

## WLAN Base Configuration

ArubaOS 3.1

### Abstract

This document describes a typical configuration for a base production Aruba Networks infrastructure. The document demonstrates a typical configuration with complete step-by-step instructions for configuring:

- ◆ Master mobility controller setup
- ◆ Secure employee WLAN
- ◆ Adaptive Radio Management

### Recommended Reading

The following pre-requisite documentation is highly recommended before reading this document:

- ◆ *Best Practices: WLAN Scaling and Performance*

# Table of Contents

<b>WLAN BASE CONFIGURATION .....</b>	<b>1</b>
<b>Design Summary .....</b>	<b>3</b>
<b>Design Guidelines.....</b>	<b>5</b>
<b>Installation Procedure .....</b>	<b>8</b>
<b>Initial Master Controller Setup .....</b>	<b>9</b>
<b>Core VLAN Configuration.....</b>	<b>10</b>
<b>VLAN and IP Configuration.....</b>	<b>12</b>
<b>Firewall Policies .....</b>	<b>14</b>
<b>Create the User Roles.....</b>	<b>16</b>
<b>Configuring Authentication Services .....</b>	<b>18</b>
<b>Define a Wireless LAN .....</b>	<b>23</b>
<b>AP Deployment Planning.....</b>	<b>28</b>
<b>AP Provisioning .....</b>	<b>30</b>
<b>Design Review.....</b>	<b>32</b>

# Design Summary

## Overview

This section describes a typical base configuration for an Aruba production network.

## Features and functionality

The base configuration includes the following features and functionality:

- ◆ Standards-based, industrial strength security for wireless employee users (WPA2)
- ◆ Automatic and dynamic RF management and self-healing
- ◆ Radius Based Role Derivation

## Topology

The following network diagram shows the basic topology for this network design:

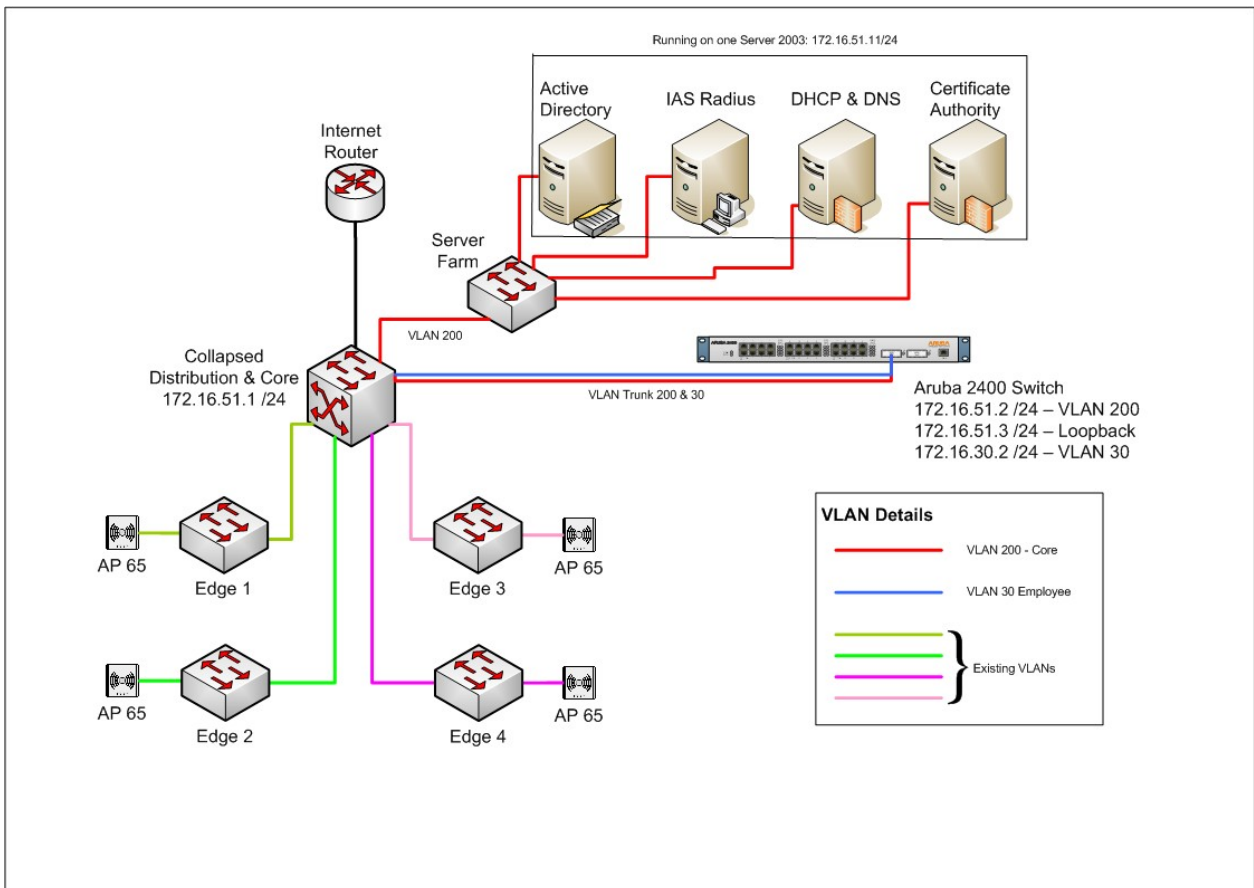


Figure 1 - Base Configuration Reference Topology

## Design Summary continued

- Required licenses** Valid licenses for the following software modules are required to configure the reference network design:
- ◆ **ArubaOS** (standard with all mobility controllers)
    - *Note: this design requires ArubaOS version 3.1 or higher*
  - ◆ **Policy Enforcement Firewall module** - (allows us to define user roles, firewall ACL policies, and role derivation rules. This module is an additional cost and requires licensing beyond the base software.
- Required hardware** At least one Aruba mobility controller is required to manage and control the mobility domain and the Aruba APs. At least one AP is needed to test wireless functionality and to complete the AP provisioning portions of this guide.
- External hardware** This best practice is intended as a guide for configuring secure and scalable wireless networks on an existing wired infrastructure. The existing infrastructure is assumed to have DHCP, DNS, and PoE where the AP's are to be deployed.
- Scaling notes** The reference design is for a single controller but can be extended to support master and local controller combinations.
- For more information on determining the right number and disposition of your mobility controllers, please see the *Best Practices: WLAN Scaling and Performance* document for a detailed discussion.
- Further reading** Please see the *Aruba User Guide* documentation for more information on installation, features and advanced or alternate configuration.

