CHAPTER 12

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 two or three 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.

Note In release 4.0.206.0 and greater, Hybrid REAP can be used with up to eight access points.

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 and 1240AG 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. Figure 12-1 illustrates a typical hybrid-REAP deployment.

Figure 12-1 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 and configuration from the controller, 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 can discover a controller through the regular LWAPP 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 LWAPP 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 LWAPP 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.

Note Refer to Chapter 7 or the *Deploying Cisco 440X Series Wireless LAN Controllers* at this URL for more information on how access points find controllers:
http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html

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. Refer to 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 is tunneled 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 for central switching) or the “authentication down, local switching” state (if the WLAN was configured for local switching).

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 mode.

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. Once a client is assigned to a quarantined VLAN, all of its data packets are centrally switched. See the "Configuring Dynamic Interfaces" section on page 3-15 for information on creating quarantined VLANs.

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 up to four fragmented packets or a minimum 500-byte maximum transmission unit (MTU) WAN link.
- Roundtrip latency must not exceed 100 milliseconds (ms) between the access point and the controller, and LWAPP 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 can receive 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, 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

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 Refer to 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 in created in the local switch for both VLANs in the switch. The first DHCP pool (NATIVE) will be used by the hybrid-REAP access point, and the second DHCP pool (LOCAL-SWITCH) will be 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.

Sample local switch configuration:

```
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 using either the GUI or the CLI.

Using the GUI to Configure the Controller for Hybrid REAP

The controller configuration for hybrid REAP consists of creating centrally switched and locally switched WLANs. Follow the steps in this section to use the GUI to configure the controller for these WLANs. 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 (locally switched VLAN)
guest-central	Web authentication	Central	management (centrally switched VLAN)

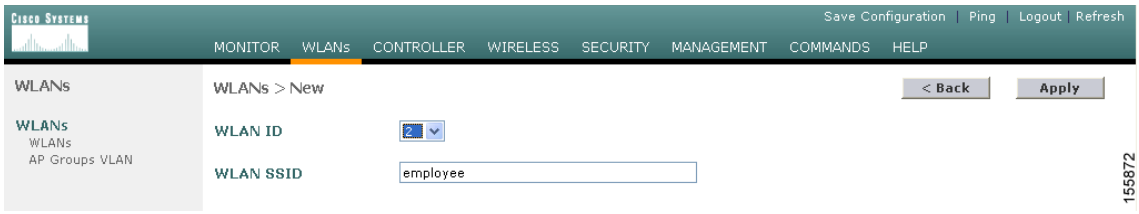
Note See the "Using the CLI to Configure the Controller for Hybrid REAP" section on page 12-12 if you would prefer to configure the controller for hybrid REAP using the CLI.

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

a. Click **WLANs** to access the WLANs page.

b. Click **Next** to access the WLANs > New page (see Figure 12-2).

