ArubaOS Remote Networking Version 3.1

User Guide

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. The Open Source code used can be found at this site:

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.

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1

Introduction

The ArubaOS Secure Remote Access Point Service allows users at any remote location equipped with an AP to connect to an Aruba controller over the Internet. These remote APs connect to the controller using Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPsec) and send 802.11 data traffic through this tunnel. Secure Remote Access Point Service extends the corporate office to the remote site by giving remote users access to some of the same network features as corporate office users. For example, voice over IP (VoIP) applications can be extended to remote sites while the servers and the PBX remain secure in the corporate office.

This ArubaOS Remote Networking User Guide is a resource for network administrators who have some familiarity with Aruba controllers and APs, and want to extend the benefits of remote networking to users in branch and home offices. If you have not yet designed your remote network topology, or if you are not familiar with the Aruba Networks products, you may want to refer to the Remote Networks Validated Reference Design, available for download at the Aruba Networks website.

This first chapter of the ArubaOS Remote Networking User Guide describes the following topics:

Remote AP Topology Overview

Secure Remote Access Point Service can also be used to secure control traffic between an AP and the controller in a corporate environment. In this case, both the AP and controller are in the company's private address space.

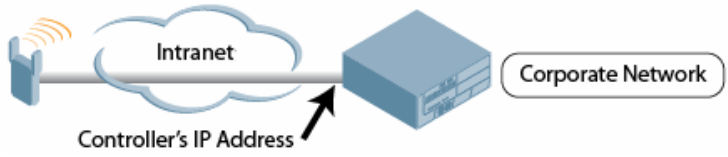
The following APs support remote AP operation:

- AP-60
- AP-61
- AP-65
- AP-70
- AP-80M
- AP-85
- AP-120 series
- RAP-2WG
- RAP-5WN
- RAP-5
- AP-2E

The remote AP must be configured with the IP address of the IPsec VPN tunnel termination point, which can be the controller IP address, or the IP address of the corporate firewall. Once the VPN tunnel is established, the remote AP bootstraps and becomes operational. The tunnel termination point used by the remote AP depends upon the AP deployment, as shown in the following scenarios:

- **Deployment Scenario 1:** The remote AP and controller reside in a private network which is used to secure AP-to-controller communication. (Aruba recommends this deployment when AP-to-controller communications on a private network need to be secured.) In this scenario, the remote AP uses the controller's IP address on the private network to establish the IPsec VPN tunnel.

Figure 1 *Remote AP with a Private Network*

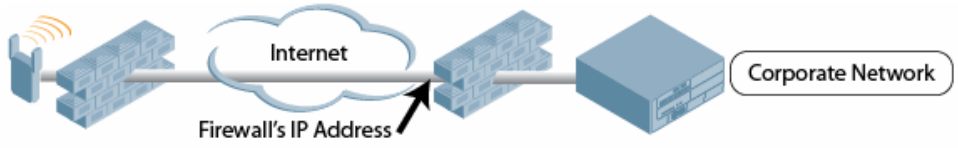


- **Deployment Scenario 2:** The remote AP is on the public network or behind a NAT device and the controller is on the public network. The remote AP must be configured with the tunnel termination point which must be a publicly routable IP address. In this scenario, a routable interface is configured on the controller in the DMZ. The remote AP uses the controller's IP address on the public network to establish the IPsec VPN tunnel.

Figure 2 *Remote AP with Controller on Public Network*

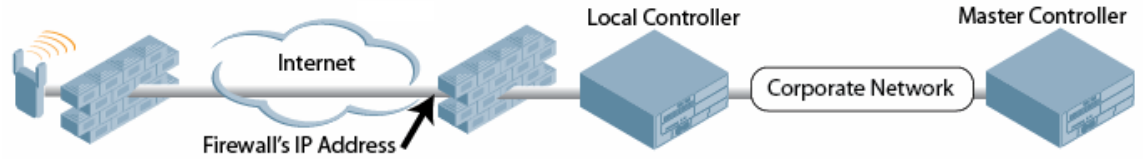
- **Deployment Scenario 3:** The remote AP is on the public network or behind a NAT device and the controller is also behind a NAT device. (Aruba recommends this deployment for remote access.) The remote AP must be configured with the tunnel termination point which must be a publicly routable IP address. In this scenario, the remote AP uses the public IP address of the corporate firewall. The firewall forwards traffic to an existing interface on the controller. (The firewall must be configured to pass NAT-T traffic (UDP port 4500) to the controller.)

Figure 3 *Remote AP with Controller Behind Firewall*



In any of the above deployment scenarios, the IPsec VPN tunnel can be terminated on a local controller, with a master controller located elsewhere in the corporate network (Figure 4). The remote AP must be able to communicate with the master controller after the IPsec tunnel is established. Make sure that the L2TP IP pool configured on the local controller (from which the remote AP obtains its address) is reachable in the network by the master controller.

Figure 4 *Remote AP in a Multi-Controller Environment*

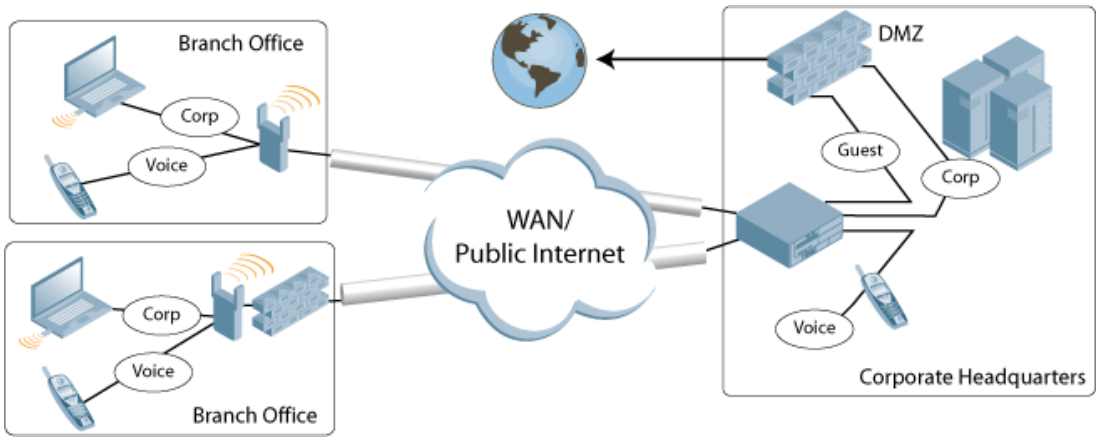


Deploying a Branch Office/Home Office Solution

In a branch office, the AP is deployed in a separate IP network from the corporate network. Typically, there are one or two NAT devices between the two networks. Branch office users need access to corporate resources like printers and servers but traffic to and from these resources must not impact the corporate head office.

The Figure 5 is a graphic representation of a remote AP in a branch or home office with a single controller providing access to both a corporate WLAN and a branch office WLAN.

Figure 5 *Remote AP with Single Controllers*



Branch office users want continued operation of the branch office WLAN even if the link to the corporate network goes down. The branch office AP solves these requirements by providing the following capabilities on the branch office WLAN:

- Local termination of 802.11 management frames, which provides survivability of the branch office WLAN.
- All 802.1x authenticator functionality is implemented in the AP. The controller is used as a RADIUS pass-through when the authenticator has to communicate with a RADIUS server (which also supports survivability).
- 802.11 encryption/decryption functionality is also in the AP, which provides access to local resources.
- Local bridging of client traffic connected to the WLAN or to an AP-70 wired port to provide access to local resources.

Understanding Remote AP Modes of Operation

Table 1 summarizes the different remote AP modes of operation. You can specify both the forward mode setting (which controls whether 802.11 frames are tunneled to the controller using GRE, bridged to the local Ethernet LAN, or a combination thereof) and the remote AP mode of operation (when the virtual AP operates on a remote AP) in the virtual AP profile.

The column on the left of the table lists the remote AP operation settings. The row across the top of the table lists the forward mode settings. To understand how these settings work in concert, scan the desired remote AP operation with the forward mode setting and read the information in the appropriate table cell.

The “all” column and row lists features that all remote AP operation and forward mode settings have in common regardless of other settings. For example, at the intersection of “all” and “bridge,” the description outlines what happens in bridge mode regardless of the remote AP mode of operation.

802.1x and PSK authentication is supported when you configure the remote AP to operate in bridge or split-tunnel mode.

Table 1 *Remote AP Modes of Operation and Behavior*

Remote AP Operation Setting	Forward Mode Setting			
	all	**bridge**	**split-tunnel**	**tunnel**
all		Management frames are handled on the remote AP. Frames are bridged between wired and wireless interfaces. No frames are tunneled to the controller. Station acquires its IP address locally from the RAP internal DHCP server or from an external DHCP server.	Some management frames are handled on the remote AP, while others are handled on the controller. (This can vary, depending on whether 802.1x authentication is used.) Frames are either GRE tunneled to the controller or NATed and bridged on the wired interface according to user role and session ACL. Typically, the station obtains an IP address from a VLAN on the controller and the AP has ACLs that forward corporate traffic through the tunnel and source NAT the non-corporate traffic to the Internet.	Some management frames are handled on the remote AP, while others are handled on the controller. (This can vary, depending on whether 802.1x authentication is used.) Frames are GRE tunneled to the controller. All of the station frames are tunneled to the controller.
always	ESSID is always up when the AP is up regardless if the controller is reachable. Supports PSK ESSID only. SSID configuration stored in flash on AP.	Provides an SSID that is always available for local access.	Not supported	Not supported
backup	ESSID is only up when controller is unreachable. Supports PSK ESSID only. SSID configuration stored in flash on AP.	Provides a backup SSID for local access only when the controller is unreachable.	Not supported	Not supported

Table 1 *Remote AP Modes of Operation and Behavior (Continued)*

Remote AP Operation Setting	Forward Mode Setting			
persistent	ESSID is up when the AP contacts the controller and stays up if connectivity is disrupted with the controller. SSID configuration obtained from the controller. Designed for 802.1x SSIDs.	Same behavior as standard, described below, except the ESSID is up if connectivity to the controller is lost.	Not supported	Not supported
standard	ESSID is up only when there is connectivity with the controller. SSID configuration obtained from the controller.	Behaves like a classic Aruba branch office AP. Provides a bridged ESSID that is configured from the controller and stays up if there is controller connectivity.	Split tunneling mode.	Classic Aruba thin AP operation.

Hardware-Specific Features

Some new software feature are hardware specific. Table 2 lists these software features and the hardware supported on each feature.

Table 2 *Software Feature that are Hardware Specific*

Controller	Cert Based	Zero Touched Provisioning	USB Modem
200, 800, 2400, SC1, SCII	Not Supported	Not Supported	AP-70, 2E, RAP-5, RAP-5WN
3000, Multi-Service Mobility Module (M3)	RAP-5, RAP-5WN, RAP-2WG	RAP-5, RAP-5WN, RAP-2WG	AP-70, 2E,RAP-5, RAP-5WN

The RAP-5, RAP-5WN, and RAP-2WG are compatible with any standard compliance VoIP phone. Extensive inter-operability tests were performed on the VoIP devices in Table 3.

Table 3 *Validated VoIP Phones*

Vendor	Model
Ascom	i75 (in SIP mode)
Avaya	3631, 4610, and 4621
Cisco	7921 and 7960
Hitachi	Wireless IP 5000
Nokia	E51
SJ Phones	Cisco 7960
SVP	8020 and 8030
Vocera	B1000A and B2000

The RAP-5, RAP-5WN, and RAP-2WG are compatible with the scanners and printer listed in Table 4.

Table 4 *Validated Scanners*

Vendor	Model
Symbol Scanner	MC 3090, MC 5040, MC 9090G, PPT 8864
Intermec Scanner	CN2B
HP Printer	HP6988

Remote User Age-Out Behavior

Tunnel, split tunnel or bridge users have different age out behaviors.

- Tunnel (wired or wireless) users—The remote user age-out is based on the AAA age-out timer
- Split Tunnel (wired or wireless) users—Remote user age-out is based on AAA age-out timer for wireless. Not dependant on AAA age-out timer for wired user.
- Bridge (wired or wireless) users—Remote users age-out immediately; not dependant on AAA age-out timer.

Chapter 2

Configuring the Controller for Remote Networking

Configuring your Controller

Before you can install a remote AP, you must configure the VPN server, and get your local controller ready to authenticate these APs. you must have already verified that you have installed one or more remote AP licenses in the controller. There are several remote AP licenses available that support different maximum numbers of APs. The licenses are cumulative; each additional license installed increases the maximum number of remote APs supported by the controller Verify that you have these licenses before begin.

- **Remote AP Licenses**: The Secure Remote Access Point Service requires that you install one or more remote AP licenses in the controller on which you terminate the VPN tunnel that carries traffic from the remote AP. There are several remote AP licenses available that support different maximum numbers of APs. The licenses are cumulative; each additional license installed increases the maximum number of remote APs supported by the controller.

  You must install a remote AP license on any controller that you use to *provision* a remote AP.
- **Policy Enforcement License**: If you configure custom user roles or policies, you must install a Policy Enforcement license in the controller.


NOTE

Although the VPN service is used for Remote Networking, the VPN software license is not required for basic Remote Networking operations unless your deployment requires site-to-site VPN between controllers,

This chapter describes the tasks for configuring an Aruba controller for the basic Secure Remote Access Point Service:

- "Step 1: Configure the Controller IP Address" on page 11.
- "Step 2: Configure the VPN authentication Server" on page 12
- "Step 3: Configure the Remote AP User Role" on page 13
- "Step 4: Configure VPN Authentication" on page 14
- "Step 5: (Optional) Configure Remote AP Authentication" on page 15
- "Step 6: (Optional) Configure Controller DNS Settings" on page 18
- "Step 7: (Optional) Configure Double Encryption" on page 18


NOTE

Advanced controller configuration options not required for an initial remote AP deployment are described in "Managing the RAP Network" on page 47

Step 1: Configure the Controller IP Address

A remote AP needs an IP address to which it can connect in order to establish a VPN tunnel. The remote AP can either use the routable IP address that has already been configured on the controller, or the address of an external router or firewall that forwards traffic to the controller. If you are not sure which topology your remote APs will use, refer to "Remote AP Topology Overview" on page 5.

If the remote APs can establish a VPN tunnel directly to a controller, you can skip this step and use the controller's currently configured IP address. However, if the remote AP must establish a VPN tunnel to an external router or firewall, you must define a DMZ address that will forward traffic to the controller. If both

the controller and the remote AP are behind a NAT device, you must also configure the NAT device to forward traffic to the controller.

Define a DMZ Address

The following procedures describe how to define a routable DMZ address on the controller using the WebUI and the Command Line Interface (CLI).

Using the WebUI to create a DMZ address

1. Navigate to the **Configuration > Network > VLANs** window.
2. Click **Add** to add a VLAN.
3. Enter the VLAN ID.
4. Select the port that belongs to this VLAN.
5. Click **Apply**.
6. Navigate to the **Configuration > Network > IP** window.
7. Click **Edit** for the VLAN you just created.
8. Enter the appropriate IP address and netmask in the **IP Address** and **Net Mask** fields.
9. Click **Apply**.

Using the CLI to create a DMZ address

```
vlan <id>
interface fastethernet <slot>/<port>
   switchport access vlan <id>
interface vlan <id>
   ip address <ipaddr> <mask>
```

Configure the NAT Device

Communication between the remote AP and secure controller uses the UDP 4500 port. When both the controller and the AP are behind NAT devices, configure the AP to use the NAT device's public address as its master address. On the NAT device, you must enable NAT-T (UDP port 4500 only) and forward all packets to the public address of the NAT device on UDP port 4500 to the controller to ensure that the remote AP boots successfully.

Step 2: Configure the VPN authentication Server

This section describes how to configure the IPsec VPN server on the controller. The remote AP will be a VPN client that connects to the VPN server on the controller.

Configure the VPN Server

This section describes how to configure the IPsec VPN server on the controller. For more details, refer to the ArubaOS User Guide. The remote AP will be a VPN client that connects to the VPN server on the controller.

Using the WebUI to configure VPN server

1. Navigate to the **Configuration > Advanced Services > VPN Services**
2. Select the **IPSEC** tab.
3. Click **Add** in the **Address Pools** section.
4. Enter a name for the L2TP pool from which the APs will be assigned addresses, then specify the start and end addresses.

5. Click **Done** to return to the IPSEC tab.

The size of the pool should correspond to the maximum number of remote APs that the controller is licensed to manage. If you configure the pool on a local controller, it must be routable on the Internet to reach the master controller.

6. To configure an Internet Security Association and Key Management Protocol (ISAKMP) encrypted subnet and preshared key, click **Add** in the **IKE Shared Secrets** section and configure the preshared key. Click **Done** to return to the **IPSEC** tab.
7. Click **Apply**.

Using the CLI to configure VPN server

```
ip local pool <pool> <start-ipaddr> <end-ipaddr>
crypto isakmp key <key> address <ipaddr> netmask <mask>
```

Step 3: Configure the Remote AP User Role

Once the remote AP is authenticated for the VPN and established a IPsec connection, it is assigned a role. This role is a temporary role assigned to the AP until it completes the bootstrap process after which it inherits the ap-role. The appropriate ACLs need to be enabled to permit traffic from the controller to the AP and back to facilitate the bootstrap process.

User roles and policies require the Policy Enforcement Firewall license. You must install the Policy Enforcement Firewall license, as described in the ArubaOS User Guide.

To configure the user role, you first create a policy that permits the following traffic:

- AP control traffic via the Aruba PAPI protocol
- GRE tunnel traffic
- TFTP traffic from the remote AP to the controller
- FTP traffic from the remote AP to the controller

Then, you create a user role that contains this policy.

Using the WebUI to configure the user role

1. Navigate to the **Configuration > Security > Access Control > Policies** window.
2. Click **Add** to create a policy.
3. Enter the Policy Name (for example, remote-AP-access).
4. From the **Policy Type** drop-down list, select **IPv4 Session**.
5. To create the first rule:
   a. Under **Rules**, click **Add**.
   b. For **Source**, select **any**.
   c. For **Destination**, select **any**.
   d. For **Service**, select **service**, then select **svc-papi**.
   e. Click **Add**.
6. To create the next rule:
   a. Under **Rules**, click **Add**.
   b. For **Source**, select **any**.

c. For **Destination**, select **any**.

d. For **Service**, select **service**, then select **svc-gre**.

e. Click **Add**.

