Configuring WLANs

This chapter describes how to configure up to 512 WLANs for your Cisco UWN Solution. It contains these sections:

WLAN Overview

The Cisco UWN solution can control up to 512 WLANs for lightweight access points. Each WLAN has a separate WLAN ID (1 through 512), a separate profile name, and a WLAN SSID and can be assigned unique security policies. All controllers publish up to 16 WLANs to each connected access point, but you can create up to 512 WLANs and then selectively publish these WLANs (using access point groups) to different access points to better manage your wireless network.

Note Cisco 2106, 2112, and 2125 controllers support only up to 16 WLANs.

Note All OfficeExtend access points should be in the same access point group, and that group should contain no more than 15 WLANs. A controller with OfficeExtend access points in an access point group publishes only up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID.

You can associate up to 16 WLANs with each access point group and assign specific access points to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point does not advertise disabled WLANs in its access point group or WLANs that belong to another group. Refer to the "Creating Access Point Groups" section on page 6-54 for more information on access point groups.

Note Controller software releases prior to 5.2 support up to only 16 WLANs. Cisco does not support downgrading the controller from software release 5.2 or later to a previous release as inconsistencies might occur for WLANs and wired guest LANs. As a result, you would need to reconfigure your WLAN, mobility anchor, and wired LAN configurations.

Note Cisco recommends that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers properly route VLAN traffic.

Configuring WLANs

These sections describe how to configure WLANs:

- Creating WLANs, page 6-3
- Searching WLANs, page 6-8
- Configuring DHCP, page 6-9
- Configuring MAC Filtering for WLANs, page 6-16
- Assigning WLANs to Interfaces, page 6-17
- Configuring the DTIM Period, page 6-18
- Configuring Peer-to-Peer Blocking, page 6-20
- Configuring Layer 2 Security, page 6-23
- Configuring a Session Timeout, page 6-31

Creating WLANs

This section provides instructions for creating up to 512 WLANs using either the controller GUI or CLI.

Note Each AP can broadcast only up to 16 WLANs.

WLANs with ID that is higher than 16 are not applied to the default AP group, regardless of the number of WLANs configured. For WLANs with ID that is higher than 16, you need to configure a separate AP group.

You can configure WLANs with different service set identifiers (SSIDs) or with the same SSID. An SSID identifies the specific wireless network that you want the controller to access. Creating WLANs with the same SSID enables you to assign different Layer 2 security policies within the same wireless LAN. To distinguish among WLANs with the same SSID, you must create a unique profile name for each WLAN.

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in beacon and probe responses. These are the available Layer 2 security policies:

- None (open WLAN)
- Static WEP or 802.1X

  Note Because static WEP and 802.1X are both advertised by the same bit in beacon and probe responses, they cannot be differentiated by clients. Therefore, they cannot both be used by multiple WLANs with the same SSID.

- CKIP
- WPA/WPA2

Note Although WPA and WPA2 cannot both be used by multiple WLANs with the same SSID, two WLANs with the same SSID could be configured with WPA/TKIP with PSK and WPA/TKIP with 802.1X, respectively, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X, respectively.

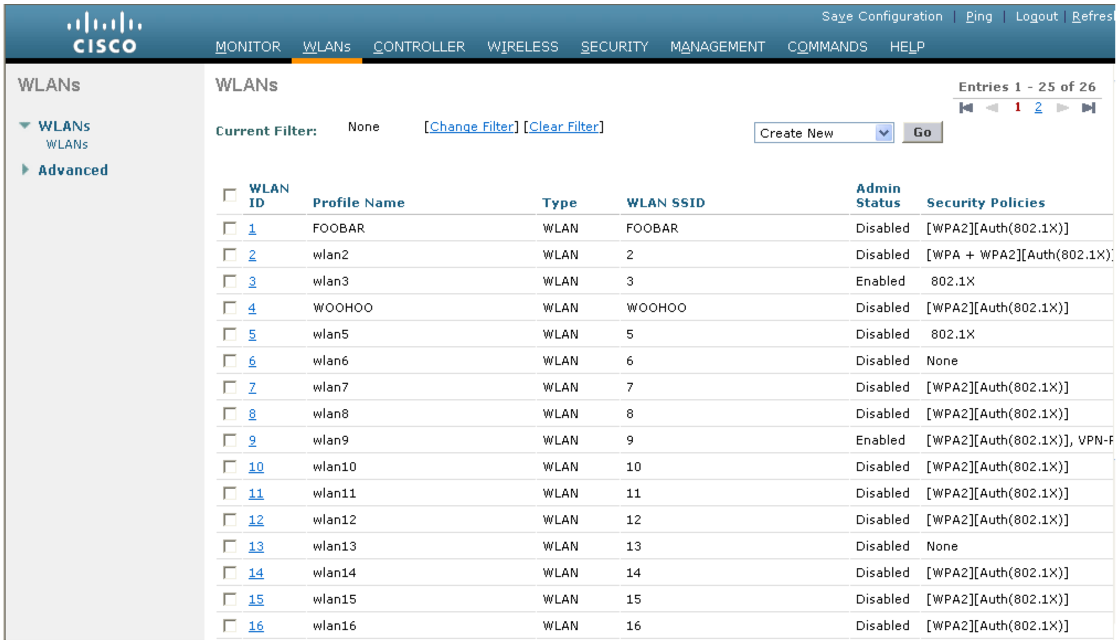
Note If a WLAN is configured to an 802.11g only radio policy and a LAP is configured to channel 14, then the WLAN clients try to associate with the LAP, which does not work as expected because of the 802.11g only policy. The workaround to the problem is one of the following:
- Disable channel 14 manually when 802.11g only policy is configured in WLANs.
- Do not select 802.11g only policy when channel 14 is configured to a LAP.

Using the GUI to Create WLANs

Follow these steps to create WLANs using the GUI.

Step 1 Choose **WLANs** to open the WLANs page (see Figure 6-1).

Figure 6-1 WLANs Page



WLANs

Entries 1 - 25 of 26

1 2

Current Filter: None [Change Filter] [Clear Filter]

□	WLAN ID	Profile Name	Type	WLAN SSID	Admin Status	Security Policies
□	1	FOOBAR	WLAN	FOOBAR	Disabled	[WPA2][Auth(802.1X)]
□	2	wlan2	WLAN	2	Disabled	[WPA + WPA2][Auth(802.1X)
□	3	wlan3	WLAN	3	Enabled	802.1X
□	4	WOOHOO	WLAN	WOOHOO	Disabled	[WPA2][Auth(802.1X)]
□	5	wlan5	WLAN	5	Disabled	802.1X
□	6	wlan6	WLAN	6	Disabled	None
□	7	wlan7	WLAN	7	Disabled	[WPA2][Auth(802.1X)]
□	8	wlan8	WLAN	8	Disabled	[WPA2][Auth(802.1X)]
□	9	wlan9	WLAN	9	Enabled	[WPA2][Auth(802.1X)], VPN-F
□	10	wlan10	WLAN	10	Disabled	[WPA2][Auth(802.1X)]
□	11	wlan11	WLAN	11	Disabled	[WPA2][Auth(802.1X)]
□	12	wlan12	WLAN	12	Disabled	[WPA2][Auth(802.1X)]
□	13	wlan13	WLAN	13	Disabled	None
□	14	wlan14	WLAN	14	Disabled	[WPA2][Auth(802.1X)]
□	15	wlan15	WLAN	15	Disabled	[WPA2][Auth(802.1X)]
□	16	wlan16	WLAN	16	Disabled	[WPA2][Auth(802.1X)]

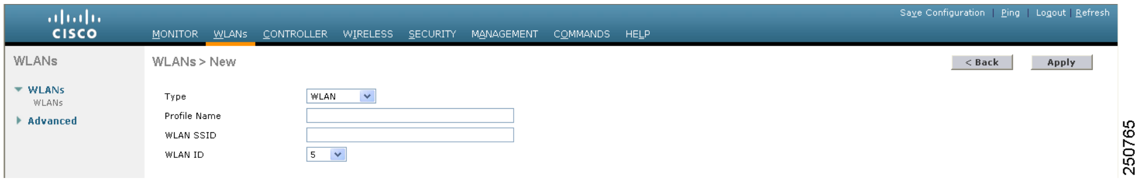
This page lists all of the WLANs currently configured on the controller. For each WLAN, you can see its WLAN ID, profile name, type, SSID, status, and security policies.

The total number of WLANs appears in the upper right-hand corner of the page. If the list of WLANs spans multiple pages, you can access these pages by clicking the page number links.

Note If you want to delete a WLAN, hover your cursor over the blue drop-down arrow for that WLAN and choose **Remove**, or check the check box to the left of the WLAN, choose **Remove Selected** from the drop-down box, and click **Go**. A message appears asking you to confirm your decision. If you proceed, the WLAN is removed from any access point group to which it is assigned and from the access point's radio.

Step 2 To create a new WLAN, choose **Create New** from the drop-down box and click **Go**. The WLANs > New page appears (see Figure 6-2).

Figure 6-2 WLANs > New Page



WLANs > New

Type: WLAN

Profile Name:

WLAN SSID:

WLAN ID: 5

Step 3 From the Type drop-down box, choose **WLAN** to create a WLAN.

Note If you want to create a guest LAN for wired guest users, choose **Guest LAN** and follow the instructions in the "Configuring Wired Guest Access" section on page 10-28.

Step 4 In the Profile Name field, enter up to 32 alphanumeric characters for the profile name to be assigned to this WLAN. The profile name must be unique.

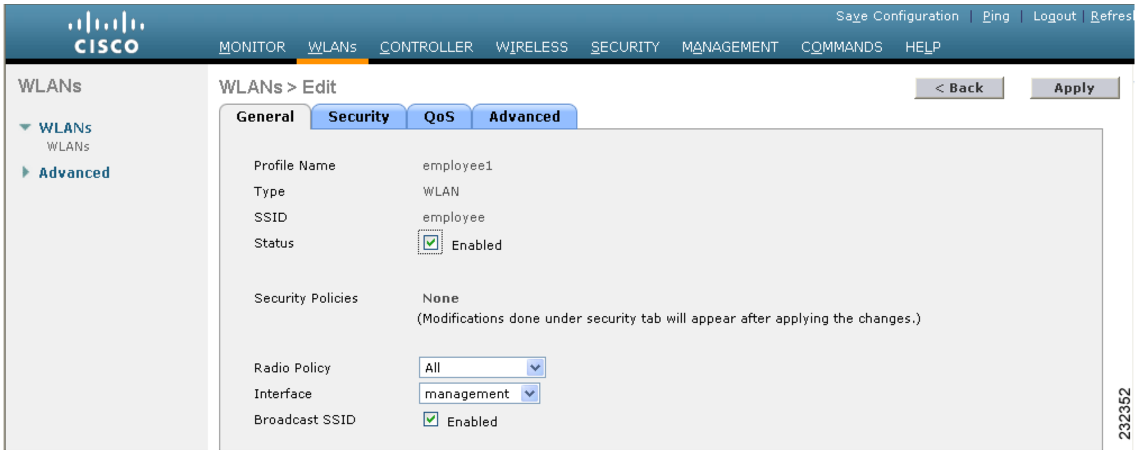
Step 5 In the WLAN SSID field, enter up to 32 alphanumeric characters for the SSID to be assigned to this WLAN.

Step 6 From the WLAN ID drop-down box, choose the ID number for this WLAN.

Step 7 Click **Apply** to commit your changes. The WLANs > Edit page appears (see Figure 6-3).

Note You can also open the WLANs > Edit page from the WLANs page by clicking the ID number of the WLAN that you want to edit.

Figure 6-3 WLANs > Edit Page



Profile Name employee1
Type WLAN
SSID employee
Status ☑ Enabled

Security Policies None
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All
Interface management
Broadcast SSID ☑ Enabled

Step 8 Use the parameters on the General, Security, QoS, and Advanced tabs to configure this WLAN. Refer to the sections in the rest of this chapter for instructions on configuring specific features for WLANs.

Step 9 On the General tab, check the **Status** check box to enable this WLAN. Be sure to leave it unchecked until you have finished making configuration changes to the WLAN.

Note You can also enable or disable WLANs from the WLANs page by checking the check boxes to the left of the WLANs that you want to enable or disable, choosing **Enable Selected** or **Disable Selected** from the drop-down box, and clicking **Go**.

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

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

Using the CLI to Create WLANs

Use these commands to create WLANs using the CLI.

1. To view the list of existing WLANs and to see whether they are enabled or disabled, enter this command:

   show wlan summary

2. To create a new WLAN, enter this command:

   config wlan create *wlan_id* {*profile_name* | *foreign_ap*} *ssid*

   Note If you do not specify an *ssid*, the *profile_name* parameter is used for both the profile name and the SSID.

Note When WLAN 1 is created in the configuration wizard, it is created in enabled mode. Disable it until you have finished configuring it. When you create a new WLAN using the **config wlan create** command, it is created in disabled mode. Leave it disabled until you have finished configuring it.

Note If you want to create a guest LAN for wired guest users, follow the instructions in the "Configuring Wired Guest Access" section on page 10-28.

3. To disable a WLAN (for example, before making any modifications to a WLAN), enter this command:

   config wlan disable {*wlan_id* | *foreign_ap* | **all**}

   where

   - *wlan_id* is a WLAN ID between 1 and 512,
   - *foreign_ap* is a third-party access point, and
   - **all** is all WLANs.

   Note If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.

4. To enable a WLAN (for example, after you have finished making configuration changes to the WLAN), enter this command:

   config wlan enable {*wlan_id* | *foreign_ap* | **all**}

   Note If the command fails, an error message appears (for example, "Request failed for wlan 10 - Static WEP key size does not match 802.1X WEP key size").

5. To delete a WLAN, enter this command:

   config wlan delete {*wlan_id* | *foreign_ap*}

   Note An error message appears if you try to delete a WLAN that is assigned to an access point group. If you proceed, the WLAN is removed from the access point group and from the access point's radio.

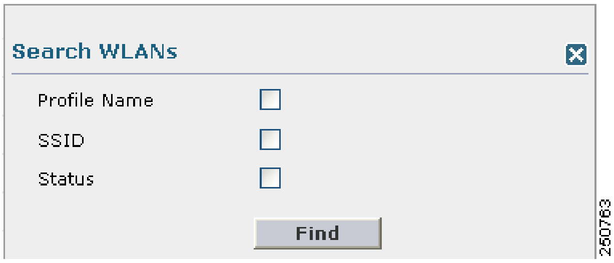
Searching WLANs

You can search for specific WLANs in the list of up to 512 WLANs on the WLANs page. This feature is especially useful if your WLANs span multiple pages, preventing you from viewing them all at once.

Follow these steps to search for WLANs using the controller GUI.

Step 1 On the WLANs page, click **Change Filter**. The Search WLANs window appears (see Figure 6-4).

Figure 6-4 Search WLANs Window



Step 2 Perform one of the following:

- To search for WLANs based on profile name, check the **Profile Name** check box and enter the desired profile name in the edit box.
- To search for WLANs based on SSID, check the **SSID** check box and enter the desired SSID in the edit box.
- To search for WLANs based on their status, check the **Status** check box and choose **Enabled** or **Disabled** from the drop-down box.
- To close the Search WLANs window without making any changes, click the **X** in the upper right-hand corner.

Step 3 Click **Find**. Only the WLANs that match your search criteria appear on the WLANs page, and the Current Filter field at the top of the page specifies the search criteria used to generate the list (for example, None, Profile Name:user1, SSID:test1, Status:disabled).

Note To clear any configured search criteria and display the entire list of WLANs, click **Clear Filter**.

Configuring DHCP

WLANs can be configured to use the same or different Dynamic Host Configuration Protocol (DHCP) servers or no DHCP server. Two types of DHCP servers are available: internal and external.

Internal DHCP Server

The controllers contain an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server. The wireless network generally contains 10 access points or fewer, with the access points on the same IP subnet as the controller. The internal server provides DHCP addresses to wireless clients, direct-connect access points, appliance-mode access points on the management interface, and DHCP requests that are relayed from access points. Only lightweight access points are supported. When you want to use the internal DHCP server, you must set the management interface IP address of the controller as the DHCP server IP address.

DHCP option 43 is not supported on the internal server. Therefore, the access point must use an alternative method to locate the management interface IP address of the controller, such as local subnet broadcast, DNS, priming, or over-the-air discovery.

Note Refer to Chapter 7, "Controlling Lightweight Access Points" or the *Controller Deployment Guide* at this URL for more information on how access points find controllers:

http://www.cisco.com/c/en/us/support/wireless/4400-series-wireless-lan-controllers/products-technical-reference-list.html

External DHCP Servers

The operating system is designed to appear as a DHCP Relay to the network and as a DHCP server to clients with industry-standard external DHCP servers that support DHCP Relay. This means that each controller appears as a DHCP Relay agent to the DHCP server. This also means that the controller appears as a DHCP server at the virtual IP Address to wireless clients.

Because the controller captures the client IP address obtained from a DHCP server, it maintains the same IP address for that client during intra-controller, inter-controller, and inter-subnet client roaming.

DHCP Assignment

You can configure DHCP on a per-interface or per-WLAN basis. The preferred method is to use the primary DHCP server address assigned to a particular interface.

Per-Interface Assignment

You can assign DHCP servers for individual interfaces. The management interface, AP-manager interface, and dynamic interfaces can be configured for a primary and secondary DHCP server, and the service-port interface can be configured to enable or disable DHCP servers.

Note Refer to the *Configuring Ports and Interfaces* chapter for information on configuring the controller's interfaces.

Per-WLAN Assignment

You can also define a DHCP server on a WLAN. This server will override the DHCP server address on the interface assigned to the WLAN.

Security Considerations

For enhanced security, Cisco recommends that you require all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, all WLANs can be configured with a DHCP Addr. Assignment Required setting, which disallows client static IP addresses. If DHCP Addr. Assignment Required is selected, clients must obtain an IP address via DHCP. Any client with a static IP address is not be allowed on the network. The controller monitors DHCP traffic because it acts as a DHCP proxy for the clients.

Note WLANs that support management over wireless must allow management (device-servicing) clients to obtain an IP address from a DHCP server. See the "Using Management over Wireless" section on page 5-54 for instructions on configuring management over wireless.

If slightly less security is tolerable, you can create WLANs with DHCP Addr. Assignment Required disabled. Clients then have the option of using a static IP address or obtaining an IP address from a designated DHCP server.

You are also allowed to create separate WLANs with DHCP Addr. Assignment Required disabled; then define the primary/secondary DHCP server as 0.0.0.0 on the interface assigned to the WLAN. These WLANs drop all DHCP requests and force clients to use a static IP address. Note that these WLANs do not support management over wireless connections.

Note Refer to the *Configuring Controller Settings* chapter for instructions on globally configuring DHCP proxy.

Note If you want to specify a static IP address for an access point rather than having one assigned automatically by a DHCP server, refer to the "Configuring a Static IP Address on a Lightweight Access Point" section on page 7-47 for more information.

This section provides both GUI and CLI instructions for configuring DHCP.

Using the GUI to Configure DHCP

Follow these steps to configure DHCP using the GUI.

Step 1 Follow the instructions in the "Using the GUI to Configure the Management, AP-Manager, Virtual, and Service-Port Interfaces" section on page 3-12 or "Using the GUI to Configure Dynamic Interfaces" section on page 3-18 to configure a primary DHCP server for a management, AP-manager, or dynamic interface that will be assigned to the WLAN.

Note When you want to use the internal DHCP server, you must set the management interface IP address of the controller as the DHCP server IP address.

Step 2 Choose **WLANs** to open the WLANs page.

Step 3 Click the ID number of the WLAN for which you wish to assign an interface. The WLANs > Edit (General) page appears.

Step 4 On the General tab, uncheck the **Status** check box and click **Apply** to disable the WLAN.

Step 5 Re-click the ID number of the WLAN.

Step 6 On the General tab, choose the interface for which you configured a primary DHCP server to be used with this WLAN from the **Interface** drop-down box.

Step 7 Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 8 If you want to define a DHCP server on the WLAN that will override the DHCP server address on the interface assigned to the WLAN, check the **DHCP Server Override** check box and enter the IP address of the desired DHCP server in the **DHCP Server IP Addr** edit box. The default value for the check box is disabled.

Note The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override.

Step 9 If you want to require all clients to obtain their IP addresses from a DHCP server, check the **DHCP Addr. Assignment Required** check box. When this feature is enabled, any client with a static IP address is not allowed on the network. The default value is disabled.

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

Step 11 On the General tab, check the **Status** check box and click **Apply** to re-enable the WLAN.

Step 12 Click **Save Configuration** to save your changes.

Using the CLI to Configure DHCP

Follow these steps to configure DHCP using the CLI.

Step 1 Follow the instructions in the "Using the GUI to Configure the Management, AP-Manager, Virtual, and Service-Port Interfaces" section on page 3-12 or "Using the GUI to Configure Dynamic Interfaces" section on page 3-18 to configure a primary DHCP server for a management, AP-manager, or dynamic interface that will be assigned to the WLAN.