## Design Guidelines

<b>Overview</b>	This section describes how to design the reference base configuration topology.
<b>Network configuration</b>	<p>The Aruba Mobility Controller in this reference design is configured with the following:</p> <ul style="list-style-type: none"><li>◆ Core VLAN (200)<ul style="list-style-type: none"><li>• This VLAN is used for the Aruba controller to connect into the core of the existing wired network. In the event that this configuration is to be used with an existing network, the VLAN number and IP subnet can be changed, along with the controller default gateway, to provide access to an existing core network switch.</li></ul></li><li>◆ Employee User VLAN (30)<ul style="list-style-type: none"><li>• Users connecting to the VLAN will have an employee role with limited rights to switch management, but with full access to the internal network.</li></ul></li></ul>
<b>System Architecture</b>	<p>In this scenario only a single controller is used, referred to as the Master controller. The system can be extended through the use of local controllers. The master controller is responsible for configuration and management of the mobility domain and as such the local controllers simply download most of their configuration from the master.</p> <p>The master controller manages the Aruba APs. Each Aruba AP is connected to the wired network and would normally acquire an IP address via DHCP from an external server located in the data center<sup>1</sup>. The APs auto-discover the master controller by several methods: querying DNS for Aruba-master, using DHCP option 43 to return the IP address of the master controller, or using Aruba discovery protocol (ADP). If directed by the master, the APs will connect to a local management system (LMS), which is a controller configured by the master to handle AP traffic.</p>

---

<sup>1</sup> All Aruba mobility controllers also support an internal DHCP server, which may be used instead. For more information, please see the Aruba user guide documentation.

## Design Guidelines continued

<b>System management</b>	The Aruba mobility controller is configured in the appropriate time zone and should point to a Network Time Protocol (NTP) server. With time synchronized, the controller can be configured to send log information to a syslog server for historical tracking and debugging. An SNMP trap receiver may also be configured.
<b>WLANs and SSIDs</b>	The wireless LAN SSID is called <i>employee</i> . This identifies it as a WLAN for employee and internal use only.
<b>Employee authentication</b>	The <i>employee</i> SSID uses the Wireless Protected Access 2 (WPA2) <sup>2</sup> standard to securely authenticate employees before network access is granted. WPA2 ensures no IP address or network access is available until the employee's credentials has been validated by a RADIUS server against the corporate Active Directory. Once this is validated, the user is placed into a VLAN based on the RADIUS response and receives an IP address from the DHCP server. Authentication between the client supplicant and the RADIUS server uses the Protected Extensible Authentication Protocol (PEAP). All data is encrypted by WPA2 using the AES security standard.
<b>External AAA server</b>	<p>Users are authenticated via an authentication server – in this example it is an Active Directory server called <i>Employee_Radius</i>. Since the WPA2 standard requires that the client supplicant software authenticate using the RADIUS standard (which Active Directory does not support directly), a RADIUS authentication server such as the Internet Authentication Server (IAS) is also required.</p> <p>In this example, the RADIUS server is configured to support client authentication via the Protected EAP (PEAP) protocol over RADIUS.</p> <p>The <i>Aruba-master</i> mobility controller is also configured as a Network Access System (NAS) device on the RADIUS server, with its own shared secret that enables the controller to communicate with the RADIUS server and pass on client authentication requests.</p>
<b>Policy enforcement &amp; access control</b>	All client devices are subject to policy rules and restrictions that limit what they may do. This policy enforcement is enforced by the policy-control engine of the Aruba mobility controller.

---

<sup>2</sup> For more information on WPA2 and other types of wireless client security, check out the Aruba app note: *Wireless Client Security*.

## Design Guidelines continued

- Employee and super user policies** In this design example, successfully authenticated super users are granted full and unrestricted access to all internal network resources. Standard employees have a subset of rights.
- Transparent Layer 3 mobility** Although the design reference shows users remaining on a single VLAN throughout the entire enterprise, there is no reason why multiple VLANs cannot be supported. Thus, a client device that associates on one AP may be assigned VLAN 30 (the VLAN was created for the sake of example) and then move to an AP in another building that normally places clients into VLAN 31. In this case, the user will keep their original IP address and transparently roam without needing to drop their IP address and acquire a new one.
- ARM/RF management** All Aruba APs are configured to run the Adaptive Radio Management (ARM) algorithm. This allows the AP to automatically scan the RF environment and do the following:
- ◆ Proactively manage AP power and channel settings for optimal performance
  - ◆ Scan for channel interference
  - ◆ Build RF heat maps
- In addition, the APs are also configured to automatically self-heal in the event of an AP failure and to detect coverage holes.
- AP deployment** The number of APs and their deployment locations were determined using the Aruba RF Plan tool<sup>3</sup>. The floor plans for all buildings that require coverage were first imported along with information on the building dimensions and the amount of coverage required.
- Air Monitors (AMs) may also be configured at this time. Any Aruba AP automatically provides monitoring when it is not busy servicing clients.
- Although not required, AMs are highly recommended in environments where monitoring or monitoring-based applications such as location tracking and high-resolution heat maps are critical.

---

<sup>3</sup> For more information on the RF Plan tool, please refer to the Aruba RF Plan documentation.

