CHAPTER 15

# Configuring Hybrid REAP

This chapter describes hybrid REAP and explains how to configure this feature on controllers and access points. It contains these sections:

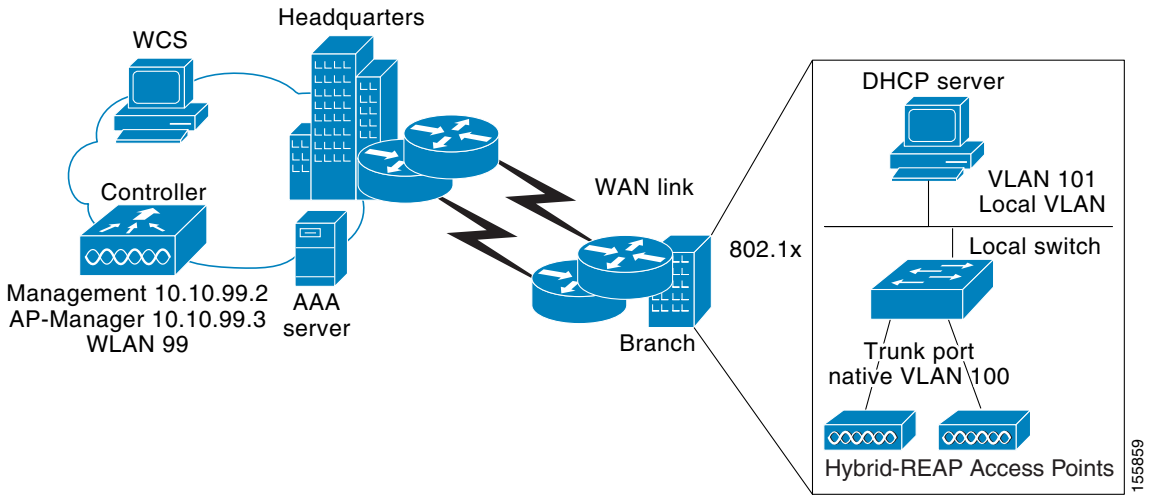


## Overview of Hybrid REAP

*Hybrid REAP* is a solution for branch office and remote office deployments. It enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. There is no deployment restriction on the number of hybrid-REAP access points per location. The hybrid-REAP access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller.

Hybrid REAP is supported only on the 1130AG, 1240AG, 1142 and 1252 access points and on the 2000 and 4400 series controllers, the Catalyst 3750G Integrated Wireless LAN Controller Switch, the Cisco WiSM, and the Controller Network Module for Integrated Services Routers, and the controller within the Catalyst 3750G Integrated Wireless LAN Controller Switch. Figure 15-1 illustrates a typical hybrid-REAP deployment.

*Figure 15-1 Hybrid REAP Deployment*




# Hybrid-REAP Authentication Process

When a hybrid-REAP access point boots up, it looks for a controller. If it finds one, it joins the controller, downloads the latest software image from the controller and configuration information, and initializes the radio. It saves the downloaded configuration in non-volatile memory for use in standalone mode.

A hybrid-REAP access point can learn the controller IP address in one of these ways:

- If the access point has been assigned an IP address from a DHCP server, it discovers a controller through the regular CAPWAP discovery process [Layer 3 broadcast, over-the-air provisioning (OTAP), DNS, or DHCP option 43.]

**Note** OTAP does not work on the first boot out of the box.

- If the access point has been assigned a static IP address, it can discover a controller through any of the CAPWAP discovery process methods except DHCP option 43. If the access point cannot discover a controller through Layer 3 broadcast or OTAP, Cisco recommends DNS resolution. With DNS, any access point with a static IP address that knows of a DNS server can find at least one controller.
- If you want the access point to discover a controller from a remote network where CAPWAP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the access point CLI) the controller to which the access point is to connect.

When a hybrid-REAP access point can reach the controller (referred to as *connected mode*), the controller assists in client authentication. When a hybrid-REAP access point cannot access the controller, the access point enters standalone mode and authenticates clients by itself.

**Note** The LEDs on the access point change as the device enters different hybrid-REAP modes. See the Hardware Installation Guide for your access point for information on LED patterns.

When a client associates to a hybrid-REAP access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration. With respect to client authentication (open, shared, EAP, web authentication, and NAC) and data packets, the WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

- **central authentication, central switching**—In this state, the controller handles client authentication, and all client data tunnels back to the controller. This state is valid only in connected mode.
- **central authentication, local switching**—In this state, the controller handles client authentication, and the hybrid-REAP access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the hybrid-REAP access point to start switching data packets locally. This message is sent per client. This state is applicable only in connected mode.
- **local authentication, local switching**—In this state, the hybrid-REAP access point handles client authentication and switches client data packets locally. This state is valid only in standalone mode.
- **authentication down, switching down**—In this state, the WLAN disassociates existing clients and stops sending beacon and probe responses. This state is valid only in standalone mode.
- **authentication down, local switching**—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

When a hybrid-REAP access point enters standalone mode, WLANs that are configured for open, shared, WPA-PSK, or WPA2-PSK authentication enter the "local authentication, local switching" state and continue new client authentications. Other WLANs enter either the "authentication down, switching down" state (if the WLAN was configured to central switching) or the "authentication down, local switching" state (if the WLAN was configured to local-switch).