Step 2 To disable the WLAN, enter this command:

config wlan disable *wlan_id*

Step 3 To specify the interface for which you configured a primary DHCP server to be used with this WLAN, enter this command:

config wlan interface *wlan_id interface_name*

Step 4 If you want to define a DHCP server on the WLAN that will override the DHCP server address on the interface assigned to the WLAN, enter this command:

config wlan dhcp_server *wlan_id dhcp_server_ip_address*

Note The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override. If you enable the override, you can use the **show wlan** command to verify that the DHCP server has been assigned to the WLAN.

Step 5 To re-enable the WLAN, enter this command:

config wlan enable *wlan_id*

Using the CLI to Debug DHCP

Use these CLI commands to obtain debug information:

- **debug dhcp packet** {**enable** | **disable**}—Enables or disables debugging of DHCP packets.
- **debug dhcp message** {**enable** | **disable**}—Enables or disables debugging of DHCP error messages.
- **debug dhcp service-port** {**enable** | **disable**}—Enables or disables debugging of DHCP packets on the service port.

Configuring DHCP Scopes

Controllers have built-in DHCP relay agents. However, when network administrators desire network segments that do not have a separate DHCP server, the controllers can have built-in DHCP scopes that assign IP addresses and subnet masks to wireless clients. Typically, one controller can have one or more DHCP scopes that each provide a range of IP addresses.

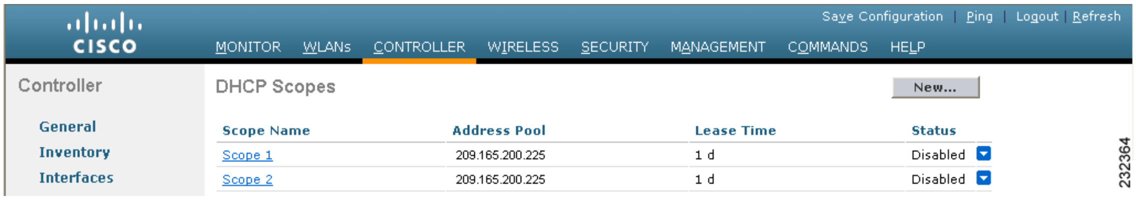
DHCP scopes are needed for internal DHCP to work. Once DHCP is defined on the controller, we can then point the primary DHCP server IP address on the management, AP-manager, and dynamic interfaces to controller's management interface. You can configure up to 16 DHCP scopes using the controller GUI or CLI.

Using the GUI to Configure DHCP Scopes

Follow these steps to configure DHCP scopes using the GUI.

Step 1 Choose **Controller** > **Internal DHCP Server** > **DHCP Scope** to open the DHCP Scopes page (see Figure 6-5).

Figure 6-5 DHCP Scopes Page



Scope Name	Address Pool	Lease Time	Status
Scope 1	209.165.200.225	1 d	Disabled
Scope 2	209.165.200.225	1 d	Disabled

This page lists any DHCP scopes that have already been configured.

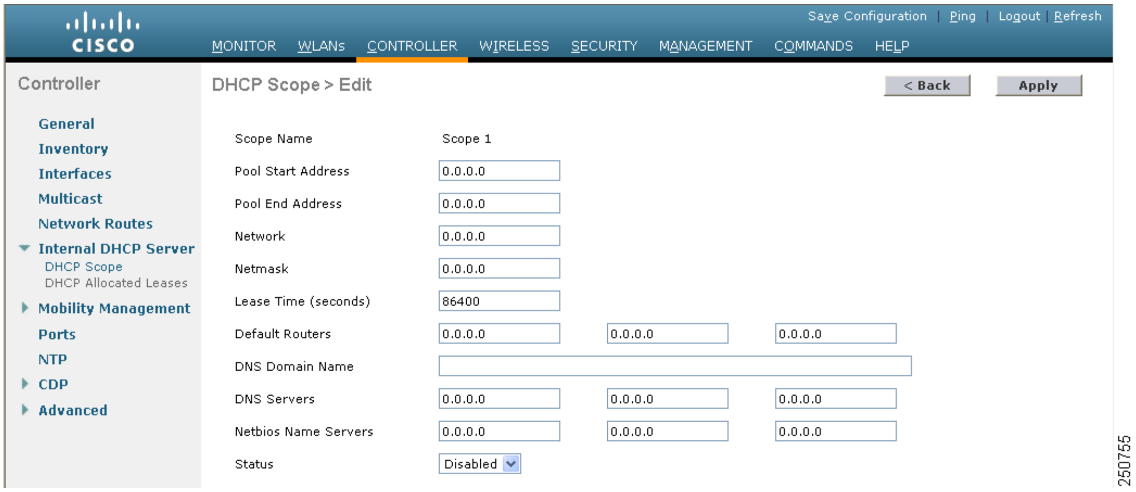
Note If you ever want to delete an existing DHCP scope, hover your cursor over the blue drop-down arrow for that scope and choose **Remove**.

Step 2 To add a new DHCP scope, click **New**. The DHCP Scope > New page appears.

Step 3 In the Scope Name field, enter a name for the new DHCP scope.

Step 4 Click **Apply**. When the DHCP Scopes page reappears, click the name of the new scope. The DHCP Scope > Edit page appears (see Figure 6-6).

Figure 6-6 DHCP Scope > Edit Page



DHCP Scope > Edit

Scope Name	Scope 1		
Pool Start Address	0.0.0.0		
Pool End Address	0.0.0.0		
Network	0.0.0.0		
Netmask	0.0.0.0		
Lease Time (seconds)	86400		
Default Routers	0.0.0.0	0.0.0.0	0.0.0.0
DNS Domain Name			
DNS Servers	0.0.0.0	0.0.0.0	0.0.0.0
Netbios Name Servers	0.0.0.0	0.0.0.0	0.0.0.0
Status	Disabled		

Step 5 In the Pool Start Address field, enter the starting IP address in the range assigned to the clients.

Note This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 6 In the Pool End Address field, enter the ending IP address in the range assigned to the clients.

Note This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 7 In the Network field, enter the network served by this DHCP scope. This is the IP address used by the management interface with Netmask applied, as configured on the Interfaces page.

Step 8 In the Netmask field, enter the subnet mask assigned to all wireless clients.

Step 9 In the Lease Time field, enter the amount of time (from 0 to 65536 seconds) that an IP address is granted to a client.

Step 10 In the Default Routers field, enter the IP address of the optional router(s) connecting the controllers. Each router must include a DHCP forwarding agent, which allows a single controller to serve the clients of multiple controllers.

Step 11 In the DNS Domain Name field, enter the optional domain name system (DNS) domain name of this DHCP scope for use with one or more DNS servers.

Step 12 In the DNS Servers field, enter the IP address of the optional DNS server(s). Each DNS server must be able to update a client's DNS entry to match the IP address assigned by this DHCP scope.

Step 13 In the Netbios Name Servers field, enter the IP address of the optional Microsoft Network Basic Input Output System (NetBIOS) name server(s), such as a s Internet Naming Service (WINS) server.

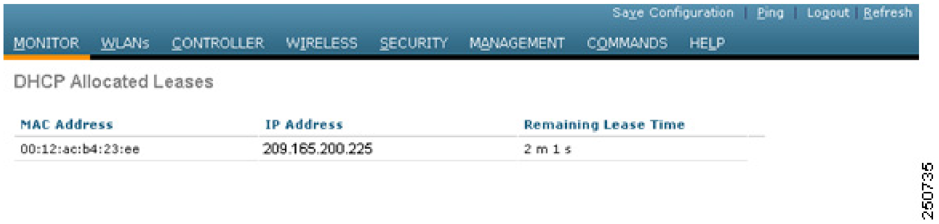
Step 14 From the Status drop-down box, choose **Enabled** to enable this DHCP scope or **Disabled** to disable it.

Step 15 Click **Apply** to commit your changes.

Step 16 Click **Save Configuration** to save your changes.

Step 17 To see the remaining lease time for wireless clients, choose **DHCP Allocated Leases**. The DHCP Allocated Lease page appears (see Figure 6-7), showing the MAC address, IP address, and remaining lease time for the wireless clients.

Figure 6-7 DHCP Allocated Lease Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
250735

DHCP Allocated Leases

MAC Address	IP Address	Remaining Lease Time
00:12:ac:b4:23:ee	209.165.200.225	2 m 1 s

Using the CLI to Configure DHCP Scopes

Follow these steps to configure DHCP scopes using the CLI.

Step 1 To create a new DHCP scope, enter this command:

config dhcp create-scope *scope*

Note If you ever want to delete a DHCP scope, enter this command: **config dhcp delete-scope** *scope*.

Step 2 To specify the starting and ending IP address in the range assigned to the clients, enter this command:

config dhcp address-pool *scope start end*

Note This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 3 To specify the network served by this DHCP scope (the IP address used by the management interface with Netmask applied) and the subnet mask assigned to all wireless clients, enter this command:

config dhcp network *scope network netmask*

Step 4 To specify the amount of time (from 0 to 65536 seconds) that an IP address is granted to a client, enter this command:

config dhcp lease *scope lease_duration*

Step 5 To specify the IP address of the optional router(s) connecting the controllers, enter this command:

config dhcp default-router *scope router_1* [*router_2*] [*router_3*]

Each router must include a DHCP forwarding agent, which allows a single controller to serve the clients of multiple controllers.

Step 6 To specify the optional domain name system (DNS) domain name of this DHCP scope for use with one or more DNS servers, enter this command:

config dhcp domain *scope domain*

Step 7 To specify the IP address of the optional DNS server(s), enter this command:

config dhcp dns-servers *scope dns1* [*dns2*] [*dns3*]

Each DNS server must be able to update a client's DNS entry to match the IP address assigned by this DHCP scope

Step 8 To specify the IP address of the optional Microsoft Network Basic Input Output System (NetBIOS) name server(s), such as a s Internet Naming Service (WINS) server, enter this command:

config dhcp netbios-name-server *scope wins1* [*wins2*] [*wins3*]

Step 9 To enable or disable this DHCP scope, enter this command:

config dhcp {**enable** | **disable**} *scope*

Step 10 To save your changes, enter this command:

save config

Step 11 To see the list of configured DHCP scopes, enter this command:

show dhcp summary

Information similar to the following appears:

```
Scope Name           Enabled           Address Range
Scope 1                No          0.0.0.0 -> 0.0.0.0
Scope 2                No          0.0.0.0 -> 0.0.0.0
```

Step 12 To display the DHCP information for a particular scope, enter this command:

show dhcp *scope*

Information similar to the following appears:

```
Enabled....................................... No
Lease Time.................................. 0
Pool Start.................................. 0.0.0.0
Pool End.................................... 0.0.0.0
Network..................................... 0.0.0.0
Netmask..................................... 0.0.0.0
Default Routers............................. 0.0.0.0 0.0.0.0 0.0.0.0
DNS Domain..................................
DNS......................................... 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers........................ 0.0.0.0 0.0.0.0 0.0.0.0
```

Configuring MAC Filtering for WLANs

When you use MAC filtering for client or administrator authorization, you need to enable it at the WLAN level first. If you plan to use local MAC address filtering for any WLAN, use the commands in this section to configure MAC filtering for a WLAN.

Enabling MAC Filtering

Use these commands to enable MAC filtering on a WLAN:

- Enter **config wlan mac-filtering enable** *wlan_id* to enable MAC filtering.
- Enter **show wlan** to verify that you have MAC filtering enabled for the WLAN.

When you enable MAC filtering, only the MAC addresses that you add to the WLAN are allowed to join the WLAN. MAC addresses that have not been added are not allowed to join the WLAN.

Creating a Local MAC Filter

Controllers have built-in MAC filtering capability, similar to that provided by a RADIUS authorization server.

Use these commands to add MAC addresses to a WLAN MAC filter:

- Enter **config macfilter add** *mac_addr wlan_id* [*interface_name*] [*description*] [*IP_addr*] to create a MAC filter entry on the controller, where the following parameters are optional:
  - *mac_addr*—MAC address of the the client.
  - *wlan_id*—WLAN id on which the client is associating.
  - *interface_name*—The name of the interface. This interface name is used to override the interface configured to the WLAN.

  Note You must have AAA enabled on the WLAN to override the interface name.

  - *description*—A brief description of the interface in double quotes (for example, "Interface1").
  - *IP_addr*—The IP address which is used for a passive client with the MAC address specified by the *mac_addr* value above.
- Enter **config macfilter ip-address** *mac_addr IP_addr* to assign an IP address to an existing MAC filter entry, if one was not assigned in the **config macfilter add** command.
- Enter **show macfilter** to verify that MAC addresses are assigned to the WLAN.

Configuring a Timeout for Disabled Clients

You can configure a timeout for disabled clients. Clients who fail to authenticate three times when attempting to associate are automatically disabled from further association attempts. After the timeout period expires, the client is allowed to retry authentication until it associates or fails authentication and is excluded again. Use these commands to configure a timeout for disabled clients:

- Enter **config wlan exclusionlist** *wlan_id timeout* to configure the timeout for disabled clients. Enter a timeout from **1** to **65535** seconds, or enter **0** to permanently disable the client.
- Use the **show wlan** command to verify the current timeout.

Assigning WLANs to Interfaces

Use these commands to assign a WLAN to an interface:

- Enter this command to assign a WLAN to an interface:

config wlan interface {*wlan_id* | **foreignAp**} *interface_id*

- Use the *interface_id* option to assign the WLAN to a specific interface.
- Use the **foreignAp** option to use a third-party access point.

- Enter **show wlan summary** to verify the interface assignment status.

Configuring the DTIM Period

In 802.11a/n and 802.11b/g/n networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Normally, the DTIM value is set to 1 (transmit broadcast and multicast frames after every beacon) or 2 (transmit after every other beacon). For instance, if the beacon period of the 802.11a/n or 802.11b/g/n network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames 5 times per second. Either of these settings may be suitable for applications, including VoIP, that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (transmit broadcast and multicast frames after every 255th beacon) if all 802.11a/n or 802.11b/g/n clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently, resulting in longer battery life. For instance, if the beacon period is 100 ms and the DTIM value is set to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds, allowing the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, resulting in longer battery life.

Many applications cannot tolerate a long time between broadcast and multicast messages, resulting in poor protocol and application performance. Cisco recommends a low DTIM value for 802.11a/n and 802.11b/g/n networks that support such clients.

In controller software release 5.0 or later, you can configure the DTIM period for the 802.11a/n and 802.11b/g/n radio networks on specific WLANs. In previous software releases, the DTIM period was configured per radio network only, not per WLAN. The benefit of this change is that now you can configure a different DTIM period for each WLAN. For example, you might want to set different DTIM values for voice and data WLANs.

Note When you upgrade the controller software to release 5.0 or later, the DTIM period that was configured for a radio network is copied to all of the existing WLANs on the controller.

Using the GUI to Configure the DTIM Period

Using the GUI, follow these steps to configure the DTIM period for a WLAN.

Step 1 Choose **WLANs** to open the WLANs page.

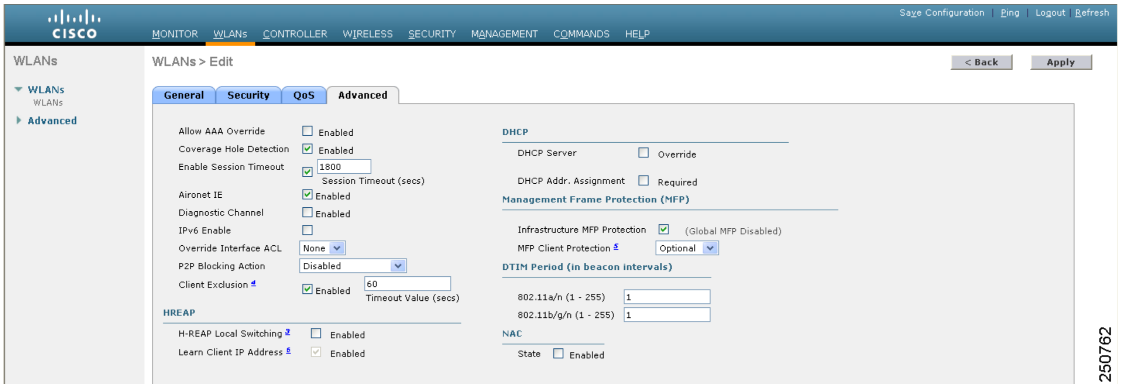
Step 2 Click the ID number of the WLAN for which you want to configure the DTIM period.

Step 3 Uncheck the **Status** check box to disable the WLAN.

Step 4 Click **Apply** to commit your changes.

Step 5 Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page (see Figure 6-8).

Figure 6-8 WLANs > Edit (Advanced) Page



WLANs > Edit

Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] ☑ Enabled 60 Timeout Value (secs)

HREAP

H-REAP Local Switching [3] □ Enabled
Learn Client IP Address [6] ☑ Enabled

DHCP

DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)

Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC

State □ Enabled

Step 6 Under DTIM Period, enter a value between 1 and 255 (inclusive) in the 802.11a/n and 802.11b/g/n fields. The default value is 1 (transmit broadcast and multicast frames after every beacon).

Step 7 Click **Apply** to commit your changes.

Step 8 Choose the **General** tab to open the WLANs > Edit (General) page.

Step 9 Check the **Status** check box to re-enable the WLAN.

Step 10 Click **Save Configuration** to save your changes.

Using the CLI to Configure the DTIM Period

Using the CLI, follow these steps to configure the DTIM period for a WLAN.

Step 1 To disable the WLAN, enter this command:

config wlan disable *wlan_id*

Step 2 To configure the DTIM period for either the 802.11a/n or 802.11b/g/n radio network on a specific WLAN, enter this command:

config wlan dtim {**802.11a** | **802.11b**} *dtim wlan_id*

where *dtim* is a value between 1 and 255 (inclusive). The default value is 1 (transmit broadcast and multicast frames after every beacon).

Step 3 To re-enable the WLAN, enter this command:

config wlan enable *wlan_id*

Step 4 To save your changes, enter this command:

save config

Step 5 To verify the DTIM period, enter this command:

show wlan *wlan_id*

Information similar to the following appears:

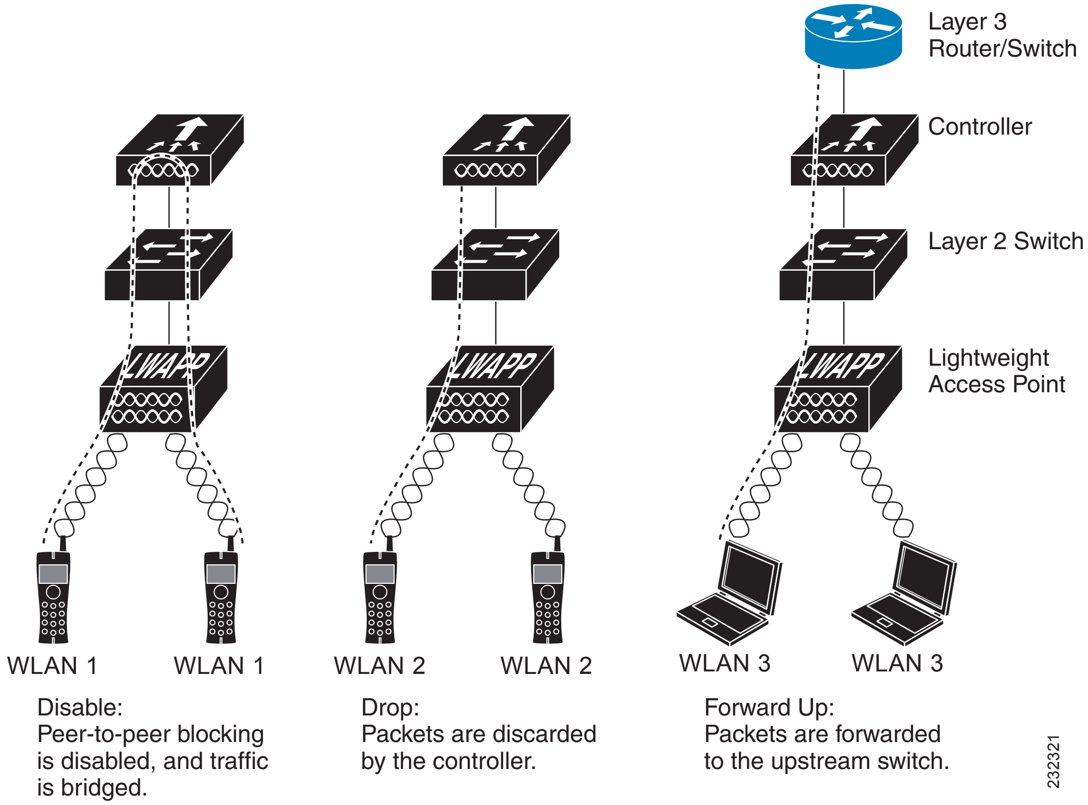
```
WLAN Identifier................................. 1
Profile Name.................................... employee1
Network Name (SSID)............................. employee
Status.......................................... Enabled
...
DTIM period for 802.11a radio................... 1
DTIM period for 802.11b radio................... 1
Local EAP Authentication..................... Disabled
...
```

Configuring Peer-to-Peer Blocking

In controller software releases prior to 4.2, peer-to-peer blocking is applied globally to all clients on all WLANs and causes traffic between two clients on the same VLAN to be transferred to the upstream VLAN rather than being bridged by the controller. This behavior usually results in traffic being dropped at the upstream switch because switches do not forward packets out the same port on which they are received.