7. To create the next rule:
   a. Under **Rules**, click **Add**.
   b. For **Source**, select **any**.
   c. For **Destination**, select **alias**, then select **controller**.
   d. For **Service**, select **service**, then select **svc-tftp**.
   e. Click **Add**.
8. To create the next rule:
   a. Under **Rules**, click **Add**.
   b. For **Source**, select **any**.
   c. For **Destination**, select **alias**, then select **controller**.
   d. For **Service**, select **service**, then select **svc-ftp**.
   e. Click **Add**.
9. Click **Apply**.
10. Click the **User Roles** tab.
    a. Click **Add**.
    b. Enter the Role Name (for example, RemoteAP).
    c. Click **Add** under Firewall Policies.
    d. In the Choose from Configured Policies menu, select the policy you just created.
    e. Click **Done**.
11. Click **Apply**.

Using the CLI to configure the user role

```
ip access-list session <policy>
   any any svc-papi permit
   any any svc-gre permit
   any alias controller svc-tftp permit
   any alias controller svc-ftp permit

user-role <role>
   session-acl <policy>
```

Step 4: Configure VPN Authentication

When you provision a remote AP, you must configure IPsec settings for the AP. The authentication server can be any type of server supported by the controller, including the controller's internal database. A username and password must be validated by an authentication server before the remote AP is allowed to establish a VPN tunnel to the controller.

Follow the steps below if you are provisioning a RAP-5x series or RAP-2x series remote AP using certificated-based authentication and a RAP whitelist, or if you are provisioning legacy APs for authentication using an IKE pre-shared KEY and a RAP username and password.

Set the Default VPN Authentication Role

1. Navigate to the **Configuration > Security > Authentication > L3 Authentication** window.
2. In the Profiles list, select **VPN Authentication Profile**.
3. For Default Role, enter the user role you created in "Step 3: Configure the Remote AP User Role" on page 13 (for example, rap_role).
4. Click **Apply**.
5. In the Profile list, under VPN Authentication Profile, select **Server Group**.
6. Select the **internal** server group from the drop-down list.
7. Click **Apply**.

Configure VPN authentication Using the CLI

```
aaa authentication vpn
   default-role rap_role
   server-group internal
```

Add the Remote AP User to the Internal Database

Finally, you just add the remote AP user to the internal database.

1. Navigate to the **Configuration > Security > Authentication > Servers** window.
2. Select **Internal DB**.
3. Click **Add User** in the Users section. The user configuration window displays.
4. Enter the user name and password.

If your deployment requires higher levels of security, Aruba recommends you assign a unique username and password to each remote AP.

5. Click **Enabled** to activate this entry on creation.
6. Click **Apply** to apply the configuration. Note that the configuration does not take effect until you perform this step.
7. From the **Servers** window, click **Apply**.

Add the Remote AP User Using the CLI

```
local-userdb add username rapuser1 password <password>
```

Step 5: (Optional) Configure Remote AP Authentication

When you provision a remote AP to use certificated-based authentication, the AP's MAC address is automatically added to the RAP whitelist.

You can also set up additional control mechanisms to ensure your remote APs are securely authenticated and connected to your enterprise network. This type of certificate-based authentication is only supported by AP models RAP-2WG,RAP-5 and RAP-5WN. Legacy RAPs do not support this type of remote AP authentication.

Create an Authorization Profile Using the CLI

You can create an authorization profile for an AP group to force the unauthorized RAPs in that group to use a different AP group configuration. The authorization profile **default** is predefined, and provides a simple way to configure an authorization profile without manually defining each individual related profile. This default authorization profile allows RAPs to access a wired port and authenticate using captive portal.

The **default** authorization profile references the authorization AP group **NoAuthApGroup,** which has been predefined with references to the AAA profile **NoAuthAAAProfile and the** wired Ap profile **NoAuthWiredPort.** If these profiles have been deleted or significantly changed from their default settings, the default authorization profile may not work correctly.

The following CLI commands add the default authentication profile to an AP group named RAP-group1. For WebUI configuration steps, see "Create an Authorization Profile Using the WebUI" on page 16.

1. Specify the group of remote APs to which you want to assign the default authorization profile.

```
(host) (config) #ap-group RAP-group1
(host) (AP group "RAP-group1") #authorization-profile default
```

2. The AAA profile used by the default authorization profile, **NoAuthAAAProfile**, uses the **logon** user role as its initial role. You should verify that the captive portal profile for this user role, and make sure that profile has a correctly configured server group.
   a. Identify the initial user role for the AAA profile **NoAuthAAAProfile**. This should be the **logon** role, unless the profile has been changed from its original settings.

```
{host) #show aaa profile NoAuthAAAProfile
```

   b. Identify the captive portal profile for the user role identified in step a.

```
{host) #show rights logon
```

   c. Define the server group for the captive portal profile identified in step b.

```
{host) (config) #aaa authorization captive-portal default server-group internal
```

Create an Authorization Profile Using the WebUI

You can also use the controller's WebUI to set up an Authorization profile. The following procedures step you through this WebUI configuration process.

1. Navigate to the **Configuration** > **AP Configuration** window and click the **AP Group** tab.
2. Now you must decide if you want to assign an Authorization profile to an existing AP group or a new AP group.
   a. **To select an existing AP group**, click the **Edit** button by the AP group name.
   -or-
   b. **To create a new AP group**, click the **New** button at the bottom of the AP group list, enter a name for the new group, then click **Add**. The new AP group will appear in the AP group list. Click the **Edit** button by the new AP group.
3. In the Profiles list, expand the **AP** menu, then select **Authorization Profile.**
4. Click the **Ap authorization profile** drop-down list and select the **default** profile.
5. Click **Apply** to save this setting.

As mentioned in the CLI instructions, the AAA profile used by the default authorization profile, **NoAuthAAAProfile**, uses the **logon** user role as its initial role. You should verify that the captive portal profile for this user role, and make sure that profile has a correctly configured server group.

1. Navigate to the **Security** > **Authentication** window and click the **AAA Profiles** tab.
2. In the AAA Profile list, select **NoAuthAAAProfile**. The right window pane will display the initial role associated with this profile. (By default, this is the **logon** user role.)
3. Now, verify the captive portal profile associated with the this user role.
4. Navigate to the **Configuration>Access Control** window, and click the **User Roles** tab.
5. Click the **Edit** button by the initial role you identified in step 2, above.
6. Scroll down the **Security>User Roles>Edit Role** window to the Captive Portal Profile section. Make a note of the profile name listed under the Captive Portal Profile heading. (The default captive portal profile for the **logon** role is **default**.)

7. Now, you must verify the server group used by this captive portal profile. Navigate to **Configuration>All Profiles** and expand the **Wireless Lan** menu.
8. Expand the **Captive Portal Authentication Profile** menu, and select the captive portal profile you identified in step 6, above.
9. Click the name of the Server Group associated with this profile to display the **Profile Details** window for this server profile. Review the configuration parameters for this server group and verify that it is configured correctly.

Rebooting Unauthenticated RAPs

You can selectively reboot unauthenticated remote APs that are part of an AP group to which an authorization profile is applied. Use the **show ap database** command to view the remote APs in your database. The *R-* flags indicates an unauthorized remote AP.

```
(host) (config) # show ap database
AP Database
-----------
Name  Group    AP Type  IP Address   Status     Flags  Switch IP
----  -----    -------  ----------   ------     -----  ---------
Sam   default  RAP-5    172.16.0.42  Up 2m:47s  R-     10.10.10.50
Doe   local    RAP-5WN  172.16.0.41  Up 3m:2s   R      10.10.10.50
```

To reboot unauthenticated RAPs in your the AP group **default**, run the following command:

```
(host) (config) #apboot ap-group default global provisioned
```

To reboot all unauthenticated RAPs, run the following command:

```
(host) (config) #apboot all global provisioned
```

Step 6: (Optional) Configure Controller DNS Settings

In addition to specifying IP addresses for controllers, you can also specify the master DNS name for the controller when provisioning the remote AP. The name must be resolved to an IP address when attempting to setup the IPsec tunnel. For information on how to configure a host name entry on the DNS server, refer to the vendor documentation for your server. Aruba recommends using a maximum of 8 IP addresses to resolve a controller name.

If the remote AP gets multiple IP addresses responding to a host name lookup, the remote AP can use one of them to establish a connection to the controller. For more detailed information, see the next section "Backup Controller List" on page 60.

Specifying the name also lets you move or change remote AP concentrators without reprovisioning your APs. For example, in a DNS load-balancing model, the host name resolves to a different IP address depending on the location of the user. This allows the remote AP to contact the controller to which it is geographically closest.

The DNS setting is part of provisioning the AP. The easiest way to provision an AP is to use the Provisioning window in the WebUI. These instructions assume you are only modifying the controller information in the Master Discovery section of the Provision window.


NOTE

Reprovisioning the AP causes it to automatically reboot.

To specify the DNS name:

1. Navigate to the **Configuration > Wireless > AP Installation > Provisioning** window. Select the remote AP and click **Provision**.
2. Under **Master Discovery** enter the master DNS name of the controller.
3. Click **Apply and Reboot**.

Step 7: (Optional) Configure Double Encryption

The double encryption feature applies only for traffic to and from a wireless client that is connected to a tunneled SSID. When this feature is enabled, all traffic (which is already encrypted using Layer-2 encryption) is re-encrypted in the IPsec tunnel. When this feature is disabled, the wireless frame is only encapsulated inside the IPsec tunnel.

All other types of data traffic between the controller and the AP (wired traffic and traffic from a split-tunneled SSID) are always encrypted in the IPsec tunnel.


NOTE

Aruba recommends that double-encryption not be turned on for inter-device communication over untrusted networks, as doing so is redundant and adds significant processing overhead for APs.

Using the WebUI to Enable Double Encryption

1. Navigate to the **Configuration > Wireless > AP Configuration > AP Specific** window. Click **Edit** for the remote AP.
2. Under Profiles, select AP, then select AP system profile.
3. Under Profile Details, select the AP system profile for this AP from the drop-down list. Select **Double Encrypt**. Click **Apply**.

Using the CLI to Enable Double Encryption

```
ap system-profile <profile>
   double-encrypt
   exit
ap-name <name>
   ap-system-profile <profile>
```

Chapter 3

Provisioning Remote APs

The first part of this chapter describes the basic procedures to provision a remote AP using the AP provisioning Wizard in the WebUI, the **Configuration > Wireless > AP Installation > Provisioning** window in the WebUI, or the Command Line Interface (CLI). If you are provisioning a remote AP that will use a USB modem or has multiple interfaces, be sure to review the additional information for these deployments at the end of this chapter.

This chapter includes the following information:

Before you Begin

The two most common ways to provision an AP for remote authentication are certificate-based AP provisioning and provisioning using a pre-shared key. Although both options allow for a simple secure setup of your remote network, you should make sure that the procedure you select is supported by your controller, the remote AP model type and the end user's client software. Before you select a provisioning method, consider the following requirements and limitations:

- If you are using an Aruba 200/800/2400/SC-I/SC-II controller, you must provision your APs using a pre-shared key, because these controller models to not support certificate based provisioning.
- Only the remote AP models RAP-2WG, RAP-5 and RAP-5WN can be provisioned two different ways; via certificate-based AP provisioning *or* provisioning using a pre-shared key. All other remote AP models must be provisioned using a pre-shared key.
- End users who install an remote AP using certificated-based provisioning must activate their remote AP using a client running Windows XP Professional, Windows Vista or Mac OS X Version 10.5. and one of the following validated browsers:
  - Google Chrome 1.0.154.43
  - IE 7 Version: 7.0.5730.13
  - Firefox 3.0.5
  - Firefox 2.0.0.20
  - Safari 3.1 (525.13)

  If any of your end users use clients running another operating system, they must either provision their remote AP using a pre-shared key, or gain temporary access to a client running one of the operating systems and browsers described above in order to provision a certificate-based Zero-touch AP.

AP Provisioning Wizard

The easiest way to provision any remote AP is to use the ArubaOS AP Wizard in the WebUI. This wizard will walk you through the specific steps required to provision a remote AP (or any other AP type). To access the AP wizard to provision a remote AP:

1. Select **Configuration>Wizards>AP Wizard**. The Specify Deployment Scenario window appears.
2. Select the **Remote** deployment scenario option.
3. The wizard allows you to configure remote APs to be provisioned by a user at a remote location, or provisioned by a network administrator who will connect those APs directly to the controller as the wizard is being run.
   - Select the **User-Provisioned** option to provision AP models RAP-2WG, RAP-5 and RAP-5WN using certificate-based AP provisioning.
   - Select the **Administrator-Provisioned** option to provision any AP model authenticated using a Pre-Shared Key (PSK).
4. Click **Next** to continue to the next window in the Wizard. Continue working your way through the wizard to complete the provisioning process.

If you do not want to use the provisioning wizard, you can also define certificate-based and PSK provisioning parameters for a remote AP using the **Configuration > Wireless > AP Installation > Provisioning** window in the WebUI.

Certificate-Based AP Provisioning

Certificate based authentication allows a controller to authenticate a remote AP using its certificates instead of a PSK. **This type of authentication is supported by certificated-based RAPs only (models RAP-2WG, RAP-5 and RAP-5WN).** Other remote AP models do not support this type of remote AP Authentication.

You can manually provision an individual remote AP with a full set of provisioning parameters, or simultaneously provision an entire group of remote APs by defining a provisioning profile which contains a smaller set of provisioning parameters that can be applied the entire AP group.

When you manually provision an individual remote AP to use certificated-based authentication, you must connect that AP to the controller before you can define its provisioning settings. Aruba's Zero-touch bulk provisioning feature allows you to provision a group of remote APs without ever connecting those APs to the controller, or even taking them out of the box.

- If you want to provision an individual AP for certificate-based AP provisioning see "Provisioning an Individual AP using Certificate-based Authentication" on page 22.
- If you want to provision a group of remote APs for Zero-touch certificated-based AP provisioning using a provisioning profile and the Remote AP whitelist, see "Provisioning Multiple Remote APs using a Provisioning Profile" on page 24

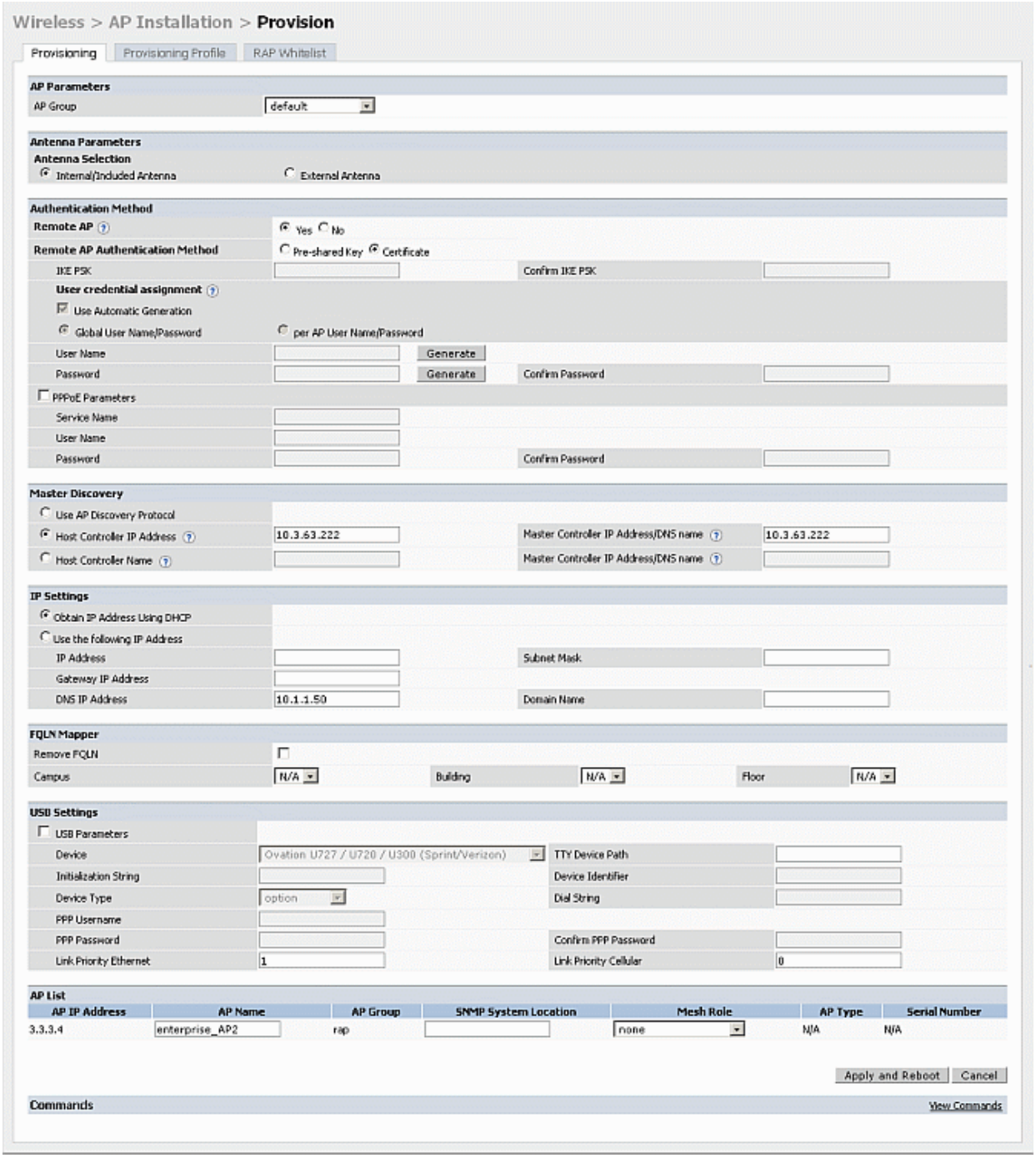
The section below describes the process to manually provision an individual Remote AP will a full set of provisioning parameters.

