prevents bridges, external to the region, from becoming the root bridge and influencing the active spanning tree topology.

## Portfast

When the link on a bridge port goes up, spanning tree runs its algorithm on that port. If the port is connected to a host that does not communicate with the spanning tree, it takes approximately 30 seconds for the port to transition to the forwarding state. During this time, no user data passes through this bridge port and some user applications may timeout.

## Loopguard

Loopguard provides additional protection against Layer 2 forwarding loops (spanning tree loops). A spanning tree loop is created when a spanning tree blocking port, in a redundant topology, erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the spanning tree blocking port) is no longer receiving spanning tree BPDUs.

If loopguard is enabled on a non-designated port receiving BPDUs, then that non-designated port is moved into the spanning tree loop-inconsistent blocking state.

## Configuring a Rapid PVST+ Profile

1. To configure a Rapid PVST Profile, navigate to the **Layer 2 Features > STP > Rapid PVST+ > Global Config** page and click **Add New Rapid-PVST+ Profile**.
2. Specify values for this profile
3. Click **Add** to save the profile. Additional Rapid PVST+ Profiles can then be added and edited from this page.

### Refer to

- Refer to the Rapid PVST+ chapter in the *ArubaOS User Guide* for more information about Rapid PVST.
- Refer to the "vlan-profile pvst-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Configuring an Interface PVST Bridge Profile

1. To configure an Interface PVST+ Bridge profile, navigate to the **Layer 2 Features > STP > Rapid PVST+ > Interface Config** page and click **Add New Rapid-PVST Port Profile**.
2. Specify values for this profile.
3. Click **Add** to save the new profile. Additional Interface PVST Bridge profiles can then be added and edited from this page.

### Refer to

- Refer to the Rapid PVST+ chapter in the *ArubaOS User Guide* for more information about interface PVST bridge profiles.
- Refer to the "interface-profile pvst-port-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## VLAN Profiles

A VLAN Profile (as opposed to interface profile) can be created to enable/modify IGMP-Snooping settings.

1. To configure a VLAN profile, navigate to the **Layer 2 Features > VLAN** page and click **Add New VLAN Profile**.
2. Specify values for this VLAN.
3. Click **Add** to save the new profile. Additional VLAN profiles can then be added and edited from this page.

### Refer to

- Refer to the VLANs chapter in the *ArubaOS User Guide* for more information about VLANs.
- Refer to the "vlan-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## VoIP Profiles

The VoIP VLAN feature enables access ports to accept both untagged (data) and tagged (voice) traffic from IP phones connected directly to the Mobility Access Switch and separate these traffic into different VLANs (namely data VLAN and voice VLAN). You can configure a voice VLAN using the `voip-profile`. The `dot1p` and `DSCP` values in the VoIP profile are communicated to the phone using LLDP. VoIP profile does not affect the QoS behavior on the switch. The QoS behavior depends on the QoS configuration on the port.

You can configure VoIP either in static mode or auto-discover mode. By default, VoIP is configured in static mode. When VoIP operates in static mode, the phone is expected to know the Voice VLAN to be used and send the Voice traffic with the Voice VLAN tag. This is achieved, only if the Voice VLAN is configured statically on the phone or propagated to the phone using LLDP-MED. In auto-discover mode, when LLDP-MED or CDP discovers a phone, the switch creates a rule to associate all the traffic originating from the phone to the Voice VLAN. Hence, the Voice VLAN need not be configured statically on the phone. The Voice VLAN can be tagged or untagged depending on the LLDP-MED configuration.

When VoIP is configured in auto-discover mode applies the Voice VLAN only to the first neighbor discovered in an interface. If both LLDP-MED and CDP neighbors are discovered, the preference is always given to the first LLDP-MED neighbor even if a CDP neighbor is already associated.

1. To configure a VoIP profile, navigate to the **Layer 2 Features > VoIP** page and click **Add New VoIP Profile**. Be sure to review the *ArubaOS User Guide* for important limitations and guidelines to consider when creating a VoIP profile.
2. Specify values for this profile.
3. Click **Add** to save the new profile. Additional VoIP profiles can then be added and edited from this page.