When a hybrid-REAP access point enters standalone mode, it disassociates all clients that are on centrally switched WLANs. For 802.1X or web-authentication WLANs, existing clients are not disassociated, but the hybrid-REAP access point stops sending beacons when the number of associated clients reaches zero (0). It also sends disassociation messages to new clients associating to 802.1X or web-authentication WLANs. Controller-dependent activities such as 802.1X authentication, NAC, and web authentication (guest access) are disabled, and the access point does not send any intrusion detection system (IDS) reports to the controller. Furthermore, most radio resource management (RRM) features (such as neighbor discovery; noise, interference, load, and coverage measurements; use of the neighbor list; and rogue containment and detection) are disabled. However, a hybrid-REAP access point supports dynamic frequency selection in standalone modes.

**Note** If your controller is configured for network access control (NAC), clients can associate only when the access point is in connected mode. When NAC is enabled, you need to create an unhealthy (or quarantined) VLAN so that the data traffic of any client that is assigned to this VLAN passes through the controller, even if the WLAN is configured for local switching. After a client is assigned to a quarantined VLAN, all of its data packets are centrally switched.

The hybrid-REAP access point maintains client connectivity even after entering standalone mode. However, once the access point re-establishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and reallows client connectivity.

## Hybrid REAP Guidelines

Keep these guidelines in mind when using hybrid REAP:

- A hybrid-REAP access point can be deployed with either a static IP address or a DHCP address. In the case of DHCP, a DHCP server must be available locally and must be able to provide the IP address for the access point at bootup.
- Hybrid REAP supports a 500-byte maximum transmission unit (MTU) WAN link at minimum.
- Roundtrip latency must not exceed 100 milliseconds (ms) between the access point and the controller, and CAPWAP control packets must be prioritized over all other traffic.
- The controller can send multicast packets in the form of unicast or multicast packets to the access point. In hybrid-REAP mode, the access point receives multicast packets only in unicast form.
- Hybrid REAP supports CCKM full authentication but not CCKM fast roaming.
- Hybrid REAP supports a 1-1 network address translation (NAT) configuration. It also supports port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option.
- VPN, IPSec, L2TP, PPTP, Fortress authentication, and Cranite authentication are supported for locally switched traffic, provided that these security types are accessible locally at the access point.

# Configuring Hybrid REAP

To configure hybrid REAP, you must follow the instructions in these sections in the order provided:

- Configuring the Switch at the Remote Site, page 15-4
- Configuring the Controller for Hybrid REAP, page 15-5
- Configuring an Access Point for Hybrid REAP, page 15-9
- Connecting Client Devices to the WLANs, page 15-12

## Configuring the Switch at the Remote Site

Follow these steps to prepare the switch at the remote site.

**Step 1** Attach the access point that will be enabled for hybrid REAP to a trunk or access port on the switch.

**Note** The sample configuration below shows the hybrid-REAP access point connected to a trunk port on the switch.

**Step 2** See the sample configuration below to configure the switch to support the hybrid-REAP access point.

In this sample configuration, the hybrid-REAP access point is connected to trunk interface FastEthernet 1/0/2 with native VLAN 100. The access point needs IP connectivity on the native VLAN. The remote site has local servers/resources on VLAN 101. A DHCP pool is created in the local switch for both VLANs in the switch. The first DHCP pool (NATIVE) is used by the hybrid-REAP access point, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched. The bolded text in the sample configuration illustrates these settings.