Provisioning an Individual AP using Certificate-based Authentication

The following steps describe the process to provision a remote AP using Certificate-based Authentication:

1. If you are provisioning a new AP that has never been provisioned before, connect the AP to the controller according the instructions included with that AP. If you are reprovisioning existing active APs as remote APs, this step is not necessary, as the APs are already communicating with the controller.
2. Navigate to the **Configuration > Wireless > AP Installation > Provisioning** window.

3. Click the checkbox by the AP you want to provision, then click **Provision**. The Provisioning window opens.



4. In the **AP Parameters** section, click the **AP Group** drop-down list and select the AP group to which this AP should be assigned.
5. (Optional) Some AP models support an external antenna in addition to their internal antenna. If the AP you are provisioning supports an external antenna, the Provisioning window displays an additional **Antenna Parameters** section. If you want to use an External antenna for the remote AP you are provisioning, select **External Antenna** and define settings for that antenna. Otherwise, the remote AP will use its internal antenna by default.
6. Click **Yes** for the **Remote AP** option.
7. In the **Remote IP Authentication Method** section, select **Certificate**.

8. (Optional) If your remote AP will use Point-to-Point Protocol over Ethernet (PPPoE) to authenticate itself to a service provider, select the **PPPoE Parameters** checkbox and enter the following PPPoE values:
   - Service Name: Either an ISP name or a class of service configured on the PPPoE server.
   - User Name: Set the PPPoE User Name for this remote AP.
   - Password: Enter and then confirm the PPPoE password for this remote AP.
9. In the **Master Discovery** section, set the Master IP Address as shown below.

Deployment Scenario	Master IP Address Value
"Remote AP with a Private Network" on page 6	Enter the controller's IP address.
"Remote AP with Controller on Public Network" on page 6	Enter the controller's public IP address.
"Remote AP with Controller Behind Firewall" on page 6	Enter the public address of the NAT device to which the controller is connected.

10. Under IP Settings, select **Obtain IP Address Using DHCP** to obtain an IP address for your AP using DHCP.

    -or-

    select **Use the Following IP address** and enter the appropriate values in the following fields:
    - IP address: IP address for the AP, in dotted-decimal format
    - Subnet mask: Subnet mask for the IP, in dotted-decimal format.
    - Gateway IP address: The IP address the AP uses to reach other networks.
    - DNS IP address: The IP address of the Domain Name Server.
    - Domain name: (optional) The default domain name.
11. (Optional) In the FQLN Mapper section, you may click the **Campus**, **Building** and **Floor** drop-down lists to identify a fully qualified location name (FQLN) for the remote AP. To clear an existing FQLN, click the **Remove FQLN checkbox.**
12. (Optional) If you are provisioning AP models AP-70, 2E, RAP-5, and RAP5-WN USB, and you want to configure them to support USB cellular modems, you must complete the fields in the **USB settings** section. For details on completing this section, see "Additional Provisioning Requirements for USB Link Interfaces" on page 29.
13. The **AP list** section displays current information for the AP you are provisioning or reprovisioning, and allows you to define additional parameters for your remote AP, such as AP Name, SNMP System Location and (if your are provisioning a Remote Mesh Point or Portal) the AP's Mesh role.
14. Click **Apply and Reboot**. (Reprovisioning the AP causes it to automatically reboot) The AP's is automatically added to the RAP whitelist in the local user database.

Provisioning Multiple Remote APs using a Provisioning Profile

Certificated-based AP provisioning also allows a network administrator to pre-provision multiple remote APs via a provisioning profile and the remote AP (RAP) whitelist. The network administrator can perform these provisioning tasks without having to plug the remote AP into the controller; the remote AP remains in its packaging untouched.

When you provision a remote AP in this manner, the RAP whitelist validates the remote AP when it is first activated and identifies the AP group to which it should be assigned. The provisioning profile assigned to that group then pushes its provisioning values to the remote AP.

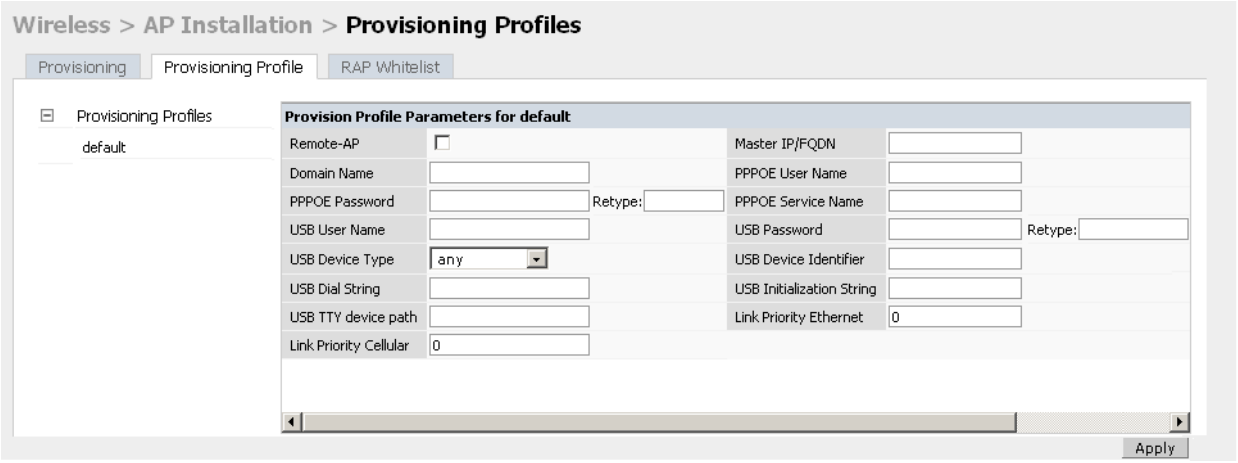
Keep the following information in mind as you create a provisioning profile.

- Provisioning profiles can apply only to remote APs using certificated-based authentication. Remember, you should not use provisioning profiles on Aruba 200/800/2400/SC-I/SC-II controllers because these controller models to not support certificate based provisioning.
- By default, an AP group does not have a provisioning profile Make sure that any provisioning profiles you create are complete and accurate before you assign that profile to an AP group. If a misconfigured provisioning profile is assigned to a group of remote APs, the remote APs in that group may be automatically provisioned with erroneous parameters and become lost.

Create A Provisioning Profile

When you create a provisioning profile, you can then apply that profile to an AP group and provision that entire group of APs with the settings in that profile.

1. Navigate to the **Configuration > Wireless > AP Installation > Provisioning** window.
2. Next, select the **Provisioning Profile** tab and enter a provisioning profile name in the text box (next to the Add button).
3. Click the **Add** button to add the profile name.
4. Select your new provisioning profile name from the list at the left.
5. Select the **Remote-AP** checkbox.
6. Enter the IP address or the fully qualified domain name of the master controller in the **Master IP/FQDN** field.



7. If your remote AP will use Point-to-Point Protocol over Ethernet (PPPoE) to authenticate itself to a service provider, select the **PPPoE Parameters** checkbox and enter the following PPPoE values:
   - PPPoE User Name: Set the PPPoE User Name for this remote AP.
   - PPPoE Password: Enter and then confirm the PPPoE password for this remote AP.
   - PPPoE Service Name: Either an ISP name or a class of service configured on the PPPoE server.
8. (Optional) If you want to use this provisioning profile to provision APs with more than one interface, you must also configure the USB settings and priority levels for this profile, as described in "Additional Provisioning Requirements for USB Link Interfaces" on page 29.
9. Click **Apply**.

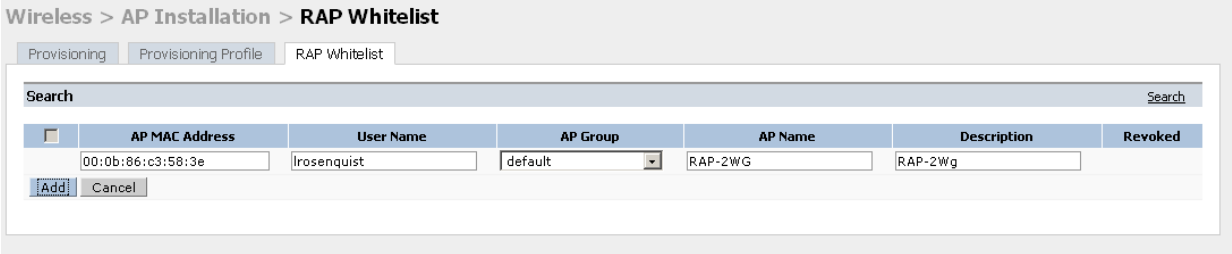
Once you have defined a provisioning profile, you must assign that profile to an AP group.

1. Navigate to the **Configuration>AP configuration** window and select the **AP group** tab.
2. Click the **Edit** button by the name of the AP group to which you want to assign the provisioning profile.

3. In the profiles list, expand the **AP** menu, and select **Provisioning Profile.** The Profile Details window appears.
4. Click the **Provisioning Profile** drop-down list and select the name of the provisioning profile you want to assign to this AP group.
5. Click **Apply**.

Finally, add information for your remote APs into the RAP whitelist.

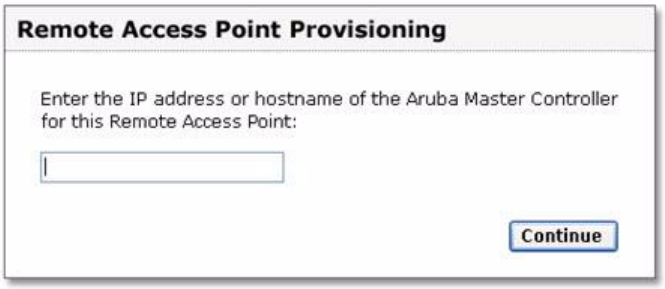
1. Navigate to the **Configuration>AP Installation** window and click the **RAP whitelist** tab. The **RAP whitelist** window opens, as shown below.



2. Click **New**.
3. Fill in the fields in this window with the following information:
   - **AP MAC Address**: MAC address of the remote AP, in colon-separated octets.
   - **User Name**: Name of the end user who will provision and use the remote AP.
   - **AP Group**: Select the name of the AP group to which the remote AP will be assigned.
   - **AP Name**: (Optional) Name of the remote AP. If you not specify a name, the AP will use its MAC address as a name.
   - **Description**: (Optional) A brief description to help you identify the AP.
4. Click **Add** to add the remote AP to the whitelist.
5. Repeat the above steps for each remote AP you are provisioning via a provisioning profile.

Zero-Touch (Certificate-based) Local Provisioning for a Remote AP

Once a network administrator has provisioned the remote APs, end users can activate their remote AP by connecting their client to the remote AP and entering the IP address or hostname of the Aruba master controller into the **Remote Access Point Provisioning** dialog box (below).



The Aruba RAP-5, RAP-5WN and RAP-2WG must be in controller-less environment (L3 separated) for Zero-touch provisioning to be successful. Customers using cable modems might need to reboot their modems if connected clients for Zero-touch provisioning do not negotiate their IP or get a limited network connections.

For additional troubleshooting information for Zero-touch provisioning and local debugging of a remote AP, see "Local Debugging" on page 47 and "Resetting the RAP-2x and RAP-5x to Factory Settings" on page 73. For complete information on local provisioning for a Remote AP, refer to the documentation included with that AP.

Provisioning a Remote AP using Pre-Shared Key

This Pre-Shared Key (PSK) authentication is supported by all Aruba APs. You can configure Pre-Shared Key (PSK) remote AP provisioning for an individual remote AP, or configure a group of remote APs in bulk.

- **PSK based per-RAP Provisioning:** This feature provides automatic generation of both user name and password per RAP. Manual generation of user names and passwords is still available.
- **PSK based Bulk RAP Provisioning:** This feature, available through the WebUI only, allows you to select multiple remote APs in the same group and of the same AP type from the **Configuration>AP Installation** window, and then define a set of provisioning parameters to provision them all at once, or in "Bulk". Using bulk-provisioning you can change the remote APs in one group to another group all at once, and generate new user credentials for those remote APs in the local database, by generating user names and passwords either manually or by automatic generation.

  There are two options for automatically generating user credentials for bulk RAP provisioning:

  - Per AP User Names/Passwords—each RAP is given its own user name and password.
  - Global User Name/Password—all selected RAPs are given the same (shared) user name and password.

Defining Provisioning Parameters for Remote APs using PSK

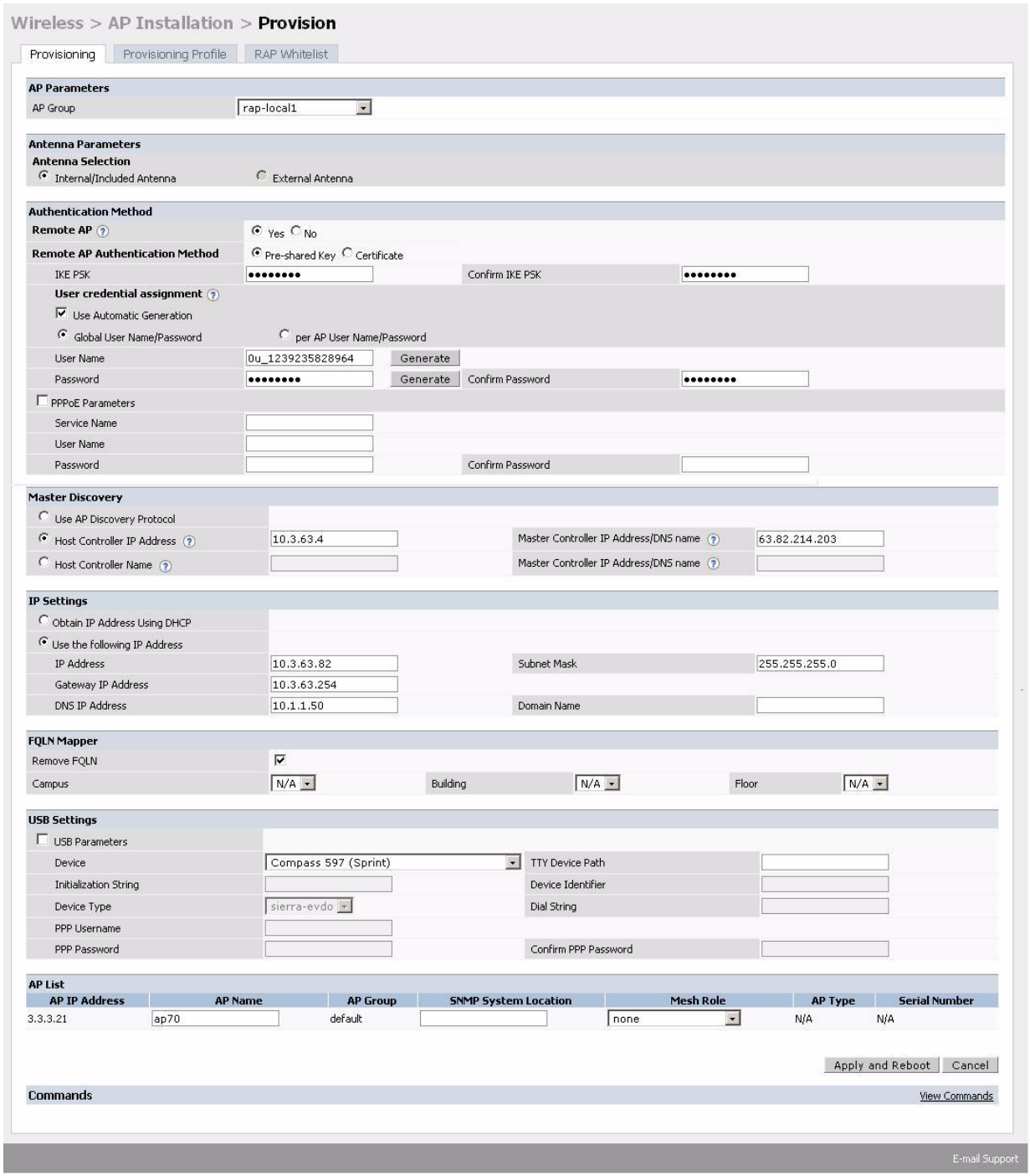
The following steps describe the process to provision a remote AP using PSK:

1. If you are provisioning a new AP that has never been provisioned before, connect the AP to the controller according the instructions included with that AP. If you are reprovisioning existing active APs as remote APs, this step is not necessary, as the APs are already communicating with the controller.
2. Navigate to the **Configuration > Wireless > AP Installation > Provisioning** window.
3. To provision a single remote AP, click the checkbox by the AP you want to provision, then click **Provision**.

   -or-

   To provision a group of APs in bulk, select multiple APs *of the same AP model*, then click **Provision**. You will not be allowed to bulk provision APs of different model types or APs currently assigned to different AP groups.

4. The Provisioning window appears, as shown below.



5. In the **AP Parameters** section, click the **AP Group** drop-down list and select the AP group to which this AP should be assigned.
6. (Optional) Some AP models support an external antenna in addition to their internal antenna. If the AP you are provisioning supports an external antenna, the Provisioning window displays an additional **Antenna Parameters** section. If you want to use an External antenna for the AP you are provisioning, select **External Antenna**. Otherwise, the AP will use its internal antenna by default.
7. Click **Yes** for the **Remote AP** option.
8. In the **Remote IP Authentication Method** section of this window, select **certificate**.

9. In the **Master Discovery** section, set the Master IP Address as shown below.

Deployment Scenario	Master IP Address Value
"Remote AP with a Private Network" on page 6	Enter the controller's IP address.
"Remote AP with Controller on Public Network" on page 6	Enter the controller's public IP address.
"Remote AP with Controller Behind Firewall" on page 6	Enter the public address of the NAT device to which the controller is connected.

10. Under IP Settings, select **Obtain IP Address Using DHCP** to obtain an IP address for your AP using DHCP.

    -or-

    select **Use the Following IP address** and enter the appropriate values in the following fields:

    - IP address: IP address for the AP, in dotted-decimal format
    - Subnet mask: Subnet mask for the IP, in dotted-decimal format.
    - Gateway IP address: The IP address the AP uses to reach other networks.
    - DNS IP address: The IP address of the Domain Name Server.
    - Domain name: (optional) The default domain name.