# Installation Procedure

**Overview** This section describes the overall steps involved in configuring a network according to the reference network design described in the previous section.

**Procedure steps** Here are the steps required and the order to perform them:

## **Master mobility controller configuration**

- 1 Initial setup of *Aruba-master*
- 2 VLAN and IP configuration
- 3 Firewall policy (access rights)
- 4 User role definition
- 5 Authentication services
- 6 Wireless LAN definition
- 7 Define Access Point groups and names
- 8 AP provisioning

# Initial Master Controller Setup

- Overview** This section describes how to configure the initial setup of the reference design on an Aruba mobility controller.
- Controller setup** All Aruba controllers are shipped in a factory-default configuration. Initial configuration is command-line only and is performed via the serial port.
- Aruba-master setup** The following script shows how to do the initial configuration of the *Aruba-master* controller via the serial port<sup>4</sup>:

```

Enter System name [Aruba2400]: Aruba-master
Enter VLAN 1 interface IP address [172.16.0.254]: 172.16.0.254
Enter VLAN 1 interface subnet mask [255.255.255.0]: 255.255.255.0
Enter IP Default gateway [none]:
Enter Switch Role, (master|local) [master]: master
Enter Country code (ISO-3166), <ctrl-I> for supported list: gb5
You have chosen Country code GB for United Kingdom (yes|no)?: yes
Enter Time Zone [PST-8:0]: GMT-0:0
Enter Time in GMT [14:27:05]: 14:27:05
Enter Date (MM/DD/YYYY) [2/20/2007]: 02/21/2007
Enter Password for admin login (up to 32 chars): admin (displays *****)
Re-type Password for admin login: *****
Enter Password for enable mode (up to 15 chars): enable
Re-type Password for enable mode: *****
Do you wish to shutdown all the ports (yes|no)? [no]:
Current choices are:
System name: Aruba_master
VLAN 1 interface IP address: 172.16.0.254
VLAN 1 interface subnet mask: 255.255.255.0
IP Default gateway: none
Switch Role: master
Time Zone: GMT-0:0
Ports shutdown: no
If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)yes
Creating configuration... Done.
System will now restart!

```

<sup>4</sup> This design guide concentrates on the graphical user interface rather than the command line. As much configuration as possible will be done via the GUI. Therefore a temporary IP network (172.16.0.254) on VLAN 1 will be used for the initial configuration. This VLAN will not be used in the reference design – it is used as a convenience during the initial setup only.

<sup>5</sup> In compliance with US FCC regulations, all Aruba Mobility Controllers shipped to the US will be restricted to the US regulatory domain (country code). In addition, all controllers currently using the US country code will be permanently restricted to the US country code when upgraded to ArubaOS 3.1 or above. **This change is irreversible.** If the controller is inadvertently restricted to the US, the unit must be replaced (RMA). If you are outside of the US, double-check your country code before upgrading to ensure it is set correctly. For more information, please refer to the Tech Bulletin on country codes available with the 3.1 documentation.

# Final Command-line Configuration

## Overview

This section describes some final configuration via the command-line interface prior to moving to the Web User Interface.

## Core VLAN configuration and addressing

As soon as the controller reboots, we will configure our first VLAN – the core VLAN. In our reference design, this is VLAN 200 and the network is 172.16.51.0/24.

! **Important:** To avoid disruption it is highly recommended that this be done via the serial connection. All other configurations afterwards will be done via the Graphical User Interface (GUI).

The following script shows how to configure VLAN 200, add a loopback address and remove the temporary VLAN information entered during the initial boot process, from the CLI of the Aruba-master controller:

```
(Aruba_master)
User: admin
Password: ****
(Aruba-master) >enable
Password:*****
(Aruba-master) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(Aruba-master) (config) #vlan 200
(Aruba-master) (config-subif)#interface vlan 200
(Aruba-master) (config-subif)#ip address 172.16.51.2 255.255.255.0

(Aruba-master) (config-subif)#interface loopback
(Aruba-master) (config-loop)#ip address 172.16.51.3
Switch IP Address is Modified. Switch should be rebooted now.

(Aruba-master) (config) #interface vlan 1
(Aruba-master) (config-subif)#no ip address

(Aruba-master) (config-loop)#interface fastethernet 1/0
(Aruba-master) (config-if)#switchport access vlan 200
```

Log in to controller

Create VLAN 200 & assign an IP address

Set Loopback Address

Remove Temporary VLAN 1 Address

Set port 1/0 into VLAN 200

- **Note:** The above commands were done on an Aruba 2400 controller, the port configured for VLAN 200, fastethernet 1/0 in this case - would need to be adapted dependent on the specific controller used. This port will be used to manage the controller via the GUI, and the appropriate gigabit Ethernet port will be set up as a trunk port into the core of the network.

# Final Command-line Configuration continued

## Set the default gateway

The last thing we will do is set the default gateway (the gateway of last resort):

```
(Aruba-master) (config-if) #exit
(Aruba-master) (config) # ip default-gateway 172.16.51.1

(Aruba-master) (config) #exit
(Aruba-master) #write mem
Saving Configuration...

Configuration Saved
(Aruba_2400_Test_System) #reload
Do you really want to reset the system(y/n): y
System will now restart!
```

Set the default gateway

Save configuration  
& reboot controller

# VLAN Configuration

## Overview

This section describes how to configure the VLANs required for this project as well as the ports and IP addresses associated with those VLANs.

## Connection to the Web GUI

VLAN 200 is already configured and the controller has an IP address of 172.16.51.2 in that VLAN. The controller's loopback address can be accessed also at 172.16.51.3.

Since no DHCP server is available at this point, the PC that is used to connect to the controller's Web UI will need to be configured with a static IP address.

Configure your PC with the following information:

Parameter	Value
PC IP address	172.16.51.10
Subnet mask	255.255.255.0
Ethernet port to connect the PC	Port 1/0 on the controller

Launch a web browser and enter the URL <http://172.16.51.3>. Enter the admin username and password at the first screen.