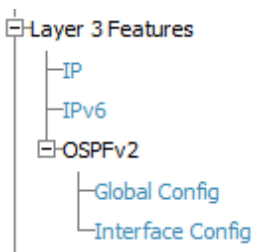
### Refer to

- Refer to the VoIP chapter in the *ArubaOS User Guide* for more information about VoIP.
- Refer to the `"interface-profile voip-profile"` command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Layer 3 Features

Switch Configuration supports a variety of profiles that can be associated with routes and protocols. Refer to the **Layer 3 Features** portion of the navigation pane on the **Switch Config** page, as illustrated in [Figure 14](#):

**Figure 14** *Layer 3 Components in Switch Config*



This sections that follow describes the profiles for all Layer 3 components in **Switch Config**.

### IP Profile

The Aruba Mobility Access Switch supports static routes configuration. You can configure a default gateway and multiple static routes within the global IP-profile to route packets outside the local network. The static routes are active or added to the routing table only when the next hop is reachable, and can be removed from the static routes list.

Each static route requires a destination, netmask, and nexthop addresses. Equal-Cost Multi-Path (ECMP) is not supported in the current release. This implies that each destination/netmask needs a unique nexthop address. The static routes are inserted in to the FIB, only when the nexthop matches the subnet of any of the RVI interfaces or the management interface. If the nexthop becomes unreachable, the RIB gets purged but the static route is still retained.

### Important Points to Remember

- You can have only one default gateway. However, you can have multiple static routes.
- You can have both an IPv4 and an IPv6 default gateway simultaneously.
- Static routes become active only when the nexthop is reachable.
- Nexthops have to be within the local network.
- Each destination/netmask needs a unique nexthop address.
- The nexthop of the default gateway can either be the management interface or a routed VLAN interface.

### Default Gateways

A default gateway is a special case of static route where the destination mask and prefix is 0/0. The next hop in a default gateway can be any valid IP address that can be reached through a routing table or the management interface.

1. To configure a static route, navigate to the **Layer 3 Features > IP** page.
2. Specify values for this profile.
3. Click **Save** to save the route.

#### Refer to

- Refer to the Ethernet Interfaces and PoE chapter in the *ArubaOS User Guide* for more information about IP profiles.
- Refer to the "ip-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

### IPv6 Profile

The IPv6 protocol enables the next generation of large-scale IP networks by supporting addresses that are 128 bits long. This allows  $2^{128}$  possible addresses (versus  $2^{32}$  possible IPv4 addresses).

1. To configure an IPv6 Default Gateway, navigate to the **Layer 3 Features > IPv6** page.
2. Specify the default gateway for this profile.
3. Click **Save** to save the IPv6 default gateway address.

#### Refer to

- Refer to the IPv6 chapter in the *ArubaOS User Guide* for more information about IPv6.
- Refer to the "ipv6-profile" command in the *ArubaOS CLI Guide* for information about configuring IPv6.

### OSPFv2

Open Shortest Path First (OSPFv2) is a dynamic interior gateway routing protocol (IGP) based on IETF RFC 2328. The Aruba implementation of OSPFv2 allows the Mobility Access Switch (MAS) to be effectively deployed in a Layer 3 topology.

### Key Features Supported by MAS

- All stub area types
- Area border router (ABR)
- OSPF on VLAN and loopback interfaces
- OSPF MD5 authentication

- One OSPF instance
- Redistribute VLANs
- OSPF interface can belong to only one area

## LSAs Originated by MAS

With current implementation, the following Link State Advertisement (LSA) types are generated by MAS:

- Type 1 Router LSA
- Type 2 Network LSA
- Type 3 Summary LSA
- Type 4 ASBR Summary LSA

### Notes:

- Routes learned from VLAN-based access interfaces are distributed to OSPF as Router LSAs (Type 1).
- MAS can process Type 5 AS External LSA.

## OSPFv2 Global Config

Use the OSPFv2 Global Config to configure a global OSPFv2 profile. This profile can then be applied to Routed VLAN interfaces or Loopback Interfaces.

1. To change the mode, navigate to the **Layer 3 Features > OSPFv2 > Global Config** page.
2. Enable or disable OSPF and specify settings for this profile.
3. Click **Save** to save the settings.

### Refer to

- Refer to the OSPFv2 chapter in the *ArubaOS User Guide* for more information about OSPF.
- Refer to the "router ospf" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Interface OSPF Profiles

Aruba's implementation of Open Shortest Path First (OSPFv2) is based on RFC 2328. OSPF profiles can be applied to Layer 3 routed VLAN interfaces and to loopback interfaces.