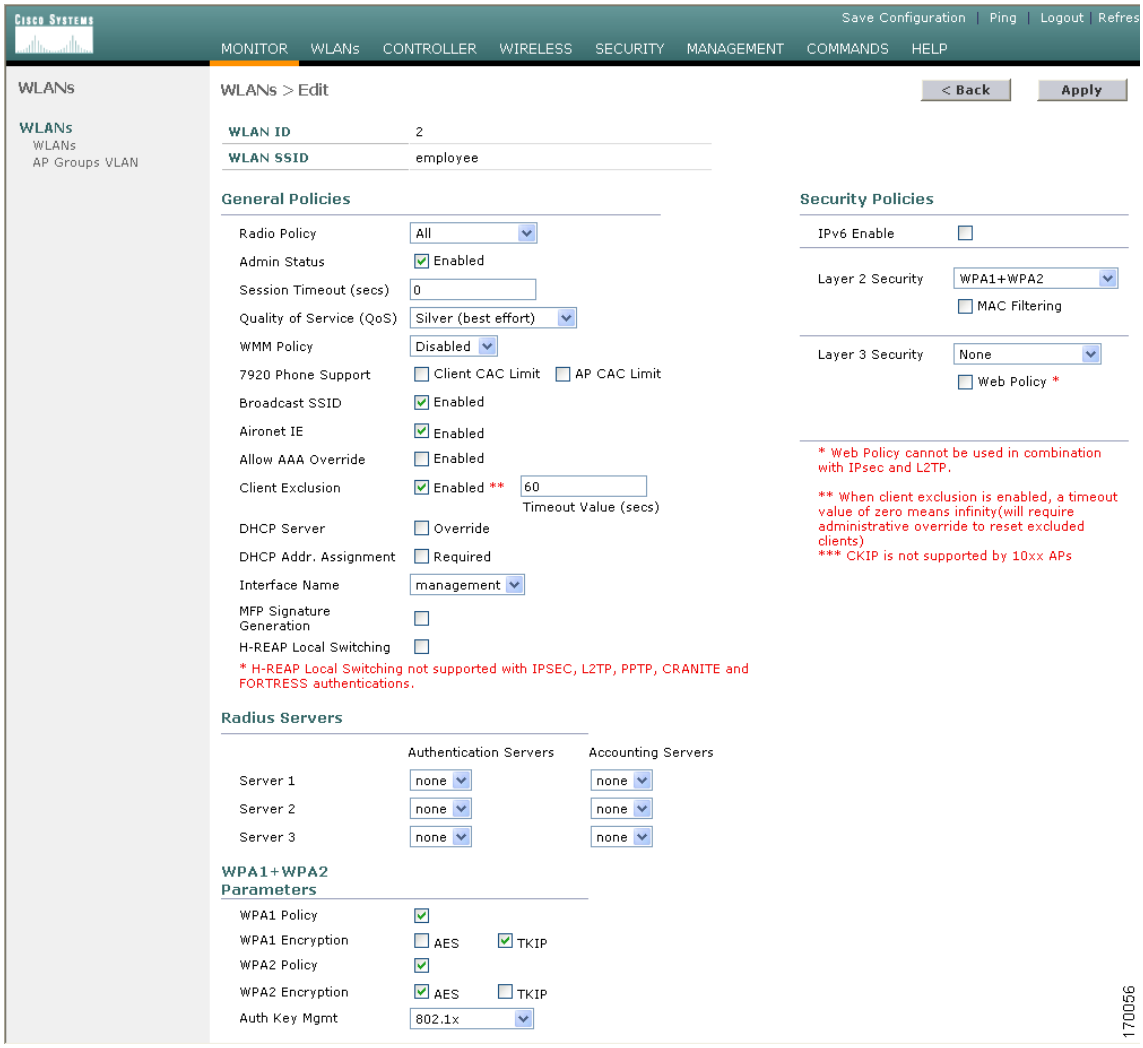
Figure 12-2 WLANs > New Page



c. Enter a name for the WLAN in the WLAN SSID field.

d. Click **Apply** to commit your changes. The WLANs > Edit page appears (see Figure 12-3).

Figure 12-3 WLANs > Edit Page (Centrally Switched WLAN)



e. Modify the configuration parameters for this WLAN using the settings in Figure 12-3 as a reference. In our employee WLAN example, you would need to choose **WPA1+WPA2** from the Layer 2 Security drop-down box and then set the WPA1+WPA2 parameters at the bottom of the page.

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

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

f. Click **Apply** to commit your changes.

g. Click **Save Configuration** to save your changes.