**Note** The addresses in this sample configuration are for illustration purposes only. The addresses that you use must fit into your upstream network.

```
ip dhcp pool NATIVE
   network 10.10.100.0 255.255.255.0
   default-router 10.10.100.1
!
ip dhcp pool LOCAL-SWITCH
   network 10.10.101.0 255.255.255.0
   default-router 10.10.101.1
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 10.10.98.2 255.255.255.0
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
switchport mode trunk
 spanning-tree portfast
!
interface Vlan100
 ip address 10.10.100.1 255.255.255.0
 ip helper-address 10.10.100.1
!
interface Vlan101
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

# Configuring the Controller for Hybrid REAP

This section provides instructions for configuring the controller for hybrid REAP. The controller configuration for hybrid REAP consists of creating centrally switched and locally switched s. This procedure uses these three WLANs as examples:

| WLAN | Security | Switching | Interface Mapping (VLAN) |
|---|---|---|---|
| employee | WPA1+WPA2 | Central | management (centrally switched VLAN) |
| employee-local | WPA1+WPA2 (PSK) | Local | 101 (local switched VLAN) |
| guest-central | Web authentication | Central | management (centrally switched VLAN) |

**Step 1** Follow these steps to create a centrally switched WLAN. In our example, this is the first WLAN (employee).

a. Choose **Configure > Controllers**.

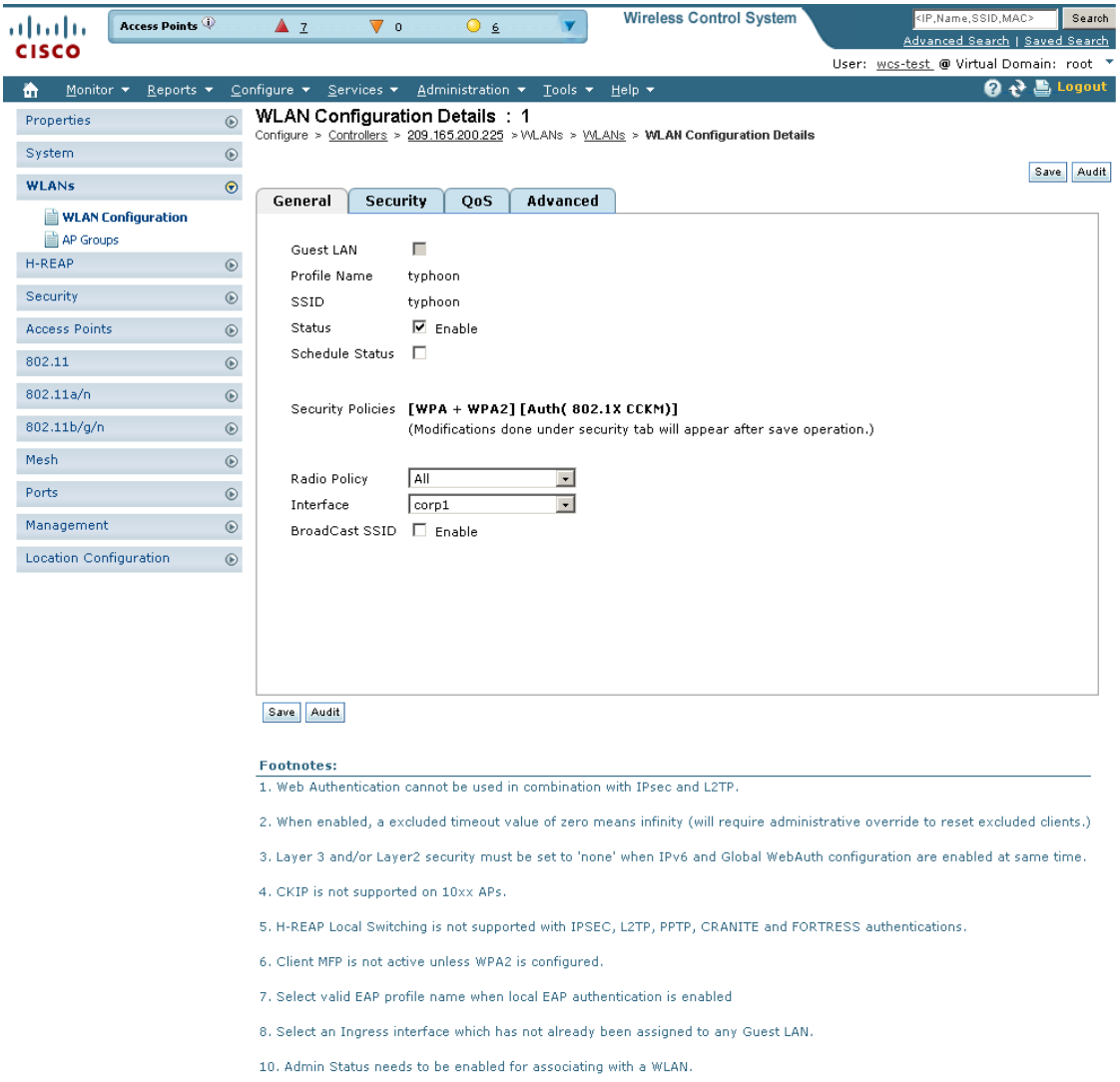
b. Click in the IP Address column for a particular controller.

c. Click **WLANs > WLAN Configuration** to access the s page.

d. Choose **Add a WLAN** from the Select a command drop-down list, and click **Go** (see Figure 15-2).

**Note** Cisco access points can support up to 16 WLANs per controller. However, some Cisco access points do not support WLANs that have a WLAN ID greater than 8. In such cases, when you attempt to create a WLAN, you get a message that says "Not all types of AP support WLAN ID greater than 8, do you wish to continue?". Clicking OK creates a WLAN with the next available WLAN ID. However, if you delete a WLAN that has a WLAN ID less than 8, then the WLAN ID of the deleted WLAN is applied to the next created WLAN.

*Figure 15-2 WLANs > New Page*



e. If you want to apply a template to this controller, choose a template name from the drop-down list. The parameters populate according to how the template is set. If you want to create a new WLAN template, use the *click here* link to be redirected to the template creation page (see the "Configuring WLAN Templates" section on page 12-18).

f. Modify the configuration parameters for this WLAN. In our employee WLAN example, you would need to choose **WPA1+WPA2** from the Layer 2 Security drop-down box.

g. Be sure to enable this WLAN by checking the **Status** check box under General Policies.

**Note** If NAC is enabled and you created a quarantined VLAN for use with this, make sure to select it from the Interface drop-down box under General Policies. Also, select the **Allow AAA Override** check box to ensure that the controller validates a quarantine VLAN assignment.

h. Click **Save** to commit your changes.