## Create the employee VLAN

As shown in our topology diagram, employees will be placed in VLAN30. So the first thing we need to do is to create VLAN30:

**Network**  
Controller  
VLANs  
Ports  
IP

Here are the steps to configure the employee VLAN:

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu click on **Network: VLANs**
- 3 In the main window click the Add button
- 4 In the VLAN ID field enter 30
- 5 Click the Apply button on the right-hand side of the main window

## Why did we do that?

Why don't we add any ports to the employee VLAN? The employee VLAN has no reason to exist anywhere except the Aruba mobility controller. VLANs that only exist on the controller may be routed or trunked out. In this case we will be trunking VLAN 30 to an upstream router.

# VLAN Configuration continued

## Assign an IP address to the employee VLAN

- Network
- Controller
- VLANs
- Ports
- IP

Let's give the employee VLAN an IP address:

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu select **Network: IP**
- 3 In the main window on VLAN 30 click the Edit button
- 4 Enter the following values:

Parameter	Value
Use the following IP address	Select the radio button
IP Address	172.16.30.2
Net Mask	255.255.255.0

- 5 Click the Apply button to save your changes

## Add ports to the core VLAN

Now we'll add some additional ports to the core management VLAN on the controller. Here are the steps:

- 6 On the top of the screen, click on the **Configuration** tab
- 7 In the left-hand menu, select **Network: Ports**
- 8 Select all the ports, except port 24 in the port selection screen at the top of the main window
- 9 Click the Edit button for VLAN 200
- 10 Click the Apply button

## Create a trunk port

- Network
- Controller
- VLANs
- Ports
- IP

Next, let's enable VLAN trunking<sup>6</sup> on an uplink port of the controller:

- 1 On the top of the screen, click on the **Configuration** tab
- 2 In the left-hand menu, select **Network: Ports**
- 3 In the main window, select port 24
- 4 Select the trunk radio button in the Port Mode section
- 5 In the VLAN field select 200 from the drop-down box and click on the left arrow to update the native VLAN field
- 6 Click the Apply button to save your changes

## Save your configuration!

Click the Save Configuration button in the upper right corner of the screen to save your configuration.

<sup>6</sup> Do I really need VLAN trunking on the controller uplink? In a flat network topology probably not. However best practice in most enterprises is to use VLAN trunking to a core router, which can then route as necessary. Therefore we use this in our best practice reference network design.

# Firewall Policies

## Overview

Firewall policies provide a flexible approach to user-differentiated security. In this network, we will use both built-in firewall policies as well as some we create ourselves. In this section we will create a policy that denies access to the core network. It is typically a good idea to lock-down access to network resources such as controllers from wireless users who normally have no reason to access them.

## Create an alias for the core network

- Advanced Services
- Redundancy
- IP Mobility
- Stateful Firewall
- External Services
- VPN Services
- Wired Access
- Wireless
- All Profiles

Since we may want to deny access to multiple network resources, it often makes sense to create an *alias* first. The alias is simply a construct that contains all of the networks and devices we might want to commonly use as part of a firewall policy. This way, instead of entering each device or network IP address every time need to refer to them in a firewall policy, we just reference the alias instead.

Here is how to create an alias for our core network:

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu select **Advanced Services: Stateful Firewall**
- 3 In the main window click the Destination tab
- 4 Click the Add button to add a new alias
- 5 In Destination Name enter 'Core\_Network'
- 6 Under Type click the Add button
- 7 Enter the following values:

Parameter	Value
Rule Type	Network
IP Address	172.16.51.0
Network Mask/Range	255.255.255.0

- 8 Click the Add button below the network mask box to add this destination to your alias

Now, we will add a second destination to this alias for the IP address of the Aruba controller:

- 9 Click the Add button again to add another destination
- 10 Enter the following values:

Parameter	Value
Rule Type	Host
IP Address	172.16.30.2

- 11 Click the Add button below the Network Mask box
- 12 Click the Apply button to save the Core\_Network alias

# Firewall Policies continued

## Create a policy to deny core access

- Security
- Authentication
- Access Control

Now that the alias exists, we can use it anywhere we want to refer to those resources. Our next step is to create a firewall policy that uses this alias to prevent clients from accessing the networks and hosts we put in the Core\_Network alias:

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu select **Security: Access Control**
- 3 In the main window select the Policies tab
- 4 Click the Add button to create a new firewall policy
- 5 In Policy name enter Core\_Network\_Deny
- 6 Click the Add button to add a firewall rule
- 7 Enter the following values:

Parameter	Value
Policy Type	Session
Source	any
Destination	alias
Alias	Core_Network
Service	any
Action	drop
Log	<i>Select this checkbox</i>

- 8 Click on the Add button at the bottom of the screen to add this rule to the firewall policy
- 9 Click the Apply button to save this firewall policy

### Why did we do that?

We chose the drop action for our rule so the firewall within the Aruba mobility controller will drop any packets that meet this rule. Drop indicates no response will be sent back to the client.

We also selected the Log box so any attempts to access these network resources will generate an audit log.

# Create the User Roles

## Overview

The roles within the Aruba controller are the most powerful feature and allow superior management of user access and control. By default, all users are placed in the *Logon* role. Users are only moved to another user role after they have satisfied a configured requirement such as passing 802.1x authentication. It is tempting to simply set the firewall policy contained with the Logon role to allow all traffic. This ensures any client connection will have full access. However it also defeats the entire point of the Aruba security controls.

## Employee

The Employee role has full rights to internal networks but cannot manage the infrastructure components such as the Aruba controller in this case. This could be expanded to ensure isolation of the users from additional network components.