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

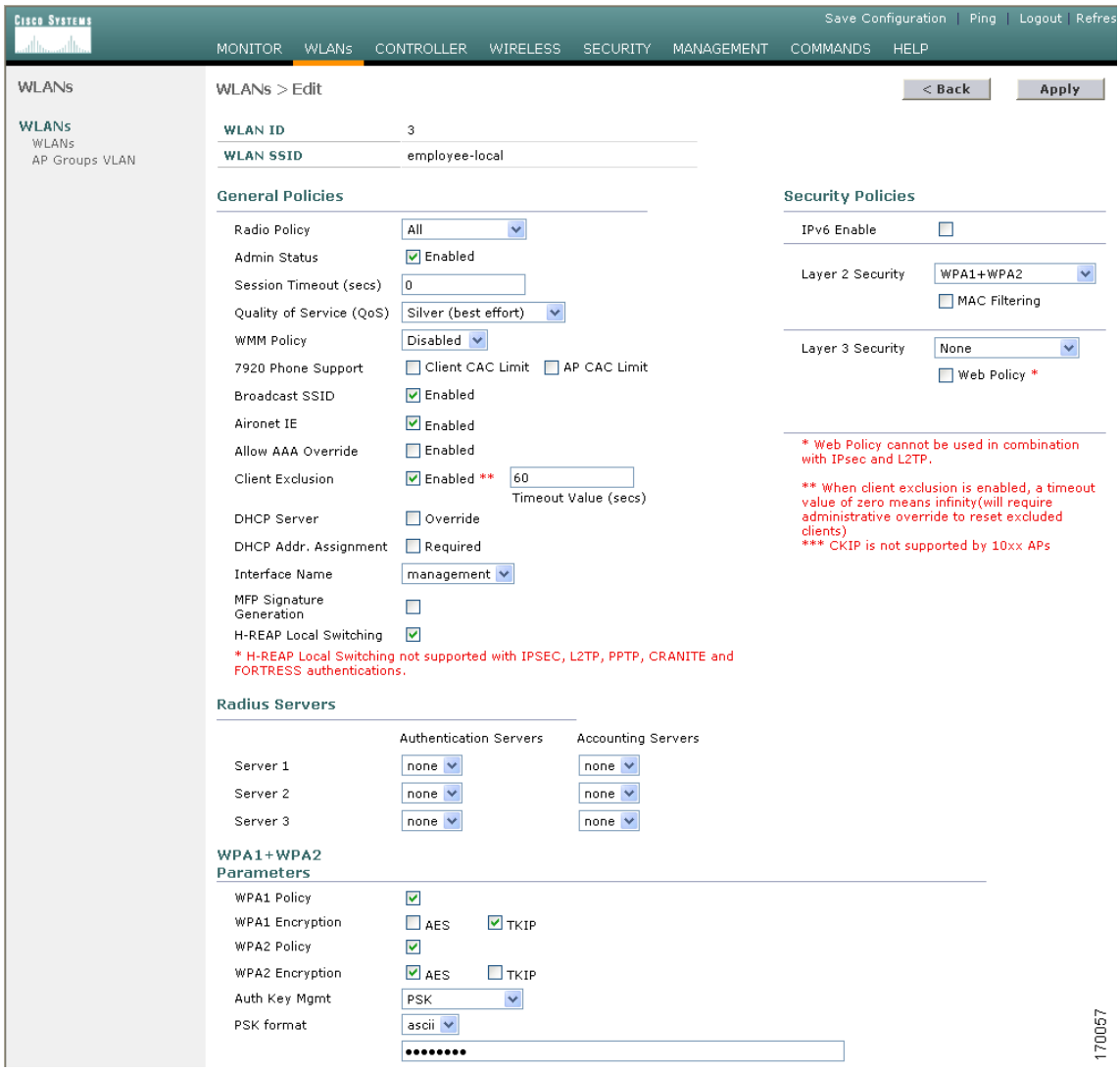
a. Follow the substeps in Step 1 to create a new WLAN. In our example, this WLAN is named "employee-local."

b. When the WLANs > Edit page appears, modify the configuration parameters for this WLAN using the settings in Figure 12-4 as a reference. In our employee WLAN example, you would need to choose **WPA1+WPA2** from the Layer 2 Security drop-down box and then set the WPA1+WPA2 parameters at the bottom of the page. Make sure to choose PSK authentication key management and enter a pre-shared key.