1. To configure an Interface OSPF profile, navigate to the **Layer 3 Features OSPFv2 > Interface Config** page and click **Add New OSPFv2 Interface Profile**.
2. Specify values for this profile.
3. Click **Add** to save the new profile. Additional Interface OSPF profiles can then be added and edited from this page.

### Refer to

- Refer to the OSPFv2 chapter in the *ArubaOS User Guide* for more information about OSPFv2.
- Refer to the "interface-profile ospf-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Quality of Service Profile

A Quality of Service (QoS) profile can be configured to assign specific TC/DP, DSCP, and 802.1p values. This profile can then be applied to an interface profile, a stateless access list, user roles, and policer profiles.

The Aruba Mobility Access Switch supports the following with regards to QoS profiles:

- A QoS profile can be applied to an interface, user role, and traffic flow.
- Eight queues are available per interface in the hardware.
- Eight traffic classes (TC) are available, which map to the corresponding queue (0 – 7).
- A drop-precedence of "low" or "high" for controlling tail-drop.

QoS Profiles can be configured in Trusted or Untrusted modes.

## Trusted Mode

When the QoS mode on a port is set to be trusted, the received 802.1p/DSCP is considered trustworthy and the frame is allowed to exit with those values intact. The received DSCP or 802.1p value is used to index predefined QoS profiles to determine traffic class and drop precedence. These QoS profiles cannot be edited at this time.

The Mobility Access Switch supports the following Trust modes:

- Layer 2 QoS Trust Mode: The port is configured to trust the IEEE 802.1p user priority. This is relevant for 802.1q packets.
- Layer 3 QoS Trust Mode: The port is configured to trust the received DSCP value of the frame.
- Auto (L2+L3) Trust Mode: This mode prioritizes DSCP over 802.1p. If the received frame is IP, the DSCP value is used for indexing the QoS profile. If the received tagged frame is non-IP, then the 802.1p value is used for indexing the QoS profile.

Table 3 below shows DSCP-Queue mapping:

**Table 3:** *DSCP-Queue Mapping*

DSCP	802.1p	Queue
0-7	0	0
8-15	1	1
16-23	2	2
24-31	3	3
32-39	4	4
40-47	5	5
48-55	6	6
56-63	7	7

## Drop Precedence

Drop precedence can be defined as Low or High. The drop precedence is Low for the first 4 values (0-3) and Hi for the last for values (4-7) for each DSCP range. For 802.1p, the drop precedence is defined as Low for all values.

## Untrusted Mode

Untrusted Mode is the default for all interfaces where incoming traffic is mapped to TC "0" and then subsequently mapped to egress queue "0."

## Profile

- QoS profile can be configured to assign specific TC/DP, DSCP, and 802.1p values.



- The QoS profile can be then applied to:
  - Interface (interface-profile)
  - Stateless access-list
  - User-role
  - Policer profile

## Policing

- Limits inbound transmission rate of a class of traffic on the basis of user-defined criteria.
- Policer can be applied to stateless ACL, interface, and user-role.
- 1-rate 3-color policer is supported at FCS.
  - Traffic rate below CIR or burst below CBS limit is considered “conforming” and is allowed to pass through the policer.
  - Traffic rate exceeding CIR, and bursting below EBS limit is considered “exceeding” and is allowed to pass through the policer by default.
  - Traffic rate exceeding CIR, and bursting above EBS limit is considered “violating” and is dropped at the policer by default.

## Configuring QoS

1. To configure a QoS Profile, navigate to the **Quality of Service > QoS** page and click **Add New QoS Profile**.
2. Specify values for this profile.
3. Click **Add** to save the profile. Additional QoS Profiles can then be added and edited from this page.

### Refer to

- Refer to the Quality of Service chapter in the *ArubaOS User Guide* for more information about QoS.
- Refer to the "qos-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Configuring Policer

1. To configure a Policer profile, navigate to the **Quality of Service > Policer** page and click **Add New Policer Profile**.
2. Specify values for this profile.
3. Click **Add** to save the profile. Additional Policer profiles can then be added and edited from this page.

### Refer to

- Refer to the Quality of Service chapter in the *ArubaOS User Guide* for more information about Policer profiles.
- Refer to the "policer-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Multicast Features

Aruba Mobility Access Switches include support for multicast routing protocols including IGMPv1/v2, MLDv1, and PIM-SM.