In controller software release 4.2 or later, peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. In 4.2 or later, you also have more control over how traffic is directed. For example, you can choose to have traffic bridged locally within the controller, dropped by the controller, or forwarded to the upstream VLAN. Figure 6-9 illustrates each option.

Figure 6-9 Peer-to-Peer Blocking Examples



Guidelines for Using Peer-to-Peer Blocking

Follow these guidelines when using peer-to-peer blocking:

- In controller software releases prior to 4.2, the controller forwards Address Resolution Protocol (ARP) requests upstream (just like all other traffic). In controller software release 4.2 or later, ARP requests are directed according to the behavior set for peer-to-peer blocking.
- Peer-to-peer blocking does not apply to multicast traffic.
- Locally switched hybrid-REAP WLANs and hybrid-REAP access points in standalone mode do not support peer-to-peer blocking.
- If you upgrade to controller software release 4.2 or later from a previous release that supports global peer-to-peer blocking, each WLAN is configured with the peer-to-peer blocking action of forwarding traffic to the upstream VLAN.

Using the GUI to Configure Peer-to-Peer Blocking

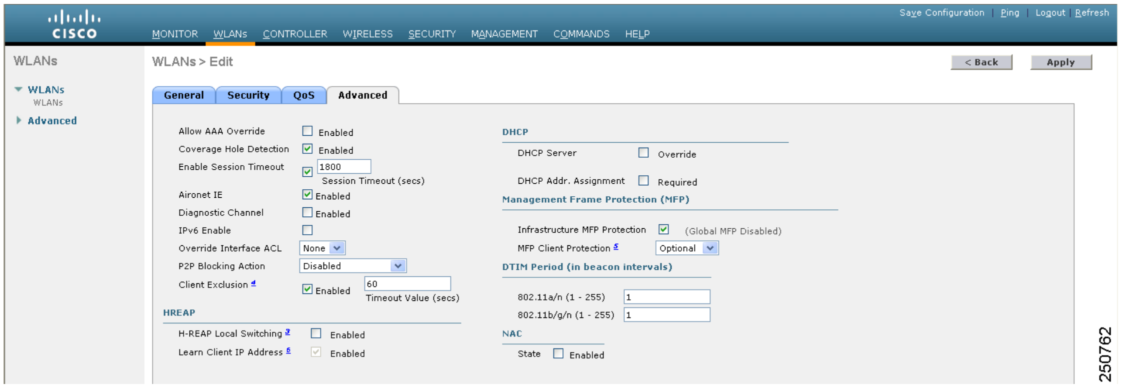
Follow these steps to configure a WLAN for peer-to-peer blocking using the GUI.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure peer-to-peer blocking.

Step 3 Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page (see Figure 6-10).

Figure 6-10 WLANs > Edit (Advanced) Page



Allow AAA Override ☐ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel ☐ Enabled
IPv6 Enable ☐
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] ☑ Enabled 60 Timeout Value (secs)

HREAP

H-REAP Local Switching [3] ☐ Enabled
Learn Client IP Address [6] ☑ Enabled

DHCP

DHCP Server ☐ Override
DHCP Addr. Assignment ☐ Required

Management Frame Protection (MFP)

Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC

State ☐ Enabled

Step 4 Choose one of the following options from the P2P Blocking drop-down box:

- **Disabled**—Disables peer-to-peer blocking and bridges traffic locally within the controller whenever possible. This is the default value.

Note Traffic is never bridged across VLANs in the controller.

- **Drop**—Causes the controller to discard the packets.
- **Forward-UpStream**—Causes the packets to be forwarded on the upstream VLAN. The device above the controller decides what action to take regarding the packets.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Using the CLI to Configure Peer-to-Peer Blocking

Follow these steps to configure a WLAN for peer-to-peer blocking using the CLI.

Step 1 To configure a WLAN for peer-to-peer blocking, enter this command:

config wlan peer-blocking {**disable** | **drop** | **forward-upstream**} *wlan_id*

Note See the description of each parameter in the "Using the GUI to Configure Peer-to-Peer Blocking" section above.

Step 2 To save your changes, enter this command:

save config

Step 3 To see the status of peer-to-peer blocking for a WLAN, enter this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
Status........................................... Enabled
...
...
...
Peer-to-Peer Blocking Action..................... Disabled
Radio Policy..................................... All
Local EAP Authentication..................... Disabled
```

Configuring Layer 2 Security

This section explains how to assign Layer 2 security settings to WLANs.

Static WEP Keys

Controllers can control static WEP keys across access points. Use these commands to configure static WEP for WLANs:

- Enter this command to disable 802.1X encryption:

  config wlan security 802.1X disable *wlan_id*

- Enter this command to configure 40/64-bit or 104/128-bit WEP keys:

  config wlan security static-wep-key encryption *wlan_id* {**40** | **104**} {**hex** | **ascii**} *key key_index*

  - Use the **40** or **104** option to specify 40/64-bit or 104/128-bit encryption. The default setting is 104/128.
  - Use the **hex** or **ascii** option to specify the character format for the WEP key.
  - Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F) or five printable ASCII characters for 40-bit/64-bit WEP keys or enter 26 hexadecimal or 13 ASCII characters for 104-bit/128-bit keys.
  - Enter a key index (sometimes called a *key slot*) of **1** through **4**.

Dynamic 802.1X Keys and Authorization

Controllers can control 802.1X dynamic WEP keys using Extensible Authentication Protocol (EAP) across access points and support 802.1X dynamic key settings for WLANs.

Note To use LEAP with lightweight access points and wireless clients, make sure to choose **Cisco-Aironet** as the RADIUS server type when configuring the CiscoSecure Access Control Server (ACS).

- Enter **show wlan** *wlan_id* to check the security settings of each WLAN. The default security setting for new WLANs is 802.1X with dynamic keys enabled. To maintain robust Layer 2 security, leave 802.1X configured on your WLANs.
- To disable or enable the 802.1X authentication, use this command:

  config wlan security 802.1X {**enable** | **disable**} *wlan_id*

  After you enable 802.1X authentication, the controller sends EAP authentication packets between the wireless client and the authentication server. This command allows all EAP-type packets to be sent to and from the controller.
- If you want to change the 802.1X encryption level for a WLAN, use this command:

  config wlan security 802.1X encryption *wlan_id* [**0** | **40** | **104**]

  - Use the 0 option to specify no 802.1X encryption.
  - Use the 40 option to specify 40/64-bit encryption.
  - Use the 104 option to specify 104/128-bit encryption. (This is the default encryption setting.)

Configuring a WLAN for Both Static and Dynamic WEP

You can configure up to four WLANs to support static WEP keys, and you can also configure dynamic WEP on any of these static-WEP WLANs. Follow these guidelines when configuring a WLAN for both static and dynamic WEP:

- The static WEP key and the dynamic WEP key must be the same length.
- When you configure both static and dynamic WEP as the Layer 2 security policy, no other security policies can be specified. That is, you cannot configure web authentication. However, when you configure either static or dynamic WEP as the Layer 2 security policy, you can configure web authentication.

WPA1 and WPA2

Wi-Fi Protected Access (WPA or WPA1) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA1 is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard.

The following are some of the Layer 2 Security methods that a client can use to log on to a wireless system:

- 801X—This includes:
  - Original 802.1x authentication method
  - No rekeying method; wireless clients must authenticate to the RADIUS server every time they associate to a new AP
  - Dynamic WEP (can be configured with static WEP) for data protection
- WPA1—This includes:
  - 802.1x EAP based authentication method: LEAP, EAP-FAST, PEAP, EAP-TLS
  - PSK, 802.1x, and CCKM rekeying mechanisms
  - Temporal Key Integrity Protocol (TKIP) (dynamic WEP encryption) with message integrity check (MIC) for data protection
- WPA2—This includes:
  - 802.1x EAP based authentication method: LEAP, EAP-FAST, PEAP, EAP-TLS
  - PSK, 802.1x, and CCKM rekeying mechanisms
  - Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) for data protection

The following are the rekeying mechanisms used by both WPA1 and WPA2, with the default being 802.1X:

- **802.1X**—802.11i International Engineering Task Force (IETF) standard rekeying mechanism. We recommend this mechanism for non-Cisco hardware clients.
- **PSK**—When you choose PSK (also known as *WPA pre-shared key* or *WPA passphrase*), you need to configure a pre-shared key (or a passphrase). This key is used as the pairwise master key (PMK) between the clients and the authentication server.
- **CCKM**—Cisco Centralized Key Management (CCKM) uses a fast rekeying technique that enables clients to roam from one access point to another without going through the controller, typically in under 150 milliseconds (ms). CCKM reduces the time required by the client to mutually authenticate with the new access point and derive a new session key during reassociation. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications such as wireless Voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions. CCKM is a CCXv4-compliant feature. If CCKM is selected, only CCKM clients are supported.

Note The 4.2 or later release of controller software supports CCX versions 1 through 5. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to limit client functionality. Clients must support CCXv4 or v5 in order to use CCKM. See the "Configuring Cisco Client Extensions" section on page 6-49 for more information on CCX.

- **802.1X+CCKM**—During normal operation, 802.1X-enabled clients mutually authenticate with a new access point by performing a complete 802.1X authentication, including communication with the main RADIUS server. However, when you configure your WLAN for 802.1X and CCKM fast secure roaming, CCKM-enabled clients securely roam from one access point to another without the need to reauthenticate to the RADIUS server. 802.1X+CCKM is considered optional CCKM because both CCKM and non-CCKM clients are supported when this option is selected.

Note When the AP advertises its security capabilities via the Robust Security Network Information Element (RSNIE) in the beacons and probe responses of the access point, CCKM rekeying capability is communicated by a MAC organizationally unique identifier (OUI) value of 00:40:96 and a type value of 0 in the Authenticated Key Management (AKM) suite selector of the RSNIE. 802.1x rekeying mechanism uses the MAC OUI of 00:0f:ac and a type value of 1 in the AKM suite selector of the RSNIE. The PSK uses a MAC OUI of 00:0F:AC with a type value of 6 in the AKM suite selector of the RSNIE.

On a single WLAN, you can allow WPA1, WPA2, and 802.1X/PSK/CCKM/802.1X+CCKM clients to join. All of the access points on such a WLAN advertise WPA1, WPA2, and 802.1X/PSK/CCKM/802.1X+CCKM information elements in their beacons and probe responses. When you enable WPA1 and/or WPA2, you can also enable one or two *ciphers*, or cryptographic algorithms, designed to protect data traffic. Specifically, you can enable AES and/or TKIP data encryption for WPA1 and/or WPA2. TKIP is the default value for WPA1, and AES is the default value for WPA2.

Note WLAN should be enabled only after WPA1 and WPA2 ciphers are enabled. You can enable WPA1 and WPA2 using the **`config wlan security wpa {wpa1/wpa2} enable`** command. You can not enable ciphers from the GUI unless WPA1 and WPA 2 are enabled.

Using the GUI to Configure WPA1+WPA2

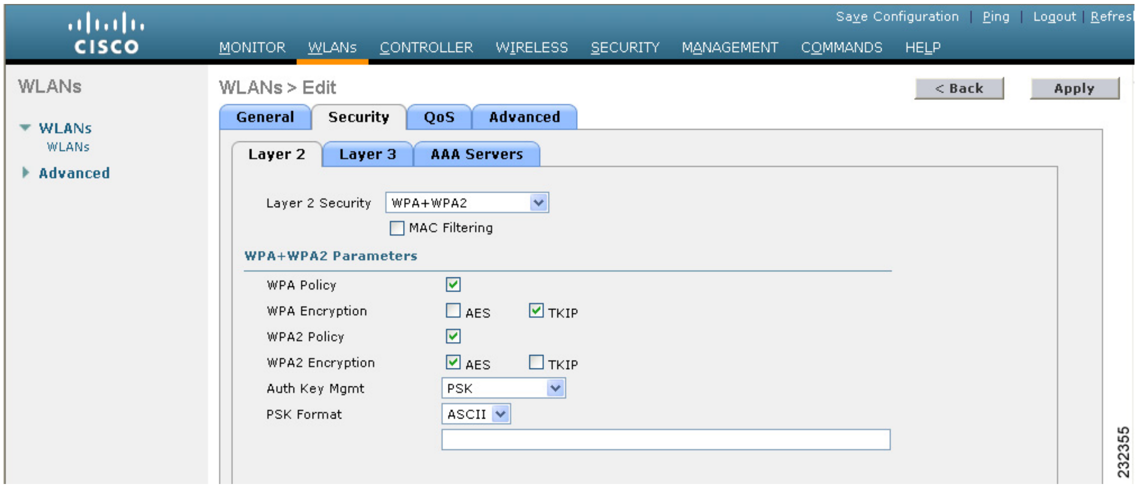
Follow these steps to configure a WLAN for WPA1+WPA2 using the controller GUI.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Choose the **Security** and **Layer 2** tabs to open the WLANs > Edit (Security > Layer 2) page (see Figure 6-11).

Figure 6-11 WLANs > Edit (Security > Layer 2) Page


Save Configuration | Ping | Logout | Refres
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General Security QoS Advanced
Layer 2 Layer 3 AAA Servers
232355

Layer 2 Security WPA+WPA2
□ MAC Filtering

WPA+WPA2 Parameters

WPA Policy	☑	
WPA Encryption	□ AES	☑ TKIP
WPA2 Policy	☑	
WPA2 Encryption	☑ AES	□ TKIP
Auth Key Mgmt	PSK	
PSK Format	ASCII	

Step 4 Choose **WPA+WPA2** from the Layer 2 Security drop-down box.

Step 5 Under WPA+WPA2 Parameters, check the **WPA Policy** check box to enable WPA1, check the **WPA2 Policy** check box to enable WPA2, or check both check boxes to enable both WPA1 and WPA2.

Note The default value is disabled for both WPA1 and WPA2. If you leave both WPA1 and WPA2 disabled, the access points advertise in their beacons and probe responses information elements only for the authentication key management method you choose in Step 7.

Step 6 Check the **AES** check box to enable AES data encryption or the **TKIP** check box to enable TKIP data encryption for WPA1, WPA2, or both. The default values are TKIP for WPA1 and AES for WPA2.

Step 7 Choose one of the following key management methods from the Auth Key Mgmt drop-down box: **802.1X**, **CCKM**, **PSK**, or **802.1X+CCKM**.

Step 8 If you chose PSK in Step 7, choose **ASCII** or **HEX** from the PSK Format drop-down box and then enter a pre-shared key in the blank field. WPA pre-shared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Using the CLI to Configure WPA1+WPA2

Follow these steps to configure a WLAN for WPA1+WPA2 using the controller CLI.

Step 1 Enter this command to disable the WLAN:

config wlan disable *wlan_id*

Step 2 Enter this command to enable or disable WPA for the WLAN:

config wlan security wpa {**enable** | **disable**} *wlan_id*

Step 3 Enter this command to enable or disable WPA1 for the WLAN:

config wlan security wpa wpa1 {**enable** | **disable**} *wlan_id*

Step 4 Enter this command to enable or disable WPA2 for the WLAN:

config wlan security wpa wpa2 {**enable** | **disable**} *wlan_id*

Step 5 Enter these commands to enable or disable AES or TKIP data encryption for WPA1 or WPA2:

- **config wlan security wpa wpa1 ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*
- **config wlan security wpa wpa2 ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

The default values are TKIP for WPA1 and AES for WPA2.

Step 6 Enter this command to enable or disable 802.1X, PSK, or CCKM authenticated key management:

config wlan security wpa akm {**802.1X** | **psk** | **cckm**} {**enable** | **disable**} *wlan_id*

The default value is 802.1X.

Step 7 If you enabled PSK in Step 6, enter this command to specify a pre-shared key:

config wlan security wpa akm psk set-key {**ascii** | **hex**} *psk-key wlan_id*

WPA pre-shared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

Step 8 If you enabled WPA2 with 802.1X authenticated key management or WPA1 or WPA2 with CCKM authenticated key management, the PMK cache lifetime timer is used to trigger reauthentication with the client when necessary. The timer is based on the timeout value received from the AAA server or the WLAN session timeout setting. To see the amount of time remaining before the timer expires, enter this command:

show pmk-cache all

Information similar to the following appears:

```
PMK-CCKM Cache
                            Entry
Type        Station         Lifetime   VLAN Override        IP Override
------  ------------------- --------   ------------------   ---------------
CCKM    00:07:0e:b9:3a:1b   150                          0.0.0.0
```

If you enabled WPA2 with 802.1X authenticated key management, the controller supports opportunistic PMKID caching but not sticky (or non-opportunistic) PMKID caching. In sticky PMKID caching, the client stores multiple PMKIDs. This approach is not practical because it requires full authentication for each new access point and is not guaranteed to work in all conditions. In contrast, opportunistic PMKID caching stores only one PMKID per client and is not subject to the limitations of sticky PMK caching.

Step 9 Enter this command to enable the WLAN:

config wlan enable *wlan_id*

Step 10 Enter this command to save your settings:

save config

CKIP

Cisco Key Integrity Protocol (CKIP) is a Cisco-proprietary security protocol for encrypting 802.11 media. CKIP improves 802.11 security in infrastructure mode using key permutation, message integrity check (MIC), and message sequence number. Software release 4.0 or later supports CKIP with static key. For this feature to operate correctly, you must enable Aironet information elements (IEs) for the WLAN.

A lightweight access point advertises support for CKIP in beacon and probe response packets by adding an Aironet IE and setting one or both of the CKIP negotiation bits [key permutation and multi-modular hash message integrity check (MMH MIC)]. Key permutation is a data encryption technique that uses the basic encryption key and the current initialization vector (IV) to create a new key. MMH MIC prevents bit-flip attacks on encrypted packets by using a hash function to compute message integrity code.

The CKIP settings specified in a WLAN are mandatory for any client attempting to associate. If the WLAN is configured for both CKIP key permutation and MMH MIC, the client must support both. If the WLAN is configured for only one of these features, the client must support only this CKIP feature.

CKIP requires that 5-byte and 13-byte encryption keys be expanded to 16-byte keys. The algorithm to perform key expansion happens at the access point. The key is appended to itself repeatedly until the length reaches 16 bytes. All lightweight access points support CKIP.

You can configure CKIP through either the GUI or the CLI.

Using the GUI to Configure CKIP

Follow these steps to configure a WLAN for CKIP using the controller GUI.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Choose the **Advanced** tab.

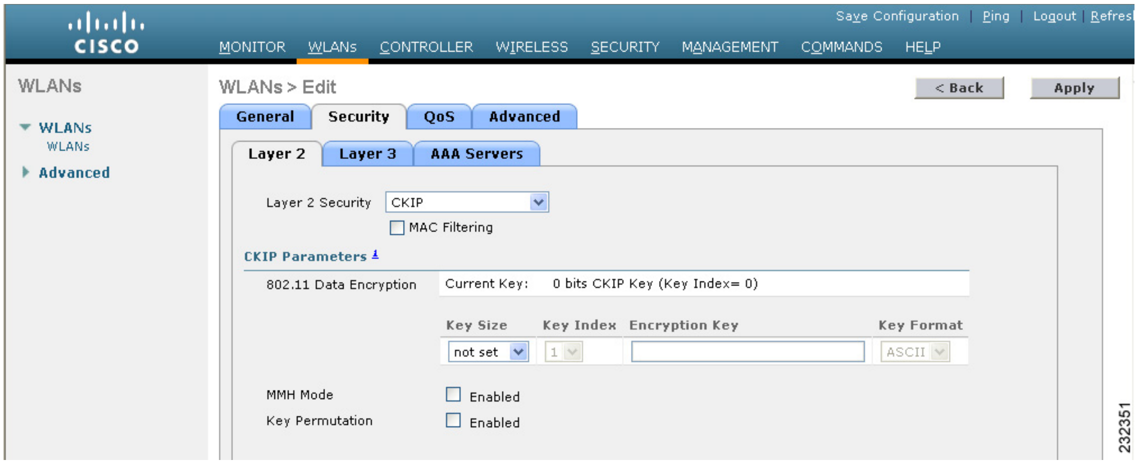
Step 4 Check the **Aironet IE** check box to enable Aironet IEs for this WLAN and click **Apply**.

Step 5 Choose the **General** tab.

Step 6 Uncheck the **Status** check box, if checked, to disable this WLAN and click **Apply**.

Step 7 Choose the **Security** and **Layer 2** tabs to open the WLANs > Edit (Security > Layer 2) page (see Figure 6-12).

Figure 6-12 WLANs > Edit (Security > Layer 2) Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
232351

Layer 2 Security: CKIP

□ MAC Filtering

CKIP Parameters

802.11 Data Encryption — Current Key: 0 bits CKIP Key (Key Index= 0)

Key Size	Key Index	Encryption Key	Key Format
not set	1		ASCII

MMH Mode □ Enabled

Key Permutation □ Enabled

Step 8 Choose **CKIP** from the Layer 2 Security drop-down box.

Step 9 Under CKIP Parameters, choose the length of the CKIP encryption key from the Key Size drop-down box.

Range: Not Set, 40 bits, or 104 bits

Default: Not Set

Step 10 Choose the number to be assigned to this key from the Key Index drop-down box. You can configure up to four keys.

Step 11 Choose **ASCII** or **HEX** from the Key Format drop-down box and then enter an encryption key in the Encryption Key field. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.

Step 12 Check the **MMH Mode** check box to enable MMH MIC data protection for this WLAN. The default value is disabled (or unchecked).

Step 13 Check the **Key Permutation** check box to enable this form of CKIP data protection. The default value is disabled (or unchecked).

Step 14 Click **Apply** to commit your changes.

Step 15 Choose the **General** tab.

Step 16 Check the **Status** check box to enable this WLAN.

Step 17 Click **Apply** to commit your changes.

Step 18 Click **Save Configuration** to save your changes.

Using the CLI to Configure CKIP

Follow these steps to configure a WLAN for CKIP using the controller CLI.

Step 1 Enter this command to disable the WLAN:

config wlan disable *wlan_id*

Step 2 Enter this command to enable Aironet IEs for this WLAN:

config wlan ccx aironet-ie enable *wlan_id*

Step 3 Enter this command to enable or disable CKIP for the WLAN:

config wlan security ckip {**enable** | **disable**} *wlan_id*

Step 4 Enter this command to specify a CKIP encryption key for the WLAN:

config wlan security ckip akm psk set-key *wlan_id* {**40** | **104**} {**hex** | **ascii**} *key key_index*

Step 5 Enter this command to enable or disable CKIP MMH MIC for the WLAN:

config wlan security ckip mmh-mic {**enable** | **disable**} *wlan_id*

Step 6 Enter this command to enable or disable CKIP key permutation for the WLAN:

config wlan security ckip kp {**enable** | **disable**} *wlan_id*

Step 7 Enter this command to enable the WLAN:

config wlan enable *wlan_id*

Step 8 Enter this command to save your settings:

save config

Configuring a Session Timeout

Using the controller GUI or CLI, you can configure a session timeout for wireless clients on a WLAN. The session timeout is the maximum time for a client session to remain active before requiring reauthorization.

Using the GUI to Configure a Session Timeout

Using the controller GUI, follow these steps to configure a session timeout for wireless clients on a WLAN.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to assign a session timeout.

Step 3 When the WLANs > Edit page appears, choose the **Advanced** tab. The WLANs > Edit (Advanced) page appears.

Step 4 To configure a session timeout for this WLAN, check the **Enable Session Timeout** check box. Otherwise, uncheck the check box. The default value is checked.

Step 5 In the Session Timeout field, enter a value between 300 and 86400 seconds to specify the duration of the client session. The default value is 1800 seconds for the following Layer 2 security types: 802.1X; Static WEP+802.1X; and WPA+WPA2 with 802.1X, CCKM, or 802.1X+CCKM authentication key management and 0 seconds for all other Layer 2 security types. A value of 0 is equivalent to no timeout.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Using the CLI to Configure a Session Timeout

Using the controller CLI, follow these steps to configure a session timeout for wireless clients on a WLAN.

Step 1 To configure a session timeout for wireless clients on a WLAN, enter this command:

config wlan session-timeout *wlan_id timeout*

The default value is 1800 seconds for the following Layer 2 security types: 802.1X; Static WEP+802.1X; and WPA+WPA2 with 802.1X, CCKM, or 802.1X+CCKM authentication key management and 0 seconds for all other Layer 2 security types. A value of 0 is equivalent to no timeout.

Step 2 To save your changes, enter this command:

save config

Step 3 To see the current session timeout value for a WLAN, enter this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 9
Profile Name..................................... test12
Network Name (SSID).......................... test12
...
Number of Active Clients........................ 0
Exclusionlist Timeout........................... 60 seconds
Session Timeout.............................. 1800 seconds
...
```