Note Be sure to enable this WLAN by checking the **Admin Status** check box under General Policies. Also, be sure to enable local switching by checking the **H-REAP Local Switching** check box. When you enable local switching, any hybrid-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, 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.

Figure 12-4 WLANs > Edit Page (Locally Switched WLAN)



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

d. Click **Save Configuration** to save 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.

Note Chapter 9 provides additional information on creating guest user accounts.

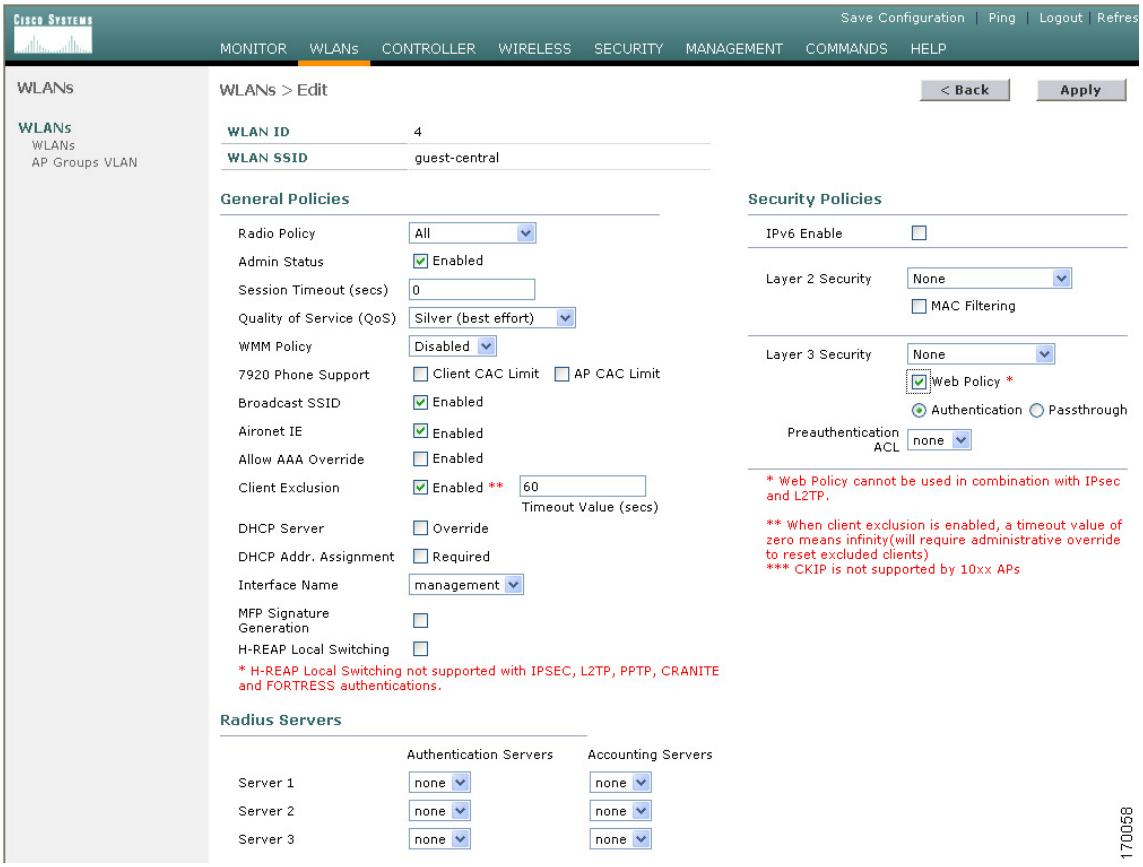
a. Follow the substeps in Step 1 to create a new WLAN. In our example, this WLAN is named "guest-central."

b. When the WLANs > Edit page appears, modify the configuration parameters for this WLAN using the settings in Figure 12-5 as a reference. In our employee WLAN example, you would need to choose **None** from both the Layer 2 Security and Layer 3 Security drop-down boxes, check 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 under Security Policies > Web Policy. See Chapter 5 for more information on ACLs.