### Interface IGMP Profiles

The Mobility Access Switch supports Internet Group Management Protocol (IGMP) as defined in IETF RFC 1112 (IGMPv1) and RFC 2236 (IGMPv2). IGMP allows hosts and adjacent routers on IP networks to establish multicast group

memberships.

1. To configure IGMP Snooping for interfaces, navigate to the **Multicast Features > IGMP** page and click **Add New IGMP Interface Profile**.
2. Enable or disable IGMP for this profile, and specify a query interval value.
3. Click **Add** to save the new profile. Additional IGMP profiles can then be added and edited from this page.

#### Refer to

- Refer to the IGMP and PIM-SM chapter in the *ArubaOS User Guide* for more information about IGMP and PIM support.
- Refer to the "interface-profile igmp-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## IGMP Snooping

The Mobility Access Switch supports IGMPv1 and v2 snooping, which prevents multicast flooding on Layer 2 network treating multicast traffic as broadcast traffic. All streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would be receiving all the streams only to be discarded without snooping.

When you enable IGMP snooping, the switch becomes IGMP-aware and processes the IGMP control messages as received. You must do this to correctly process all IGMP membership reports and IGMP leave messages. IGMP snooping is handled by the hardware for performance. Multicast routers and multicast receivers associated with each IP multicast group are learned dynamically.

1. To configure IGMP Snooping for interfaces, navigate to the **Multicast Features > IGMP Snooping (v1/v2)** page and click **Add New IGMP Snooping**.
2. Specify values for this profile.
3. Click **Add** to save the new profile. Additional IGMP Snooping Profiles can then be added and edited from this page.

#### Refer to

- Refer to the IGMP Snooping chapter in the *ArubaOS User Guide* for more information about IGMP Snooping.
- Refer to the "vlan-profile igmp-snooping-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## MLDv1 Snooping

Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link. When multicast is supported at the IPv6 level, it often broadcasts at lower levels. So, for example, an Ethernet switch broadcasts multicast traffic on all ports, even if only one host wants to receive it.

To prevent entire Ethernet segments from being flooded, MLD snooping can be implemented on Ethernet switches. The MLD snooping solution is similar to the IGMP snooping solution for IPv4. When MLD snooping is implemented on a switch, it detects all MLD version 1 messages that are exchanged on the link. It also maintains a table that indicates which IPv6 multicast groups should be forwarded for each of the interfaces.

#### Important Notes

- ArubaOS 7.2.0.0 supports MLDv1 (RFC 2710), so MLDv2 specific packets are not processed.
- MLD snooping prevents multicast flooding on an Ethernet link, but it requires complex processing for each of the interfaces on switches that were not initially designed for this kind of task.
- Unlike IGMP, which uses a separate protocol, MLD is embedded in ICMPv6. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.

## Configuring an MLDv1 Snooping Profile

1. To configure an MLD Snooping Profile, navigate to the **Multicast Features > MLDv1 Snooping** page and click **Add New MLDv1 Snooping Profile**.
2. Specify values for this profile.
3. Click **Add** to save the profile. Additional MLD Snooping Profiles can then be added and edited from this page.

### Refer to

- Refer to the MLD Snooping chapter in the *ArubaOS User Guide* for more information about MLD Snooping.
- Refer to the "vlan-profile mld-snooping-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Protocol Independent Multicast

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols. There are four variants of PIM. Currently, Switch Config supports PIM Sparse Mode (PIM-SM) only. PIM-SM explicitly builds unidirectional shared trees rooted at a rendezvous point (RP) per group, and optionally creates shortest-path trees per source. PIM-SM is recognized for scaling well for wide-area usage. PIM-SM is useful for routing multicast streams between VLANs, subnets, or local area networks (LANs) in applications such as IPTV.

## Configuring a Global PIM Rendezvous Point

1. To configure a Global PIM profile, navigate to the **Multicast Features > PIM > Interface PIM** page and click **Add New Static Rendezvous Point**.
2. Specify the IP address, group address, and mask value.
3. Select **Add** to save the new rendezvous point. Additional Rendezvous Points can then be added and edited from this page.