**Step 2** Follow these steps to create a locally switched WLAN. In our example, this is the second WLAN (employee-local).

a. Follow the substeps in Step 1 to create a new WLAN. In our example, this WLAN is named "employee-local."

b. Click a WLAN ID from the original WLAN page to move to a WLANs edit page. Modify the configuration parameters for this WLAN. In our employee WLAN example, you would need to choose **WPA1+WPA2** from the Layer 2 Security drop-down box. Make sure to choose PSK authentication key management and enter a pre-shared key.

**Note** Make sure to enable this WLAN by checking the **Admin Status** check box under General Policies. Also, make sure to enable local switching by checking the **H-REAP Local Switching** check box. When you enable local switching, any hybird-REAP access point that advertises this WLAN is able to locally switch data packets (instead of tunneling them to the controller).

**Note** For hybrid-REAP access points, the interface mapping at the controller for WLANs configured for H-REAP Local Switching is inherited at the access point as the default VLAN tagging. This can be easily changed per SSID and per hybrid-REAP access point. Non-hybrid-REAP access points tunnel all traffic back to the controller, and VLAN tagging is dictated by each WLAN's interface mapping.

c. Click **Save** to commit your changes.

**Step 3** Follow these steps if you also want to create a centrally switched WLAN that is used for guest access. In our example, this is the third WLAN (guest-central). You might want to tunnel guest traffic to the controller so you can exercise your corporate data policies for unprotected guest traffic from a central site.

a. Follow the substeps in Step 1 to create a new WLAN. In our example, this WLAN is named "guest-central."

b. In the WLANs Edit page, modify the configuration parameters for this WLAN. In our employee WLAN example, you would need to choose **None** from both the Layer 2 Security and Layer 3 Security drop-down boxes from the Security tab, select the **Web Policy** check box, and make sure **Authentication** is selected.

**Note** If you are using an external web server, you must configure a preauthentication access control list (ACL) on the WLAN for the server and then choose this ACL as the WLAN preauthentication ACL.

c. Make sure to enable this by checking the **Status** check box under General Policies.

d. Click **Save** to commit your changes.

e. If you want to customize the content and appearance of the login page that guest users see the first time they access this, follow the instructions in the "Configuring a Web Authentication Template" section on page 12-64.

f. To add a local user to this WLAN, choose **Configure > Controller Template Launch Pad**.

g. Choose **Security > Local Net Users** from the left sidebar menu.

h. When the Local Net Users page appears, choose **Add Template** from the Select a command drop-down list, and click **Go**.

i. Unselect the Import from File check box.

j. Enter a username and password for the local user.

k. From the Profile drop-down list, choose the appropriate SSID.

l. Enter a description of the guest user account.

m. Click **Save**.