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

Figure 12-5 WLANs > Edit Page (Centrally Switched Guest Access WLAN)



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

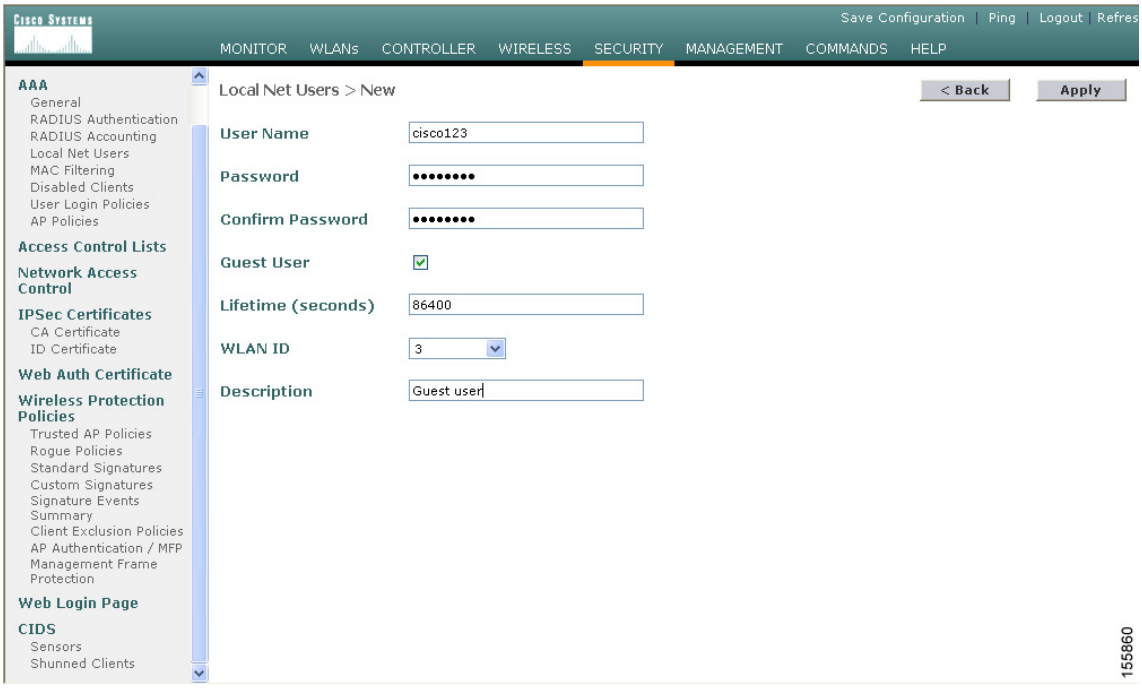
d. Click **Save Configuration** to save your changes.

e. If you want to customize the content and appearance of the login page that guest users will see the first time they access this WLAN, follow the instructions in Chapter 5.

f. To add a local user to this WLAN, click **Security** and then click **Local Net Users** under AAA.

g. When the Local Net Users page appears, click **New**. The Local Net Users > New page appears (see Figure 12-6).

Figure 12-6 Local Net Users > New Page



h. In the User Name and Password fields, enter a username and password for the local user.

i. In the Confirm Password field, re-enter the password.

j. Check the **Guest User** check box to enable this local user account.

k. In the Lifetime field, enter the amount of time (in seconds) for this user account to remain active.

l. In the WLAN ID field, enter the number of the WLAN that will be accessed by the local user.

m. In the Description field, enter a descriptive title for the local user (such as “Guest user”).

n. Click **Apply** to commit your changes.

o. Click **Save Configuration** to save your changes.

Step 4 Go to the “Configuring an Access Point for Hybrid REAP” section on page 12-12 to configure two or three access points for hybrid REAP.

