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

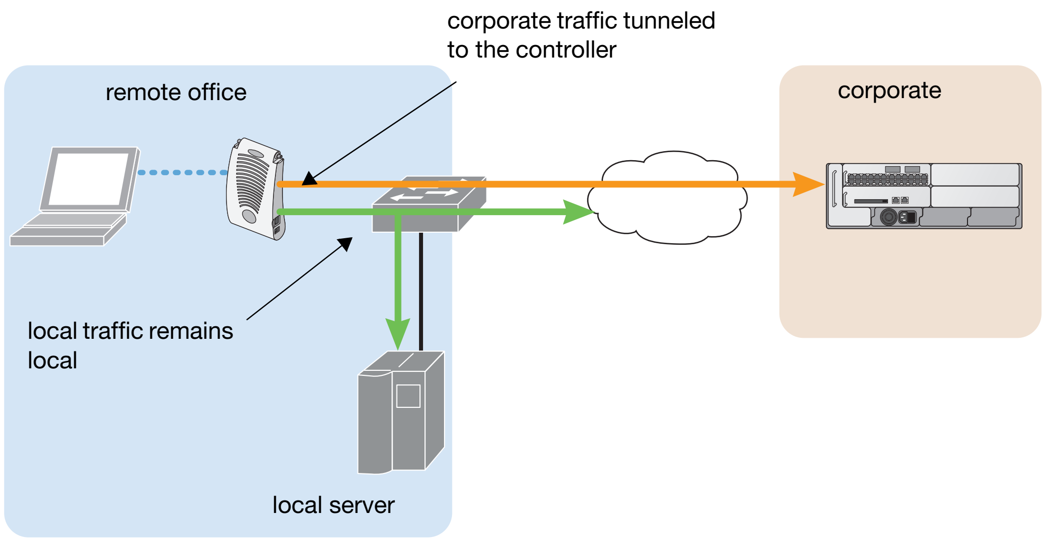
corporate traffic tunneled to the controller
remote office
corporate
local traffic remains local
local server

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.