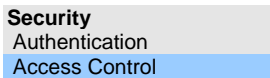
## Process

Here is what we will do to create this role:

- ◆ Create the user role
- ◆ Assign firewall policies to the role that give the employee access to anything except the core management network itself
- ◆ Assign employees to the employee VLAN (VLAN 30)

## Create the employee role

Here are the steps to create the employee user role:



- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu select **Security: Access Control**
- 3 On the upper tabs select User Roles
- 4 In the main window click the Add button to create a user role
- 5 In Role Name field enter 'Employee'

## Assign firewall policies to this role

- 6 In the Firewall Policies section click the Add button
- 7 In the Choose from Configured Policies section select Control from the drop down list
- 8 Click the Done button to add this firewall policy to the user role
- 9 Add another firewall policy by clicking the Add button again
- 10 In the Choose from Configured Policies section select Core\_Network\_Deny from the drop-down list
- 11 Click the Done button at the bottom of the screen
- 12 Add a final policy by clicking on the Add button again
- 13 In the Choose from Configured Policies drop down box select Allowall
- 14 Click the Done button

## Assign employees to employee VLAN

- 15 In the Role VLAN ID section, select VLAN 30 and the click on the Change button to update the field
- 16 Click the Apply button on the bottom of the screen to create the user role

## Create the User Roles continued

**Why did we do that?** Hey, didn't you say we shouldn't use allow-all to open up client traffic? Indeed we did. However you'll notice there are several other firewall policies that occur before. Order is important. The built-in firewall on the controller starts from the top down. It will check the first rule and attempt to match it to the user traffic. If there is no match, it will go the next one, and so on. The control firewall policy is a built-in policy that allows some common protocols such as DHCP and DNS. The next rule is our Core\_Network\_Deny policy and finally a rule that allows all other traffic.

➡ **Note:** If in doubt as to what rules are in a policy, just go to the Policies tab and click the Edit button next to the firewall policy. This will show you everything in that policy and allow changes if necessary.

### Create the super user role

Security  
Authentication  
Access Control

Next we'll create a user role for the super user. This is exactly the same as creating the employee role except we omit the Core\_Network\_Deny policy. We use the same steps:

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu select **Security: Access Control**
- 3 On the upper tabs select User Roles
- 4 In the main window click the Add button
- 5 In Role Name enter 'Superuser'
- 6 In the Firewall Policies section click the Add button
- 7 In the Choose from Configured Policies drop down box select Allowall
- 8 Click the Done button to add this firewall policy to your user role
- 9 In the Role VLAN ID section, select VLAN 30 and the click on the Change button to update the field
- 10 Click on the Apply button on the bottom of the screen to save the user role

### Save your configuration!

Click the Save Configuration button in the upper right corner of the screen to save your configuration.

# Configuring Authentication Services

## Overview

Authentication is a very important part of any modern wireless deployment; it provides security and assurance of identity, which is unavailable by any other means in the wireless space. It is one of the areas, which causes the most concern for implementations.

This section will cover the integration of an Aruba controller with a Windows 2003 Server running IAS and Active Directory. For more information on RADIUS configuration, please refer to the *RADIUS Configuration* guide.

## Process

Here is what we will do to configure authentication services:

- ◆ Add a RADIUS server definition
- ◆ Create a server group and add our RADIUS server
- ◆ Specify a server derivation rule for special handling of Superusers
- ◆ Add a AAA profile that describes the support authentication methods and servers

## Add the RADIUS server definition to the controller

This step provides information about the RADIUS server we will use for authentication. It describes how the controller can interoperate with the RADIUS server; server IP address, communication ports, shared secret, etc.

Security
Authentication
Access Control

Here are the steps to create a RADIUS server definition:

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu select **Security: Authentication**
- 3 On the upper tab select Servers
- 4 In the main window click on RADIUS Server
- 5 In the right-hand window enter Employee\_Radius in the Instance field and click the Add button
- 6 In the right-hand window under the Instance column, click Employee\_Radius to edit this server definition
- 7 Enter the following values:

Parameter	Value
Host	172.16.51.11
Shared Secret	aruba
NAS ID	Employee
NAS IP	172.16.51.2

- 8 Click the Apply button at the bottom of the screen to save your changes to the server definition

# Configuring Authentication Services continued

**Why did we do that?** Wondering what the heck a NAS is? Or when and where the key gets used? These are not Aruba-specific but rather are a common feature of communication with any standards-based RADIUS server. For more information, please check out the *RADIUS Configuration* guide.

## Radius server groups

Security
Authentication
Access Control

Many enterprises have more than one RADIUS server. Indeed, there are often several servers to offer redundancy in the case of failure. Aruba supports this by grouping related servers together. Thus, clients authenticate against a group of servers rather than just a single server. If the first server does not respond, the controller goes to the next.

Here are the steps necessary to create a server group:

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu select **Security: Authentication**
- 3 On the upper tab select Servers
- 4 On the left-hand side of the main window click on Server Group
- 5 In the main window enter Employee\_Auth\_Servers in the Instance field and click the Add button to create a new instance
- 6 In the main Server Group window, click on Employee\_Auth\_Servers
- 7 Under the Servers section in the main window click the New button to choose an authentication server to add to this group
- 8 Under Server Name drop-down box, select Employee\_Radius
- 9 Click on the Add button under Actions to add the server
- 10 Click the Apply button to save your changes

Don't have multiple authentication servers? No problem. However you will still need to put it in a server group.

## Special handling for the Superuser role

We have created two user roles so far: Employee and Superuser. You may be wondering at this point how the Aruba mobility system will recognize whether or not a client is an employee or a superuser. After all, the users connect to the same network and authenticate to the save server. So what can we do?

## Server derivation rules

Aruba uses *Server Derivation Rules* to distinguish between different types of users. This recognition allows the system to immediately place clients into different user roles or VLANs and apply their specific privileges and access rights. It does this by looking for a defined RADIUS attribute field in the response message from the authentication server. There is no specific attribute that needs to be used – it can be anything, including a custom created attribute.

In this network, we use an attribute called *Reply-Message*. This is a standard attribute that is typically included in the response message from most RADIUS servers.