Using the CLI to Configure the Controller for Hybrid REAP

Use these commands to configure the controller for hybrid REAP:

- **config wlan h-reap local-switch** *wlan-id* **enable**—Configures the WLAN for local switching.
- **config wlan h-reap local-switch** *wlan-id* **disable**—Configures the WLAN for central switching. This is the default value.

Note Go to the "Configuring an Access Point for Hybrid REAP" section on page 12-12 to configure two or three access points for hybrid REAP.

Use these commands to obtain hybrid-REAP information:

- **show ap config general** *Cisco_AP*—Shows VLAN configurations.
- **show wlan wlan_id**—Shows whether the WLAN is locally or centrally switched.
- **show client detail** *client_mac*—Shows whether the client is locally or centrally switched.

Use these commands to obtain debug information:

- **debug lwapp events enable**—Provides debug information on LWAPP events.
- **debug lwapp error enable**—Provides debug information on LWAPP errors.
- **debug pem state enable**—Provides debug information on the policy manager State Machine.
- **debug pem events enable**—Provides debug information on policy manager events.
- **debug dhcp packet enable**—Provides debug information on DHCP packets.
- **debug dhcp message enable**—Provides debug information on DHCP error messages.

Configuring an Access Point for Hybrid REAP

This section provides instructions for configuring an access point for hybrid REAP using either the controller GUI or CLI.

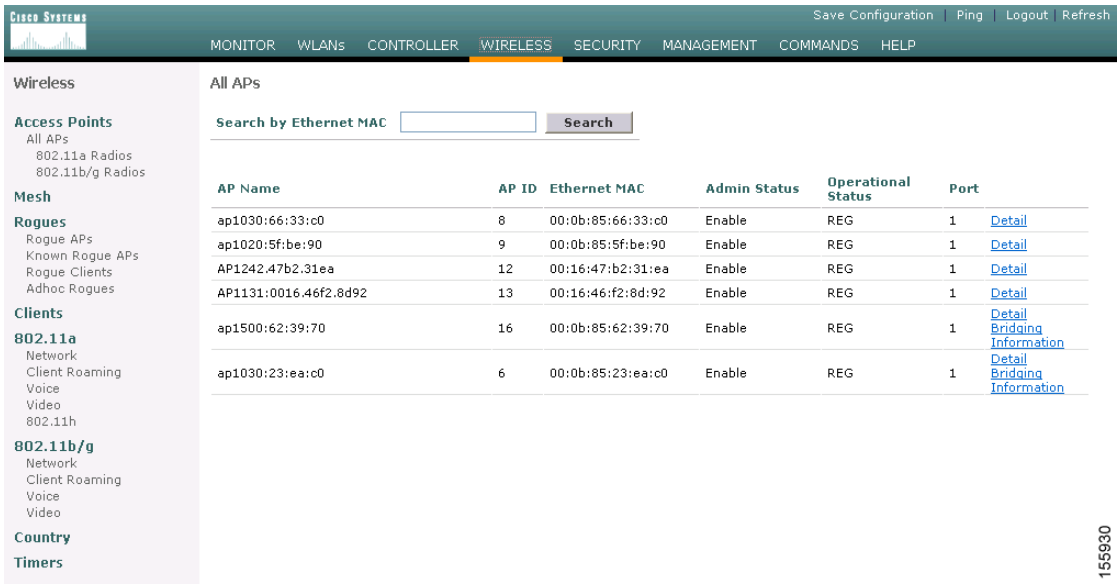
Using the GUI to Configure an Access Point for Hybrid REAP

Follow these steps to configure an access point for hybrid REAP using the controller GUI.