11. (Optional) In the FQLN Mapper section, you may click the Campus, Building and Floor drop-down lists to identify a fully qualified location name (FQLN) for the remote AP. To clear an existing FQLN, click the **Remove FQLN checkbox.**
12. (Optional) If you are provisioning AP models AP-70, 2E, RAP-5, and RAP5-WNUSB, you can configure them to support cellular modems, you must complete the fields in the USB settings section. For details on completing this section, see "Additional Provisioning Requirements for USB Link Interfaces" below.
13. The **AP list** section displays current information for the AP you are provisioning or reprovisioning, and allows you to define additional parameters for your remote AP, such as AP Name, SNMP System Location and (if your are provisioning a Remote Mesh Point or Portal) the AP's Mesh role.
14. Click **Apply and Reboot**. (Reprovisioning the AP causes it to automatically reboot)

Additional Provisioning Requirements for USB Link Interfaces

Redundant Uplink Support with Configurable Priorities

AP models AP-70, RAP-5 and RAP5-WN support both ethernet and USB-based modem interfaces. This software release also supports several EVDO (Evolution Data Optimized, up to 3.1 Mbps, CDMA) and 3G HSPA (High-Speed Packet Access, 3G data service) modems. The ArubaOS built-in flexibility will be able to support future USB modems and protocols without a software code change.

When a remote AP has more than one link, you can designate one link interface as the primary link, and any additional interfaces as backup links. When you provision a remote AP, either through the AP provisioning wizard, a provisioning profile or the **Configuration > Wireless > AP Installation > Provisioning** window in the WebUI, you can identify an AP's primary and backup links by assigning a priority level to each interface.

When an AP reboots after being provisioned (or reprovisioned), the AP determines which interface links are up and ready for use. The AP then uses the up interface with the highest defined priority level as its primary link.

NOTE

In the event that both a USB modem interface and an ethernet interface are assigned the same priority level, the AP will first attempt to use the ethernet interface. By default, the ethernet and USB modem interfaces have same priority.

Lower-priority interfaces with an enabled link are held in a ready state. If the higher-priority link gets disconnected, the AP immediately activates the lower-priority link. The AP will use this backup link until a higher-priority link becomes active again, at which time the AP will disconnect the lower-priority backup link and reconnect using the higher-priority primary link.

USB Modems

To use the USB Cellular Modems, provision the AP as a remote AP and ensure your controller is configured and licensed to support remote APs.

Plug the USB Cellular Modem into the USB port before supplying power to the remote AP. Once powered up, the remote AP automatically detects the USB Cellular Modem and negotiates a PPP IP address. If the modem fails to obtain a PPP IP address within 45 seconds, the remote AP ignores the modem's presence, and boots as a *wired* remote AP. Should it also fail to receive a DHCP IP address or contact a controller, the remote AP will start a re-boot sequence.

Provisioning Parameters for Verified USB Modems

The 3G High Speed Packet Access (HSPA) protocol is provided by AT&T in the United States and numerous other 3G providers worldwide. Aruba has assembled key provisioning settings for each of the USB modems that have been tested and verified with this software release. This information is subject to change without notice by the modem manufacturers; it is provided only as a convenience for our customers.

NOTE

For a list of other devices validated for use with Aruba APs, see "Validated Devices" on page 69.

Table 5 *3G Modem Configuration Settings by Carrier*

Carrier	Model	Device Vendor ID	Provisioning Parameters
ATT	USBConnect 881 (Sierra 881U)	0x1199 6856	`usb_type=sierra-gsm (4)`
	Quicksilver (Globetrotter ICON 322)	0x0af0 d033	`usb_type=hso (6) usb_init=AT+CGDCONT=1,'IP','wap.cingular' usb_dial=ATDT*99***1# usb_user=internet usb_passwd=internet` **NOTE:** Any **usb_user** and **usb_passwd** value is allowed, as long as those parameters are present.)
	Mercury (Sierra Compass 885)	0x1199 6880	`usb_type=sierra-gsm (4) usb_tty=ttyUSB4`
	Huawei E272,E170, E220	0x12d1 1003	`usb_type=option (2) usb_init=AT+CGDCONT=1,'IP','wap.cingular' usb_dial=ATDT*99***1#`

Table 5 *3G Modem Configuration Settings by Carrier*

Carrier	Model	Device Vendor ID	Provisioning Parameters
Sprint	Compass 597 (Sierra)	0x1199 0023	`usb_type=sierra-evdo (5)`
	Compass 598 (Sierra)	0x11990025	`usb_type=sierra-evdo (5)`
	Ovation U727 (Novatel)	0x1410 4100	`usb_type=option (2)`
	U300 (Franklin wireless)	0x16d8 6002	`usb_type=option (2)`

TataIndicom (india)	SXC-1080 (Qualcomm)	0x1b7d 070a	`usb_type=acm (3)`
			`usb_init=ATQ0V1E1S0=0&C1&D2`
			`usb_user=internet usb_passwd=internet`

Telecom (New Zealand)	Tstick C597 (Sierra)	0x1199 0023	`usb_type=sierra-evdo (5)`
			`usb_user=mobile@jamamobile`
			`usb_passwd=telecom`

Telenor (Sweden)	Globetrotter ICON 225	0x0af0 6971	`usb_type=hso (6)`
			`usb_init=AT+CGDCONT=1,'IP','telenor'`
			`usb_dial=ATDT*99***1# usb_user=internet`
			`usb_passwd=internet`

Verizon	USB U727 (Novatel)	0x1410 4100	`usb_type=option (2) USB`
	U720 (Novatel/ Qualcomm)	0x1410 2110	`usb_type=option (2)`
	UM175 (Pantech)	0x106c 3714	`usb_type=acm (3)`
	UM150 (Pantech)	0x106c 3711	`usb_type=acm (3)`
	U597 (Sierra)	0x1199 0023	`usb_type=sierra-evdo (5)`

Vodafone/ SmarTone (Hong Kong)	Huawei E272	0x12d1 1003	`usb_type=option (2)`
			`usb_init=AT+CGDCONT=1,'IP','internet'`
			`usb_dial=ATDT*99***1#`

Vodafone/ SmarTone (New Zealand and Japan)	Huawei E220	0x12d1 1003	`usb_type=option (2)`
			`usb_init=AT+CGDCONT=1,'IP','internet'`
			`usb_dial=ATDT*99***1#`

Vodafone/ SmarTone (T-Mobile)	Huawei E272	0x12d1 1003	`usb_type=option (2) usb_dev=0x12d11414` `usb_init=AT+CGDCONT=1,'IP','epc.tmobile .com' usb_dial=ATDT*99***1#`

Many of the newer modems contain multiple USB devices; creating a very elegant plug-and-play solution. When your USB Cellular Modem is first powered on, a storage device is registered. This storage device contains the software driver/executable necessary to install and operate the modem.

Once the software installation is complete, the modem must *mode-switch* from a storage device to a registered modem device. Mode-switching varies by manufacturer. For example, The Novatel modem mode-switches via a SCSI eject command; the Huawei modem mode-switches via a SCSI rezero command, while the Sierra modem mode-switches via a specific USB command. Once the mode-switching is complete, the modem automatically registers itself.

The RAP can dial (via the modem) your Service Provider to initiate a PPP session. During the boot sequence, the RAP issues your device's mode-switching command, every few seconds, until the PPP link connects.

Provision an AP for a USB Modem using the WebUI

There are *two* places in the WebUI that allow you to configure USB modem and cellular link settings.

- To configure settings for one (or more) individual remote APs, use the **USB Settings** section of the **Wireless > AP Installation > Provisioning** window
- To configure settings for an AP group, use the using the **USB Settings** section of the **Wireless > AP Installation > Provisioning Profile** window.

The table below describes the USB modem provisioning parameters available in the WebUI. For a complete list of service providers, their Access Point Names (APNs), and information on which service providers require user name and/or passwords see http://www.pinstack.com/carrier_settings_apn_gateway.html.

Table 6 *USB Modem Provisioning Parameters in the WebUI*

Parameter	Description
USB Parameters	Select this checkbox to enable USB parameter defined in this section of the WebUI.
Device	Click the Device drop-down list and select the USB device type.
Initialization String	Initialization string for the USB modem.
Device Identifier	Enter the device identifier for the USB device.
Device Type	Enter the USB driver type.
Dial String	Enter the dial string for the USB modem.
PPP Username	Enter the PPP username, if provided by the cellular service provider.
PPP Password	Enter the PPP password, if provided by the cellular service provider.
Confirm PPP Password	Re-type the PPP password.
Link Priority Ethernet	Specify the priority level of the Ethernet link (0-255). The ethernet or cellular link with the highest priority will be the primary link. Links with lower priorities will be backup links.
Link Priority Cellular	Specify the priority level of the USB Cellular link (0-255). If you assign the same link priority to both the Ethernet and USB cellular link, the AP will use the Ethernet interface as its primary link.

Provision a Remote AP for a USB Modem using the CLI

To support the USB cellular modems, new USB specific parameters are available with the **provision-ap** and **ap provision-profile** CLI commands. Use the following CLI parameters to provision a remote AP for a USB modem.

To provision an individual remote AP:

```
(host) (config) #provision-ap
   link-priority-cellular
   link-priority-ethernet
   usb-dev
```

```
  usb-dial
  usb-init
  usb-passwd
  usb-tty
  usb-type
  usb-user
```

To define modem settings for an AP group via a provisioning profile:

```
(host) (config) #ap provisioning-profile <profile>
  link-priority-cellular
  link-priority-ethernet
  usb-dev
  usb-dial
  usb-init
  usb-passwd
  usb-tty
  usb-type
  usb-user
```

Sample USB Provisioning Configurations

Generally, provisioning the initialization and dial variables are required. The identifier is the USB vendor (in the form 0xABCD) and the product ID (in the form 0x1234) concatenated to form 0xABCD1234. The driver type is based on the modem.

Provisioning a 3G Modem

For a 3G modem, provision the **usb-dial** and the **usb-init** commands:

```
(host) (config) #provision-ap
(host) (AP provisioning) #usb-dial ATDT*99#
(host) (AP provisioning) #usb-init AT+CGDCONT=1, 'IP','ISP.CINGULAR'
(host) (AP provisioning)
```

The dial string in the example above works with most providers. The APN (access point name) is AT&T Cingular specific ('ISP.CINGULAR'). The required single quotes designate the APN. Each service provider has their own APN. For a listing of service providers and their APNs, see http://www.pinstack.com/carrier_settings_apn_gateway.html.

Provisioning an AT&T USBConnect 881 Modem

In this example, *sierra* is the default USB type for Sierra Wireless supported by AT&T.

```
(host) (config) #provision-ap
(host) (AP provisioning) #usb-type sierra
(host) (AP provisioning) #
```

Provisioning an EVDO Verizon/Sprint Modem

This example provisions a EVDO Verizon/Sprint modem with the dial string **ATDT#7777** and the initialization string **ATQ0VIE0**.

Do not use VLAN 4094 for any VAP or wired port configuration for RAPs using EVDO as uplink. This port is reserved for local debugging. This restriction does not apply to RAPs using Ethernet as uplink

```
(host) (config) #provision-ap
(host) (AP provisioning) #usb-dial ATDT#7777
(host) (AP provisioning) #usb-init ATQ0VIE0
(host) (AP provisioning) #
```

Captive Portal

Split tunnel captive portal is one of the methods of authentication supported on remote APs. A captive portal presents a web page that requires action on the part of the user before network access is granted. You can configure captive portal for guest users, where no authentication is required, or for registered users who must be authenticated against an external server or the controller's internal database.

While you can use captive portal to authenticate users, it does not provide for encryption of user data and should not be used in networks where data security is required. Captive portal is most often used for guest access, access to open systems (such as public hot spots), or as a way to connect to a VPN.

The default captive portal web page displays a login prompt for both registered users and guests. Note, however that the AP does not offer automatic redirection from captive portal to the home page. After remote AP is authorized, you must reload the open browser to launch the home page.

The tasks for setting up RAPs for authentication using split-tunnel captive portal are:

- "Install a Captive Portal Server Certificate" on page 35
- "Using the WebUI to Configure Split Tunnel Captive Portal" on page 36

  -or-

  "Using the CLI to Configure Split Tunnel Captive Portal" on page 37

Install a Captive Portal Server Certificate

The Aruba controller is designed to provide secure services through the use of digital certificates. A server certificate installed in the controller verifies the authenticity of the controller for captive portal.

Aruba controllers ship with a demonstration digital certificate. Until you install a customer-specific server certificate in the controller, this demonstration certificate is used by default for all secure HTTP connections such as captive portal. This certificate not intended for long-term use in production networks. Users in a production environment are urged to obtain and install a certificate issued for their site or domain by a well-known certificate authority (CA). You can generate a Certificate Signing Request (CSR) on the controller to submit to a CA. Once you have imported a server certificate into the controller, you can select the certificate for used with captive portal as described in the following sections.

Using the WebUI to select a captive portal server certificate

1. Navigate to the **Configuration > Management > General** window.
2. Scroll down to the **Captive Portal Certificate** section and use the drop-down list to select the new imported certificate.
3. Click **Apply** (at the bottom right of the window).

Using the CLI to select a captive portal server certificate

```
web-server
   captive-portal-cert <certificate>
```

To specify a different server certificate for captive portal with the CLI, use the **no** command to revert back to the default certificate *before* you specify the new certificate:

```
web-server
   captive-portal-cert ServerCert1
```

```
no captive-portal-cert
captive-portal-cert ServerCert2
```

Using the WebUI to Configure Split Tunnel Captive Portal

1. Navigate to the **Configuration > Security > Authentication > L3 Authentication** window.
2. Select **Captive Portal Authentication Profile**.
3. Enter the name for a new captive portal authentication profile in the text box, then click **Add**.
4. Double click on the new profile name to launch the **Captive Portal Profile Authentication > your_profile_name** window.
   a. Enable user login and/or guest login, and configure other parameters as desired. (For a complete description of these parameters, see Table 7).
   b. Click **Apply**.
5. Select the Server Group under the captive portal authentication profile you just configured.
   a. Use the drop-down list to select your server group (for example **radius)**.
   b. Click **Apply**.
6. Navigate to **Security > Access Control > User Roles Tab > Add Role** and create the new user-role "splitcp-logon".
7. Assign the pre-defined firewall policy "logon-control" to position one and the policy "captiveportal" to position two for this user role.
8. Assign the captive portal profile created in step 3.
   a. Select the **AAA Profiles** tab.
   b. Click **Add** at the bottom of the AAA Profile Summary and enter the profile name you created in step 3. Click **Add**.
   c. Double click on the AAA profile you just created.
   d. Select **splitcp-logon** from the **Initial Role** drop-down list.
   e. Click **Apply**.
9. Navigate to the **Configuration > Wireless > AP Configuration** window. Select either the AP Group or AP Specific tab. Click **Edit** for the applicable AP group name or AP name.
10. In the **Profiles** list, expand the **Wireless LAN** menu, then select **Virtual AP**.
11. Select **NEW** from the **Add a profile** drop-down list to create a new virtual AP profile. Enter a name for the virtual AP profile and then click **Add**.
    a. In the Profile Details window for the Virtual APs, select your recently created AAA profile from the **AAA Profile** drop-down list. A pop-up window displays the configured AAA profile parameters. Click **Apply** in the pop-up window.
    b. From the **SSID profile** drop-down list, select **NEW**.
    c. Enter the name for the SSID profile.
    d. Enter the Network Name for the SSID.
    e. Click **Apply** in the pop-up window.
    f. At the bottom of the Profile Details window, click **Apply**.
12. Click the new virtual AP name, in the Profiles list or in the Profile Details window, to its display configuration parameters.
    a. Select the **Virtual AP enable** check box.
    b. Select **split-tunnel** from the **Forward mode** drop-down list.
    c. In the **VLAN** section, select the ID number of the VLAN to which users are assigned (for example, **20**).

d. Click **Apply**.

Using the CLI to Configure Split Tunnel Captive Portal

1. Create a captive portal profile, assigning the post-captive portal role and server group.

```
aaa authentication captive-portal <CP_Profile_name>
   default-role "rapuser"
   server-group "radius"
```

2. Create a pre-captive portal user-role (initial-role) and then apply the captive portal profile created in step 1.

```
user-role splitcp-logon
    captive-portal <CP_Profile_name>
    session-acl logon-control
    session-acl captiveportal
```

3. Apply the pre-captive portal role (created in step 2) to the AAA profile as the initial-role.

```
aaa profile <AAA_Profile_name>
   initial-role "splitcp-logon"
   aaa authentication dot1x default
!
```

4. Create an SSID profile.

```
wlan ssid-profile <SSID_Profile_name>
   essid "split-tunnel-cp"
   opmode wpa2-psk-aes
   wpa-passphrase <some_wpa_passphrase>
```

5. Create a Virtual AP profile and apply the AAA profile and SSID profile to it.

```
wlan virtual-ap <Virtual-AP_Profile_name>
   vlan 30
   aaa-profile <AAA_Profile_name>
   ssid-profile <SSID_Profile_name>
   forward-mode split-tunnel
```

6. Apply this configuration to the ap-group/ap-name

```
ap-group <AP_Group_Name>
   virtual-ap <Virtual-AP_Profile_name>
```

Modifying Guest Captive Portal User Role

When you define a captive portal guest login role, users are assigned to that role after guest login from captive portal. Typically this role allows guest users to obtain DHCP from corporate networks as well as all other traffic (such as DNS, DHCP, ICMP) routed on their local network to the remote AP. If user's defined role is not specified in the AAA profile, the standard *guest* role is applied to the user.

Using the WebUI to modify and apply the split-tunnel captive portal guest role

1. Navigate to the **Configuration > Security > Authentication > L3 Authentication** window.
2. Create a new role "splitcp-guest".
3. Add firewall policies to this role by selecting Add to create a new firewall policy that permits DHCP, route src-nat HTTP, HTTPS, DNS and ICMP traffic.
4. Click Apply (at the bottom right of the window) to apply this firewall policy to the user role.
5. Navigate to Captive portal configuration **Security > Authentication > L3 Authentication** and select a role from the **Default Guest Role** drop-down list.

Using the CLI to create a split-tunnel captive portal guest role

Using the CLI to create split-tunnel captive portal guest role.