### Refer to

- Refer to the IGMP and PIM-SM chapter in the *ArubaOS User Guide* for more information about PIM profiles.
- Refer to the "router-pim" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Configuring an Interface PIM Profile

1. To configure an Interface PIM profile, navigate to the **Multicast Features > PIM > Interface PIM** page and click **Add New PIM Interface Profile**.
2. Specify values for this profile.
3. Select **Add** to save the new profile. Additional Interface PIM profiles can then be added and edited from this page.

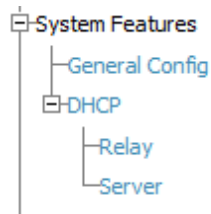
### Refer to

- Refer to the IGMP and PIM-SM chapter in the *ArubaOS User Guide* for more information about PIM profiles.
- Refer to the "interface-profile pim-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## System Features

Switch Configuration supports a variety of profiles that can be associated with DHCP. Refer to the **Layer 3** portion of the navigation pane on the **Switch Config** page, as illustrated in [Figure 15](#):

**Figure 15** *System Features Components in Switch Config*



This sections that follow describes the profiles for all System Features components in **Switch Config**.

### General Config

The General Config component is used for local configuration of switching devices. Locally configured settings are not pushed to local switches by the master controller.

Select the **System Features > General Config** page to specify whether to enable DHCP services. [Table 4](#) describes the fields for this page.

**Table 4:** *System Features > General Config fields*

Field	Default	Description
<b>Other Settings</b>		
Enable DHCP Service	No	Specify whether to enable the DHCP service for the group.
<b>NTP Servers</b>		
NTP Server	blank	Optionally specify the IP address of the Network Time Protocol server.
<b>Certificates</b>		
Select the Certificates to apply to devices in this Group	N/A	Select an available certificate, or use the + sign to add additional certificates.

Select **Save** when you are finished.

### DHCP Relay Profile

DHCP-Relay is supported with DHCP Option 82. DHCP Option 82 allows a DHCP relay agent to insert circuit specific information into a request that is being forwarded to a DHCP server.

Clients on subnets that are not directly connected to a DHCP server must go through a "relay agent." If DHCP relay is not enabled on the VLAN on which the request is received, but a pool is configured for that subnet, the IP is assigned from the internal DHCP server.

DHCP relay is enabled when a DHCP relay profile is attached to a VLAN interface. At this point, the relay agent receives the DHCP broadcast packets from the client and unicasts them to one or more of the DHCP servers that are configured on the VLAN interface. The relay agent stores its own IP address in the Gateway IP Address (GIADDR) field of the DHCP packet. The DHCP server uses the GIADDR to determine the subnet on which the relay agent received the broadcast and allocates an IP address on that subnet. When the DHCP server replies to the client, the reply is unicasted to the GIADDR. The relay agent then retransmits the response on the local network.

DHCP Option 82 works by setting two sub-options:

- Circuit ID: The circuit ID includes information specific to the circuit on which the request arrives. Circuit identifier parameters can be interface name, VLAN ID, or both.
- Remote ID: The remote ID carries information relating to the remote host end of the circuit. Remote identifier parameters can be the MAC address or the hostname of the relay agent.

DHCP Relay Option 82 can be configured using a DHCP Relay profile.

## Configuring a DHCP Relay Profile

1. You can configure a DHCP Relay profile by selecting the **Add New DHCP Relay Profile** button on the **DHCP > Relay** page of Switch Config.
2. Specify values for the new profile.
3. Select **Add** to create the DHCP Relay profile.

### Refer to

- Refer to the DHCP Server & DHCP Relay chapter in the *ArubaOS User Guide* for more information about DHCP Relay profiles.
- Refer to the "interface-profile dhcp-relay-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## DHCP Server Profile

Dynamic Host Configuration Protocol (DHCP) automates network-parameter assignment to network devices from one or more DHCP servers. When a DHCP-configured client connects to a network, the DHCP client sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, servers, etc.

On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting, and must complete before the client can initiate IP-based communication with other hosts. During initialization, network clients try to dynamically obtain their IP addresses. In small networks, where all the systems are in the same IP subnet, the client and the server can communicate directly.

## Configuring a DHCP Server Profile

1. You can configure a DHCP Relay profile by selecting the **Add New DHCP Server Profile** button on the **DHCP > Server** page of Switch Config.
2. Specify values for the new profile.
3. Select **Add** to create the DHCP Server profile.