# Configuring Authentication Services continued

**Create a server rule** Here are the steps to create a server derivation rule to determine if a user should be given the Superuser role:

- 1 Make sure you are still in the edit screen for the server group you created called Employee\_Auth\_Servers
- 2 Under Server Rules click the New button to add a rule
- 3 Enter the following values:

Parameter	Value
Condition	Reply-Message
Attribute	equals
Operation	Super
Operand	set role
Value	Superuser

- 4 Click the Add button to add this rule for the server group
- 5 Click the Apply button to save the server group definition with the new rule

**Save your configuration!** Click the Save Configuration button in the upper right corner of the screen to save your configuration.

**Checkpoint** So what have we done so far? We've

- ◆ Created the Employee and Superuser roles
- ◆ Created firewall policies and added them to the user roles to control access rights for each group of users
- ◆ Defined a group of authentication servers
- ◆ Added a derivation rule to our authentication server group that checks if the user is a Superuser

The observant reader may have noticed that nowhere have we actually tied together our users roles with the authentication server group. In cases where we have multiple authentication server groups, how do we know which one should be used?

The answer to this is a *AAA Profile*. The AAA profile defines exactly how users authenticate and how they are authenticated. The AAA profile also determines which user roles are applied after successful authentication.

# Configuring Authentication Services continued

In cases where different authentication mechanisms are needed, you will need multiple AAA profiles. For example, assume we have two different locations where we want the employee WLAN available: Sunnyvale and Amsterdam. Each location has its own RADIUS server. So we keep the employee WLAN the same, but will have two AAA profiles – one for Sunnyvale and one for Amsterdam.

In this example, we have just one location (Sunnyvale) and one authentication server group that can authenticate every user. We will also support just one authentication mechanism (WPA2). So one AAA profile is all we will need.

**Create a AAA profile** Let's see this in action.

Security  
 Authentication  
 Access Control

Here are the steps to create our AAA profile:

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu select **Security: Authentication**
- 3 On the upper tabs select AAA Profiles
- 4 In the main window click on the Add button
- 5 Enter Employee\_AAA\_Sunnyvale and click the Add button to create the profile
- 6 In the main window, AAA Profiles Summary, click on Employee\_AAA\_Sunnyvale to edit the profile<sup>7</sup>
- 7 In the 802.1x Authentication Default Role field, select Employee from the drop-down box
- 8 Click the Apply button to save the AAA profile

➡ **Note:** You may have noticed two fields called Initial Role and Success Role. The initial role defines the role new users are placed into. The success role is where they are placed after successful authentication.

Now we have a AAA profile that will place users into the Employee role<sup>8</sup> upon successful authentication. Next we need to specify the authentication mechanism (WPA2) and add it to the AAA profile.

<sup>7</sup> Did you notice? In the AAA Profiles Summary, there is a Role column next to each AAA profile. This tells you what user role uses this profile. We mentioned earlier that all users are placed into the logon role. From there, they must satisfy the rules of Employee\_AAA\_Sunnyvale before being placed in the Employee or Superuser role.

<sup>8</sup> What happened to the Superuser role? Remember that the authentication server group contains the rule to move an user into the Superuser role. We haven't added this yet. Read on!

## Configuring Authentication Services continued

Here are the steps to configure WPA2 as the authentication mechanism:

- 9 On the left-hand menu, find Employee\_AAA\_Sunnyvale under AAA Profile, and click on 802.1x Authentication Profile
- 10 In the drop-down box which has appeared on the right-hand side of the screen select –NEW-- in the drop down list.
- 11 Enter Employee\_Dot1x\_Sunnyvale as the name for the 802.1x profile<sup>9</sup>
- 12 Click the Apply button to save the 802.1x authentication profile

So now we've configured our authentication mechanism, 802.1x, but we still haven't defined which RADIUS server group should be used. Let's do that now.

- 13 On the left-hand menu of the main window, under AAA Profiles->Employee\_AAA\_Sunnyvale, click on 802.1x Authentication Server Group
- 14 In the box which has appeared on the right-hand side of the screen select Employee\_Auth\_Servers from the drop-down box
- 15 Click the Apply button to save your changes to the AAA profile

**Save your configuration!**

Click the Save Configuration button in the upper right corner of the screen to save your configuration.

---

<sup>9</sup> It is always good practice to provide descriptive names for profiles. This is particularly true when you have multiples of the same type.

# Define a Wireless LAN

## Overview

All of the authentication and user security has been defined. We're done with that and ready to take on the WLAN side of the configuration.

This will comprise the following steps:

- 1 Create a configuration group for all APs that will broadcast the employee ESSID
- 2 Create the virtual AP for the employee ESSID<sup>10</sup>
- 3 Create radio profiles for APs in this WLAN
- 4 Create ARM and RF optimization profiles for this WLAN

## Employee ESSID

The employee ESSID will make use of everything we have configured so far. It will require every user that associates to this ESSID to pass WPA2 with RADIUS authentication. Authenticated users gets the Employee role, unless the RADIUS server passes back the attribute 'super' in which case the user will be elevated to the Superuser role.

## AP groups

Since not all APs need to support the same SSIDs, it makes sense to think of them as groups. One AP group supports the employee SSID. We may have another group of APs that offers a different SSID (such as guest) for some other kind of WLAN.

## Virtual APs

All Aruba APs support a concept called *Virtual APs*. A virtual AP defines an access point – ESSID, radio information, etc. We call them virtual because every Aruba access point can support multiple virtual APs. This allows an administrator to mix and match which APs are members of any particular WLAN. Some APs may be part of WLAN A only. Other APs may be part of WLAN A *and* B. In this example there would be two AP groups. One for the WLAN A only APs and one for the WLAN A + B APs.

Because the AP configuration is virtual, the underlying access point hardware inconsequential.