1. Create a firewall policy.

```
ip access-list session splitcp-guest
   any any svc-dhcp permit
   any any svc-dns route src-nat
   any any svc-icmp route src-nat
   any any svc-http route src-nat
   any any svc-https route src-nat
!
```

2. Apply firewall policy to user role

```
user-role splitcp-guest
session-acl splitcp-guest
!
```

3. Apply this role to default-guest-role of captive portal profile.

```
aaa authentication captive-portal "PROFILE_NAME"
default-guest-role "splitcp-guest"
   guest-logon
```

Captive Portal Configuration Parameters

Table 7 describes the configuration parameters on the WebUI Captive Portal Authentication profile window.


NOTE

In the CLI, you configure these options with the **aaa authentication captive-portal** commands.

Table 7 *Captive Portal Authentication Profile Parameters*

Parameter	Description
Default role	Role assigned to the Captive Portal user upon login. When both user and guest logon are enabled, the default role applies to the user logon; users logging in using the guest interface are assigned the default-guest-role. The Policy Enforcement Firewall license must be installed. Default: guest
default-guest-role	Role assigned to the Captive Portal guest users that logon using the guest interface are assigned this role by default. The Policy Enforcement Firewall license must be installed.
Redirect Pause	Time, in seconds, that the system remains in the initial welcome page before redirecting the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link. Default: 10 seconds.
User Login	Enables Captive Portal with authentication of user credentials. Default: enabled
Guest Login	Enables Captive Portal logon without authentication. Default: disabled
Logout popup window	Enables a pop-up window with the Logout link for the user to logout after logon. If this is disabled, the user remains logged in until the user timeout period has elapsed or the station reloads. Default: enabled
Use HTTP for authentication	Use HTTP protocol on redirection to the Captive Portal page. If you use this option, modify the captiveportal policy to allow HTTP traffic. Default: Disabled (HTTPS is used)

Table 7 *Captive Portal Authentication Profile Parameters (Continued)*

Parameter	Description
Logon wait minimum wait	Minimum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter. Default: 5 seconds.
Logon wait maximum wait	Maximum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter. Default: 10 seconds.
Logon wait CPU utilization threshold	CPU utilization percentage above which the Logon wait interval is applied when presenting the user with the logon page. Default: 60%
Max authentication failures	Maximum number of authentication failures before the user is blacklisted. Default: 0
Show FQDN	Allows the user to see and select the fully-qualified domain name (FQDN) on the login page. Default: disabled
Use CHAP	Use CHAP protocol. You should not use this option unless instructed to do so by an Aruba representative. Default: PAP
Sygate-on-demand-agent	Enables client remediation with Sygate-on-demand-agent (SODA). Default: disabled
Login page	URL of the page that appears for the user logon. This can be set to any URL. Default: /auth/index.html
Welcome page	URL of the page that appears after logon and before redirection to the web URL. This can be set to any URL. Default: /auth/welcome.html
Show Welcome Page	Enables the display of the welcome page. If this option is disabled, redirection to the web URL happens immediately after logon. Default: Enabled
Proxy Server Configuration	Configures IP address and port number for proxy server. **NOTE**: This option is only available in the base operating system. Default: N/A
Adding switch ip address in redirection URL	Sends the controller's IP address in the redirection URL when external captive portal servers are used. An external captive portal server can determine the controller from which a request originated by parsing the 'switchip' variable in the URL. Default: disabled

Deploying Remote Mesh Portals

You can deploy mesh portals to create a hybrid mesh/remote AP environment to extend network coverage to remote locations; referred to as remote mesh portal.

The Remote Mesh Portal feature documented in this Addendum is *not* supported for deployments:

- Remote Mesh portal functionality is not supported on RAP-5WN and RAP-2WG model.
- Remote Mesh portal functionality is a demo-only feature and is not supported for deployments in this release.

The Remote Mesh Portal feature allows you to configure a remote AP at a branch office to operate as a mesh portal for a mesh cluster. Other Remote Mesh Points belonging to that cluster get their IP address and configuration settings from the main office via a VPN tunnel between the remote mesh portal and the main office controller. This feature is useful for deploying an all-wireless branch office or creating a complete wireless network in locations where there is no wired infrastructure in place.

This configuration requires that both the remote AP and mesh licenses be installed, because the remote mesh portal consumes one mesh license when it registers with the controller. For more information about Aruba software licenses, see the *ArubaOS User Guide*.

Configuring a Remote Mesh Portal

A remote mesh portal must be provisioned as both a remote access point and a mesh portal. For instructions on provisioning the remote mesh portal as a remote access point, see the *ArubaOS User Guide*.

Configuring an AP as a remote mesh portal

1. Navigate to the **Configuration > Wireless > AP Installation > Provisioning** window. Select the AP to provision as a remote mesh portal and click **Provision**.
2. Provision the AP parameters according to the descriptions in "Certificate-Based AP Provisioning" on page 22 or "Provisioning a Remote AP using Pre-Shared Key" on page 27.
3. In the **AP List** section, click the **Mesh Role** drop-down list and select **Remote Mesh Portal**.

Configuring the mesh private VLAN

Edit the mesh radio profile for the remote mesh portal and choose a new, non-zero tag value for the mesh private VLAN Make sure that the mesh private VLAN does not conflict with any local tags assigned in the mesh network. This mesh private VLAN must not be used as a VLAN for any other virtual AP.

1. Navigate to the **Configuration > Wireless > AP Configuration** window. Select either the **AP Group** or **AP Specific** tab.
   - If you selected the AP Group tab, click the Edit button by the remote mesh portal AP group with the profile you want to edit.
   - If you selected the **AP Specific** tab, click the **Edit** button by the remote mesh portal with the profile you want to edit.
2. In the Profiles list, expand the **Mesh** menu, then select **Mesh radio profile**.
3. In the **Profile Details** window pane, click the **Mesh radio profile** drop-down list and select the name of the profile you want to edit.

4. Set the **Mesh Private VLAN** parameter to define a VLAN ID (0-4094) for control traffic between an remote mesh point and mesh nodes.
5. Click **Apply** to save your changes.

Next, assign the remote mesh points with the same mesh cluster profile, 802.11a and 802.11g RF management profiles, and mesh radio profile as the remote mesh portal. If you have defined an AP group for all your remote mesh points, you can just assign the required profiles to the remote mesh point AP group. Otherwise, you must assign the required profiles to each individual remote AP.

Using the WebUI to select a mesh radio profile for a remote mesh AP or AP group

The mesh radio profile allows you to specify the set of rates used to transmit data on the mesh link. Aruba provides a "default" version of the mesh radio profile. You can use the "default" version or create a new instance of a profile which you can then edit as you need.

1. Navigate to the **Configuration > Wireless > AP Configuration** window. Select either the **AP Group** or **AP Specific** tab.
   - If you selected **AP Group**, click the **Edit** button by the AP group to which you want to assign a new mesh radio profile.
   - If you selected **AP Specific**, click the **Edit** button by the AP to which you want to assign a new mesh radio profile.
2. Under the Profiles list, expand the **Mesh** menu, then select **Mesh radio profile**.
3. In the **Profile Details** window pane, click the **Mesh radio profile** drop-down list and select the desired mesh radio profile from the list. Click **Apply**.

The profile name appears in the Mesh Radio Profile list with your configured settings. If you configure this for the AP group, this profile also becomes the selected radio profile used by the mesh portal for your mesh network.

Using the WebUI to select a 802.11a or 802.11g RF management profile for a remote mesh AP or AP group

The two 802.11a and 802.11g RF management profiles for an AP configure its 802.11a (5 Ghz) and 802.11b/g (2.4 GHz) radio settings. Use these profile settings to determine the channel, beacon period, transmit power, and ARM profile for a remote mesh AP's 5 GHz and 2.5 Ghz frequency bands. You can either use the "default" version of each profile, or create a new 802.11a or 802.11g profile which you can then configure as necessary. Each RF management profile also has a radio-enable parameter that allows you to enable or disable the AP's ability to simultaneously carry WLAN client traffic and mesh-backhaul traffic on that radio. This value is enabled by default.

1. Navigate to the **Configuration > Wireless > AP Configuration** window. Select either the **AP Group** or **AP Specific** tab.
   - If you selected **AP Group**, click the **Edit** button by the AP group name to which you want to assign a new 802.11a or 802.11g RF management profile.
   - If you selected **AP Specific**, click the **Edit** button by the AP to which you want to assign a new 802.11a or 802.11g RF management profile
2. Under the Profiles list, expand the **RF management** menu.
3. To select a **802.11a radio profile** for an AP or AP group, click **802.11a radio profile**. In the **Profile Details** window pane, click the **802.11a radio profile** drop-down list and select the desired profile from the list.

   or

   To select a **802.11g radio profile** for an AP or AP group, click **802.11g radio profile**. In the **Profile Details** window pane, click the 802.11g radio profile drop-down list and select the desired profile from the list. Click **Apply**.

The profile name appears in the Profile list with your configured settings. If you configure this for the AP group, this profile also becomes the selected 802.11a or 802.11g RF management profile used by the mesh portal for your mesh network.

Using the WebUI to add a mesh cluster profile to a remote mesh AP or AP group

Mesh clusters are grouped and defined by a mesh cluster profile, which provides the framework of the mesh network. Similar to virtual AP profiles, the mesh cluster profile contains the MSSID (mesh cluster name), authentication methods, security credentials, and cluster priority required for mesh nodes to associate with their neighbors and join the cluster. If you have multiple cluster profiles, the mesh portal uses the profile with the highest priority to bring up the mesh network. Mesh points, in contrast, go through the list of mesh cluster profiles in order of priority to decide which profile to use to associate themselves with the network. The mesh cluster priority determines the order by which the mesh cluster profiles are used. This allows you, rather than the link metric algorithm, to explicitly segment the network by defining multiple cluster profiles.

1. Navigate to the **Configuration > Wireless > AP Configuration** window. Select either the **AP Group** or **AP Specific** tab.
   - If you selected **AP Group**, click the **Edit** button by the AP group name to which you want to assign a new mesh cluster profile.
   - If you selected **AP Specific**, click the **Edit** button by the AP to which you want to assign a new mesh cluster profile
2. Under the Profiles list, expand the **Mesh** menu, then select **Mesh Cluster profile**.
3. To create a new mesh cluster profile, click the **Add a profile** drop-down list in the **Profile Details** window pane, and select **New**.
   -or-
   To add an existing mesh cluster profile, click the **Add a profile** drop-down list and select a profile name from the list.
4. Click the **using priority** drop-down list to select a priority for the mesh cluster profile. The lower the number, the higher the priority.


NOTE

If you configure multiple cluster profiles with different cluster priorities, you manually override the link metric algorithm because the priority takes precedence over the path cost. In this scenario, the mesh portal uses the profile with the highest priority to bring-up the mesh network.

5. Click **Add** to add the mesh cluster profile to the AP group.

Configure a DHCP pool

In this next step, you must configure a DHCP pool where the DHCP server is on the subnet associated with mesh private VLAN. Mesh points will get their IP address from this subnet pool. To complete this task, refer to the *ArubaOS User Guide* and the procedure described in the section “Configuring the DHCP Server on the Remote AP”.

Configure the VLAN ID of the virtual AP profile

The VLAN of this Virtual AP must have the same VLAN ID as the mesh private VLAN.

1. Navigate to **Configuration > Wireless > AP Configuration** window. Select either the **AP Group** or **AP Specific** tab. Click the **Edit** button **by** the applicable AP group name or AP name with the virtual AP profile you want to configure.
2. Under Profiles, select **Wireless LAN**, then **Virtual AP**.

3. To create a new virtual AP profile in the WebUI, select **New** from the **Add a profile** drop-down list. Enter the name for the virtual AP profile, and click **Add**.

Add this virtual AP profile only to the AP Group or the AP specific profile for the Remote Mesh Portal. Do not add the virtual AP profile to the Remote Mesh *Point*.

Whenever you create a new virtual AP profile in the WebUI, the profile automatically contains the “default” SSID profile with the default “aruba-ap” ESSID. You must configure a new ESSID and SSID profile for the virtual AP profile before you apply the profile

   a. In the **Profile Details** window, click the **AAA Profile** drop-down list and select the previously configured AAA profile. The **AAA Profile** pop-up window appears.
   b. To set the AAA profile and close the window, click **Apply**.
   c. In the **Profile Details** entry for the new virtual AP profile, select **NEW** from the **SSID Profile** drop-down list. A pop-up window displays to allow you to configure the SSID profile.
   d. Enter the name for the SSID profile.
   e. Under **Network**, enter a name in the Network Name (SSID) field.
   f. Under **Security**, select the network authentication and encryption methods.
   g. To set the SSID profile and close the window, click **Apply**.
4. Click **Apply** at the bottom of the **Profile Details** window.
5. Click the new virtual AP name in the **Profiles list** or **Profile Details** window pane to display the configuration parameters for this profile.
6. In the **Profile Details** window:
   a. Make sure **Virtual AP enable** is selected.
   b. Make sure the **Allowed band** is set to **all**
   c. Click the **VLAN** drop-down list and select the VLAN ID for the mesh private VLAN.
   d. Click the **Forward mode** drop-down list and select **split-tunnel**.
   e. Click **Apply**.

Important Things to Remember—Remote Mesh Portal

By default the data frames, the mesh portal receives on its mesh link, are forwarded according to the bridge table entries on the portal. However, frames received on mesh private VLAN (MPV) are treated differently by the remote mesh portal. These frames are treated the same as frames received on a split SSID and are routed rather than bridged. Mesh points obtain DHCP addresses from the corporate network. then register with the controller using these IP addresses. When these mesh points send and receive PAPI control traffic from the main office controller, it controls these mesh points just as if they were on a local VLAN. PAPI traffic containing keys and other secret information receives IPsec encryption and decryption when it is forwarded to the controller through the VPN tunnel.

Not all traffic from a mesh point is sent on the mesh private VLAN. When a mesh point bridges data received via its Ethernet interface or from clients connected to an access radio VAP, the mesh point does not tag the frame with the mesh private VLAN tag when it sends the data through mesh link to the remote mesh portal. Note that the mesh point may still tag the frame depending on the VLAN of the virtual AP and the native VLAN specified in the system profile. Care must be taken to assign the MPV value so that it does not clash with any local tags assigned in the mesh network. In this case, the portal performs the default operation that is to bridge the frame based on its bridge table.

Traffic destined to the Internet is recognized as such by the remote mesh portal based on ACL rules. This traffic is NATed on the remote mesh portal’s Ethernet interface.

Chapter 6

Managing the RAP Network

The information in this chapter describes additional remote network features that can be implemented either before after your Remote APs have been deployed, and gives troubleshooting suggestions for both Remote APs and Remote AP Users.

This chapter contains the following sections:

Local Debugging

Local Debugging is A WebUI feature that allows end users to perform diagnostics and view the status of their remote AP through a wired or wireless client. This feature is useful for troubleshooting connectivity problems on remote AP and to performing throughput tests. There are three tabs in the Local Debugging WebUI window, **Summary**, **Connectivity** and **Diagnostics**. Each tab displays different information for the AP, but all three tabs include a **Generate & save support file** link that, when clicked, will automatically generate a **support.tgz** file that can be sent to a corporate IT department for additional analysis and debugging.

Remote AP Summary

The **Summary** tab has two views; basic and advanced. Click the **basic** or **advanced** links at the top of this tab to toggle between the two views. The table below shows the information displayed for both the basic and advanced views of the **Summary** tab.

Table 1 *RAP Console Summary Tab Information*

Summary Table Name	Basic View Information	Advanced View Information
Wired Ports Status	• **Port:** Port numbers of the wired ports on the AP. • **Status**: Current status of each port (*Connected*, *Link Down* or *Disabled*).	The advanced view of the Wired Access Ports table displays the following data: • **Port:** Port numbers of the wired ports on the AP. • **Status**: Current status of each port (*Connected*, *Link Down* or *Disabled*). • **MAC Address:** MAC address of the wired port. • **Speed**: Speed of the link. • **Duplex Type**: Duplex mode of the link, full or half. • **Forwarding** mode: Forwarding mode for the port: *Bridge*, *Tunnel* or *Split Tunnel*. • **Users**: Number of users accessing each port. • **Rx Packets**: Number of packets received on the port. • **Tx packet**s: Number of packets transmitted via the port.
Wireless SSIDs	• **SSID**: Name of the SSID. • **Status**: SSID Status (up, down, or disabled). • **Band**: Radio band available on the SSID.	• **SSID**: Name of the SSID. • **Status**: SSID Status (up, down, or disabled). • **Band**: Radio band available on the SSID. • **Channel**: Channel used on the radio band. • **BSSID**: BSSID of the wireless SSID. • **Forwarding Mode**: Forwarding mode used by the Wireless SSID (Bridge, Tunnel or Split-Tunnel). • **EIRP**: Equivalent Isotropic Radiated Power, in dBm. • **Noise floor**: The residual background noise detected by an AP. Noise seen by an AP is reported as -dBm. Therefore, a noise floor of -100 dBm is smaller (lower) than a noise floor of -50 dBm. • **Users**: Number of users on the radio band. • **Rx Packets**: Number of packets received on the BSSID. • **Tx packet**s: Number of packets transmitted via the BSSID.
Wired Users	• **MAC Address**: MAC address of the wired user. • **IP address**: IP address of the wired user.	• **MAC Address**: MAC address of the wired user. • **IP address**: IP address of the wired user. • **Port**: AP port used by the wired user.