Configuring Layer 3 Security

This section explains how to configure Layer 3 security settings for a WLAN on the controller.

Note

- Layer 2 Tunnel Protocol (L2TP) and IPSec are not supported on controllers running software release 4.0 or later.
- The Layer 3 securities are not supported when Client IP Address is disabled on a WLAN.

VPN Passthrough

The controller supports VPN passthrough, or the “passing through” of packets that originate from VPN clients. An example of VPN passthrough is your laptop trying to connect to the VPN server at your corporate office.

Note The VPN Passthrough option is not available on 5500 series and 2100 series controllers. However, you can replicate this functionality on a 5500 or 2100 series controller by creating an open WLAN using an ACL.

Using the GUI to Configure VPN Passthrough

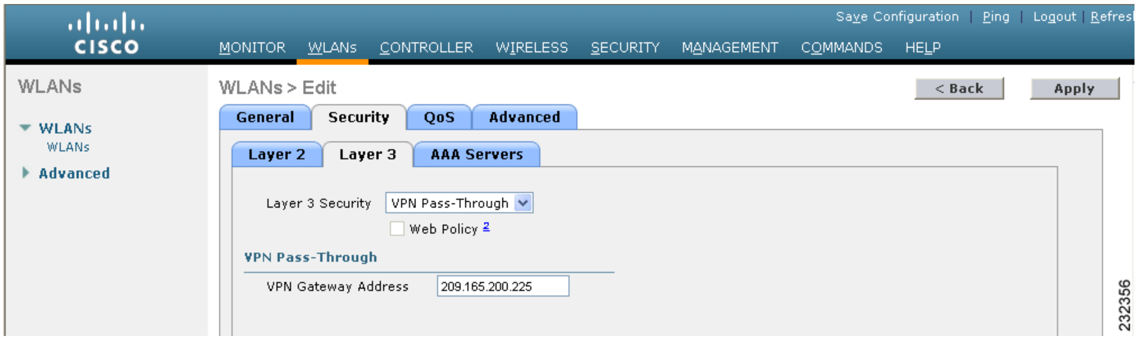
Follow these steps to configure a WLAN for VPN passthrough using the controller GUI.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure VPN passthrough. The WLANs > Edit page appears.

Step 3 Choose the **Security** and **Layer 3** tabs to open the WLANs > Edit (Security > Layer 3) page (see Figure 6-13).

Figure 6-13 WLANs > Edit (Security > Layer 3) Page



Layer 3 Security VPN Pass-Through

□ Web Policy 2

VPN Pass-Through

VPN Gateway Address 209.165.200.225

Step 4 Choose **VPN Pass-Through** from the Layer 3 Security drop-down box.

Step 5 In the VPN Gateway Address field, enter the IP address of the gateway router that is terminating the VPN tunnels initiated by the client and passed through the controller.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your settings.

Using the CLI to Configure VPN Passthrough

Enter these commands to configure a WLAN for VPN passthrough using the controller CLI:

- **config wlan security passthru** {**enable** | **disable**} *wlan_id gateway*

  For *gateway*, enter the IP address of the router that is terminating the VPN tunnel.

- Enter **show wlan** to verify that the passthrough is enabled.

Web Authentication

WLANs can use web authentication only if VPN passthrough is not enabled on the controller. Web authentication is simple to set up and use and can be used with SSL to improve the overall security of the WLAN.

Note Web authentication is supported only with these Layer 2 security policies: open authentication, open authentication+WEP, and WPA-PSK. It is not supported for use with 802.1X.

Note The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.

Note Before enabling web authentication, make sure that all proxy servers are configured for ports other than port 53.

Note When you enable web authentication for a WLAN, a message appears indicating that the controller forwards DNS traffic to and from wireless clients prior to authentication. Cisco recommends that you have a firewall or intrusion detection system (IDS) behind your guest VLAN to regulate DNS traffic and to prevent and detect any DNS tunneling attacks.

Using the GUI to Configure Web Authentication

Using the controller GUI, follow these steps to configure a WLAN for web authentication.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure web authentication. The WLANs > Edit page appears.

Step 3 Choose the **Security** and **Layer 3** tabs to open the WLANs > Edit (Security > Layer 3) page.

Step 4 Check the **Web Policy** check box.

Step 5 Make sure that the **Authentication** option is selected.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your settings.

Step 8 Refer to the *Managing User Accounts* chapter for more information on using web authentication.

Using the CLI to Configure Web Authentication

Using the controller CLI, follow these steps to configure a WLAN for web authentication.

Step 1 To enable or disable web authentication on a particular WLAN, enter this command:

config wlan security web-auth {**enable** | **disable**} *wlan_id*

Step 2 To release the guest user IP address when the web authentication policy timer expires and prevent the guest user from acquiring an IP address for 3 minutes, enter this command:

config wlan webauth-exclude *wlan_id* {**enable** | **disable**}

The default value is disabled. This command is applicable when you configure the internal DHCP scope on the controller. By default, when the web authentication timer expires for a guest user, the user can immediately reassociate to the same IP address before another guest user can acquire it. If there are many guest users or limited IP addresses in the DHCP pool, some guest users might not be able to acquire an IP address.

When you enable this feature on the guest WLAN, the guest user's IP address is released when the web authentication policy timer expires and the guest user is excluded from acquiring an IP address for 3 minutes. The IP address is available for another guest user to use. After 3 minutes, the excluded guest user can reassociate and acquire an IP address, if available.

Step 3 To see the status of web authentication, enter this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... cjtalwar
Network Name (SSID).............................. cjtalwar
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Network Admission Control

  NAC-State...................................... Disabled
  Quarantine VLAN................................ 0
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
CHD per WLAN................................. Enabled
Webauth DHCP exclusion........................... Disabled
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required............. Disabled
...
Web Based Authentication......................... Disabled
Web-Passthrough.............................. Disabled
...
```

Step 4 For more information on using web authentication, refer to the *Managing User Accounts* chapter.

Assigning a QoS Profile to a WLAN

Cisco UWN Solution WLANs support four levels of QoS: Platinum/Voice, Gold/Video, Silver/Best Effort (default), and Bronze/Background. You can configure the voice traffic WLAN to use Platinum QoS, assign the low-bandwidth WLAN to use Bronze QoS, and assign all other traffic between the remaining QoS levels.

The WLAN QoS level defines a specific 802.11e user priority (UP) for over-the-air traffic. This UP is used to derive the over-the-wire priorities for non-WMM traffic, and it also acts as the ceiling when managing WMM traffic with various levels of priorities. The access point uses this QoS-profile-specific UP in accordance with the values in Table 6-1 to derive the IP DSCP value that is visible on the wired LAN.

Table 6-1 Access Point QoS Translation Values

AVVID Traffic Type	AVVID IP DSCP	QoS Profile	AVVID 802.1p	IEEE 802.11e UP
Network control	56 (CS7)	Platinum	7	7
Inter-network control (CAPWAP control, 802.11 management)	48 (CS6)	Platinum	6	7
Voice	46 (EF)	Platinum	5	6
Interactive video	34 (AF41)	Gold	4	5
Mission critical	26 (AF31)	Gold	3	4
Transactional	18 (AF21)	Silver	2	3
Bulk data	10 (AF11)	Bronze	1	2
Best effort	0 (BE)	Silver	0	0
Scavenger	2	Bronze	0	1

Note The IEEE 802.11e UP value for DSCP values that are not mentioned in the table is calculated by considering 3 MSB bits of DSCP.
For example, the IEEE 802.11e UP value for DSCP 32 (100 000 in binary), would be the decimal converted value of the MSB (100) which is 4. The 802.11e UP value of DSCP 32 is 4.

You can assign a QoS profile to a WLAN using the controller GUI or CLI.

Using the GUI to Assign a QoS Profile to a WLAN

Using the controller GUI, follow these steps to assign a QoS profile to a WLAN.

Step 1 If you have not already done so, configure one or more QoS profiles using the instructions in the "Using the GUI to Configure QoS Profiles" section on page 4-67.

Step 2 Choose **WLANs** to open the WLANs page.

Step 3 Click the ID number of the WLAN to which you want to assign a QoS profile.

Step 4 When the WLANs > Edit page appears, choose the **QoS** tab.

Step 5 From the Quality of Service (QoS) drop-down box, choose one of the following:

- Platinum (voice)
- Gold (video)
- Silver (best effort)
- Bronze (background)

Note Silver (best effort) is the default value.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Using the CLI to Assign a QoS Profile to a WLAN

Using the controller CLI, follow these steps to assign a QoS profile to a WLAN.

Step 1 If you have not already done so, configure one or more QoS profiles using the instructions in the "Using the CLI to Configure QoS Profiles" section on page 4-69.

Step 2 To assign a QoS profile to a WLAN, enter this command:

config wlan qos *wlan_id* {**bronze | silver | gold | platinum**}

Silver is the default value.

Step 3 To save your changes, enter this command:

save config

Step 4 To verify that you have properly assigned the QoS profile to the WLAN, enter this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist.................................... Disabled
Session Timeout.................................. 0
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... 1.100.163.24
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
...
```

Configuring QoS Enhanced BSS

The QoS Enhanced Basis Service Set (QBSS) information element (IE) enables the access points to communicate their channel usage to wireless devices. Because access points with high channel usage might not be able to handle real-time traffic effectively, the 7921 or 7920 phone uses the QBSS value to determine if they should associate to another access point. You can enable QBSS in these two modes:

- Wi-Fi Multimedia (WMM) mode, which supports devices that meet the 802.11E QBSS standard (such as Cisco 7921 IP Phones)
- 7920 support mode, which supports Cisco 7920 IP Phones on your 802.11b/g network

  The 7920 support mode has two options:

  - Support for 7920 phones that require call admission control (CAC) to be configured on and advertised by the client device (these are typically older 7920 phones)
  - Support for 7920 phones that require CAC to be configured on and advertised by the access point (these are typically newer 7920 phones)

    When access point-controlled CAC is enabled, the access point sends out a Cisco proprietary CAC Information Element (IE) and does not send out the standard QBSS IE.

You can use the controller GUI or CLI to configure QBSS. QBSS is disabled by default.

Guidelines for Configuring QBSS

Follow these guidelines when configuring QBSS on a WLAN:

- 7920 phones are non-WMM phones with limited CAC functionality. The phones look at the channel utilization of the access point to which they are associated and compare that to a threshold that is beaconed by the access point. If the channel utilization is less than the threshold, the 7920 places a call. In contrast, 7921 phones are full-fledged WMM phones that use traffic specifications (TSPECs) to gain access to the voice queue before placing a phone call. The 7921 phones work well with load-based CAC, which uses the percentage of the channel set aside for voice and tries to limit the calls accordingly.

  Because 7921 phones support WMM and 7920 phones do not, capacity and voice quality problems can arise if you do not properly configure both phones when they are used in a mixed environment. To enable both 7921 and 7920 phones to co-exist on the same network, make sure that load-based CAC and 7920 AP CAC are both enabled on the controller and the WMM Policy is set to Allowed. This becomes particularly important if you have many more 7920 users than 7921 users.

Note Refer to the *Configuring Controller Settings* chapter for more information and configuration instructions for load-based CAC.

Additional Guidelines for Using 7921 and 7920 Wireless IP Phones

Follow these guidelines to use Cisco 7921 and 7920 Wireless IP Phones with controllers:

- Aggressive load balancing must be disabled for each controller. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.
- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the **config 802.11b dtpc enable** command. The DTPC IE is a beacon and probe information element that allows the access point to broadcast information on its transmit power. The 7921 or 7920 phone uses this information to automatically adjust its transmit power to the same level as the access point to which it is associated. In this manner, both devices are transmitting at the same level.
- Both the 7921 and 7920 phones and the controllers support Cisco Centralized Key Management (CCKM) fast roaming.
- When configuring WEP, there is a difference in nomenclature for the controller and the 7921 or 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7921 or 7920.

- For standalone 7921 phones, load-based CAC must be enabled, and the WMM Policy must be set to Required on the WLAN.
- The controller supports traffic classification (TCLAS) coming from 7921 phones using firmware version 1.1.1. This feature ensures proper classification of voice streams to the 7921 phones.
- When using a 7921 phone with the 802.11a radio of a 1242 series access point, set the 24-Mbps data rate to Supported and choose a lower Mandatory data rate (such as 12 Mbps). Otherwise, the phone might experience poor voice quality.

Using the GUI to Configure QBSS

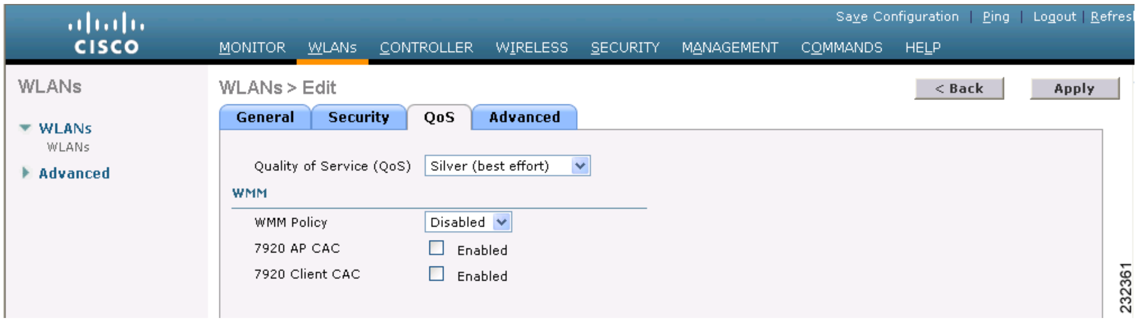
Using the controller GUI, follow these steps to configure QBSS.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure WMM mode.

Step 3 When the WLANs > Edit page appears, choose the **QoS** tab to open the WLANs > Edit (Qos) page (see Figure 6-14).

Figure 6-14 WLANs > Edit (QoS) Page



Quality of Service (QoS) Silver (best effort)

WMM

WMM Policy Disabled

7920 AP CAC □ Enabled

7920 Client CAC □ Enabled

Step 4 From the WMM Policy drop-down box, choose one of the following options, depending on whether you want to enable WMM mode for 7921 phones and other devices that meet the WMM standard:

- **Disabled**—Disables WMM on the WLAN. This is the default value.
- **Allowed**—Allows client devices to use WMM on the WLAN.
- **Required**—Requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 5 Check the **7920 AP CAC** check box if you want to enable 7920 support mode for phones that require access point-controlled CAC. The default value is unchecked.

Step 6 Check the **7920 Client CAC** check box if you want to enable 7920 support mode for phones that require client-controlled CAC. The default value is unchecked.

Note You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

Step 7 Click **Apply** to commit your changes.

Step 8 Click **Save Configuration** to save your changes.

Using the CLI to Configure QBSS

Using the controller CLI, follow these steps to configure QBSS.

Step 1 To determine the ID number of the WLAN to which you want to add QBSS support, enter this command:

show wlan summary

Step 2 To disable the WLAN, enter this command:

config wlan disable *wlan_id*

Step 3 To configure WMM mode for 7921 phones and other devices that meet the WMM standard, enter this command:

config wlan wmm {**disabled** | **allowed** | **required**} *wlan_id*

where

- The **disabled** parameter disables WMM mode on the WLAN.
- The **allowed** parameter allows client devices to use WMM on the WLAN.
- The **required** parameter requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 4 To enable or disable 7920 support mode for phones that require client-controlled CAC, enter this command:

config wlan 7920-support client-cac-limit {**enable** | **disable**} *wlan_id*

Note You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

Step 5 To enable or disable 7920 support mode for phones that require access point-controlled CAC, enter this command:

config wlan 7920-support ap-cac-limit {**enable** | **disable**} *wlan_id*

Step 6 To re-enable the WLAN, enter this command:

config wlan enable *wlan_id*

Step 7 To save your changes, enter this command:

save config

Step 8 To verify that the WLAN is enabled and the Dot11-Phone Mode (7920) field is configured for compat mode, enter this command:

show wlan *wlan_id*

Configuring VoIP Snooping

Controller software release 6.0 supports Voice over IP (VoIP) Media Session Aware (MSA) snooping and reporting. This feature enables access points to detect the establishment, termination, and failure of Session Initiation Protocol (SIP) voice calls and then report them to the controller and WCS. It can be enabled or disabled for each WLAN.

When VoIP MSA snooping is enabled, the access point radios that advertise this WLAN look for SIP voice packets that comply with SIP RFC-3261. They do not look for non-RFC-3261-compliant SIP voice packets or Skinny Call Control Protocol (SCCP) voice packets. Any SIP packets destined to or originating from port number 5060 (the standard SIP signaling port) are considered for further inspection. The access points track when Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, are already on an active call, or are in the process of ending a call. Upstream packet classification for both client types occurs at the access point whereas downstream packet classification happens at the controller for WMM clients and at the access point for non-WMM clients. The access points notify the controller and WCS of any major call events, such as call establishment, termination, and failure.