**Step 4** Go to the "Configuring an Access Point for Hybrid REAP" section on page 15-9 to configure two or three access points for hybrid REAP.

# Configuring an Access Point for Hybrid REAP

This section provides instructions for configuring an access point for hybrid REAP.

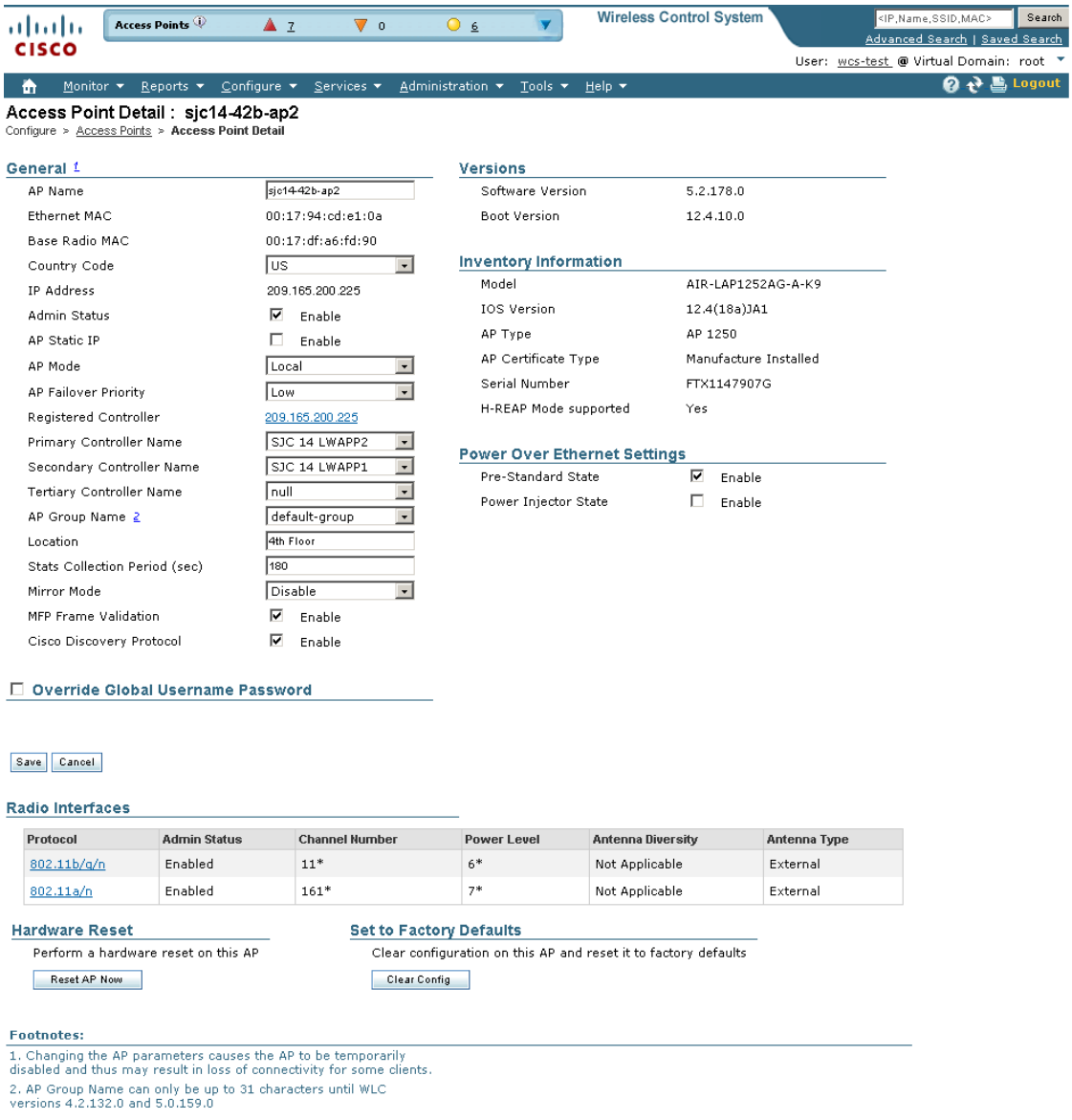
Follow these steps to configure an access point for hybrid REAP.

**Step 1** Make sure that the access point has been physically added to your network.

**Step 2** Choose **Configure > Access Points**.

**Step 3** Choose which access point you want to configure for hybrid REAP by clicking one from the AP Name list. The detailed access point page appears (see Figure 15-3).

*Figure 15-3 Detailed Access Point Page*



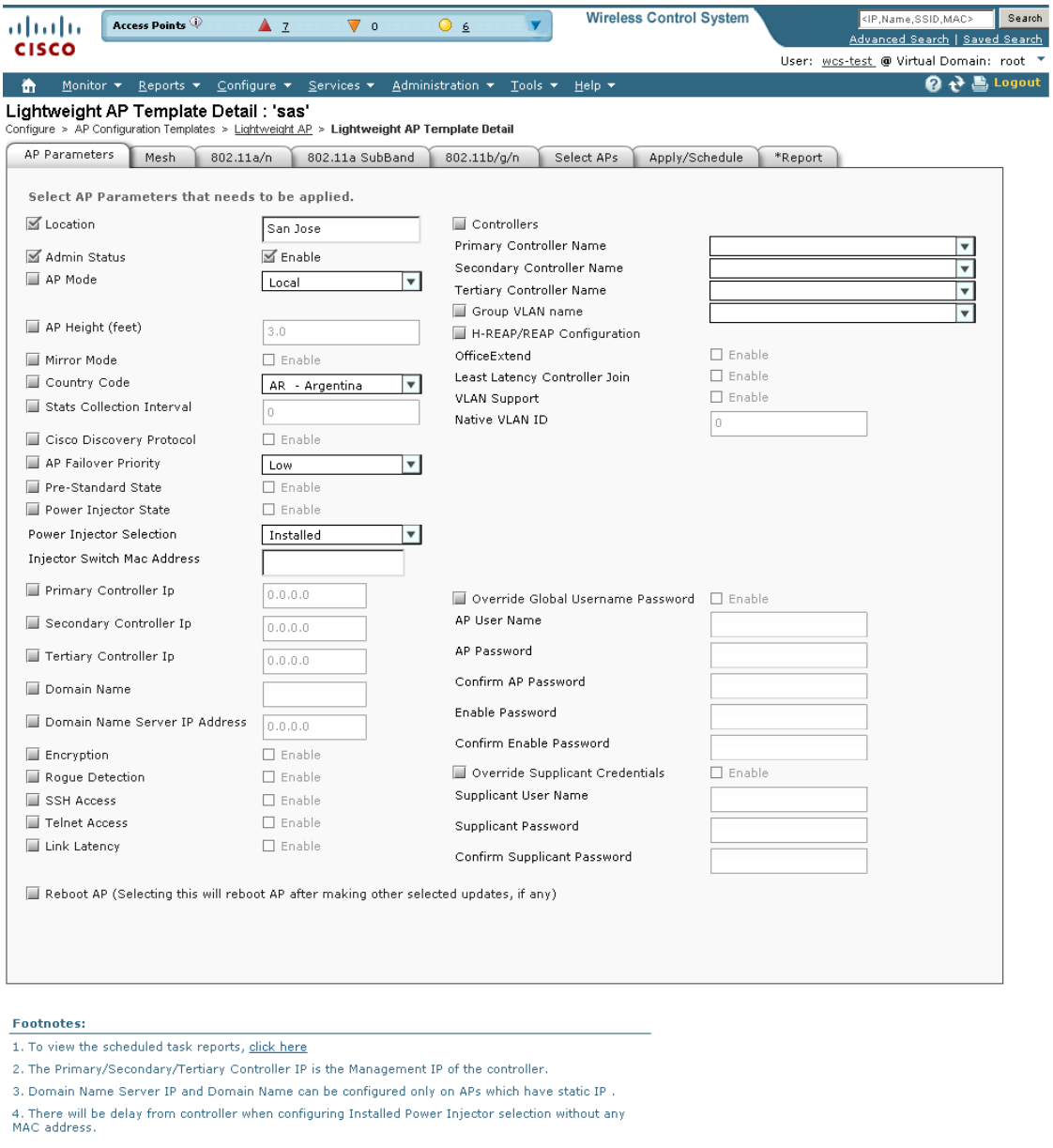

The last parameter under Inventory Information indicates whether this access point can be configured for hybrid REAP. Only the 1130AG and 1240AG access points support hybrid REAP.

**Step 4** Verify that the AP Mode parameter displays *H-REAP*. If it does not, continue to Step 5. If H-REAP is showing as supported, skip to Step 9.

**Step 5** Choose **Configure > AP Configuration Templates > Lightweight AP** or **Autonomous AP**.

**Step 6** Choose which access point you want to configure for hybrid REAP by clicking one from the AP Name list. The AP Template Detail page appears (see Figure 15-4).

*Figure 15-4 AP/Radio Template Page*




**Step 7** Click to select the H-REAP/REAP Config check box. Enabling this configuration allows you to view all profile mappings.

**Note** If you are changing the mode to H-REAP/REAP and if the access point is not already in H-REAP/REAP mode, all other H-REAP/REAP parameters will not be applied on the access point.

**Step 8** Select the **VLAN Support** check box and enter the number of the native VLAN on the remote network (such as 100) in the **Native VLAN ID** text box.

**Note** By default, a VLAN is not enabled on the hybrid-REAP access point. When hybrid REAP is enabled, the access point inherits the VLAN ID associated to the WLAN. This configuration is saved in the access point and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per hybrid-REAP access point in a VLAN-enabled domain. Otherwise, the access point cannot send and receive packets to and from the controller. When the client is assigned a VLAN from the RADIUS server, that VLAN is associated to the locally switched WLAN.

**Step 9** Click the **Apply/Schedule** tab to save your changes.

**Step 10** The Locally Switched VLANs section shows which WLANs are locally switched and provides their VLAN identifier. Click the **Edit** link to change the number of VLANs from which a client IP address is obtained. You are then redirected to a page where you can save the VLAN identifier changes.

**Step 11** Click **Save** to save your changes.

**Step 12** Repeat this procedure for any additional access points that need to be configured for hybrid REAP at the remote site.

## Connecting Client Devices to the WLANs

Follow the instructions for your client device to create profiles that connect to the WLANs you created in the "Configuring the Controller for Hybrid REAP" section on page 15-5.