## Create an AP group for APs in Sunnyvale

We'll create an AP group definition first. Here are the steps to create an AP group:

- Wireless
- AP Configuration
- AP Installation

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu select **Wireless: AP Configuration**
- 3 On the upper tabs, select AP Group
- 4 Click the New button to define a new group
- 5 Enter Sunnyvale\_APs as the group name
- 6 Click the Add button to create the group
- 7 Click the Edit button to the right of Sunnyvale\_APs

## Define a Wireless LAN continued

This creates our AP group definition for APs located in the Sunnyvale campus. Now we'll create a virtual AP within this group for the employee SSID.

### Create a virtual AP definition

Now we'll add the employee SSID as a virtual AP for this AP group:

- 8 Under the Profiles column, click on Wireless LAN
- 9 Click on Virtual AP to define a virtual AP for this AP group definition
- 10 On the right of the screen, Add a Profile appears. Select –NEW- from the drop-down box
- 11 Enter Employee\_VAP as the virtual AP name
- 12 Click the Add button to add this virtual AP to the WLAN definition for the AP group
- 13 Click the Apply button to save your changes
- 14 On the left-hand side of the main window, click on Employee\_VAP
- 15 On the left-hand side of the main window, click on AAA Profile
- 16 Select the AAA profile we just created, Employee\_AAA\_Sunnyvale, from the drop-down box in the AAA Profile field
- 17 Click the Apply button to save your changes
- 18 On the left-hand side of the main window, click on SSID Profile
- 19 In the SSID Profile drop-down box, select –NEW--
- 20 Enter Employee\_WLAN
- 21 Enter the following values:

Parameter	Value
Network Name	employee
Network Authentication	WPA2
Encryption	AES

- 22 Click the Apply button to save your changes

We've got our SSID configured on a virtual AP now. And a group of APs that can use the virtual AP. From a configuration point of view, the entire non-hardware configuration is done. It's time to move on to configuration of the AP hardware: namely radios, RF management, etc.

---

<sup>10</sup> Also called the SSID. This document uses both interchangeably.

# Define a Wireless LAN continued

## Save your configuration!

Click the Save Configuration button in the upper right corner of the screen to save your configuration.

## Create an AP radio profile

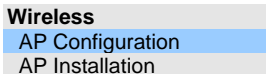
The AP Radio Profile defines the radio mode(s) for the access points in our AP group. It also specifies the behavior for the RF management (ARM).

In this network design, we will have APs, but we are also going to make use of a feature that allows Aruba APs to be configured as dedicated air monitors (AMs). This is particularly useful for location tracking, intrusion detection, and so on.

So we will create two radio profiles: one for the Access Points and a second for Air Monitors. To do all of this we will:

- ◆ Create a radio profile for any APs with 802.11a radios
- ◆ Add an ARM profile to 802.11a radio profile
- ◆ Create a radio profile for any APs with 802.11b/g radios
- ◆ Add an ARM profile to the 802.11b/g radio profile
- ◆ Define optimization parameters for RF

## Create an 802.11a radio profile for APs in Sunnyvale



Here are the steps to create an 802.11a radio profile:

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu select **Wireless: AP Configuration**
- 3 Click the Edit button next to the Sunnyvale\_APs
- 4 Click on RF Management
- 5 Click on 802.11a radio Profile
- 6 With the default profile shown in the text box, click the Save As button to create a copy of the default radio profile. We'll edit this rather than change the default profile.
- 7 Under 802.11a radio profile> enter Sunnyvale\_80211a\_Radios in the text field next to –NEW–
- 8 Click the Apply button to save your profile

## Define a Wireless LAN continued

### Add an ARM profile for 802.11a radios in Sunnyvale

Now we'll define how RF management is done for 802.11a radios:

- 1 On the left-hand side of the main window, under the 802.11a radio profile click on Adaptive Radio Management (ARM) Profile
- 2 From the drop-down box on the top of the screen, select –NEW–
- 3 Enter Sunnyvale\_80211a\_ARM in the text field
- 4 Change the following values from their defaults:

Parameter	Value
Min Tx Power	14

- 5 Click the Apply button to save your changes.

### Create an 802.11g radio profile for Sunnyvale APs

Wireless
AP Configuration
AP Installation

Here are the steps to create an 802.11g radio profile:

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu select **Wireless: AP Configuration**
- 3 Click the Edit button next to Sunnyvale\_APs
- 4 Click on RF Management
- 5 Click on 802.11g radio Profile
- 6 With the default profile shown in the text box, click the Save As button to create a copy of the default radio profile
- 7 Under 802.11g radio profile> enter Sunnyvale\_80211g\_Radios in the text field next to –NEW–
- 8 Click the Apply button to save your profile

### Add an ARM profile for 802.11ab/g radios in Sunnyvale

Now we'll define how RF management is done for 802.11b/g radios:

- 1 On the left-hand side of the main window, under the 802.11g radio profile click on Adaptive Radio Management (ARM) Profile
- 2 From the drop-down box on the top of the screen, select –NEW–
- 3 Enter Sunnyvale\_80211g\_ARM in the text field
- 4 Click the Apply button to save your changes

➤ **Note:** Although in this case we didn't make any changes from the 802.11g defaults for our 802.11b/g radios, it is good practice to make copies of profiles rather than edit the default directly. This makes later customization much simpler.

## Define a Wireless LAN continued

### RF optimization profile

This profile defines parameters for optimizing the client experience on the wireless network. As before, it is best practice to generate a new profile as a copy of the default and then make modifications if required. In the base configuration, a copy will be made of the default settings, but no parameters will be changed at this time. In general, these defaults work well in most environments.

### Add RF Optimization Profile

Wireless
AP Configuration
AP Installation

Here are the steps:

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu select **Wireless: AP Configuration**
- 3 Click the Edit button next to the Sunnyvale\_APs
- 4 Click on RF Management
- 5 Click on RF Optimization Profile
- 6 With the default profile shown in the text box, click Save As to make a copy of this profile
- 7 Enter Sunnyvale\_RF\_Optimization in the text field next to – NEW—
- 8 Click the Apply button to save your profile

### Save your configuration!

Click the Save Configuration button in the upper right corner of the screen to save your configuration.