The controller provides detailed information for VoIP MSA calls. For failed calls, the controller generates a trap log with a timestamp and the reason for failure (in the GUI) and an error code (in the CLI) to aid in troubleshooting. For successful calls, the controller shows the number and duration of calls for usage tracking purposes. WCS displays failed VoIP call information in the Events window.

Using the GUI to Configure VoIP Snooping

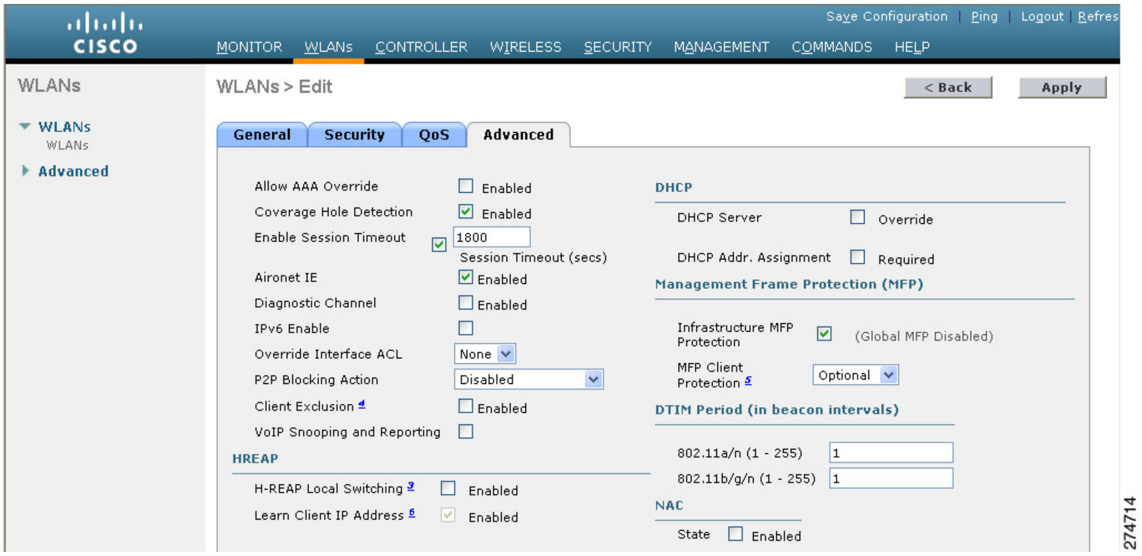
Using the controller GUI, follow these steps to configure VoIP snooping.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure VoIP snooping.

Step 3 When the WLANs > Edit page appears, choose the **Advanced** tab to open the WLANs > Edit (Advanced) page (see Figure 6-15).

Figure 6-15 WLANs > Edit (Advanced) Page


Save Configuration | Ping | Logout | Refres
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General
Security
QoS
Advanced
274714

Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] □ Enabled
VoIP Snooping and Reporting □

HREAP
H-REAP Local Switching [3] □ Enabled
Learn Client IP Address [6] ☑ Enabled

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)
Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
State □ Enabled

Step 4 Check the **VoIP Snooping and Reporting** check box to enable VoIP snooping or uncheck it to disable this feature. The default value is unchecked.

Step 5 Click **Apply** to commit your changes.

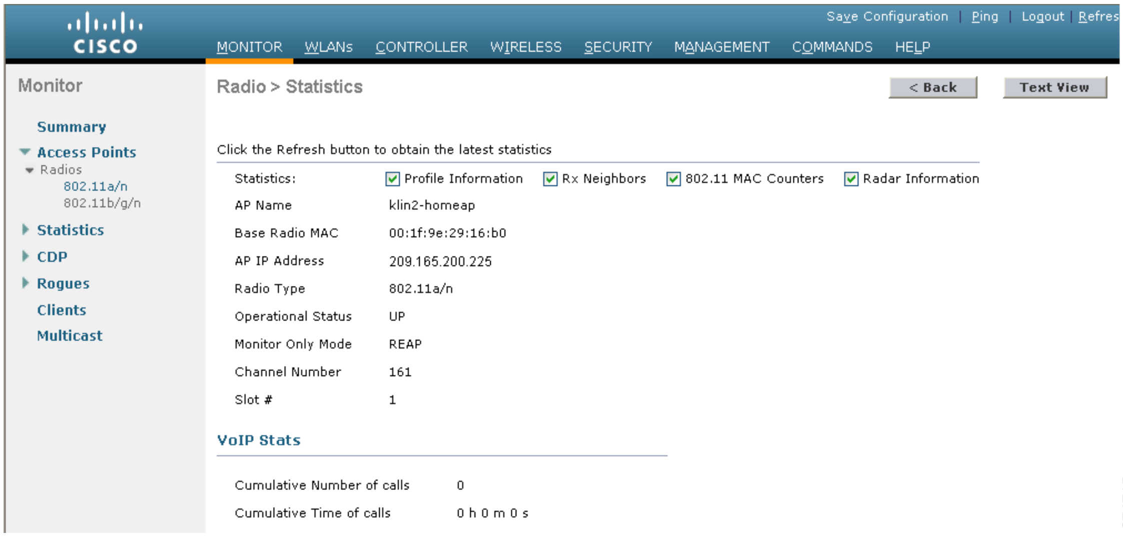
Step 6 Click **Save Configuration** to save your changes.

Step 7 To see the VoIP statistics for your access point radios, follow these steps:

a. Choose **Monitor** > **Access Points** > **Radios** > **802.11a/n** or **802.11b/g/n** to open the 802.11a/n (or 802.11b/g/n) Radios page.

b. Scroll to the right and click the **Detail** link for the access point for which you want to view VoIP statistics. The Radio > Statistics page appears (see Figure 6-16).

Figure 6-16 Radio > Statistics Page



Radio > Statistics

Click the Refresh button to obtain the latest statistics

Statistics: ☑ Profile Information ☑ Rx Neighbors ☑ 802.11 MAC Counters ☑ Radar Information

AP Name	klin2-homeap
Base Radio MAC	00:1f:9e:29:16:b0
AP IP Address	209.165.200.225
Radio Type	802.11a/n
Operational Status	UP
Monitor Only Mode	REAP
Channel Number	161
Slot #	1

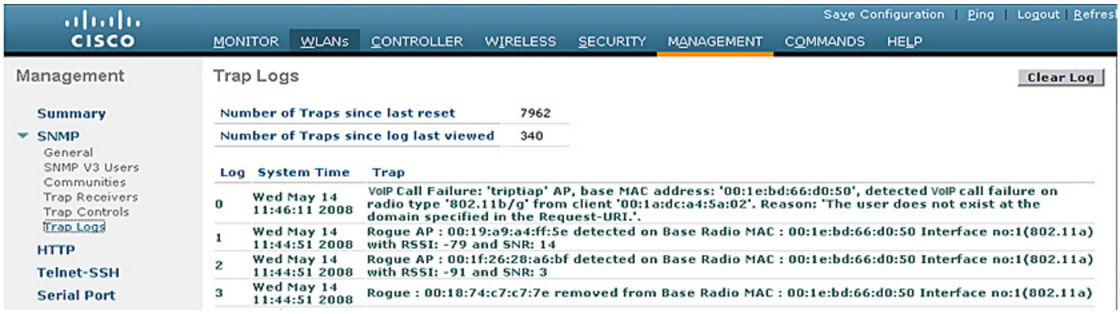
VoIP Stats

Cumulative Number of calls	0
Cumulative Time of calls	0 h 0 m 0 s

The VoIP Stats section shows the cumulative number and length of voice calls for this access point radio. Entries are added automatically when voice calls are successfully placed and deleted when the access point disassociates from the controller.

Step 8 To see the traps generated for failed calls, choose **Management** > **SNMP** > **Trap Logs**. The Trap Logs page appears (Figure 6-17).

Figure 6-17 Trap Logs Page



Trap Logs

Number of Traps since last reset	7962
Number of Traps since log last viewed	340

Log	System Time	Trap
0	Wed May 14 11:46:11 2008	VoIP Call Failure: 'triptiap' AP, base MAC address: '00:1e:bd:66:d0:50', detected VoIP call failure on radio type '802.11b/g' from client '00:1a:dc:a4:5a:02'. Reason: 'The user does not exist at the domain specified in the Request-URI.'.
1	Wed May 14 11:44:51 2008	Rogue AP : 00:19:a9:a4:ff:5e detected on Base Radio MAC : 00:1e:bd:66:d0:50 Interface no:1(802.11a) with RSSI: -79 and SNR: 14
2	Wed May 14 11:44:51 2008	Rogue AP : 00:1f:26:28:a6:bf detected on Base Radio MAC : 00:1e:bd:66:d0:50 Interface no:1(802.11a) with RSSI: -91 and SNR: 3
3	Wed May 14 11:44:51 2008	Rogue : 00:18:74:c7:c7:7e removed from Base Radio MAC : 00:1e:bd:66:d0:50 Interface no:1(802.11a)

For example, log 0 in Figure 6-17 shows that a call failed. The log provides the date and time of the call, a description of the failure, and the reason why the failure occurred.

Using the CLI to Configure VoIP Snooping

Using the controller CLI, follow these steps to configure VoIP snooping.

Step 1 To enable or disable VoIP snooping for a particular WLAN, enter this command:

config wlan call-snoop {**enable** | **disable**} *wlan_id*

Step 2 To save your changes, enter this command:

save config

Step 3 To see the status of VoIP snooping on a particular WLAN, enter this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... wpa2-psk
Network Name (SSID).............................. wpa2-psk
Status........................................... Enabled
...
    H-REAP Local Switching....................... Disabled
    H-REAP Learn IP Address...................... Enabled
    Infrastructure MFP protection............. Enabled (Global Infrastructure MFP
Disabled)
    Client MFP................................... Optional
    Tkip MIC Countermeasure Hold-down Timer....... 60
Call Snooping.................................. Enabled
```

Step 4 To see call information for an MSA client when VoIP snooping is enabled and the call is active, enter this command:

show call-control client callInfo *client_MAC_address*

Information similar to the following appears:

```
Uplink IP/port...................................... 192.11.1.71 / 23870
Downlonk IP/port.................................... 192.12.1.47 / 2070
UP.................................................. 6
Calling Party....................................... sip:1054
Called Party........................................ sip:1000
Call ID............................................. 58635b00-850161b7-14853-1501a8
Number of calls for given client is............. 1
```

Step 5 To see the metrics for successful calls or the traps generated for failed calls, enter this command:

show call-control ap {**802.11a** | **802.11b**} *Cisco_AP* {**metrics** | **traps**}

Information similar to the following appears when you enter **show call-control ap** {**802.11a** | **802.11b**} *Cisco_AP* **metrics**:

```
Total Call Duration in Seconds.................. 120
Number of Calls................................. 10
```

Information similar to the following appears when you enter **show call-control ap** {**802.11a** | **802.11b**} *Cisco_AP* **traps**:

```
Number of traps sent in one min................. 2
Last SIP error code............................. 404
Last sent trap timestamp..................... Jun 20 10:05:06
```

To aid in troubleshooting, the output of this command shows an error code for any failed calls. Table 6-2 explains the possible error codes for failed calls.

Table 6-2 Error Codes for Failed VoIP Calls

Error Code	Integer	Description
1	unknown	Unknown error.
400	badRequest	The request could not be understood because of malformed syntax.
401	unauthorized	The request requires user authentication.
402	paymentRequired	Reserved for future use.
403	forbidden	The server understood the request but refuses to fulfill it.
404	notFound	The server has information that the user does not exist at the domain specified in the Request-URI.
405	methodNotallowed	The method specified in the Request-Line is understood but not allowed for the address identified by the Request-URI.
406	notAcceptable	The resource identified by the request is only capable of generating response entities with content characteristics that are not acceptable according to the Accept header field sent in the request.
407	proxyAuthenticationRequired	The client must first authenticate with the proxy.
408	requestTimeout	The server could not produce a response within a suitable amount of time, if it could not determine the location of the user in time.
409	conflict	The request could not be completed due to a conflict with the current state of the resource.
410	gone	The requested resource is no longer available at the server, and no forwarding address is known.
411	lengthRequired	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
413	requestEntityTooLarge	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
414	requestURITooLarge	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415	unsupportedMediaType	The server is refusing to service the request because the message body of the request is in a format not supported by the server for the requested method.
420	badExtension	The server did not understand the protocol extension specified in a Proxy-Require or Require header field.
480	temporarilyNotAvailable	The callee’s end system was contacted successfully, but the callee is currently unavailable.

Table 6-2 Error Codes for Failed VoIP Calls (continued)

Error Code	Integer	Description
481	callLegDoesNotExist	The UAS received a request that does not match any existing dialog or transaction.
482	loopDetected	The server has detected a loop.
483	tooManyHops	The server received a request that contains a Max-Forwards header field with the value zero.
484	addressIncomplete	The server received a request with a Request-URI that was incomplete.
485	ambiguous	The Request-URI was ambiguous.
486	busy	The callee's end system was contacted successfully, but the callee is currently not willing or able to take additional calls at this end system.
500	internalServerError	The server encountered an unexpected condition that prevented it from fulfilling the request.
501	notImplemented	The server does not support the functionality required to fulfill the request.
502	badGateway	The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
503	serviceUnavailable	The server is temporarily unable to process the request because of a temporary overloading or maintenance of the server.
504	serverTimeout	The server did not receive a timely response from an external server it accessed in attempting to process the request.
505	versionNotSupported	The server does not support or refuses to support the SIP protocol version that was used in the request.
600	busyEverywhere	The callee's end system was contacted successfully, but the callee is busy or does not want to take the call at this time.
603	decline	The callee's machine was contacted successfully, but the user does not want to or cannot participate.
604	doesNotExistAnywhere	The server has information that the user indicated in the Request-URI does not exist anywhere.
606	notAcceptable	The user's agent was contacted successfully, but some aspects of the session description (such as the requested media, bandwidth, or addressing style) were not acceptable.

Note If you experience any problems with VoIP snooping, enter this command to debug all VoIP messages or events: **debug call-control** {**all** | **event**} {**enable** | **disable**}.

Configuring IPv6 Bridging

Internet Protocol version 6 (IPv6) is the next-generation network layer Internet protocol intended to replace version 4 (IPv4) in the TCP/IP suite of protocols. This new version increases Internet global address space to accommodate users and applications that require unique global IP addresses. IPv6 incorporates 128-bit source and destination addresses, providing significantly more addresses than the 32-bit IPv4 addresses. Follow the instructions in this section to configure a WLAN for IPv6 bridging using either the controller GUI or CLI.

Guidelines for Using IPv6 Bridging

Follow these guidelines when using IPv6 bridging:

- To use IPv6 bridging, multicast must be enabled on the controller.
- Hybrid-REAP with central switching is supported for use with IPv6 bridging. Hybrid-REAP with local switching is not supported.
- Auto-anchor mobility is not supported for use with IPv6 bridging.
- If symmetric mobility tunneling is enabled, all IPv4 traffic is bidirectionally tunneled to and from the client, but the IPv6 client traffic is bridged locally.
- Clients must support IPv6 with either static stateless auto-configuration (such as Windows XP clients) or stateful DHCPv6 IP addressing (such as Windows Vista clients).

  Note Currently, DHCPv6 is supported for use only with Windows Vista clients. For these clients, you must manually renew the DHCPv6 IP address after the client changes VLANs.

  Note Dynamic VLAN function on IPV6 bridging environment is not supported in this release.

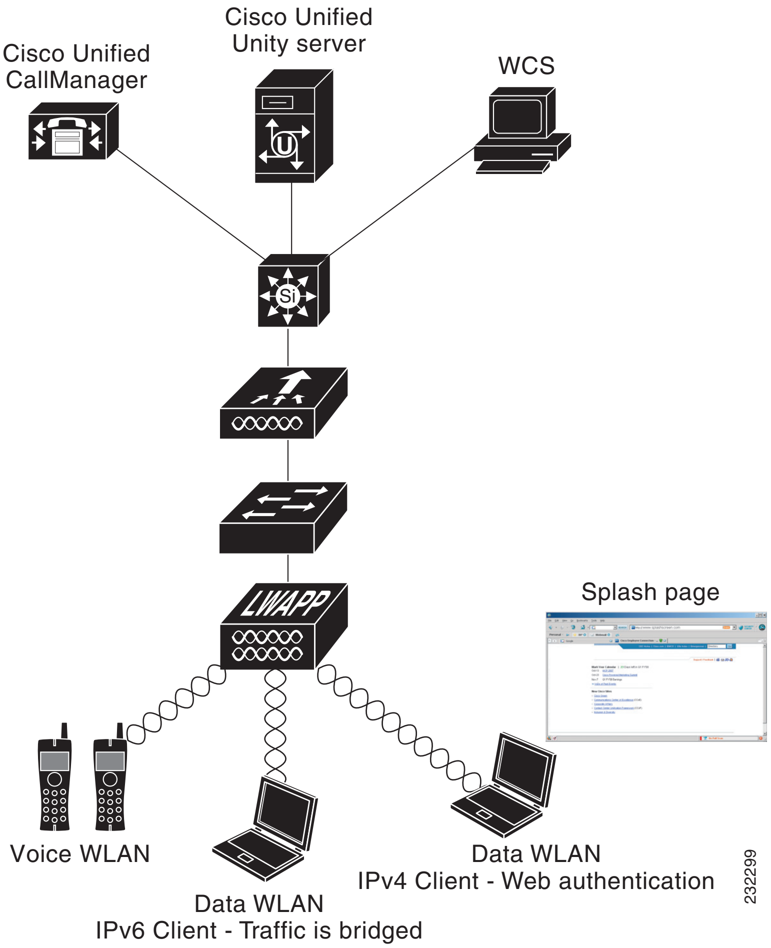
- For stateful DHCPv6 IP addressing to operate properly, you need a switch or router that supports the DHCP for IPv6 feature (such as the Cisco Catalyst 3750 switch) and is configured to act like a DHCPv6 server, or you need a dedicated server such as a Windows 2008 server with a built-in DHCPv6 server.

  Note To load the SDM IPv6 template in the Cisco Catalyst 3750 switch, enter this command and then reset the switch: **sdm prefer dual-ipv4-and-v6 default**. For more information, refer to the Cisco Catalyst 3750 switch configuration guide for Cisco IOS Release 12.2(46)SE.

- In controller software release 4.2 or later, you can enable IPv6 bridging and IPv4 web authentication on the same WLAN, a combination that previously was not supported. The controller bridges IPv6 traffic from all clients on the WLAN while IPv4 traffic goes through the normal web authentication process. The controller begins bridging IPv6 as soon as the client associates and even before web authentication for IPv4 clients is complete. No other Layer 2 or Layer 3 security policy configuration is supported on the WLAN when both IPv6 bridging and web authentication are enabled. Figure 6-18 illustrates how IPv6 bridging and IPv4 web authentication can be used on the same WLAN.

- In controller software release 6.0, all Layer 2 security policies are supported and can be configured when you enable IPv6 bridging on a WLAN.

Figure 6-18 IPv6 Bridging and IPv4 Web Authentication



Note The Security Policy Completed field in both the controller GUI and CLI shows “No for IPv4 (bridging allowed for IPv6)” until web authentication is completed. You can view this field from the Clients > Detail page on the GUI or from the **show client detail** CLI command.

Using the GUI to Configure IPv6 Bridging

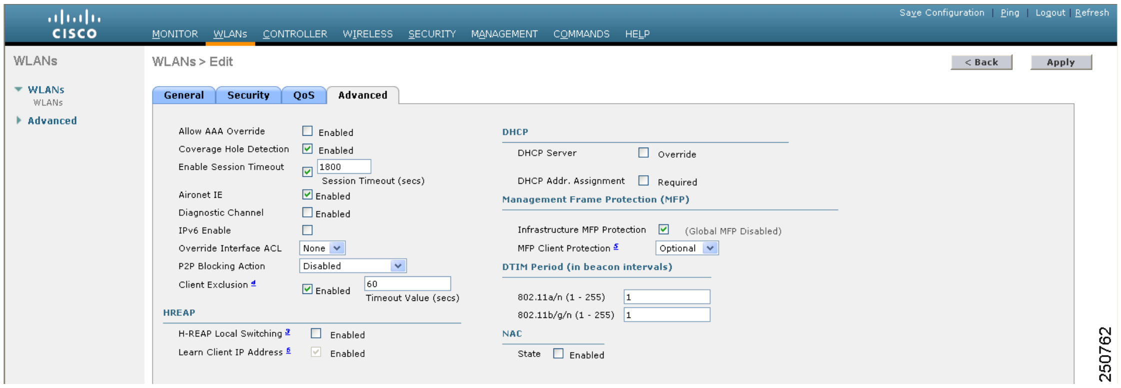
Follow these steps to configure a WLAN for IPv6 bridging using the GUI.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Choose the **Advanced** tab to open the WLANs > Edit (Advanced tab) page (see Figure 6-19).

Figure 6-19 WLANs > Edit (Advanced) Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced
250762

WLANs > Edit

Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] ☑ Enabled 60 Timeout Value (secs)

HREAP

H-REAP Local Switching [3] □ Enabled
Learn Client IP Address [6] ☑ Enabled

DHCP

DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)

Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC

State □ Enabled

Step 4 Check the **IPv6 Enable** check box if you want to enable clients that connect to this WLAN to accept IPv6 packets. Otherwise, leave the check box unchecked, which is the default value.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Using the CLI to Configure IPv6 Bridging

To configure a WLAN for IPv6 bridging using the CLI, enter this command:

config wlan IPv6support {**enable** | **disable**} *wlan_id*

The default value is disabled.

Configuring Cisco Client Extensions

Cisco Client Extensions (CCX) software is licensed to manufacturers and vendors of third-party client devices. The CCX code resident on these clients enables them to communicate wirelessly with Cisco access points and to support Cisco features that other client devices do not, including those related to increased security, enhanced performance, fast roaming, and superior power management.

The 4.2 or later release of controller software supports CCX versions 1 through 5, which enables controllers and their access points to communicate wirelessly with third-party client devices that support CCX. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. However, you can configure a specific CCX feature per WLAN. This feature is Aironet information elements (IEs).

If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

Follow the instructions in this section to configure a WLAN for the CCX Aironet IE feature and to see the CCX version supported by specific client devices using either the GUI or the CLI.

Using the GUI to Configure CCX Aironet IEs

Follow these steps to configure a WLAN for CCX Aironet IEs using the GUI.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.

Step 3 Choose the **Advanced** tab to open the WLANs > Edit (Advanced tab) page (see Figure 6-19).

Step 4 Check the **Aironet IE** check box if you want to enable support for Aironet IEs for this WLAN. Otherwise, uncheck this check box. The default value is enabled (or checked).

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

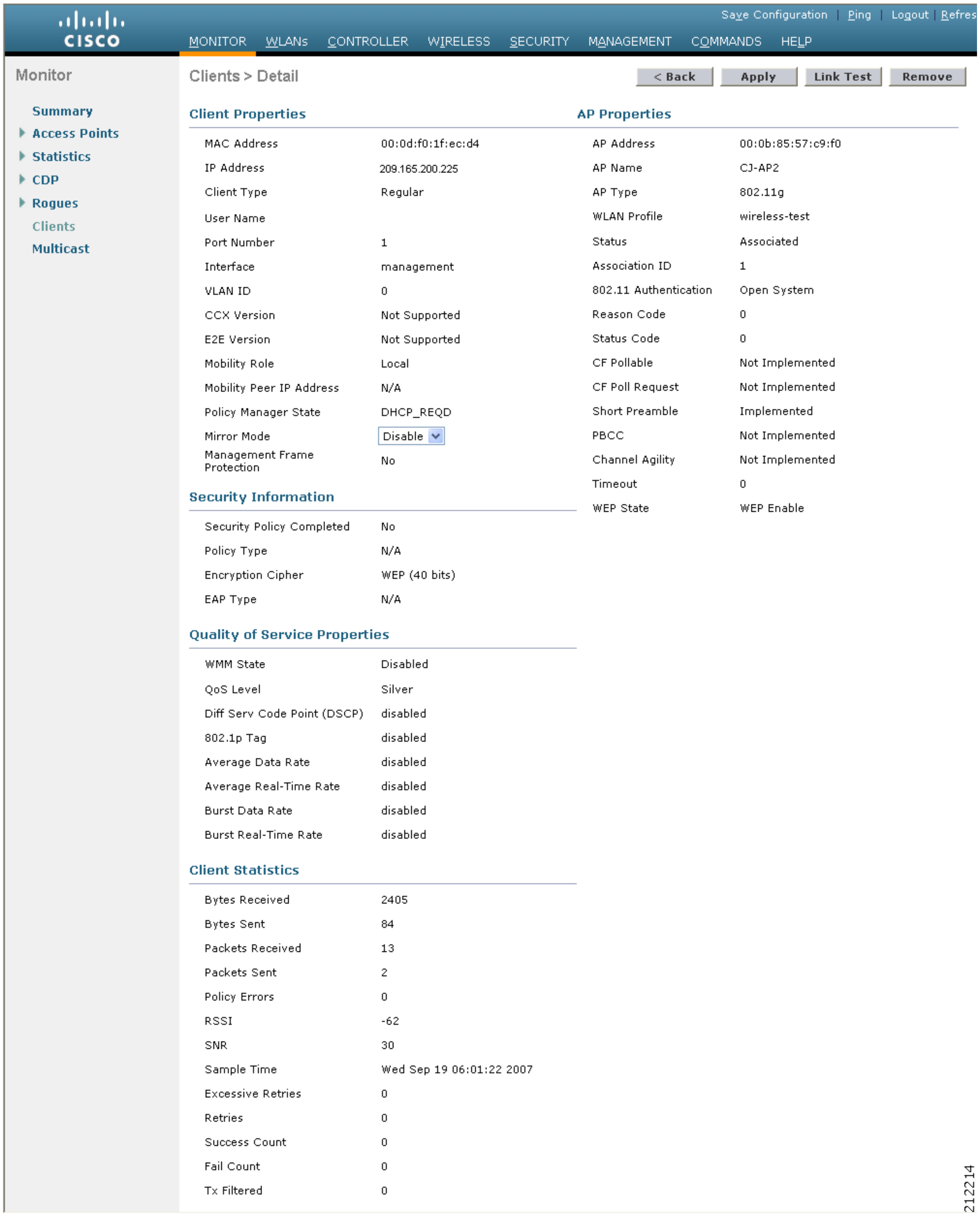
Using the GUI to View a Client's CCX Version

A client device sends its CCX version in association request packets to the access point. The controller then stores the client's CCX version in its database and uses it to limit the features for this client. For example, if a client supports CCX version 2, the controller does not allow the client to use CCX version 4 features. Follow these steps to see the CCX version supported by a particular client device using the GUI.

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

Step 2 Click the MAC address of the desired client device to open the Clients > Detail page (see Figure 6-20).

Figure 6-20 Clients > Detail Page


Save Configuration | Ping | Logout | Refres
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Access Points
Statistics
CDP
Rogues
Clients
Multicast
< Back
Apply
Link Test
Remove
212214

Clients > Detail

Client Properties

MAC Address	00:0d:f0:1f:ec:d4
IP Address	209.165.200.225
Client Type	Regular
User Name	
Port Number	1
Interface	management
VLAN ID	0
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	DHCP_REQD
Mirror Mode	Disable
Management Frame Protection	No

AP Properties

AP Address	00:0b:85:57:c9:f0
AP Name	CJ-AP2
AP Type	802.11g
WLAN Profile	wireless-test
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	No
Policy Type	N/A
Encryption Cipher	WEP (40 bits)
EAP Type	N/A

Quality of Service Properties

WMM State	Disabled
QoS Level	Silver
Diff Serv Code Point (DSCP)	disabled
802.1p Tag	disabled
Average Data Rate	disabled
Average Real-Time Rate	disabled
Burst Data Rate	disabled
Burst Real-Time Rate	disabled

Client Statistics

Bytes Received	2405
Bytes Sent	84
Packets Received	13
Packets Sent	2
Policy Errors	0
RSSI	-62
SNR	30
Sample Time	Wed Sep 19 06:01:22 2007
Excessive Retries	0
Retries	0
Success Count	0
Fail Count	0
Tx Filtered	0

The CCX Version field shows the CCX version supported by this client device. *Not Supported* appears if the client does not support CCX.

Step 3 Click **Back** to return to the previous screen.

Step 4 Repeat this procedure to view the CCX version supported by any other client devices.

Using the CLI to Configure CCX Aironet IEs

To enable or disable support for Aironet IEs for a particular WLAN, enter this command:

config wlan ccx aironet-ie {**enable** | **disable**} *wlan_id*

The default value is enabled.

Using the CLI to View a Client's CCX Version

To see the CCX version supported by a particular client device, enter this command:

show client detail *client_mac*

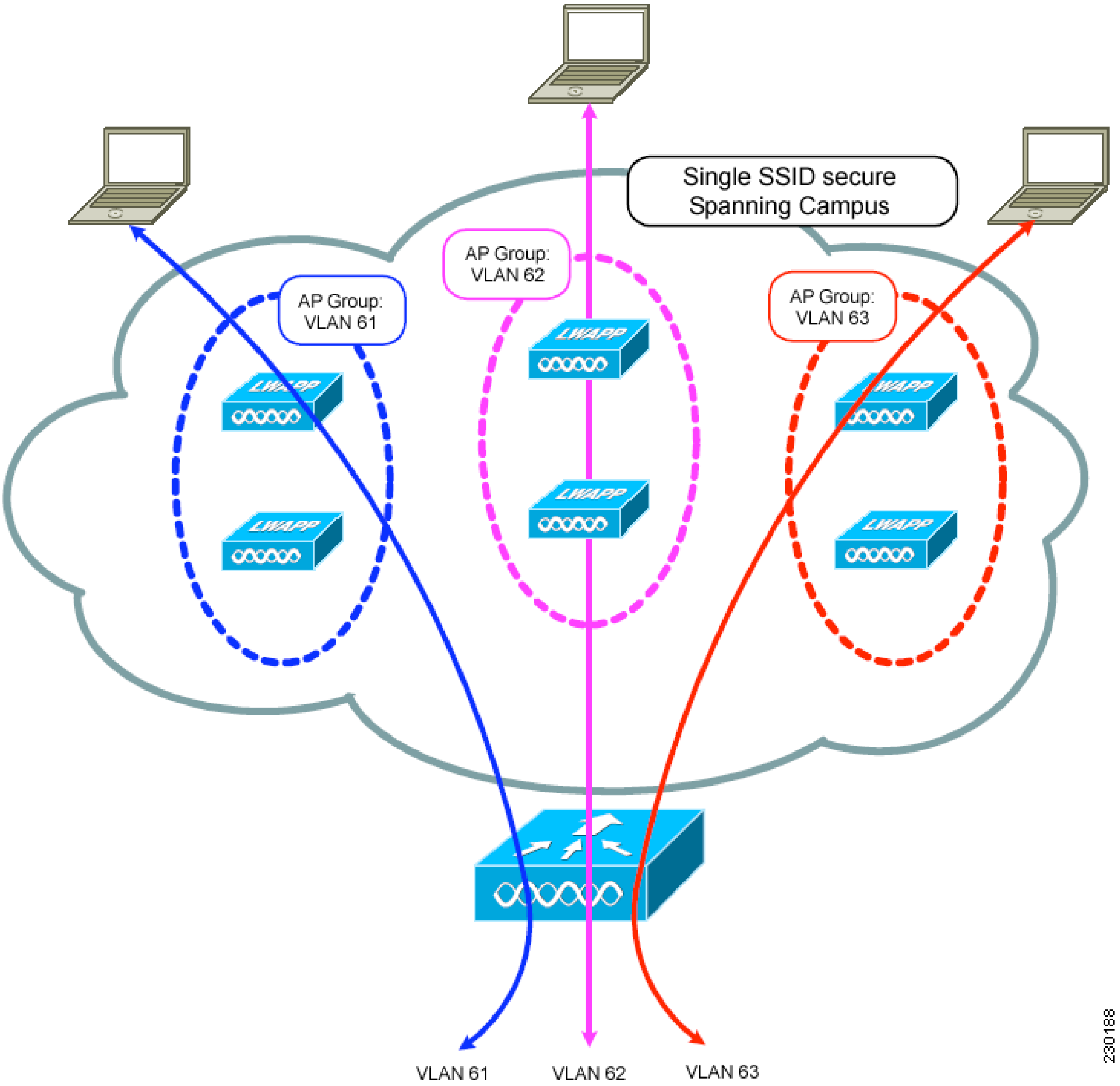
Configuring Access Point Groups

After you create up to 512 WLANs on the controller, you can selectively publish them (using access point groups) to different access points to better manage your wireless network. In a typical deployment, all users on a WLAN are mapped to a single interface on the controller. Therefore, all users associated with that WLAN are on the same subnet or VLAN. However, you can choose to distribute the load among several interfaces or to a group of users based on specific criteria such as individual departments (such as Marketing) by creating access point groups. Additionally, these access point groups can be configured in separate VLANs to simplify network administration, as illustrated in Figure 6-21.

Note The required access control list (ACL) must be defined on the router that serves the VLAN or subnet.

Note Multicast traffic is supported with access point group VLANs. However, if the client roams from one access point to another, the client might stop receiving multicast traffic, unless IGMP snooping is enabled.

Figure 6-21 Access Point Groups



In Figure 6-21, three configured dynamic interfaces are mapped to three different VLANs (VLAN 61, VLAN 62, and VLAN 63). Three access point groups are defined, and each is a member of a different VLAN, but all are members of the same SSID. A client within the wireless SSID is assigned an IP address from the VLAN subnet on which its access point is a member. For example, any user that associates with an access point that is a member of access point group VLAN 61 is assigned an IP address from that subnet.

In the example in Figure 6-21, the controller internally treats roaming between access points as a Layer 3 roaming event. In this way, WLAN clients maintain their original IP addresses.

Note Suppose the interface mapping for a WLAN in the AP group table is the same as the WLAN interface. If the WLAN interface is changed, then the interface mapping for the WLAN in the AP group table will also change to the new WLAN interface.

Suppose the interface mapping for a WLAN in the AP group table is different from the one defined for the WLAN. If the WLAN interface is changed, then the interface mapping for the WLAN in the AP group table will not be changed to the new WLAN interface.

To configure access point groups, follow these top-level steps:

1. Configure the appropriate dynamic interfaces and map them to the desired VLANs.

   For example, to implement the network in Figure 6-21, create dynamic interfaces for VLANs 61, 62, and 63 on the controller. Refer to the *Configuring Ports and Interfaces* chapter for information on how to configure dynamic interfaces.

2. Create the access point groups. Refer to the "Creating Access Point Groups" section below.

3. Assign access points to the appropriate access point groups. Refer to the "Creating Access Point Groups" section below.

Creating Access Point Groups

After all access points have joined the controller, you can create access point groups and assign up to 16 WLANs to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point does not advertise disabled WLANs in its access point group or WLANs that belong to another group.

You can create up to 50 access point groups for 2100 series controllers and controller network modules and up to 192 access point groups for 4400 series controllers, 5500 series controllers, the Cisco WiSM, and the 3750G wireless LAN controller switch.

Note All OfficeExtend access points should be in the same access point group, and that group should contain no more than 15 WLANs. A controller with OfficeExtend access points in an access point group publishes only up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID.

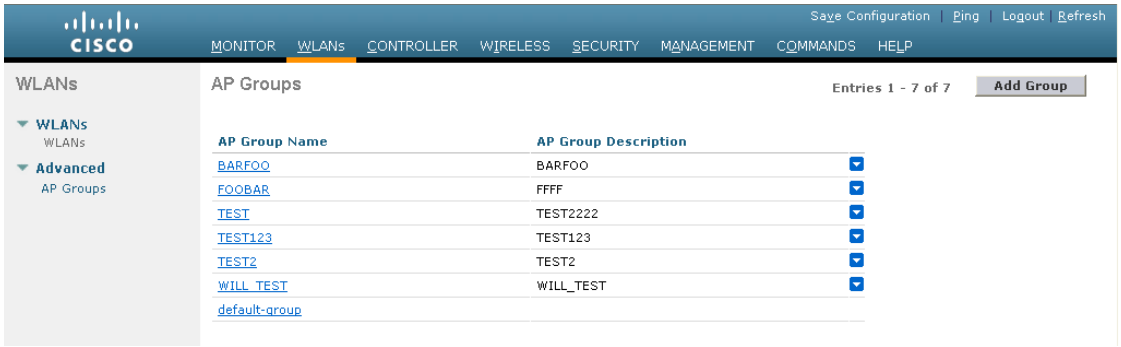
Note If you clear the configuration on the controller, all of the access point groups disappear except for the default access point group "default-group," which is created automatically.

Using the GUI to Create Access Point Groups

Using the controller GUI, follow these steps to create an access point group.

Step 1 Choose **WLANs** > **Advanced** > **AP Groups** to open the AP Groups page (see Figure 6-22).

Figure 6-22 AP Groups Page


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
AP Groups
AP Groups
Entries 1 - 7 of 7
Add Group
250726

AP Group Name	AP Group Description
BARFOO	BARFOO
FOOBAR	FFFF
TEST	TEST2222
TEST123	TEST123
TEST2	TEST2
WILL_TEST	WILL_TEST
default-group	

This page lists all the access point groups currently created on the controller. By default, all access points belong to the default access point group “default-group,” unless you assign them to other access point groups.

Note When you upgrade to controller software release 5.2 or later, the controller creates the default-group access point group and automatically populates it with the first 16 WLANs (WLANs with IDs 1 through 16, or fewer if 16 WLANs are not configured). This default group cannot be modified (you cannot add WLANs to it nor delete WLANs from it). It is dynamically updated whenever the first 16 WLANs are added or deleted. If an access point does not belong to an access point group, it is assigned to the default group and uses the WLANs in that group. If an access point joins the controller with an undefined access point group name, the access point keeps its group name but uses the WLANs in the default-group access point group.

Step 2 Click **Add Group** to create a new access point group. The Add New AP Group section appears at the top of the page.

Step 3 In the AP Group Name field, enter the group’s name.

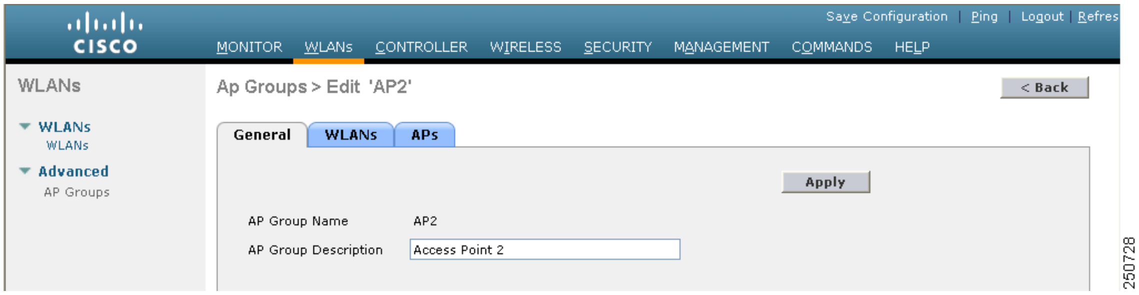
Step 4 In the Description field, enter the group’s description.

Step 5 Click **Add**. The newly created access point group appears in the list of access point groups on the AP Groups page.

Note If you ever want to delete this group, hover your cursor over the blue drop-down arrow for the group and choose **Remove**. An error message appears if you try to delete an access point group that is used by at least one access point. Before deleting an access point group in controller software release 6.0, move all access points in the group to another group. The access points are not moved to the default-group access point group as in previous releases.

Step 6 To edit this new group, click the name of the group. The AP Groups > Edit (General) page appears (see Figure 6-23).

Figure 6-23 AP Groups > Edit (General) Page



Ap Groups > Edit 'AP2'

AP Group Name AP2

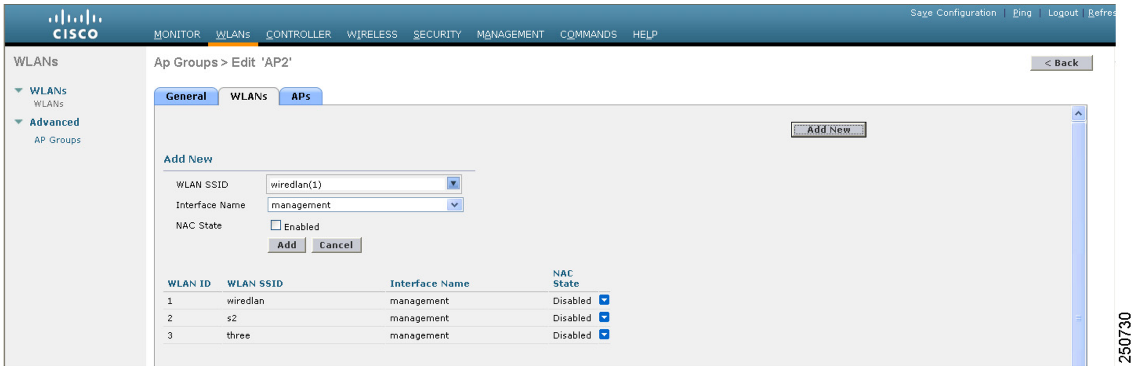
AP Group Description Access Point 2

Step 7 To change the description of this access point group, enter the new text in the AP Group Description field and click **Apply**.

Step 8 Choose the **WLANs** tab to open the AP Groups > Edit (WLANs) page. This page lists the WLANs that are currently assigned to this access point group.

Step 9 Click **Add New** to assign a WLAN to this access point group. The Add New section appears at the top of the page (see Figure 6-24).

Figure 6-24 AP Groups > Edit (WLANs) Page



Ap Groups > Edit 'AP2'

Add New

WLAN SSID wiredlan(1)

Interface Name management

NAC State □ Enabled

WLAN ID	WLAN SSID	Interface Name	NAC State
1	wiredlan	management	Disabled
2	s2	management	Disabled
3	three	management	Disabled

Step 10 From the WLAN SSID drop-down box, choose the SSID of the WLAN.

Step 11 From the Interface Name drop-down box, choose the interface to which you want to map the access point group. Choose the quarantine VLAN if you plan to enable network admission control (NAC) out-of-band support.

Note The interface name in the default-group access point group matches the WLAN interface.

Step 12 To enable NAC out-of-band support for this access point group, check the **NAC State** check box. To disable NAC out-of-band support, leave the check box unchecked, which is the default value. Refer to the "Configuring NAC Out-of-Band Integration" section on page 6-66 for more information on NAC.

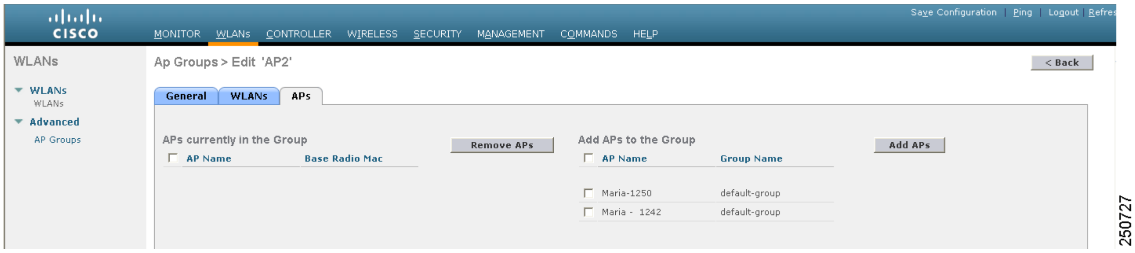
Step 13 Click **Add** to add this WLAN to the access point group. This WLAN appears in the list of WLANs that are assigned to this access point group.

Note If you ever want to remove this WLAN from the access point group, hover your cursor over the blue drop-down arrow for the WLAN and choose **Remove**.

Step 14 Repeat Step 9 through Step 13 to add any additional WLANs to this access point group.

Step 15 Choose the **APs** tab to assign access points to this access point group. The AP Groups > Edit (APs) page lists the access points that are currently assigned to this group as well as any access points that are available to be added to the group. If an access point is not currently assigned to a group, its group name appears as "default-group" (see Figure 6-25).

Figure 6-25 AP Groups > Edit (APs) Page



Ap Groups > Edit 'AP2'

APs currently in the Group

☐ AP Name	Base Radio Mac

Add APs to the Group

☐ AP Name	Group Name
☐ Maria-1250	default-group
☐ Maria - 1242	default-group

Step 16 To add an access point to this access point group, check the check box to the left of the access point name and click **Add APs**. The access point now appears in the list of access points currently in this access point group.

Note To select all of the available access points at once, check the **AP Name** check box. All of the access points are then selected.

Note If you ever want to remove an access point from the group, check the check box to the left of the access point name and click **Remove APs**. To select all of the access points at once, check the **AP Name** check box. All of the access points are then removed from this group.

Note If you ever want to change the access point group to which an access point belongs, choose **Wireless** > **Access Points** > **All APs** > *ap_name* > **Advanced** tab, choose the name of another access point group from the **AP Group Name** drop-down box, and click **Apply**.

Step 17 Click **Save Configuration** to save your changes.

Using the CLI to Create Access Point Groups

Using the controller CLI, follow these steps to create access point groups.

Step 1 To create an access point group, enter this command:

config wlan apgroup add *group_name*

Note To delete an access point group, enter this command: **config wlan apgroup delete** *group_name*. An error message appears if you try to delete an access point group that is used by at least one access point. Before deleting an access point group in controller software release 6.0, move all access points in the group to another group. The access points are not moved to the default-group access point group as in previous releases. To see the access points in a group, enter **show wlan apgroups**. To move the access points to another group, enter **config ap group-name** *group_name Cisco_AP*.

Step 2 To add a description to an access point group, enter this command:

config wlan apgroup description *group_name description*

Step 3 To assign a WLAN to an access point group, enter this command:

config wlan apgroup interface-mapping add *group_name wlan_id interface_name*

Note To remove a WLAN from an access point group, enter this command: **config wlan apgroup interface-mapping delete** *group_name wlan_id*.

Step 4 To enable or disable NAC out-of-band support for this access point group, enter this command:

config wlan apgroup nac {**enable** | **disable**} *group_name wlan_id*

Step 5 To configure a WLAN radio policy on the access point group, enter this command:

config wlan apgroup radio-policy *apgroup_name wlan-id* {**802.11a-only** | **802.11bg** | **802.11g-only** | **all**}

Step 6 To assign an access point to an access point group, enter this command:

config ap group-name *group_name Cisco_AP*

Note To remove an access point from an access point group, re-enter this command and assign the access point to another group.

Step 7 To save your changes, enter this command:

save config

Using the CLI to View Access Point Groups

Use these CLI commands to view information about or to troubleshoot access point groups.

1. To see a list of all access point groups on the controller, enter this command:

   show wlan apgroups

   Information similar to the following appears:

```
Site Name........................................ AP2
Site Description................................. Access Point 2

WLAN ID          Interface          Network Admission Control
-------         -----------        --------------------------
 1              management            Disabled
 2              management            Disabled
 3              management            Disabled
 4              management            Disabled
 9              management            Disabled
 10             management            Disabled
 11             management            Disabled
 12             management            Disabled
 13             management            Disabled
 14             management            Disabled
 15             management            Disabled
 16             management            Disabled
 18             management            Disabled

AP Name Slots AP Model      Ethernet MAC   Location Port Country Priority GroupName
------- ---- -------------- ----------------- ------- ---- ------- -------- ---------
AP1242   2   AP1242AG-A-K9 00:14:1c:ed:23:9a default  1    US       1      AP2
...
```

2. To see the BSSIDs for each WLAN assigned to an access point group, enter this command:

   show ap wlan {**802.11a** | **802.11b**} *Cisco_AP*

   Information similar to the following appears:

```
Site Name........................................ AP3
Site Description................................. Access Point 3

WLAN ID          Interface          BSSID
-------         ------------  -------------------
 10             management     00:14:1b:58:14:df
```

3. To see the number of WLANs enabled for an access point group, enter this command:

   show ap config {**802.11a** | **802.11b**} *Cisco_AP*

   Information similar to the following appears:

```
Cisco AP Identifier.............................. 166
Cisco AP Name................................. AP2
...
Station Configuration
      Configuration ............................ AUTOMATIC
      Number Of WLANs .......................... 2
...
```

4. To enable or disable debugging of access point groups, enter this command:

   debug group {**enable** | **disable**}

Configuring Web Redirect with 802.1X Authentication

You can configure a WLAN to redirect a user to a particular web page after 802.1X authentication has completed successfully. You can configure the web redirect to give the user partial or full access to the network.

Conditional Web Redirect

If you enable conditional web redirect, the user can be conditionally redirected to a particular web page after 802.1X authentication has completed successfully. You can specify the redirect page and the conditions under which the redirect occurs on your RADIUS server. Conditions might include the user's password reaching expiration or the user needing to pay his or her bill for continued usage.

If the RADIUS server returns the Cisco AV-pair "url-redirect," then the user is redirected to the specified URL upon opening a browser. If the server also returns the Cisco AV-pair "url-redirect-acl," the specified access control list (ACL) is installed as a preauthentication ACL for this client. The client is not considered fully authorized at this point and can only pass traffic allowed by the preauthentication ACL.

After the client completes a particular operation at the specified URL (for example, changing a password or paying a bill), the client must reauthenticate. When the RADIUS server does not return a "url-redirect," the client is considered fully authorized and allowed to pass traffic.

Note The conditional web redirect feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security.

After you configure the RADIUS server, you can then configure the conditional web redirect on the controller using either the controller GUI or CLI.

Splash Page Web Redirect

If you enable splash page web redirect, the user is redirected to a particular web page after 802.1X authentication has completed successfully. After the redirect, the user has full access to the network. You can specify the redirect page on your RADIUS server. If the RADIUS server returns the Cisco AV-pair "url-redirect," then the user is redirected to the specified URL upon opening a browser. The client is considered fully authorized at this point and is allowed to pass traffic, even if the RADIUS server does not return a "url-redirect."

Note The splash page web redirect feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security with 802.1x key management. Preshared key management is not supported with any Layer 2 security method.

After you configure the RADIUS server, you can then configure the splash page web redirect on the controller using either the controller GUI or CLI.

Configuring the RADIUS Server

Follow these steps to configure your RADIUS server.

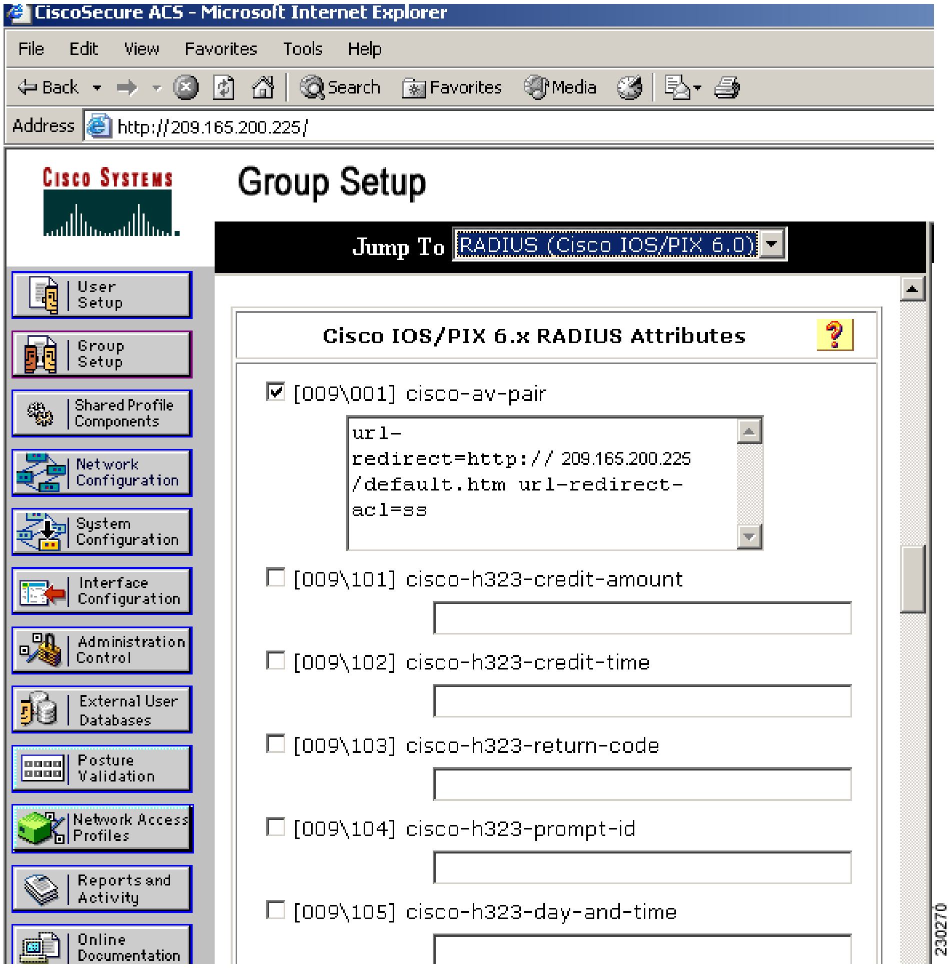
Note These instructions are specific to the CiscoSecure ACS; however, they should be similar to those for other RADIUS servers.

Step 1 From the CiscoSecure ACS main menu, choose **Group Setup**.

Step 2 Click **Edit Settings**.

Step 3 From the Jump To drop-down menu, choose **RADIUS (Cisco IOS/PIX 6.0)**. The window shown in Figure 6-26 appears.

Figure 6-26 ACS Server Configuration



Group Setup

Jump To RADIUS (Cisco IOS/PIX 6.0)

Cisco IOS/PIX 6.x RADIUS Attributes

☑ [009\001] cisco-av-pair

```
url-
redirect=http:// 209.165.200.225
/default.htm url-redirect-
acl=ss
```

☐ [009\101] cisco-h323-credit-amount

☐ [009\102] cisco-h323-credit-time

☐ [009\103] cisco-h323-return-code

☐ [009\104] cisco-h323-prompt-id

☐ [009\105] cisco-h323-day-and-time

Step 4 Check the **[009\001] cisco-av-pair** check box.

Step 5 Enter the following Cisco AV-pairs in the [009\001] cisco-av-pair edit box to specify the URL to which the user is redirected and, if configuring conditional web redirect, the conditions under which the redirect takes place, respectively:

url-redirect=http://*url*

url-redirect-acl=*acl_name*

Using the GUI to Configure Web Redirect

Using the controller GUI, follow these steps to configure conditional or splash page web redirect.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the desired WLAN. The WLANs > Edit page appears.

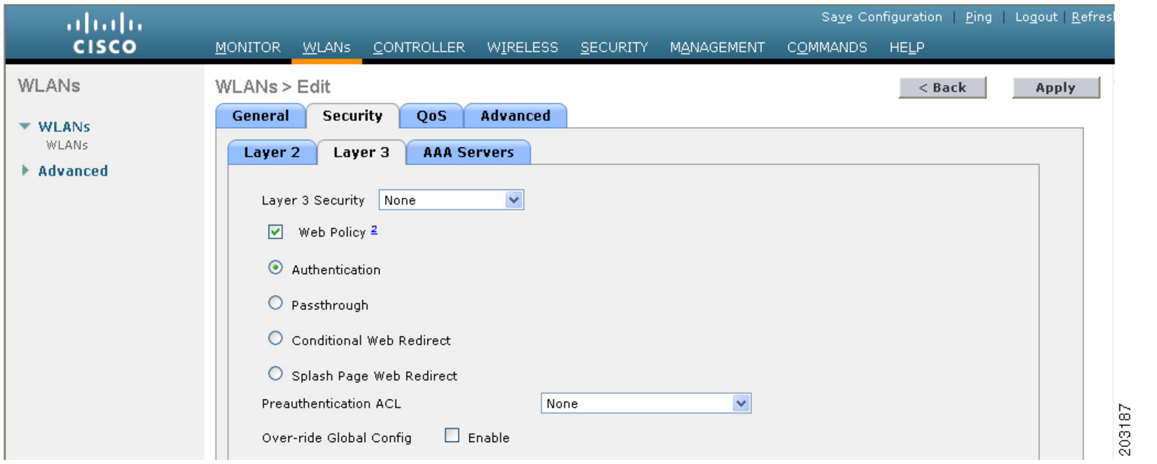
Step 3 Choose the **Security** and **Layer 2** tabs to open the WLANs > Edit (Security > Layer 2) page.

Step 4 Choose **802.1X** or **WPA+WPA2** from the Layer 2 Security drop-down box.

Step 5 Set any additional parameters for 802.1X or WPA+WPA2.

Step 6 Choose the **Layer 3** tab to open the WLANs > Edit (Security > Layer 3) page (see Figure 6-27).

Figure 6-27 WLANs > Edit (Security > Layer 3) Page



Layer 3 Security: None

☑ Web Policy 2

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

Preauthentication ACL: None

Over-ride Global Config: ☐ Enable

Step 7 Choose **None** from the Layer 3 Security drop-down box.

Step 8 Check the **Web Policy** check box.

Step 9 Choose one of the following options to enable conditional or splash page web redirect: **Conditional Web Redirect** or **Splash Page Web Redirect**. The default value is disabled for both parameters.

Step 10 If the user is to be redirected to a site external to the controller, choose the ACL that was configured on your RADIUS server from the Preauthentication ACL drop-down list.

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Using the CLI to Configure Web Redirect

Using the controller CLI, follow these steps to configure conditional or splash page web redirect.

Step 1 To enable or disable conditional web redirect, enter this command:

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

Step 2 To enable or disable splash page web redirect, enter this command:

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

Step 3 To save your settings, enter this command:

save config

Step 4 To see the status of the web redirect features for a particular WLAN, enter this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
Conditional Web Redirect......................... Disabled
Splash-Page Web Redirect......................... Enabled
...
```

Disabling Accounting Servers per WLAN

This section provides instructions for disabling all accounting servers on a WLAN. Disabling accounting servers disables all accounting operations and prevents the controller from falling back to the default RADIUS server for the WLAN.

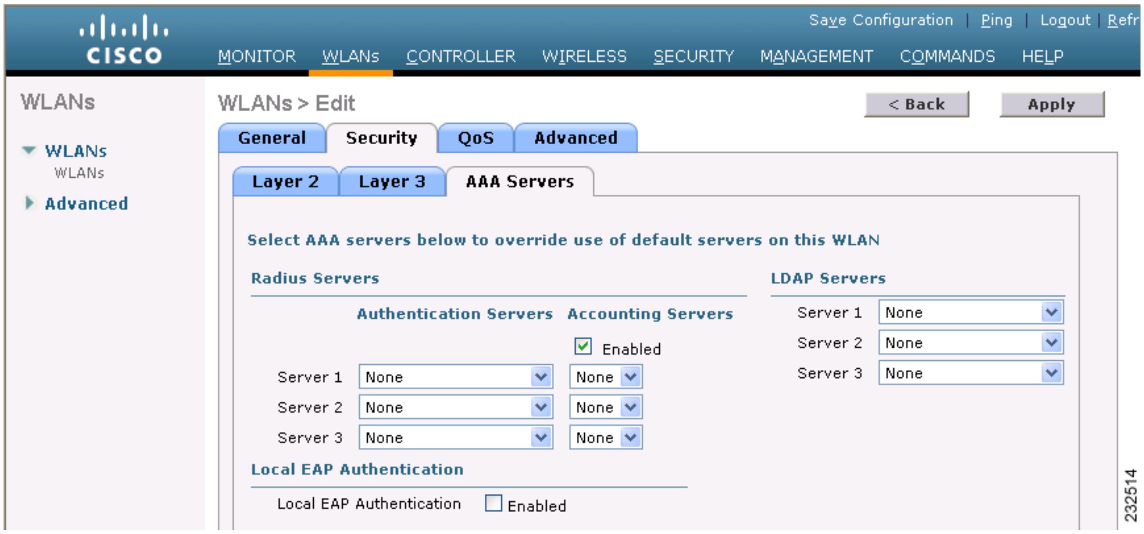
Follow these steps to disable all accounting servers for a RADIUS authentication server.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN to be modified. The WLANs > Edit page appears.

Step 3 Choose the **Security** and **AAA Servers** tabs to open the WLANs > Edit (Security > AAA Servers) page (see Figure 6-28).

Figure 6-28 WLANs > Edit (Security > AAA Servers) Page



WLANs > Edit

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

	Authentication Servers	Accounting Servers
		☑ Enabled
Server 1	None	None
Server 2	None	None
Server 3	None	None

LDAP Servers

Server 1	None
Server 2	None
Server 3	None

Local EAP Authentication

Local EAP Authentication ☐ Enabled

Step 4 Uncheck the **Enabled** check box for the Accounting Servers.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Disabling Coverage Hole Detection per WLAN

This section provides instructions for disabling coverage hole detection on a WLAN.

Coverage hole detection is enabled globally on the controller. See the "Coverage Hole Detection and Correction" section on page 11-4 and the "Using the GUI to Configure Coverage Hole Detection" section on page 11-17 for more information.

In software release 5.2 or later, you can disable coverage hole detection on a per-WLAN basis. When you disable coverage hole detection on a WLAN, a coverage hole alert is still sent to the controller, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where guests are connected to your network for short periods of time and are likely to be highly mobile.

Using the GUI to Disable Coverage Hole Detection on a WLAN

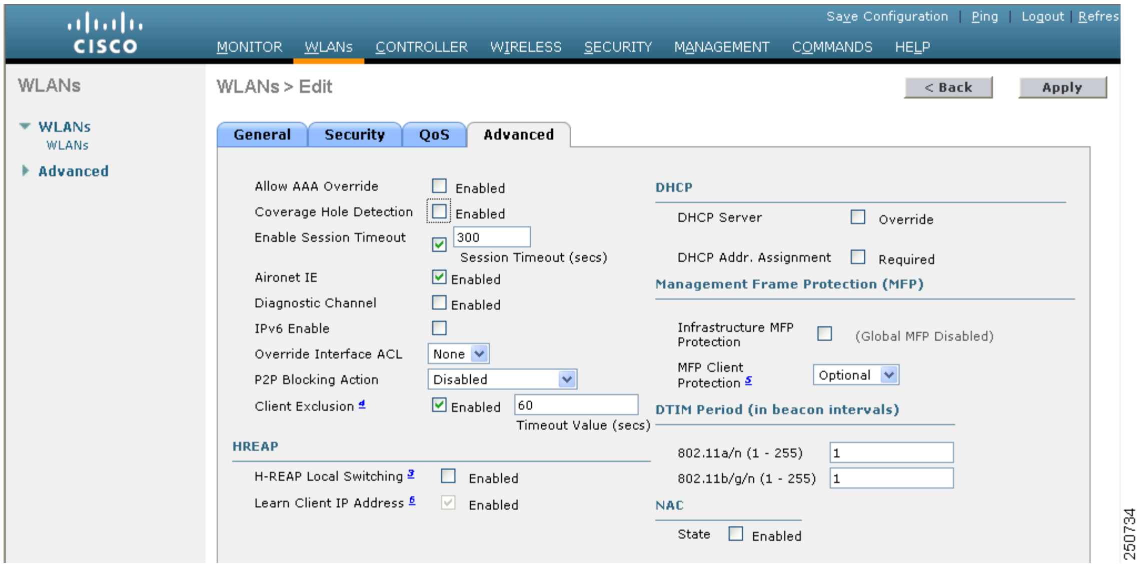
Using the controller GUI, follow these steps to disable coverage hole detection on a WLAN.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the profile name of the WLAN to be modified. The WLANs > Edit page appears.