In our example, you would create three profiles on the client:

1. To connect to the "employee" WLAN, you would create a client profile that uses WPA/WPA2 with PEAP-MSCHAPV2 authentication. When the client becomes authenticated, it gets an IP address from the management VLAN of the controller.
2. To connect to the "local-employee" WLAN, you would create a client profile that uses WPA/WPA2 authentication. When the client becomes authenticated, it gets an IP address from VLAN 101 on the local switch.
3. To connect to the "guest-central" WLAN, you would create a profile that uses open authentication. When the client becomes authenticated, it gets an IP address from VLAN 101 on the network local to the access point. After the client connects, the local user types any HTTP address in the web browser. The user is automatically directed to the controller to complete the web-authentication process. When the web login page appears, the user enters his or her username and password.

To see if a client's data traffic is being locally or centrally switched, click **Monitor > Devices > Clients.**

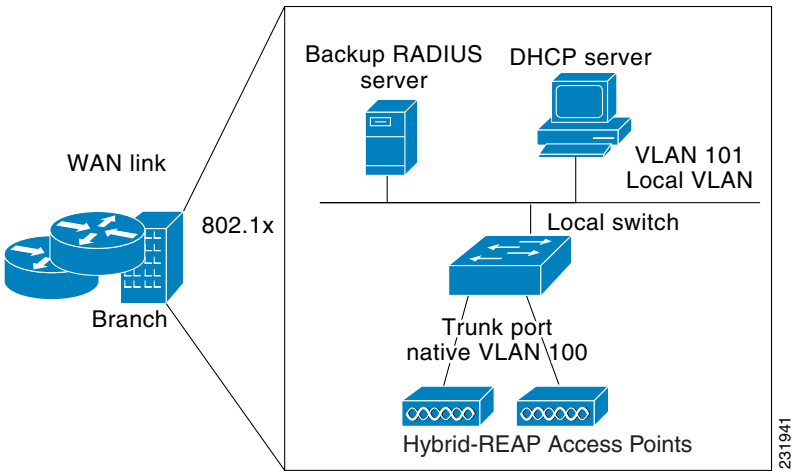
# Hybrid REAP Access Point Groups

Hybrid REAP enables you to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. There is no deployment restriction on the number of hybrid-REAP access points per location, but you can organize and group the access points per floor and limit them per building, since it is likely the branch offices share the same configuration.

By forming access point groups with similar configurations, a procedure such as CCKM fast roaming can be processed more quickly than going through the controller individually. For example, to activate CCKM fast roaming, the HREAP access points must know the CCKM cache for all clients that could associate. If you have a controller with 300 access points and 1000 clients that can potentially connect, it is quicker and more practical to process and send the CCKM cache for the HREAP group rather than for all 1000 clients. One particular HREAP group could focus on a branch office with a small number of access points so that clients in the branch office could only connect to and roam between those few access points. With the established group, features such as CCKM cache and backup RADIUS are configured for the entire HREAP group rather than being configured in each access point.

All of the hybrid-REAP access points in a group share the same WLAN, backup RADIUS server, CCKM, and local authentication configuration information. This feature is helpful if you have multiple hybrid-REAP access points in a remote office or on the floor of a building and you want to configure them all at once. For example, you can configure a backup RADIUS server for a hybrid-REAP group rather than having to configure the same server on each access point. Figure 15-5 illustrates a typical hybrid-REAP group deployment with a backup RADIUS server in the branch office.

*Figure 15-5 Hybrid-REAP Group Deployment*




# Hybrid-REAP Groups and Backup RADIUS Servers

You can configure the controller to allow a hybrid-REAP access point in standalone mode to perform full 802.1x authentication to a backup RADIUS server. You can configure a primary RADIUS server or both a primary and secondary RADIUS server.