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

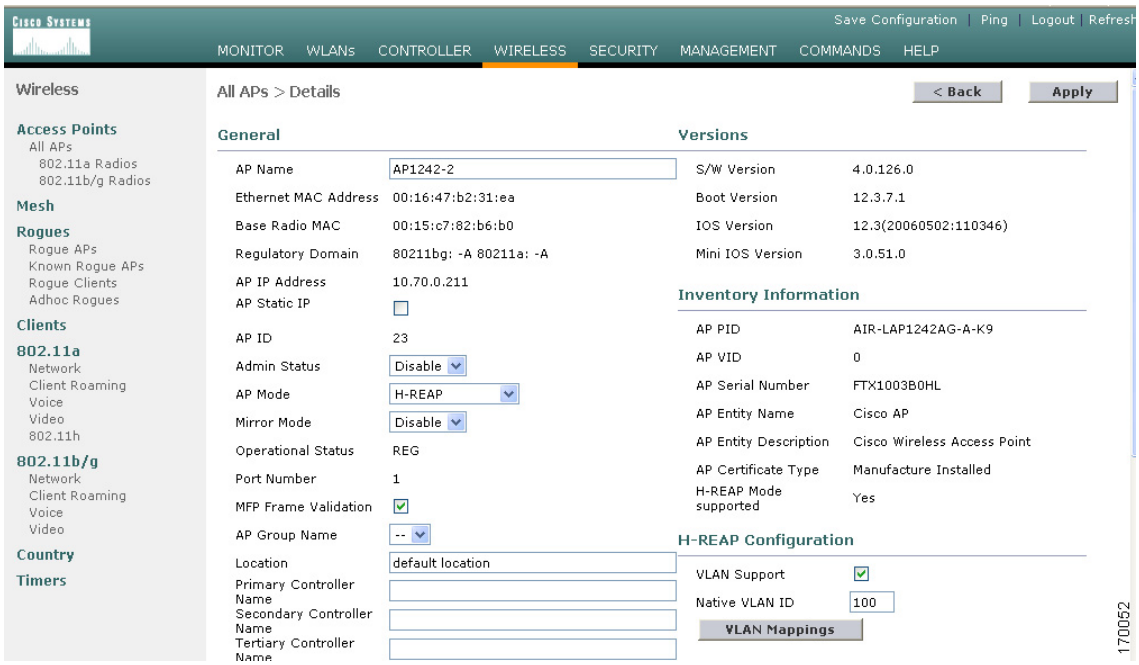
Step 2 Click **Wireless** to access the All APs page (see Figure 12-7).

Figure 12-7 All APs Page



Step 3 Click the **Details** link of the desired access point. The All APs > Details page appears (see Figure 12-8).

Figure 12-8 All APs > Details 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 Choose **H-REAP** from the AP Mode drop-down box to enable hybrid REAP for this access point.

Step 5 Click **Apply** to commit your changes and to cause the access point to reboot.

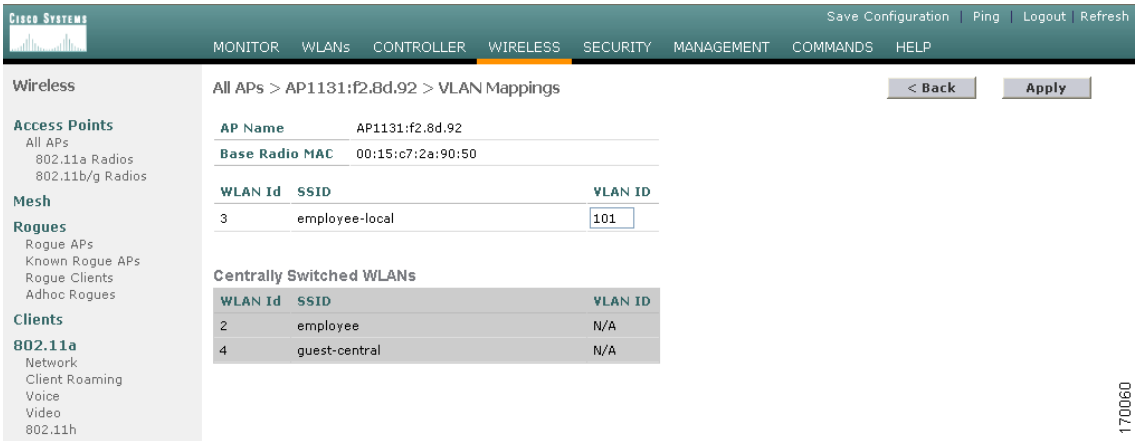
Step 6 Under H-REAP Configuration, check the **VLAN Support** check box and enter the number of the native VLAN on the remote network (such as 100) in the **Native VLAN ID** field.