Table 1 *RAP Console Summary Tab Information*

Summary Table Name	Basic View Information	Advanced View Information
Wireless User	• **MAC Address**: MAC address of the wireless user. • **IP address**: IP address of the wireless user.	• **MAC Address**: MAC address of the wired user. • **IP address**: IP address of the wired user. • **SSID**: Name of the SSID. • **BSSID**: BSSID of the wireless user. • **Assoc State**: Shows if the user is associated or just authorized. • **Auth**: Type of authentication: WPA, 802.1x, none, open, or shared. • **Encryption**: Encryption type used by the wireless user. • **Band**: Radio band used by the wireless client. • **RSSI**: The Receive Signal Strength Indicator (RSSI) value displayed in the output of this command represents signal strength as a signal to noise ratio.
Device Info	• **Type**: AP device/model type. • **Name**: Name assigned to the AP. • **Wired MAC address**: MAC address of the wired port. • **Serial #**: AP serial number. • **Tunnel IP address**: IP address of the tunnel between the AP and controller. • **Software Version**: Software version currently running on the AP. • **Uptime**: Amount of time the AP has been active since it was last reset. • **Master**: IP address of the master controller. • **lms**: IP address of the local controller.	N/A
Uplink Info	The Uplink Info table can display some or all of the following information for your remote AP, depending upon whether a link is active and the number of links supported by the AP. Active uplink information, including: • **Interface name** • **Port speed** • **IP address** Standby link information, including: • **Name** (3G) • **Device connected** (yes/no) • **Provisioned** (yes/no) • **IP address** • **Device** • **User** • **Password**	N/A

Remote AP Connectivity

The information shown on the **Connectivity** tab will vary, depending upon the current status of the remote AP. If a remote AP has been successfully provisioned and connected, it should display some or all of the following information:

Table 2 *RAP Console Connectivity Tab Information*

Data	Description
Uplink status	Shows if the link connected failed. If the link is connected, the Uplink status also displays the name of the interface.
IP Information	If the AP has successfully received an IP address, this data row will show the AP's IP address, subnet mask, and gateway IP address.
Gateway Connectivity	If successful, this item also shows the percentage of packet loss for data received from the gateway
TPM Certificates	If successful, the AP has a Trusted Platform Module (TPM) certificate.
Master Connectivity	Shows if the AP was able to connect to the master controller. This item also shows the IP address to which the AP attempted to connect, and, if the AP did connect successfully, the link that was used to connect to that controller.
LMS Connectivity	Shows if the AP was able to connect to a local controller. This item also shows the IP address to which the AP attempted to connect, and, if the AP did connect successfully, the link that was used to connect to that controller.

The top of the **Connectivity** tab has a **Refresh** link that allows users to refresh the data on their screen. Additional information at the bottom of this tab shows the date, time and reason the remote AP last rebooted. The **Reboot RAP Now** button reboots the remote AP.

Remote AP Diagnostics

Use the **Diagnostics** tab to view log files, or run diagnostic tests that can help the IT department troubleshoot errors. You can also use the **Reboot AP Now** button at the bottom of the Diagnostic window reboots the remote AP.

To run a diagnostic test on a remote AP:

1. Access the RAP console, and click the **Diagnostics** tab
2. Click the **Test** drop-down list and select **Ping**, **Traceroute**, **NSLookup** or **Throughput**.

   The *ping* and *traceroute* tests require that you enter a network destination in the form of an IP address or fully-qualified domain name, and select either **bridge** or **tunnel** mode for the test. The *NSLookup* diagnostic test requires that you enter a destination only. The *throughput* test checks the throughput of the link between the AP and the controller, and does not require any additional test configuration settings.
3. Click **OK** to start the test. The results of the test will appear in the **Diagnostics** window.

To display log files in a separate browser window, click the **logs** drop-down list at the upper right corner of the Diagnostics window, and select any of the log file name. The type of log files available will vary, depending upon your remote AP configuration.

Monitoring AP Users in the Local User Database

The CLI command **show local-userdb-ap** allows you to view detailed information for the RAP whitelist. In the example below, the command output has been divided into two tables to fit on a single page of this document. In the command-line interface, this output would appear in a single, wide table.

```
(host) #(Aruba6000) #show local-userdb-ap

AP-entry Details
----------------

Name               AP-Group  AP-Name            Full-Name    Authen-Username  Revoke-Text
----               --------  -------            ---------    ---------------  -----------
00:0b:86:c3:58:38  local     chuck              chuck        naveen
00:0b:86:66:01:aa  default   rap2               moscato                       AP is not valid anymore
00:1a:1e:c0:1b:e0  default   00:1a:1e:c0:1b:e0                naveen
00:0b:86:66:03:3f  default   rap                moscato-rap  INDIAQA\naveen
00:0b:86:66:02:09  default   00:0b:86:66:02:09

AP_Authenticated  Description  Date-Added                Enabled
----------------  -----------  ----------                -------
Authenticated                  Thu Mar  5 21:25:36 2009  Yes
Provisioned                    Thu Mar  5 21:25:49 2009  No
Authenticated                  Wed Mar  4 20:16:16 2009  Yes
Authenticated                  Tue May 19 07:53:29 2009  Yes
Provisioned                    Fri May  8 10:37:40 2009  Yes

AP Entries: 5
```

The output of this command includes the following information:

Table 3 *Output of the CLI command show local-userdb-ap*

Column	Description
`Name`	MAC address of the AP.
`AP-Group`	Name of the AP group to which the AP has been assigned.
`AP-name`	Name of the AP. If no name has been specified, this column will display the AP's MAC address
`Full-name`	Text string used to identify the AP. This field often describes the AP's user, and corresponds to the **User Name** field in the RAP whitelist in the WebUI.
`Authen-Username`	User name of the user who authenticated the remote AP. This parameter holds the user name of the user who authenticated the remote AP. This is related to the zero touch authentication feature, as a user needs authenticate an AP before it gets its complete configuration. Before the AP is authenticated, it is given a restricted configuration to allow users to perform captive portal authorization via the remote AP's ENET ports to authenticate the remote AP. The username used during captive portal authentication will be stored in this field. This cannot be added manually when creating a local-userdb-ap entry.
`Revoke-Text`	The command l**ocal-userdb-ap revoke** includes an optional **revoke-comment** parameter that allows network administrators to explain why the AP was revoked. If an AP is revoked, and a revoke comment entered, this text appears in the **revoke-text** column in the **show local-userdb-ap** command. When a local DB entry is reenabled via the command **local-userdb-ap modify mac-addr mode enable**, this field is cleared.

Table 3 *Output of the CLI command show local-userdb-ap*

Column	Description
`AP_Authenticated`	This column indicates the authorization status of the AP. An AP can either be **Authenticated** or **Provisioned**. Remote APs that *do not* support certificated-based provisioning will always display a **Provisioned** status. Remote APs that support certificated-based provisioning can display either a **Authenticated** or **Provisioned** status, depending on their configuration and authentication status. • If the remote AP has a defined AP authorization profile, the remote AP will be in a "Provisioned" state with a limited configuration until it is authenticated. After it the remote AP has been authenticated, it will be in an "Authenticated" state. • If the remote AP does not have a defined AP authorization profile, the remote AP will be in a"Provisioned" state, but will still receive the full configuration assigned to that AP and its AP group.
`Description`	A text string used to further identify the remote AP.
`Date-Added`	Date and time that the AP was added to the local user database

`Enabled`	This column shows if the entry in the database is enabled or disabled. Database entries can be enabled or disabled using the CLI commands:
	`local-userdb-ap {add|modify} mac-address <mac-addr> mode {enable|disable}`
	and
	`local-userdb-ap revoke mac-address <mac-addr>`

Backup Configuration

The backup configuration (also known as fallback mode) operates the remote AP if the master controller or the configured primary and backup LMS are unreachable. The remote AP saves configuration information that allows it to operate autonomously using one or more SSIDs in local bridging mode while supporting open association or encryption with PSKs. You can also use the backup configuration if you experience network connectivity issues, such as the WAN link or the central data center becomes unavailable. With the backup configuration, the remote site does not go down if the WAN link fails or the data center is unavailable.

You define the backup configuration in the remote AP's virtual AP profile. The remote AP checks for configuration updates each time it establishes a connection with the controller. If the remote AP detects a change, it downloads the configuration changes.

The following remote AP backup configuration options define when the SSID is advertised:

- **Always**: Permanently enables the virtual AP. Recommended for bridge SSIDs.
- **Backup**: Enables the virtual AP if the remote AP cannot connect to the controller. This SSID is advertised until the controller is reachable. Recommended for bridge SSIDs.
- **Persistent**: Permanently enables the virtual AP after the remote AP initially connects to the controller. Recommended for 802.1x SSIDs.
- **Standard**: Enables the virtual AP when the remote AP connects to the controller. Recommended for 802.1x, tunneled, and split-tunneled SSIDs. This is the default behavior.

While using the backup configuration, the remote AP periodically retries its IPsec tunnel to the controller. If you configure the remote AP in backup mode, and a connection to the controller is re-established, the remote AP stops using the backup configuration and immediately brings up the standard remote AP

configuration. If you configure the remote AP in always or persistent mode, the backup configuration remains active after the IPsec tunnel to the controller has been re-established.

This section describes the following topics:

Configuring the Backup Configuration

To configure the backup configuration, you must configure the AAA profile then configure the virtual AP profile:"

Using the WebUI to configure the AAA profile

1. Navigate to the **Security > Authentication > AAA Profiles** window. From the AAA Profiles Summary list, click **Add**.
2. Enter a AAA profile name, then click **Add**.
3. Select the AAA profile that you just created:
   a. For Initial role, select the appropriate role (for example, "logon").
   b. For 802.1X Authentication Default Role, select the appropriate role (for example, "default"), then click **Apply**.
   c. Under the AAA profile that you created, locate 802.1x Authentication Server Group, and select the authentication server group to use (for example "default"), then click **Apply**. If you want to create a new 802.1x authentication server group for this feature, select **new** from the 802.1X Authentication Server Group drop-down list, and enter the appropriate parameters.
   d. Under the AAA profile that you created, locate 802.1X Authentication Profile, and select the profile to use (for example, "default"), then click **Apply**. If you need to create an 802.1x authentication profile, select new from the 802.1X Authentication Profile drop-down list, and enter the appropriate parameters.

Using the WebUI to define the backup configuration in the virtual AP profile

1. Navigate to the **Configuration > Wireless > AP Configuration** window. Select either the AP Group or AP Specific tab. Click **Edit** by the Remote AP group or Remote AP name.
2. Under Profiles, select **Wireless LAN**, then **Virtual AP**.
3. To create a new virtual AP profile in the WebUI, select **New** from the **Add a profile** drop-down menu. Enter the name for the virtual AP profile, and click **Add**.


NOTE

Whenever you create a new virtual AP profile in the WebUI, the profile automatically contains the "default" SSID profile with the default "aruba-ap" ESSID. You must configure a new ESSID and SSID profile for the virtual AP profile before you apply the profile.

   a. In the Profile Details entry for the new virtual AP profile, go to the **AAA Profile** drop-down list and select the previously configured AAA profile (for example, "logon"). The AAA Profile pop-up window appears.
   b. To set the AAA profile and close the pop-up window, Click **Apply.**
   c. In the Profile Details entry for the new virtual AP profile, select **NEW** from the **SSID Profile** drop-down menu. The SSID Profile pop-up window displays to allow you to configure the SSID profile.
   d. Enter the name for the SSID profile (for example, "backup").

e. Under the **Network** section, enter a name in the **Network Name (SSID)** field (for example, “backup-psk”).

f. Under Security, select the network authentication and encryption methods (for example, wpa-psk-tkip, with the passphrase “remote123”).

g. To set the SSID profile and close the pop-up window, click **Apply**.

4. At the bottom of the Profile Details window, Click **Apply**.
5. Click the new virtual AP name in either the Profiles list or the Profile Details window to display configuration parameters.
6. In the Profile Details window, do the following:

a. Make sure Virtual AP enable is selected.

b. From the **VLAN** drop-down menu, select the VLAN ID to use for the virtual AP profile.

c. From the **Forward mode** drop-down menu, select **bridge**.

d. From the **Remote-AP Operation** drop-down menu, select **always**, **backup**, or **persistent**. The default is standard.

e. Click **Apply**.

Using the CLI to configure the AAA profile

```
aaa profile <name>
   initial-role <role>
   authentication-dot1x <dot1x-profile>
   dot1x-default-role <role>
   dot1x-server-group <group>
```

Using the CLI to define the backup configuration in the virtual AP profile

```
wlan ssid-profile <profile>
   essid <name>
   opmode <method>
   wpa-passphrase <string> (if necessary)


wlan virtual-ap <name>
   ssid-profile <profile>
   vlan <vlan>
   forward-mode bridge
   aaa-profile <name>
   rap-operation {always|backup|persistent}

ap-group <name>
   virtual-ap <name>
```

or

```
ap-name <name>
   virtual-ap <name>
```

Configuring the DHCP Server on the Remote AP

You can configure the internal DHCP server on the remote AP to provide an IP address for the “backup” SSID if the controller is unreachable. If configured, the remote AP DHCP server intercepts all DHCP requests and assigns an IP address from the configured DHCP pool.

To configure the remote AP DHCP server:

- Enter the VLAN ID for the remote AP DHCP VLAN in the AP system profile. This VLAN enables the DHCP server on the AP (also known as the remote AP DHCP server VLAN). If you enter the native VLAN ID, the DHCP server is not configured and is unavailable.
- Specify the DHCP IP address pool and netmask. By default, the AP assigns IP addresses from the DHCP pool 192.168.11.0/24, with an IP address range from 192.168.11.2 through 192.168.11.254. If the default 192.168.11.X address is already in use, an AP will automatically switch to a 172.16.11.X network. You can manually define the DHCP IP address pool and netmask based on your network design and IP address scheme.
- Specify the IP address of the DHCP server, DHCP router, and the DHCP DNS server. By default, the AP uses IP address 192.168.11.1 for the DHCP server, the DHCP router and the DHCP DNS server.
- Enter the amount of days the assigned IP address is valid (also known as the remote AP DHCP lease). By default, the lease does not expire, which means the IP address is always valid.
- Assign the VLAN ID for the remote AP DHCP VLAN to a virtual AP profile. When a client connects to that virtual AP profile, the AP assigns the IP address from the DHCP pool.

The following is a high-level description of the steps required to configure the DHCP server on the remote AP. The steps assume you have already created the virtual AP profile, AAA profile, SSID profile, and other settings for your remote AP operation (for information about the backup configuration, see "Configuring the Backup Configuration" on page 53).

Using the WebUI to configure the DHCP server on the AP

1. Navigate to the **Configuration > Wireless > AP Configuration** window.
2. Select either the AP Group or AP Specific tab. Click **Edit** for the AP group or AP name.
3. Under Profiles, select **AP** to display the AP profiles.
4. Select the AP system profile you want to modify.
5. Under Profile Details:
   a. At the **LMS IP** field, enter the LMS IP address.
   b. At the **Master controller IP address** field, enter the master controller IP address.
   c. At the **Remote-AP DHCP Server VLAN** field, enter the VLAN ID of the backup configuration virtual AP VLAN.
   d. At the **Remote-AP DHCP Server ID** field, enter the IP address for the DHCP server.
   e. At the **Remote-AP DHCP Default Router** field, enter the IP address for the default DHCP router.
   f. At the **Remote-AP DHCP DNS Server** list, enter an IP address in the field to right and click **Add**. You can add multiple IP addresses the same way. To delete an IP address, select an IP address from the list and click **Delete**.
   g. Specify the DHCP IP address pool. This configures the pool of IP addresses from which the remote AP uses to assign IP addresses.
      - At the Remote-AP DHCP Pool Start field, enter the first IP address of the pool.
      - At the Remote-AP-DHCP Pool End field, enter the last IP address of the pool.
      - At the Remote-AP-DHCP Pool Netmask field, enter the netmask.
   h. At the **Remote-AP DHCP Lease Time** field, specify the amount of time the IP address is valid.
6. Click **Apply**.
7. Under Profiles, select **Wireless LAN**, then **Virtual AP**, then the virtual AP profile you want to configure.

8. Under Profile Details, at the VLAN drop-list, select the VLAN ID of the remote AP DHCP VLAN, click the left arrow to move the VLAN ID to the VLAN field, and click **Apply**.

Using the CLI to configure the DHCP server on the AP

```
ap system-profile <name>
   lms-ip <ipaddr>
   master-ip <ipaddr>
   rap-dhcp-default-router <ipaddr>
   rap-dhcp-dns-server <ipaddr>
   rap-dhcp-lease <days>
   rap-dhcp-pool-end <ipaddr>
   rap-dhacp-pool-netmask <netmask>
   rap-dhcp-pool-start <ipaddr>
   rap-dhcp-server-id <ipaddr>
   rap-dhcp-server-vlan <vlan>

wlan virtual-ap <name>
   ssid-profile <profile>
   vlan <vlan>
   forward-mode bridge
   aaa-profile <name>
   rap-operation {always|backup|persistent}

ap-group <name>
   ap-system-profile <name>
   virtual-ap <name>
```

or

```
ap-name <name>
   ap-system-profile <name>
   virtual-ap <name>
```

Define Advanced Backup Configuration Options

You can also use the backup configuration to allow the remote AP to pass through a captive portal, such as network access in a hotel, airport, or other public network, to access the corporate network. For this scenario:

- Define a session ACL for the bridge SSID to source NAT all user traffic, except DHCP. For example, use **any any svc-dhcp permit** followed by **any any any route src-nat**. Apply the session ACL to a remote AP user role. (You must install the Policy Enforcement Firewall license.)
- Configure the AAA profile. Make sure the initial role contains the session ACL previously configured.

  The AAA profile defines the authentication method and the default user role.


NOTE

802.1x and PSK authentication is supported when configuring bridge or split tunnel mode.

- Configure the virtual AP profile for the backup configuration.
  - Set the remote AP operation to “always” or “backup.”
  - Create and apply the applicable SSID profile.
  - Configure a bridge SSID for the backup configuration. In the virtual AP profile, specify forward mode as “bridge.”

  For more information about the backup configuration, see “Configuring the Backup Configuration” on page 53.

- Enter the remote AP DHCP server parameters in the AP system profile. For more information about the parameters, see "Configuring the DHCP Server on the Remote AP" on page 54.

  If you use a local DHCP server to obtain IP addresses, you must define one additional ACL to permit traffic between clients without source NATing the traffic. Using the previously configured ACL, add **user alias internal-network any permit** before **any any any route src-nat**.
- Connect the remote AP to the available public network (for example, a hotel or airport network).

  The remote AP advertises the backup SSID so the wireless client can connect and obtain an IP address from the available DHCP server. After obtaining an IP address, the wireless client can connect and access the corporate network and bring up the configured corporate SSIDs.

The wireless client can obtain an IP address from the public network, for example a hotel or airport, or from the DHCP server on the remote AP.