# AP Deployment Planning

## Overview

Prior to ArubaOS 3.1, Aruba controllers determined AP configuration and ARM behavior via a *location ID*. A location ID is a numerical ID based on the building number, floor number and ID for the AP. For example: 1.2.5 would be used for building #1, floor #2, AP #5.

The profile approach we have used in this document provides a much more flexible and useful means of creating configuration profiles for different groups of APs. However, the controllers still need to understand the physical deployment of the Aps. This is required for the Adaptive Radio Management (ARM) scanning as well as location tracking services. The profiles, as we have used them so far, do not provide any information on physical location.

## Fully Qualified Location Name (FQLN)

ArubaOS 3.1 builds on these concepts by introducing *Fully Qualified Location Names (FQLN)*. FQLNs use descriptive text strings rather than numbers to provide a simpler, more intuitive naming convention. FQLNs also include a new location feature, *Campus*, which is one level above building; allowing for related multi-building groups.

## Getting started

Once a controller is configured with all of its profiles and AP groups the next process is to identify where each Access Point will be located, its name and AP group membership.

Once this has been completed, AP provisioning can take place. Each AP is provisioned with the correct name as determined from the RF Plan tool. The system can then tie the AP to a physical location and perform the relevant RF management based on this data.

## Provisioning process

The entire process for determining provision information for Aps is as follows:

- 1 Use the RF Plan tool to define your campus, buildings, floors
- 2 Use the RF Plan tool to create an AP and AM deployment model plan that determines where each device should be located based on a floor plan schematic
- 3 Use the FQLN Mapping tool to create AP and AM names

This document does not go through all of the steps required for RF Plan. Since building floor plans are unique, please use your own plans. For more information on how to use the RF Plan tool, please refer to the ArubaOS 3.1 User Guide.

# AP Deployment Planning continued

## Sample RF Plan values

For reference in the rest of this document, we are using the following assumptions:

Parameter	Value
Campus	Sunnyvale
Building	1
Floors	1,2
AP Names	Lobby-AP1, Cafeteria-AP1, Office-AP1

➡ **Note:** Although we are not configuring Ams in this example, you would follow the same steps for them in the following sections.

# AP Provisioning

## Overview

With the last section we have now completed all configuration: from WLAN configuration values to the actual hardware placement.

The final part of any deployment for an Aruba solution is the deployment of the Access Points and Air Monitors. The planning and design phase covered up until this point in the document has been aimed at making the deployment phase as simple as possible with the minimum of expertise required and the least number of potential issues.

## Provisioning options

Any provisioning of an AP requires that the hardware (as determined by the MAC address or serial number) be correctly matched to the AP name identified by the RF Plan tool.

There are two ways to do this:

- 1 Pre-configure each AP with the correct AP name and group before installation
- 2 Install factory-default (unconfigured) Aps and provision via physical ID (MAC address or serial number)

Each is an entirely valid method for AP provisioning. Which one is used will depend upon the specific expertise available at deployment time. The first option guarantees each AP is correctly configured, however it does require that the installation technician install the exact, correct AP at each location. If an AP is installed at the wrong place it can impact ARM and location tracking performance.<sup>11</sup>

The second option is somewhat simpler in that any AP of the correct type may be installed. It does, however, rely on the installer to record the MAC address or serial number of the AP and where it was installed. This will then be used to configure the AP from the management interface.

---

<sup>11</sup> So what if you don't want to match physical hardware with APs on a floor plan in the RF Planner? You will still get a nicely functional WLAN, but you will miss out on some RF optimization and the ability to track and locate a wireless device. Location tracking uses triangulation which requires, you guessed it, at least three APs or AMs whose location is known.

# AP Provisioning continued

## Provision an AP

- Wireless
- AP Configuration
- AP Installation

Regardless of which method you use, you will need to tell the Aruba management system which physical AP matches a particular AP group member. This means, at some point, you will likely end up on the management interface.

This document uses the second option. We assume all of the Aps installed are unconfigured and configure them via the management console.

Here are the steps to provision an AP from the Web UI management interface of the controller:

- 1 On the top of the screen, select the **Configuration** tab
- 2 On the left-hand menu click on **Wireless: AP Installation**
- 3 Choose an AP to configure by selecting the checkbox next to it
- 4 Click the Provision button to begin configuration
- 5 Select the AP group this AP will be a member of from the drop-down box at the top: Sunnyvale\_Aps<sup>12</sup>
- 6 Enter the FQLN name for the AP in the AP Name field at the bottom of the screen
- 7 Click the Apply and Reboot button to save your changes and reboot the AP<sup>13</sup>

## Save your configuration!

Click the Save Configuration button in the upper right corner of the screen to save your configuration.

<sup>12</sup> If you have Air Monitors, you would provision them the same way; just choose the appropriate AM group

<sup>13</sup> When changing fundamental configuration information for an AP such as the name, IP settings or the name of the master controller, a reboot is required for immediate effect

## Design Review

**Overview** This section reviews the design.

**Where did we start?** As you may recall, our original network looked like this:

Insert network diagram

**What did we do?** Now that we have finished this best practice design we have the following:

- ◆ An Aruba mobility controller, configured on the base network topology
- ◆ An enterprise-class WLAN for employees
- ◆ Employee vs. Superuser differentiation of access rights on the same VLAN
- ◆ Protected internal network resources from the employee WLAN
- ◆ Radio and RF management and optimization

<b>Network</b>
Controller
VLANs
Ports
IP
<b>Security</b>
Authentication
Access Control
<b>Wireless</b>
AP Configuration
AP Installation
<b>Management</b>
General
Administration
Certificates
SNMP
Logging
Clock
<b>Advanced Services</b>
Redundancy
IP Mobility
Stateful Firewall
External Services
VPN Services
Wired Access
Wireless
All Profiles