# Hybrid-REAP Groups and CCKM

Hybrid-REAP groups are required for CCKM fast roaming to work with hybrid-REAP access points. CCKM fast roaming is achieved by caching a derivative of the master key from a full EAP authentication so that a simple and secure key exchange can occur when a wireless client roams to a different access point. This feature prevents the need to perform a full RADIUS EAP authentication as the client roams from one access point to another. The hybrid-REAP access points need to obtain the CCKM cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller. If, for example, you have a controller with 300 access points and 100 clients that

might associate, sending the CCKM cache for all 100 clients is not practical. If you create a hybrid-REAP group comprising a limited number of access points (for example, you create a group for four access points in a remote office), the clients roam only among those four access points, and the CCKM cache is distributed among those four access points only when the clients associate to one of them.

**Note** CCKM fast roaming among hybrid-REAP and non-bybrid-REAP access points is not supported.

# Hybrid-REAP Groups and Local Authentication

You can configure the controller to allow a hybrid-REAP access point in standalone mode to perform LEAP or EAP-FAST authentication for up to 20 statically configured users. The controller sends the static list of usernames and passwords to each hybrid-REAP access point when it joins the controller. Each access point in the group authenticates only its own associated clients.

This feature is ideal for customers who are migrating from an autonomous access point network to an lightweight hybrid-REAP access point network and are not interested in maintaining a large user database nor adding another hardware device to replace the RADIUS server functionality available in the autonomous access point.

**Note** This feature can be used in conjunction with the hybrid-REAP backup RADIUS server feature. If a hybrid-REAP group is configured with both a backup RADIUS server and local authentication, the hybrid-REAP access point always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally the hybrid-REAP access point itself (if the primary and secondary are not reachable).

# Configuring Hybrid-REAP Groups

Follow these steps to configure HREAP groups. If you want to apply an H-REAP template to multiple controllers, refer to the template instructions in the "Configuring H-REAP AP Groups" section on page 12-34.

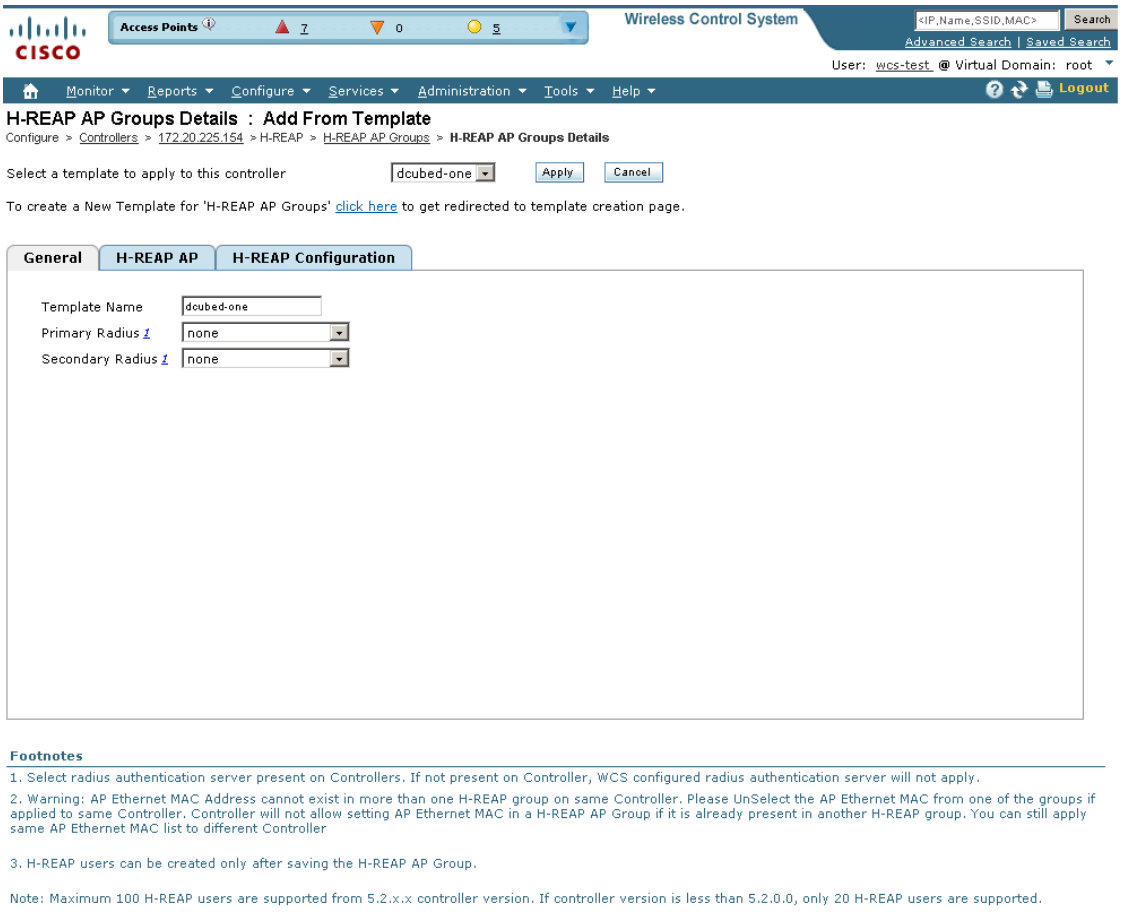
**Step 1** Choose **Configure > Controllers**.

**Step 2** Choose a specific controller by clicking on the desired IP address.

**Step 3** From the left sidebar menu choose **H-REAP > H-REAP AP Groups**. The established HREAP AP groups appear.

**Step 4** The Group Name column shows the group names assigned to the HREAP access point groups. If you want to add an additional group, choose **Add H-REAP AP Group** from the Select a command drop-down list.
- or -
To make modifications to an existing template, click a template in the Template Name column. The General tab of the H-REAP AP Groups template appears (see Figure 15-6).