The following pages contain a high-level description of what is needed to configure the remote AP to pass through a captive portal and access the corporate controller. This information assumes you are familiar with configuring session ACLs, AAA profiles, virtual APs, and AP system profiles and highlights the modified parameters.

Using the WebUI to configure the session ACL

1. Navigate to the **Configuration > Security > Access Control > Policies** window.
2. Click **Add** to crete a new policy.
3. Enter the policy name in the **Policy Name** field.
4. From the **Policy Type** drop-down list, select **IPv4 Session**.
5. To create the first rule:
   a. Under Rules, click **Add**.
   b. Under Source, select **any**.
   c. Under Destination, select **any**.
   d. Under Service, select **service**. In the service drop-down list, select **svc-dhcp**.
   e. Under Action, select **permit**.
   f. Click **Add**.
6. To create the next rule:
   a. Under Rules, click **Add**.
   b. Under Source, select **any**.
   c. Under Destination, select **any**.
   d. Under Service, select **any**.
   e. Under Action, select **route**, and select the **src-nat** checkbox.
   f. Click **Add**.
7. Click **Apply**.

If you use a local DHCP server to obtain IP addresses, you must define one additional ACL to permit traffic between clients without source NATing the traffic. Add user **alias internal-network any permit** before **any any any route src-nat**.

8. Click the **User Roles** tab.
   a. Click **Add**.
   b. Enter the Role Name.

c. Click **Add** under Firewall Policies.

d. In the Choose from Configured Policies menu, select the policy you just created.

e. Click **Done**.

Using the WebUI to configure the AAA profile

1. Navigate to the **Security > Authentication > AAA Profiles** window. From the AAA Profiles Summary list, click **Add**.
2. Enter the AAA profile name, then click **Add**.
3. Select the AAA profile that you just created:
   a. For Initial role, select the user role you just created.
   b. For 802.1X Authentication Default Role, select the appropriate role for your remote AP configuration, then click **Apply**.
   c. Under the AAA profile that you created, locate 802.1x Authentication Server Group, and select the authentication server group to use for your remote AP configuration, then click **Apply**.

If you need to create an 802.1x authentication server group, select **new** from the **802.1X Authentication Server Group** drop-down list, and enter the appropriate parameters.

   d. Under the AAA profile that you created, locate 802.1X Authentication Profile, and select the profile to use for your remote AP configuration, then click **Apply**.

Using the WebUI to define the backup configuration

1. Navigate to the **Configuration > Wireless > AP Configuration** window. Select either the AP Group or AP Specific tab. Click **Edit** for the AP group or AP name.
2. Under Profiles, select **Wireless LAN**, then **Virtual AP**.
3. To create a new virtual AP profile in the WebUI, select **New** from the **Add a profile** drop-down menu. Enter the name for the virtual AP profile, and click **Add**.

Whenever you create a new virtual AP profile in the WebUI, the profile automatically contains the “default” SSID profile with the default “aruba-ap” ESSID. You must configure a new ESSID and SSID profile for the virtual AP profile before you apply the profile.

   a. In the Profile Details entry for the new virtual AP profile, go to the **AAA Profile** drop-down list and select the previously configured AAA profile. The AAA Profile pop-up window appears.
   b. To set the AAA profile and close the pop-up window, Click **Apply.**
   c. In the Profile Details entry for the new virtual AP profile, select **NEW** from the **SSID Profile** drop-down menu. The SSID Profile pop-up window displays to allow you to configure the SSID profile.
   d. Enter the name for the SSID profile.
   e. Under Network, enter a name in the Network Name (SSID) field.
   f. Under Security, select the network authentication and encryption methods.
   g. To set the SSID profile and close the pop-up window, click **Apply**.
4. At the bottom of the Profile Details window, Click **Apply**.
5. Click the new virtual AP name in the Profiles list or the Profile Details to display configuration parameters.
6. Under Profile Details, do the following:
   a. Make sure Virtual AP enable is selected.

b. From the **VLAN** drop-down menu, select the VLAN ID to use for the Virtual AP profile.
c. From the **Forward mode** drop-down menu, select **bridge**.
d. From the **Remote-AP Operation** drop-down menu, select **always** or **backup**.
e. Click **Apply**.

7. Under Profiles, select **AP**, then **AP system profile**.
8. Under Profile Details, do the following:
   a. Select the AP system profile to edit.
   b. At the **LMS IP** field, enter the LMS IP address.
   c. At the **Master controller IP address** field, enter the master controller IP address.
   d. Configure the **Remote-AP DHCP Server** fields.
   e. Click **Apply**.

Using the CLI to configure the session ACL

The commands to configure the session ACL vary, depending upon whether you want to use the DHCP server on the remote AP, or a local DHCP server elsewhere on your network.

If you plan on using the AP's own DHCP server use the commands below to configure the session ACL.

```
ip access-list session <policy>
   any any svc-dhcp permit
   any any any route src-nat
```

If you plan on using a local DHCP server, use the following commands to configure the session ACL.

```
ip access-list session <policy>
   any any svc-dhcp permit
    user alias internal-network any permit
   any any any route src-nat
```

If you use a local DHCP server to obtain IP addresses, you must define one additional ACL to permit traffic between clients without source NATing the traffic. Add **user alias internal-network any permit** before **any any any route src-nat**.

```
user-role <role>
   session-acl <policy>
```

Using the CLI to configure the AAA profile

```
aaa profile <name>
   initial-role <role>
```

You can define other parameters as needed.

Using the CLI to define the backup configuration

```
wlan ssid-profile <profile>
   essid <name>
   opmode <method>
   wpa-passphrase <string> (if necessary)

wlan virtual-ap <name>
   ssid-profile <profile>
   vlan <vlan>
   forward-mode bridge
   aaa-profile <name>
   rap-operation {always|backup}
```

```
ap system-profile <name>
   lms-ip <ipaddr>
   master-ip <ipaddr>
   rap-dhcp-default-router <ipaddr>
   rap-dhcp-dns-server <ipaddr>
   rap-dhcp-lease <days>
   rap-dhcp-pool-end <ipaddr>
   rap-dhacp-pool-netmask <netmask>
   rap-dhcp-pool-start <ipaddr>
   rap-dhcp-server-id <ipaddr>
   rap-dhcp-server-vlan <vlan>

ap-group <name>
   virtual-ap <name>
   ap-system-profile <name>
```

or

```
ap-name <name>
   virtual-ap <name>
   ap-system-profile <name>
```

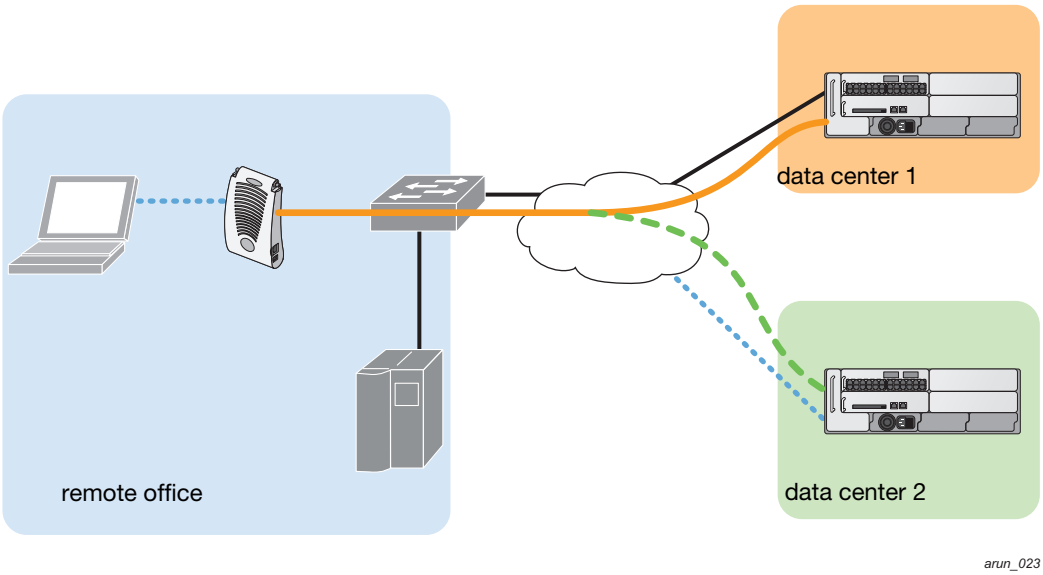
Backup Controller List

Using DNS, the remote AP receives multiple IP addresses in response to a host name lookup. Known as the backup controller list, remote APs go through this list to associate with a controller. If the primary controller is unavailable or does not respond, the remote AP continues through the list until it finds an available controller. This provides redundancy and failover protection.

If the remote AP loses connectivity on the IPsec tunnel to the controller, the remote AP establishes connectivity with a backup controller from the list and automatically reboots. Network connectivity is lost during this time. As described in the section "Remote AP Failback" on page 61, you can also configure a remote AP to revert back to the primary controller when it becomes available.To complete this scenario, you must also configure the LMS IP address and the backup LMS IP address.

For example, assume you have two data centers, data center 1 and data center 2. Data center has a master controller in the DMZ while data center 2 has a local controller only. You can provision the remote APs to use the controller in data center 1 as the primary controller, and the controller in data center 2 as the backup controller. If the remote AP loses connectivity to the primary controller, it will attempt to establish connectivity to the backup. You define the LMS parameters in the AP system profile.

Figure 1 Sample Backup Controller Scenario



Using the WebUI to configure the LMS and backup LMS IP addresses

1. Navigate to the **Configuration > Wireless > AP Configuration** window.
2. Select either the AP Group or AP Specific tab. Click **Edit** for the AP group or AP name.
3. Under Profiles, select **AP** to display the AP profiles.
4. Select the AP system profile you want to modify.
5. Under Profile Details:
   a. At the **LMS IP** field, enter the primary controller IP address.
   b. At the **Backup LMS IP** field, enter the backup controller IP address.
6. Click **Apply**.

Using the CLI to configure the LMS and backup LMS IP addresses

```
ap system-profile <profile>
   lms-ip <ipaddr>
   bkup-lms-ip <ipaddr>

ap-group <group>
   ap-system-profile <profile>

ap-name <name>
   ap-system-profile <profile>
```

Remote AP Failback

In conjunction with the backup controller list, you can configure remote APs to revert back (failback) to the primary controller if it becomes available. If you do not explicitly configure this behavior, the remote AP will keep its connection with the backup controller until the remote AP, controller, or both have rebooted or some type of network failure occurs. If any of these events occur, the remote AP will go through the backup controller list and attempt to connect with the primary controller.

Using the WebUI to configure remote AP failback

1. Navigate to the **Configuration > Wireless > AP Configuration** window.

2. Select either the AP Group or AP Specific tab. Click **Edit** for the AP group or AP name.
3. Under Profiles, select **AP** to display the AP profiles.
4. Select the AP system profile you want to modify.
5. Under Profile Details:
   a. Click (select) **LMS Preemption**. This is disabled by default.
   b. At the **LMS Hold-down period** field, enter the amount of time the remote AP must wait before moving back to the primary controller.
6. Click **Apply**.

Using the CLI to configure remote AP failback

```
ap system-profile <profile>
   lms-preemption
   lms-hold-down period <seconds>
```

Access Control Lists and Firewall Policies

Remote APs support the following access control lists (ACLs); unless otherwise noted, you apply these ACLS to user roles:

- Standard ACLs—Permit or deny traffic based on the source IP address of the packet.
- Ethertype ACLs—Filter traffic based on the Ethertype field in the frame header.
- MAC ACLs—Filter traffic on a specific source MAC address or range of MAC addresses.
- Firewall policies (session ACLs)—Identifies specific characteristics about a data packet passing through the Aruba controller and takes some action based on that identification. You apply these ACLs to user roles or uplink ports.


NOTE

To configure firewall policies, you must install the Policy Enforcement Firewall license.

For more information about ACLs and firewall policies, see “Configuring the Backup Configuration” on page 53.

Split Tunneling

The split tunneling feature allows you to optimize traffic flow by directing only corporate traffic back to the controller, while local application traffic remains local. This ensures that local traffic does not incur the overhead of the round trip to the controller, which decreases traffic on the WAN link and minimizes latency for local application traffic. This is useful for sites that have local servers and printers. With split tunneling, a remote user associates with a single SSID, not multiple SSIDs, to access corporate resources (for example, a mail server) and local resources (for example, a local printer). The remote AP examines session ACLs to distinguish between corporate traffic destined for the controller and local traffic.

Figure 2 Sample Split Tunnel Environment

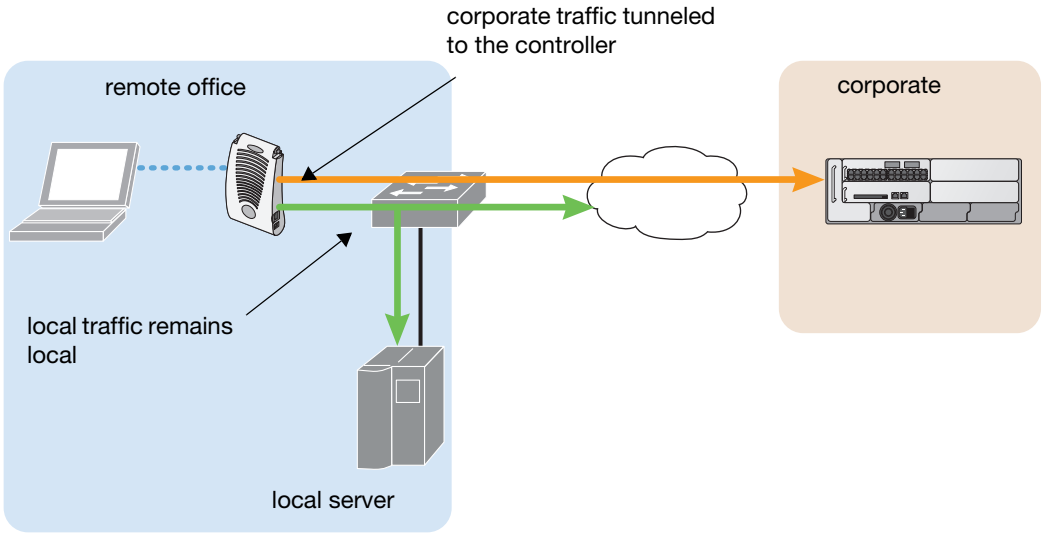


Figure 2 shows that corporate traffic is GRE tunneled to the controller through a trusted tunnel and that local traffic is source NATed and bridged on the wired interface based on the configured user role and session ACL. Split tunnel environments support both 802.1x and PSK authentication.

It is also possible to create a bridge role to prevent a client from accessing corporate or local DHCP servers until that client has been authenticated using Layer-2 (MAC or 802.1x) authentication.

Policy Driven DHCP packet forwarding

Starting with ArubaOS Remote Networking 3.1, if the AP's wired port is configured in split-tunnel mode, clients using that AP for layer-2 authentication are classified as a split-mode user or a bridge-mode user, depending on whether or not the user was successfully authenticated. This feature can be enabled in the wired port profile by defining a bridge user role to be used if split-tunnel authentication fails.

If a user successfully completes either MAC authentication or 802.1x authentication on an AP with the wired port in split-tunnel mode, the authenticated user is classified as a split-mode user and can obtain an IP address from the corporate DHCP pool.

If a user fails MAC authentication or 802.1x authentication on an AP with the wired port in split-tunnel mode, the unauthenticated user gets classified as a “bridge-mode user” and must get an IP address locally via a Remote AP, Local DHCP server, DSL router or cable modem.

This change in user classification only occurs on APs with a wired port configured for split-tunnel mode. If an AP's wired port is configured in bridge mode and a user fails layer-2 authentication, that user remains classified as a bridge mode user. Similarly, if a user fails layer-2 authentication on an AP with a wired port in tunnel mode, the user will remain classified as a tunnel mode user.

Configuring Split Tunneling

To configure split tunneling:

1. Configure the Session ACL: Define a session ACL that forwards only corporate traffic to the controller.
   - Configure a netdestination for the corporate subnets.
   - Create rules to permit DHCP and corporate traffic to the corporate controller. When specifying the action that you want the controller to perform on a packet that matches the specified criteria, “permit” implies tunneling, which is used for corporate traffic, and “route” implies local bridging, which is used for local traffic.

You must install the Policy Enforcement Firewall license in the controller. Apply the session ACL to a user role.

2. Configure the AAA Profile: The AAA profile defines the authentication method and the default user role for authenticated users. The configured user role contains the split ACL.
3. Configure the Virtual AP Profile: When configuring the virtual AP profile, you specify the AP group or AP to which the profile will apply.
   - Set the VLAN used for split tunneling. Only one VLAN can be configured for split tunneling; VLAN pooling is not allowed.
   - When specifying the use of a split tunnel configuration, use “split-tunnel” forward mode.
   - Create and apply the applicable SSID profile.
4. List the Corporate DNS Servers: Optionally, create a list of network names resolved by corporate DNS servers.

Configure the Session ACL

First you need to configure the session ACL. By applying this policy, local traffic remains local, and corporate traffic is forwarded (tunneled) to the controller.

Using the WebUI to configure the session ACL

1. Navigate to the **Configuration > Security > Access Control > Policies** window.
2. Click **Add** to crete a new policy.
3. Enter the policy name in the **Policy Name** field.
4. From the **Policy Type** drop-down list, select **IPv4 Session**.
5. To create the first rule:
   a. Under Rules, click **Add**.
   b. Under Source, select **any**.
   c. Under Destination, select **any**.
   d. Under Service, select **service**. In the service drop-down list, select **svc-dhcp**.
   e. Under Action, select **permit**.
   f. Click **Add**.
6. To create the next rule:
   a. Under Rules, click **Add**.
   b. Under Source, select **any**.
   c. Under Destination, select **alias**.

   The following steps define an alias representing the corporate network. Once defined, you can use the alias for other rules and policies. You can also create multiple destinations the same way.
7. Under the alias section, click **New**. Enter a name in the Destination Name field.
   a. Click **Add**.
   b. For Rule Type, select **Network**.
   c. Enter the public IP address of the controller.
   d. Enter the Network Mask/Range.
   e. Click **Add** to add the network range.
   f. Click **Apply**. The new alias appears in the Destination menu.
8. Under Destination, select the alias you just created.
9. Under Service, select **any**.