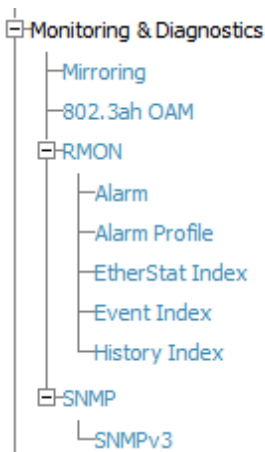
### Refer to

- Refer to the DHCP Server & DHCP Relay chapter in the *ArubaOS User Guide* for more information about DHCP Server profiles.
- Refer to the "interface-profile dhcp-server-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Monitoring and Diagnostics

Switch Configuration supports a variety of profiles that can be associated with Monitoring and Diagnostics features on your switch. Refer to the **Monitoring & Diagnostics** portion of the navigation pane on the **Switch Config** page, as illustrated in Figure 16:

**Figure 16** *Monitoring & Diagnostics Components in Switch Config*



This sections that follow describes the profiles for all Monitoring and Diagnostics components in **Switch Config**.

### Mirroring Profiles

Switch Config supports port mirroring, which can be used to send copies of all or sampled packets seen on specific port (s) or port-channel to a destination. Port mirroring can also be used for appliances such as sniffers that monitor network traffic for further analysis.

The Mirroring profile allows you to specify a destination port. A single port can be the destination interface. (Port-channels and VLANs cannot be a destination.) Normal traffic forwarding will not be performed on the destination port; only the mirrored packets can be received on the destination port. A destination port cannot be a port mirroring source port at the same time. The destination port does not participate in any Layer 2 protocol, including Spanning-tree. Switching profiles, such as access or trunk profiles, cannot be applied on the destination port.

1. To configure a Mirroring profile, navigate to the **Monitoring & Diagnostics > Mirroring** page and click **Add New Mirroring Profile**.
2. Specify the Destination GigabitEthernet Interface and the port mirroring ratio.
3. Select **Add** to save the new profile. Additional Mirroring profiles can then be added and edited from this page.

#### Refer to

- Refer to the Port Mirroring chapter in the *ArubaOS User Guide* for more information about Mirroring profiles.
- Refer to the "interface-profile mirroring-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

### 802.3ah OAM Profiles

Operations, Administration, and Maintenance (OAM) refers to the tools and utilities to install, monitor, and troubleshoot a network. OAM tools report layer-2 network behavior, which can help network administrators monitor and troubleshoot a network without sending technicians into the field to diagnose problems on location. OAM provides mechanisms to monitor link operations and health and to improve fault isolation.

The MAS OAM feature supports the following Link Fault Management options:

- Discovery – An OAM-enabled local interface discovers a remote interface enabled with OAM and notifies each other of their own capabilities. After discovery, both sides send OAM PDUs periodically to monitor the link.
  - Remote fault detection – Detection and handling of faulty links, such as those not receiving an OAM PDU from the other peer within the configured time-out or an OAM PDU with a “link-fault” flag.
  - Remote loopback – Link segment testing is controlled remotely using test frames. Usually remote loopback is used during installation or for troubleshooting.
1. To configure an OAM profile, navigate to the **Monitoring & Diagnostics > OAM** page and click **Add New OAM Profile**.
  2. Specify values for this profile.
  3. Select **Add** to save the new profile. Additional OAM profiles can then be added and edited from this page.

#### Refer to

- Refer to the Operations, Administration, and Maintenance chapter in the *ArubaOS User Guide* for more information about OAM profiles.
- Refer to the "interface-profile oam--profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Remote Monitoring (RMON)

Remote Monitoring (RMON) provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed local area networks (LANs). Monitoring devices (commonly called "probes") contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients. While both agent configuration and data collection use SNMP, RMON is designed to operate differently than other SNMP-based systems:

- Probes have more responsibility for data collection and processing, which reduces SNMP traffic and the processing load of the clients.
- Information is only transmitted to the management application when required, instead of continuous polling.

ArubaOS supports the following RMON groups:

- Ethernet statistics
- History control
- Ethernet history
- Alarm
- Event Index

## Enabling RMON

Perform the following steps to enable RMON.

1. Navigate to the **Monitoring & Diagnostics > RMON** page.
2. Select **Yes** for the Enable RMON Service option.
3. Click the **Save** button.