Step 3 Choose the **Advanced** tab to display the WLANs > Edit (Advanced) page (see Figure 6-29).

Figure 6-29 WLANs > Edit (Advanced) Page


Save Configuration | Ping | Logout | Refres
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General Security QoS Advanced
250734

WLANs > Edit

Allow AAA Override □ Enabled
Coverage Hole Detection □ Enabled
Enable Session Timeout ☑ 300 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion ☑ Enabled 60 Timeout Value (secs)

HREAP

H-REAP Local Switching □ Enabled
Learn Client IP Address ☑ Enabled

DHCP

DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)

Infrastructure MFP Protection □ (Global MFP Disabled)
MFP Client Protection Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC

State □ Enabled

Step 4 Uncheck the **Coverage Hole Detection Enabled** check box.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Using the CLI to Disable Coverage Hole Detection on a WLAN

Using the controller CLI, follow these steps to disable coverage hole detection on a WLAN.

Step 1 To disable coverage hole detection on a WLAN, enter this command:

config wlan chd *wlan_id* **disable**

Step 2 To save your settings, enter this command:

save config

Step 3 To see the coverage hole detection status for a particular WLAN, enter this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 2
Profile Name..................................... wlan2
Network Name (SSID).............................. 2
. . .
CHD per WLAN................................. Disabled
```

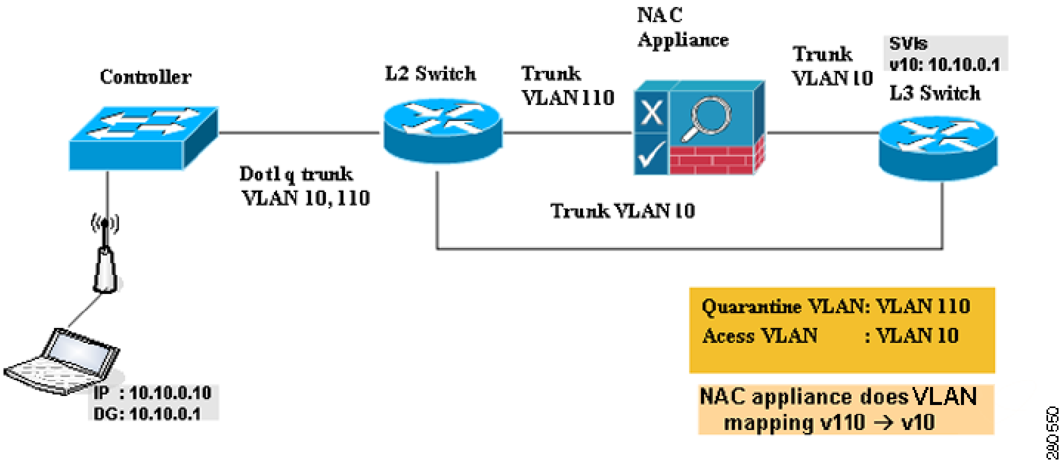
Configuring NAC Out-of-Band Integration

The Cisco NAC Appliance, also known as Cisco Clean Access (CCA), is a network admission control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether machines are compliant with security policies and repairs vulnerabilities before permitting access to the network. The NAC appliance is available in two modes: in-band and out-of-band. Customers can deploy both modes if desired, each geared toward certain types of access (in-band for supporting wireless users and out-of-band for supporting wired users, for example).

In controller software releases prior to 5.1, the controller integrates with the NAC appliance only in in-band mode, where the NAC appliance must remain in the data path. For in-band mode, a NAC appliance is required at each authentication location (such as at each branch or for each controller), and all traffic must traverse the NAC enforcement point. In controller software release 5.1 or later, the controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing.

To implement the NAC out-of-band feature on the controller, you need to enable NAC support on the WLAN or guest LAN and then map this WLAN or guest LAN to an interface that is configured with a quarantine VLAN (untrusted VLAN) and an access VLAN (trusted VLAN). When a client associates and completes Layer 2 authentication, the client obtains an IP address from the access VLAN subnet, but the client state is Quarantine. While deploying the NAC out-of-band feature, be sure that the quarantine VLAN is allowed only between the Layer 2 switch on which the controller is connected and the NAC appliance and that the NAC appliance is configured with a unique quarantine-to-access VLAN mapping. Client traffic passes into the quarantine VLAN, which is trunked to the NAC appliance. After posture validation is completed, the client is prompted to take action for remediation. After cleaning is completed, the NAC appliance updates the controller to change the client state from Quarantine to Access. Figure 6-30 provides an example of NAC out-of-band integration.

Figure 6-30 NAC Out-of-Band Integration



In Figure 6-30, the link between the controller and the switch is configured as a trunk, enabling the quarantine VLAN (110) and the access VLAN (10). On the Layer 2 switch, the quarantine traffic is trunked to the NAC appliance while the access VLAN traffic goes directly to the Layer 3 switch. Traffic that reaches the quarantine VLAN on the NAC appliance is mapped to the access VLAN based on a static mapping configuration.

Follow the instructions in this section to configure NAC out-of-band integration using either the controller GUI or CLI.

Guidelines for Using NAC Out-of-Band Integration

Follow these guidelines when using NAC out-of-band integration:

- The NAC appliance supports up to 3500 users, and the controller supports up to 5000 users. Therefore, multiple NAC appliances might need to be deployed.
- CCA software release 4.5 or later is required for NAC out-of-band integration.
- Because the NAC appliance supports static VLAN mapping, you must configure a unique quarantine VLAN for each interface configured on the controller. For example, you might configure a quarantine VLAN of 110 on controller 1 and a quarantine VLAN of 120 on controller 2. However, if two WLANs or guest LANs use the same distribution system interface, they must use the same quarantine VLAN, provided they have one NAC appliance deployed in the network. The NAC appliance supports unique quarantine-to-access VLAN mapping.
- For posture reassessment based on session expiry, you must configure the session timeout on both the NAC appliance and the WLAN, making sure that the session expiry on the WLAN is greater than that on the NAC appliance.
- When a session timeout is configured on an open WLAN, the timing out of clients in the Quarantine state is determined by the timer on the NAC appliance. Once the session timeout expires for WLANs using web authentication, clients deauthenticate from the controller and must perform posture validation again.

- NAC out-of-band integration is supported only on WLANs configured for hybrid-REAP central switching. It is not supported for use on WLANs configured for hybrid-REAP local switching.

  Note Refer to the *Configuring Hybrid REAP* chapter for more information on hybrid REAP.

- If you want to enable NAC on an access point group VLAN, you must first enable NAC on the WLAN. Then you can enable or disable NAC on the access point group VLAN. If you ever decide to disable NAC on the WLAN, be sure to disable it on the access point group VLAN as well.
- NAC out-of-band integration is not supported for use with the WLAN AAA override feature.
- All Layer 2 and Layer 3 authentication occurs in the quarantine VLAN. To use external web authentication, you must configure the NAC appliance to allow HTTP traffic to and from external web servers and to allow the redirect URL in the quarantine VLAN.

  Note Refer to the Cisco NAC appliance configuration guides for configuration instructions: http://www.cisco.com/c/en/us/support/security/nac-appliance-clean-access/products-installation-and-configuration-guides-list.html

Using the GUI to Configure NAC Out-of-Band Integration

Using the controller GUI, follow these steps to configure NAC out-of-band integration.

Step 1 To configure the quarantine VLAN for a dynamic interface, follow these steps:

a. Choose **Controller** > **Interfaces** to open the Interfaces page.

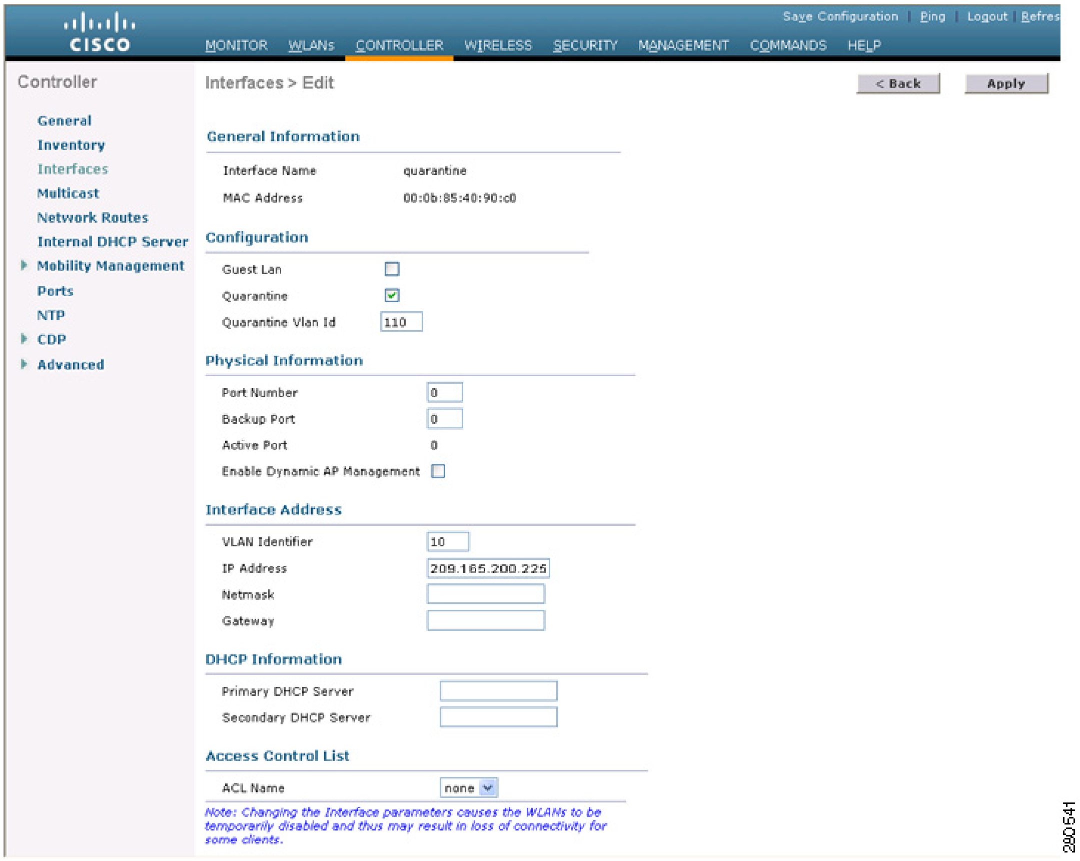
b. Click **New** to create a new dynamic interface.

c. In the Interface Name field, enter a name for this interface, such as “quarantine.”

d. In the VLAN ID field, enter a non-zero value for the access VLAN ID, such as “10.”

e. Click **Apply** to commit your changes. The Interfaces > Edit page appears (see Figure 6-31).

Figure 6-31 Interfaces > Edit Page



Interfaces > Edit

General Information

Interface Name quarantine

MAC Address 00:0b:85:40:90:c0

Configuration

Guest Lan □

Quarantine ☑

Quarantine Vlan Id 110

Physical Information

Port Number 0

Backup Port 0

Active Port 0

Enable Dynamic AP Management □

Interface Address

VLAN Identifier 10

IP Address 209.165.200.225

Netmask

Gateway

DHCP Information

Primary DHCP Server

Secondary DHCP Server

Access Control List

ACL Name none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

f. Check the **Quarantine** check box and enter a non-zero value for the quarantine VLAN ID, such as “110.”

Note Cisco recommends that you configure unique quarantine VLANs throughout your network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in the same subnet, it is mandatory to have the same quarantine VLAN if there is only one NAC appliance in the network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in different subnets, it is mandatory to have different quarantine VLANs if there is only one NAC appliance in the network.

g. Configure any remaining fields for this interface, such as the IP address, netmask, and default gateway.

h. Click **Apply** to save your changes.

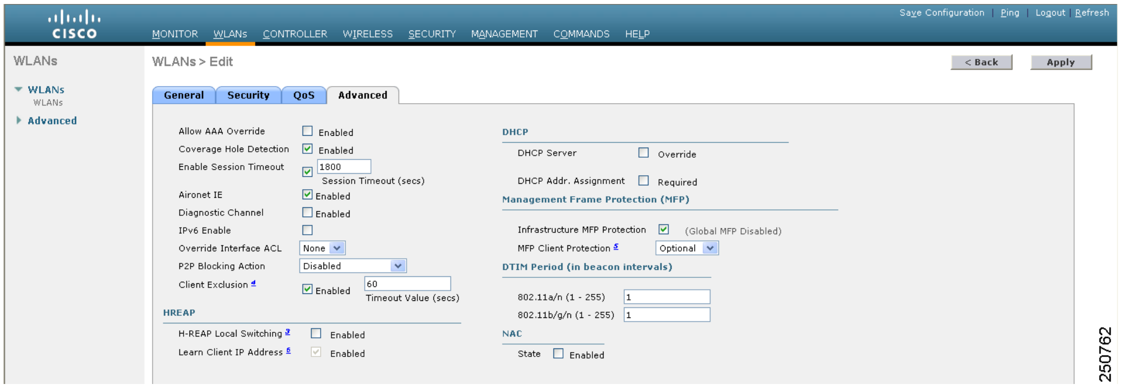
Step 2 To configure NAC out-of-band support on a WLAN or guest LAN, follow these steps:

a. Choose **WLANs** to open the WLANs page.

b. Click the ID number of the desired WLAN or guest LAN. The WLANs > Edit page appears.

c. Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page (see Figure 6-32).

Figure 6-32 WLANs > Edit (Advanced) Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General
Security
QoS
Advanced
250762

Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion [4] ☑ Enabled 60 Timeout Value (secs)

HREAP
H-REAP Local Switching [2] □ Enabled
Learn Client IP Address [5] ☑ Enabled

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)
Infrastructure MFP Protection ☑ (Global MFP Disabled)
MFP Client Protection [5] Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
State □ Enabled

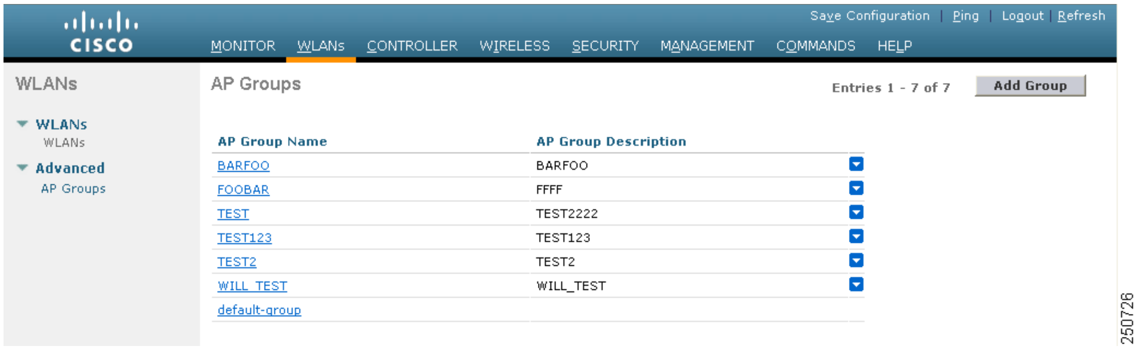
d. To configure NAC out-of-band support for this WLAN or guest LAN, check the **NAC State** check box. To disable NAC out-of-band support, leave the check box unchecked, which is the default value.

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

Step 3 To configure NAC out-of-band support for a specific access point group, follow these steps:

a. Choose **WLANs** > **Advanced** > **AP Groups** to open the AP Groups page (see Figure 6-33).

Figure 6-33 AP Groups Page


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
AP Groups
AP Groups
Entries 1 - 7 of 7
Add Group
250726

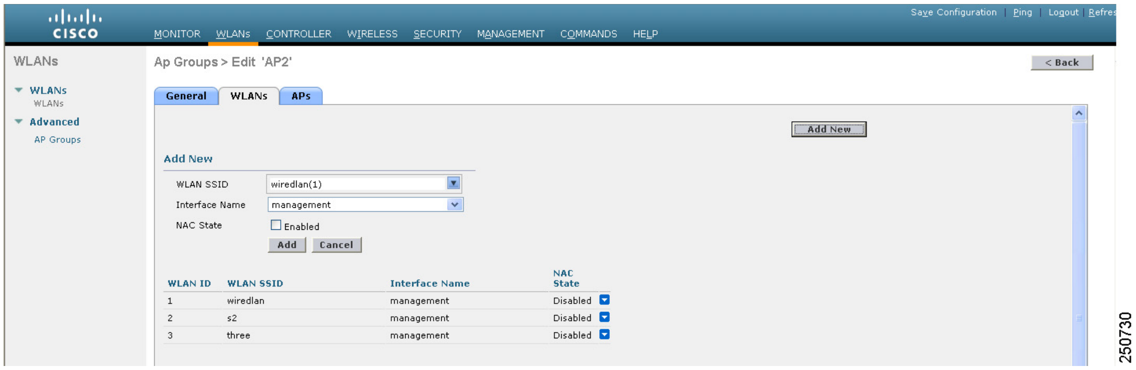
AP Group Name	AP Group Description
BARFOO	BARFOO
FOOBAR	FFFF
TEST	TEST2222
TEST123	TEST123
TEST2	TEST2
WILL_TEST	WILL_TEST
default-group	

b. Click the name of the desired access point group.

c. Choose the **WLANs** tab to open the AP Groups > Edit (WLANs) page.

d. Click **Add New** to assign a WLAN to this access point group. The Add New section appears at the top of the page (see Figure 6-34).

Figure 6-34 AP Groups > Edit (WLANs) Page



Ap Groups > Edit 'AP2'

Add New

WLAN SSID	wiredlan(1)
Interface Name	management
NAC State	□ Enabled

WLAN ID	WLAN SSID	Interface Name	NAC State
1	wiredlan	management	Disabled
2	s2	management	Disabled
3	three	management	Disabled

e. From the WLAN SSID drop-down box, choose the SSID of the WLAN.

f. From the Interface Name drop-down box, choose the interface to which you want to map the access point group. Choose the quarantine VLAN if you plan to enable NAC out-of-band support.

g. To enable NAC out-of-band support for this access point group, check the **NAC State** check box. To disable NAC out-of-band support, leave the check box unchecked, which is the default value.

h. Click **Add** to add this WLAN to the access point group. This WLAN appears in the list of WLANs assigned to this access point group.

Note If you ever want to remove this WLAN from the access point group, hover your cursor over the blue drop-down arrow for the WLAN and choose **Remove**.

Step 4 Click **Save Configuration** to save your changes.

Step 5 To see the current state of the client (either Quarantine or Access), follow these steps:

a. Choose **Monitor** > **Clients** to open the Clients page.

b. Click the MAC address of the desired client to open the Clients > Detail page. The NAC state appears under the Security Information section.

Note The client state appears as "Invalid" if the client is probing, has not yet associated to a WLAN, or cannot complete Layer 2 authentication.

Using the CLI to Configure NAC Out-of-Band Integration

Using the controller CLI, follow these steps to configure NAC out-of-band integration.

Step 1 To configure the quarantine VLAN for a dynamic interface, enter this command:

config interface quarantine vlan *interface_name vlan_id*

Note You must configure a unique quarantine VLAN for each interface on the controller.

Note To disable the quarantine VLAN on an interface, enter **0** for the VLAN ID.

Step 2 To enable or disable NAC out-of-band support for a WLAN or guest LAN, enter this command:

config {**wlan** | **guest-lan**} **nac** {**enable** | **disable**} {*wlan_id* | *guest_lan_id*}

Step 3 To enable or disable NAC out-of-band support for a specific access point group, enter this command:

config wlan apgroup nac {**enable** | **disable**} *group_name wlan_id*

Step 4 To save your changes, enter this command:

save config

Step 5 To see the configuration of a WLAN or guest LAN, including the NAC state, enter this command:

show {**wlan** *wlan_ id* | **guest-lan** *guest_lan_id*}

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... wlan
Network Name (SSID).............................. wlan
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Network Admission Control

  NAC-State...................................... Enabled
  Quarantine VLAN............................. 110
...
```

Step 6 To see the current state of the client (either Quarantine or Access), enter this command:

show client detailed *client_mac*

Information similar to the following appears:

```
Client's NAC state................................. QUARANTINE
```

Note The client state appears as “Invalid” if the client is probing, has not yet associated to a WLAN, or cannot complete Layer 2 authentication.