10. Under Action, select **permit**.
11. Click **Add**.
12. To create the next rule:
    a. Under Rules, click **Add**.
    b. Under Source, select **user**.
    c. Under Destination, select **any**.
    d. Under Service, select **any**.
    e. Under Action, select **any** and check **src-nat**.
    f. Click **Add**.
13. Click **Apply**.
14. Click the **User Roles** tab.
    a. Click **Add** to create and configure a new user role.
    b. Enter the desired name for the role in the **Role Name** field.
    c. Under Firewall Policies, click **Add**.
    d. From the **Choose from Configured Policies** drop-down menu, select the policy you just configured.
    e. Click **Done**.
15. Click **Apply**.

Using the CLI to configure the session ACL

```
netdestination <network destination>
   network <ipaddr> <netmask>
   network <ipaddr> <netmask>

ip access-list session <policy>
   any any svc-dhcp permit
   any alias <name> any permit
   user any any route src-nat

user-role <role>
   session-acl <policy>
```

When defining the alias, there are a number of other session ACLs that you can create to define the handling of local traffic, such as:

```
ip access-list session <policy>
   user alias <name> any redirect 0
   user alias <name> any route
   user alias <name> any route src-nat
```

For additional information on defining session ACLs, refer to the ArubaOS 3.2 User Guide or ArubaOS 3.2 CLI Reference Guide.

Configure the AAA Profile

After you configure the session ACL, you define the AAA profile and virtual AP used for split tunneling. When defining the AAA parameters, specify the previously configured user role that contains the session ACL used for split tunneling.

Using the WebUI to configure a AAA profile

1. Navigate to the **Security > Authentication > AAA Profiles** window. From the AAA Profiles Summary list, click **Add**.

2. Enter the AAA profile name, then click **Add**.
3. Select the AAA profile that you just created:
   a. For 802.1X Authentication Default Role, select the user role you previously configured for split tunneling, then click **Apply**.
   b. Under the AAA profile that you created, locate 802.1x Authentication Server Group, and select the authentication server group to use, then click **Apply**. If you need to create an authentication server group, select **new** and enter the appropriate parameters.

Using the CLI to configure the AAA profile

```
aaa profile <name>
  authentication-dot1x <dot1x-profile>
  dot1x-default-role <role>
  dot1x-server-group <group>
```

Configure the Virtual AP Profile

Using the WebUI to configure split tunneling in the virtual AP profile

1. Navigate to **Configuration > Wireless > AP Configuration** window. Select either the AP Group or AP Specific tab. Click **Edit** for the applicable AP group name or AP name.
2. Under Profiles, select **Wireless LAN**, then **Virtual AP**.
3. To create a new virtual AP profile in the WebUI, select **New** from the **Add a profile** drop-down menu. Enter the name for the virtual AP profile, and click **Add**.


NOTE

Whenever you create a new virtual AP profile in the WebUI, the profile automatically contains the “default” SSID profile with the default “aruba-ap” ESSID. You must configure a new ESSID and SSID profile for the virtual AP profile before you apply the profile.

   a. In the Profile Details window, select the AAA profile currently configured for the Virtual AP you want to configure. The AAA Profile window appears.
   b. Click the AAA profile drop-down list and select the AAA profile you just configured in the previous procedure. Click **Apply** to save your settings.
   c. In the Profile list in the left window pane, select the name of the virtual AP profile you are configuring, then select the SSID profile menu under the virtual AP name.
   d. In the Profile Details window, click the SSID profile drop-down list and select **NEW**.
   e. Enter the name for the SSID profile in the entry blank.
   f. Under Network, enter a name in the Network Name (SSID) field.
   g. Under Security, select the network authentication and encryption methods.
   h. To set the SSID profile and close the window, click **Apply**.
4. Click **Apply** at the bottom of the Profile Details window.
5. Click the virtual AP name in the Profiles list to display its configuration parameters.
6. In the Profile Details window, configure the following settings:
   a. Make sure Virtual AP enable is selected.
   b. From the **VLAN** drop-down menu, select the VLAN ID for the VLAN to be used for split tunneling.
   c. From the **Forward mode** drop-down menu, select **split-tunnel**.
   d. Click **Apply**.

Using the CLI to configure split tunneling in the virtual AP profile

```
wlan ssid-profile <profile>
   essid <name>
   opmode <method>

wlan virtual-ap <profile>
   ssid-profile <name>
   forward-mode split-tunnel
   vlan <vlan id>
   aaa-profile <profile>

ap-group <name>
   virtual-ap <profile>
```

or

```
ap-name <name>
   virtual-ap <profile>
```

List the Corporate DNS Servers

Clients send DNS requests to the corporate DNS server address that it learned from DHCP. If configured for split tunneling, corporate domains and traffic destined for corporate use the corporate DNS server. For non-corporate domains and local traffic, other DNS servers can be used

Using the WebUI to list the corporate DNS servers

1. Navigate to **Configuration > Wireless > AP Configuration** window.
2. Select either the AP Group or AP Specific tab. Click **Edit** for the AP group or AP name.
3. Under Profiles, select **AP**, then **AP system profile**.
4. Under Profile Details:
   a. Enter the corporate DNS servers.
   b. Click **Add**.

      The DNS name appears in Corporate DNS Domain list. You can add multiple names the same way.
5. Click **Apply**.

Using the CLI to list the corporate DNS servers

```
ap system-profile <profile>
   dns-domain <domain_name1>
   dns-domain <domain_name2>
```

Remote AP Support for Wi-Fi Multimedia

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance specification based on the IEEE 802.11e wireless Quality of Service (QoS) standard. WMM works with 802.11a, b, g, and n physical layer standards. The IEEE 802.11e standard also defines the mapping between WMM access categories (ACs) and Differentiated Services Codepoint (DSCP) tags. Remote APs support WMM.

WMM supports four ACs: **voice**, **video**, **best effort**, and **background**. You apply and configure WMM in the Remote AP's SSID profile.

When planning your configuration, make sure that immediate switches or routers do not have conflicting 802.1p or DSCP configurations/mappings. If this occurs, your traffic may not be prioritized correctly.

PSK-Refresh

Preshared key (PSK) refresh allows you to refresh the IKE PSK used by remote APs. By default, PSK-refresh is disabled. With PSK-refresh enabled, the controller accepts connections from remote APs using the previously configured PSK for the specified interval. After the interval elapses, that PSK expires and the controller uses the new PSK to authenticate remote APs.

If you enable and then disable PSK-refresh, the remote AP attempts to authenticate with the currently configured global PSK only.

To enable PSK-refresh, you must:

1. Configure the amount of time in days or hours (known as the interval), to remember the previously configured PSK used in your remote AP deployment. Aruba recommends configuring a large interval to prevent remote APs from being unable to authenticate and connect to the network.
2. Configure the global PSK. The IP address must be 0.0.0.0, and the netmask must be 0.0.0.0. Note that if you do not configure the global PSK, the PSK-refresh feature is invalid.

The PSK-refresh configuration is a global configuration. Once configure it on the master controller, the setting is "pushed" to all local and redundant master controllers.

Using the WebUI to enable PSK-refresh

1. Navigate to the **Configuration > Advanced Services > VPN Services > IPsec** window.
2. Scroll down to the IKE Shared Secrets section to configure the global PSK:
   a. Click **Add**.
   b. Use the default 0.0.0.0 addresses for both the subnet and subnet mask.
   c. Enter and verify the IKE shared secret for the PSK.
   d. Click **Done** to return to the IPSEC window.
3. Scroll down to the IKE PSK-Refresh section:
   a. Select (check) the **Enable IKE PSK-Refresh** checkbox. By default this is deselected (unchecked).
   b. Specify the **Interval Type** in either **Hours** or **Days**. You can select (check) the **Hours** or the **Days** checkbox, but not both.
   c. At the Interval value field, enter a range of either 2-24 hours or 1-365 days.
4. Click **Apply**.

Using the CLI to enable PSK-refresh

```
crypto isakmp psk-caching {days <interval> | hours <interval>}
crypto isakmp key <key> address 0.0.0.0 netmask 0.0.0.0
```

Troubleshooting PSK-Refresh

This section provides useful information for troubleshooting PSK-refresh. The information in this section assumes PSK-refresh is enabled.

- If a remote AP attempts authentication with an expired PSK, the controller generates an error message similar to:

  ```
  Dropping RAP IKE request from IP:<address> Port:<number> because old PSK is invalid.
  ```

  If this occurs, you must reprovision the remote AP. To review log messages, use the following command:

  ```
  show log security all | include ike
  ```

- You change the PSK, but the controller reboots before the refresh interval expires—If this happens, the controller will store the previously configured PSK and expiration time in flash. The controller knows the PSK state before the reboot occurred.

If the PSK does not expire before the reboot and is still active based on the configured refresh interval, the remaining time for the PSK will be in sync.

If the PSK expires in between controller reboots, you must reprovision any AP that used the old PSK.

- You want to review the PSK-refresh settings—To display the current PSK-refresh setting, use the following command:

  ```
  show crypto isakmp psk-caching
  ```

  Depending on your configuration, the output displays one of the following:

  If the previous (cached) PSK is still valid:

  ```
  Configured Caching Interval: 5 days
  Previous PSK <key> is VALID upto Fri May 30 11:45:07 2008
  Current PSK: <key1>
  ```

  If the previous (cached) PSK has expired:

  ```
  Configured Caching Interval: 24 hours
  Previous PSK <key> has EXPIRED
  Current PSK: <key1>
  ```

  If PSK is disabled:

  ```
  PSK Caching is disabled
  ```

- You want to know the number of remote AP IKE security associations (SA) that use the new, old, or expired PSK—To see how many remote APs are using the configured PSKs, use the following command:

  ```
  show crypto isakmpt stats
  ```

  The following example statistic displays the number of remote AP IKE security associations (SA) that use the new, old, or expired PSK (in this example, three use the new PSK, one uses the old PSK, and two use the expired PSK):

  ```
  The RAP-PSK-caching IKE SA: New-PSK/Old-PSK/Expired-PSK=3/1/2
  ```

Validated Devices

Validated NAT/Cable Modem for Zero Touch Provisioning

Any standard compliant NAT/Cable modem is acceptable for provisioning a remote AP using certificated-based Zero Touch Provisioning. Aruba has tested and validated the following NAT/Cable Modems for Zero Provisioning. While a modem not in that list may operate as expected, Aruba can only assure the proper performance and interoperability of the modems listed in Table 4.

Table 4 *Validated NAT/Cable Modems*

Vendor	Model
Dlink	DIR-635
Dlink	DI-604
Dlink	DIR-615
Netgear	WGR614 v7
Netgear	WGE614
Netgear	WNDR3300
Trendnet	TEW-432BRP

Table 4 *Validated NAT/Cable Modems*

Vendor	Model
Linksys	RVS4000
Linksys	BEFSR41 ver4.3
Airlink	AR430W
US Robotics	USR 8004
Apple	AirPort Extreme Base Station
2-Wire	2701HG-B
Motorola Cable Modem	Motorola Surfboard SB5101

The Aruba AP models RAP-5, RAP-5WN, and RAP-2WG are compatible with any standard compliance VoIP phone. Extensive interoperability tests were performed on the VoIP devices in Table 5.

Table 5 *Validated VoIP Phones*

Vendor	Model
Ascom	i75 (in SIP mode)
Avaya	3631, 4610, and 4621
Cisco	7921 and 7960
Hitachi	Wireless IP 5000
Nokia	E51
SJ Phones	Cisco 7960
SVP	8020 and 8030
Vocera	B1000A and B2000

The Aruba AP models RAP-5, RAP-5WN, and RAP-2WG are compatible with the scanners and printer listed in Table 6.

Table 6 *Validated Scanners*

Vendor	Model
Symbol Scanner	MC 3090, MC 5040, MC 9090G, PPT 8864
Intermec Scanner	CN2B
HP Printer	HP6988

Troubleshooting

The following section describes information and procedures useful for troubleshooting the following features:

Troubleshooting Campus APs

ArubaOS Remote Networking 3.1 does not support campus APs. Note, however, that if a remote AP flag is set in the provisioning profile on a 3000 series/M3 controller, and you try to bring up campus APs within the same AP group, legacy APs (AP-60, AP-61, AP-65, AP-70,and AP-85) in that AP group will ignore the remote AP flag and come up as a Campus APs.

Troubleshooting RAP Users

The RAP user management feature incorporates all the wired and wireless user information regardless of the mode (tunnel, split-tunnel and bridge) or firewalls. The show user command (below) displays the new detailed user information. For readability, the example below displays the output in two lines; the display output at the command line appears as one continuous line.

```
#show user
Users
-----
IP              MAC               Name         Role              Age(d:h:m)  Auth    VPN link
----------      ------------      ------       ----              ----------  ----    --------
10.4.2.254      00:21:00:30:41:1d  split        remote-user-Corp  00:00:27    802.1x  00:0b:86:ce:12:a8
192.168.11.151  00:21:5c:4c:95:d1  bridge-user  bridge-user       00:00:00    802.1x

AP name        Roaming              Essid/Bssid/Phy                    Profile            Forward mode
-------        -------              ---------------                    -------            ------------
Remote         Associated (Remote)  Corporate1/00:0b:86:61:2a:80/g     Remote-Corporate1  split tunnel
m5              Associated(Remote)   bridge-ssid/00:1a:1e:40:07:f4/a-HT  dot1x-aaa          bridge

User Entries: 2/2
```

Troubleshooting Authorization Profiles

The table below describes the predefined profiles associated with the **default** authorization profile. If any of these profiles are deleted or significantly altered, the default authorization profile may not work as expected.

Table 7 *Profiles Related to the Default Authorization Profiles*

Profile	Description

NoAuthApGroup	Unauthorized RAPs use the following configuration settings defined for the AP group **NoAuthApGroup**.
	
	`AP group "NoAuthApGroup" (Predefined (editable))`
	`-----------------------------------------------`
	`Parameter Value`
	`--------- -----`
	`Virtual AP N/A`
	`802.11a radio profile default`
	`802.11g radio profile default`
	`Ethernet interface 0 port configuration default`
	`Ethernet interface 1 port configuration NoAuthWiredPort`
	`Ethernet interface 2 port configuration NoAuthWiredPort`
	`Ethernet interface 3 port configuration NoAuthWiredPort`
	`Ethernet interface 4 port configuration NoAuthWiredPort`
	`AP system profile default`
	`VoIP Call Admission Control profile default`
	`802.11a Traffic Management profile N/A`
	`802.11g Traffic Management profile N/A`
	`Regulatory Domain profile default`
	`SNMP profile default`
	`RF Optimization profile default`
	`RF Event Thresholds profile default`
	`IDS profile ids-low-setting`
	`Mesh Radio profile default`
	`Mesh Cluster profile N/A`
	`Provisioning profile N/A`
	`AP authorization profile N/A`

NoAuthWiredPort	The AP Wired Port Profile **NoAuthWired Port** references the Wired AP Profile **NoAuthWiredAP** and the AAA Profile **NoAuthAAA Profile**, and includes the following configuration parameters:
	`Parameter Value`
	`--------- -----`
	`Wired AP profile NoAuthWiredAp`
	`Ethernet interface link profile default`
	`Shut down? No`
	`Remote-AP Backup Enabled`
	`AAA Profile NoAuthAAAProfile`
	`Bridge Role N/A`
	`Time to wait for authentication to succeed 5 sec`

Table 7 *Profiles Related to the Default Authorization Profiles*

Profile	Description

NoAuthAAAProfile	The AP group N**oAuthApGroup** references the AAA profile **NoAuthAAAProfile**. This profile specifies an intial role as the **logon** user role, which uses the **default** captive portal profile. The default parameters for this profile are as follows:
	
	`AAA Profile "NoAuthAAAProfile" (Predefined (editable))`
	`-------------------------------------------------------`
	`Parameter Value`
	`--------- -----`
	`Initial role logon`
	`MAC Authentication Profile N/A`
	`MAC Authentication Default Role guest`
	`MAC Authentication Server Group default`
	`802.1X Authentication Profile N/A`
	`802.1X Authentication Default Role guest`
	`802.1X Authentication Server Group N/A`
	`RADIUS Accounting Server Group N/A`
	`XML API server N/A`
	`RFC 3576 server N/A`
	`User derivation rules N/A`
	`Wired to Wireless Roaming Enabled`
	`SIP authentication role N/A`

NoAuthWiredAp	By default, the Wired AP Profile **NoAuthWiredAp** is configured with the following settings:
	
	`The Wired AP profile "NoAuthWiredAp" (Predefined (editable))`
	`-------------------------------------------------------`
	`Parameter Value`
	`--------- -----`
	`Wired AP enable Enabled`
	`Forward mode tunnel`
	`Switchport mode access`
	`Access mode VLAN 1`
	`Trunk mode native VLAN 1`
	`Trunk mode allowed VLANs all`
	`Trusted Not Trusted`
	`Broadcast Broadcast`

Resetting the RAP-2x and RAP-5x to Factory Settings

If you are unable to provision a Zero touch AP because your laptop is not negotiating the IP, try the following trouble shooting steps. If the procedure is not successful, contact your Aruba representative.

This procedure describes various types of connections. Pause, for a few seconds, between each connection to allow the RAP to register that connection before moving onto another connection.

1. Unplug the Power and Ethernet cables
2. Reset the RAP to its factory default setting by holding down the reset button (use a pin or paperclip to hold down the button).
3. Power on the RAP (plug-in the power cord) while still holding down the reset button.

4. Wait for the power LED to start blinking (about 5 seconds) then release the reset button.
5. Plug-in your WAN connection to port 0.
6. Connect your laptop to port 1 (or any port from 1 through 4) using the RJ-45 cable.

To verify your remote AP is properly negotiating the IP

1. From your Windows desktop, select **Start >Run** and enter the **cmd** command to launch the Windows command line.
2. Type **ipconfig** then press Enter at the prompt.

The display output should reveal your IP address on the Ethernet port in the range of 192.168.11.x or 172.16.11.X

If you are still unable to verify your IP Address, contact either your IT Support or Aruba Support.