## Configuring an Alarm

1. To configure an Alarm entry, navigate to the **Monitoring & Diagnostics > RMON > Alarm** page and click **Add New Alarm**.
2. Specify values for this Alarm entry.
3. Click **Add** to save the new Alarm entry. Additional Alarms can then be added and edited from this page.

### Refer to

- Refer to the Remote Monitoring (RMON) chapter in the *ArubaOS User Guide* for more information about Alarms.
- Refer to the "rmon alarm" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Alarm Profile

Create an alarm profile and associate that profile with an alarm entry.

1. To configure an Alarm Profile, navigate to the **Monitoring & Diagnostics > RMON > Alarm Profile** page and click **Add New Alarm Profile**.
2. Specify values for this Alarm profile.
3. Click **Add** to save the new Alarm profile. Additional Alarms profiles can then be added and edited from this page.

### Refer to

- Refer to the Remote Monitoring (RMON) chapter in the *ArubaOS User Guide* for more information about Alarms.
- Refer to the "rmon alarm-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Ethernet Statistics Index

Perform the following steps to configure Ethernet statistics collection on an interface.

1. To configure an Alarm entry, navigate to the **Monitoring & Diagnostics > RMON > EtherStat Index** page and click **Add New EtherStat Index**.
2. Specify values for this entry.
3. Click **Add** to save the new Ethernet Statistics entry. Additional Ethernet Statistic entries can then be added and edited from this page.

### Refer to

- Refer to the Remote Monitoring (RMON) chapter in the *ArubaOS User Guide* for more information about Ethernet Statistics.
- Refer to the "rmon etherstat" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## Event Index

An Event Index specifies the action to take when an alarm triggers an event.

1. To configure an Event Index, navigate to the **Monitoring & Diagnostics > RMON > Event Index** page and click **Add New Event Index**.
2. Specify values for this entry.
3. Click **Add** to save the new Event Index entry. Additional Event Index entries can then be added and edited from this page.

### Refer to

- Refer to the Remote Monitoring (RMON) chapter in the *ArubaOS User Guide* for more information about Event Index entries.
- Refer to the "rmon event" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.



## History Index

1. To configure a History Index, navigate to the **Monitoring & Diagnostics > RMON > History Index** page and click **Add New History Index**.
2. Specify values for this entry.
3. Click **Add** to save the new History Index entry. Additional History Index entries can then be added and edited from this page.

### Refer to

- Refer to the Remote Monitoring (RMON) chapter in the *ArubaOS User Guide* for more information about History Index entries.
- Refer to the "rmon history" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## SNMP Management Profile

SNMP Management profile settings for switch devices are managed locally. Management profiles for the AP are managed by group or global configuration on the **Monitoring & Diagnostics > SNMP** page. Navigate to this page to create or edit SNMP Management profile settings.



---

If you push configuration to a switch without having imported the contents of this profile, it will stop responding to AMP, because the default profile has no community strings in it.

---

### Refer to

- Refer to the MIB and SNMP chapter in the *ArubaOS User Guide* for more information about SNMP management settings.
- Refer to the "snmp-server" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## SNMPv3 User

1. To configure an SNMPv3 user on the switch, navigate to the **Monitoring & Diagnostics > SNMP > SNMPv3 User** page and click **Add New SNMPv3 User**.
2. Enter a name for the user and specify the authentication method.
3. Select **Add** to save the new user. Additional SNMPv3 users can then be added and edited from this page.

### Refer to

- Refer to the MIB and SNMP chapter in the *ArubaOS User Guide* for more information about SNMPv3 Users.
- Refer to the "snmp-server" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.

## ArubaStack

An ArubaStack is a set of interconnected Mobility Access Switches that use stacking ports to form an ArubaStack. A stacking port is a physical port configured to run the stacking protocol. In factory default settings for Mobility Access Switches, uplink ports 2 and 3 are pre-provisioned to be stacking ports. Once a port is provisioned for stacking, it is no longer available to be managed as a network port. A stacking port can only be connected to other Mobility Access Switches running the Aruba Stacking Protocol (ASP).

1. To configure an ArubaStack, navigate to the **Switch Config > ArubaStack** page.
2. Specify values for the ArubaStack.

3. Click **Save** to save the settings.

**Refer to**

- Refer to the ArubaStack chapter in the *ArubaOS User Guide* for more information.
- Refer to the "stack-profile" command in the *ArubaOS CLI Guide* for information about the options that are available on this form.