Note By default, a VLAN is not enabled on the hybrid-REAP access point. Once 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.

Step 7 Click **Apply** to commit your changes. The access point temporarily loses its connection to the controller while its Ethernet port is reset.

Step 8 Click **VLAN Mappings** to access the VLAN Mappings page (see Figure 12-9).

Figure 12-9 VLAN Mappings Page



Step 9 Enter the number of the VLAN from which the clients will get an IP address when doing local switching (VLAN 101, in this example) in the VLAN ID field.

Step 10 Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** 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.

Using the CLI to Configure an Access Point for Hybrid REAP

Use these commands on the controller to configure an access point for hybrid REAP:

- **config ap mode h-reap** *Cisco_AP***—**Enables hybrid REAP for this access point.
- **config ap h-reap vlan wlan** *wlan_id vlan-id Cisco_AP***—**Enables you to assign a VLAN ID to this hybrid-REAP access point. By default, the access point inherits the VLAN ID associated to the WLAN.
- **config ap h-reap vlan** {**enable** | **disable**} *Cisco_AP*—Enables or disables VLAN tagging for this hybrid-REAP access point. By default, VLAN tagging is not enabled. Once VLAN tagging is enabled on the hybrid-REAP access point, WLANs enabled for local switching inherit the VLAN assigned at the controller.
- **config ap h-reap vlan native** *vlan-id Cisco_AP*—Enables you to configure a native VLAN for this hybrid-REAP access point. By default, no VLAN is set as the native VLAN. One native VLAN must be configured per hybrid-REAP access point (when VLAN tagging is enabled). Make sure the switchport to which the access point is connected has a corresponding native VLAN configured as well. If the hybrid-REAP access point's native VLAN setting and the upstream switchport native VLAN do not match, the access point cannot transmit packets to and from the controller.

Use these commands on the hybrid-REAP access point to obtain status information:

- **show lwapp reap status**—Shows the status of the hybrid-REAP access point (connected or standalone).
- **show lwapp reap association**—Shows the list of clients associated to this access point and their SSIDs.

Use these commands on the hybrid-REAP access point to obtain debug information:

- **debug lwapp reap**—Shows general hybrid-REAP activities.
- **debug lwapp reap mgmt**—Shows client authentication and association messages.
- **debug lwapp reap load**—Shows payload activities, which is useful when the hybrid-REAP access point boots up in standalone mode.
- **debug dot11 mgmt interface**—Shows 802.11 management interface events.
- **debug dot11 mgmt msg**—Shows 802.11 management messages.
- **debug dot11 mgmt ssid**—Shows SSID management events.
- **debug dot11 mgmt state-machine**—Shows the 802.11 state machine.
- **debug dot11 mgmt station**—Shows client events.

Connecting Client Devices to the WLANs

Follow the instructions for your client device to create profiles to connect to the WLANs you created in the "Configuring the Controller for Hybrid REAP" section on page 12-6.

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. Once the client becomes authenticated, it should get 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-PSK authentication. Once the client becomes authenticated, it should get an IP address from VLAN 101 on the local switch.
3. To connect to the "guest-central" WLAN, you would create a client profile that uses open authentication. Once the client becomes authenticated, it should get an IP address from VLAN 101 on the network local to the access point. Once the client connects, the local user can type 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 > Clients** on the controller GUI, click the **Detail** link for the desired client, and look at the Data Switching parameter under AP Properties.