*Figure 15-6 H-REAP AP Groups*




**Note** To delete a group name, click the group name you want to remove and choose **Delete H-REAP AP Group** from the Select a command drop-down list.

The Template Name parameter shows the group name assigned to the H-REAP access point group.

**Step 5** Choose the primary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, the WCS configured RADIUS server does not apply.

**Note** You must configure the RADIUS server configuration on the controller before you apply H-REAP RADIUS server configuration from WCS.

**Step 6** Choose the secondary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, the WCS configured RADIUS server does not apply.

**Step 7** If you want to add an access point to the group, click the **H-REAP AP** tab.

**Step 8** An access point Ethernet MAC address cannot exist in more than one H-REAP group on the same controller. If more than one group is applied to the same controller, click the **Ethernet MAC** check box to unselect an access point from one of the groups. You should save this change or apply it to controllers.

**Step 9** If you want to enable local authentication for a hybrid-REAP group, click the **H-REAP Configuration** tab. The H-REAP Configuration tab appears.

**Note** Make sure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to **None** on the General tab.

**Step 10** Select the **H-REAP Local Authentication** check box to enable local authentication for this hybrid-REAP group. The default value is unselected.

**Note** When you attempt to use this feature, a warning message indicates that it is a licensed feature.

**Step 11** To allow a hybrid-REAP access point to authenticate clients using LEAP, select the **LEAP** check box. Otherwise, to allow a hybrid-REAP access point to authenticate clients using EAP-FAST, select the **EAP-FAST** check box.

**Step 12** Perform one of the following, depending on how you want protected access credentials (PACs) to be provisioned:

- To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the EAP-FAST Key text box. The key must be 32 hexadecimal characters.
- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the **Auto Key Generation** check box.

**Step 13** In the EAP-FAST Authority ID text box, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

**Step 14** In the EAP-FAST Authority Info text box, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.

**Step 15** In the EAP-FAST Pac Timeout text box, specify a PAC timeout value by entering the number of seconds for the PAC to remain viable in the edit box. The valid range is 2 to 4095 seconds.

**Note** To verify that an individual access point belongs to a hybrid-REAP group, click the **Users configured in the group** link. It advances you to the H-REAP AP Group screen which shows the names of the groups and the access points that belong in it.

# Auditing an H-REAP Group

If the H-REAP configuration changes over a period of time either on WCS or the controller, you can audit the configuration. The changes are visible on subsequent screens. You can choose to synchronize the configuration by refreshing WCS or the controller.