CHAPTER 10

Configuring Controllers and Switches

This chapter describes how to configure controllers and switches in the Cisco WCS database. This chapter contains the following sections:

- Adding Controllers, page 10-2
- Downloading Software to Controllers, page 10-5
- Discovering Templates from Controllers, page 10-9
- Displaying Templates Applied to Controller, page 10-10
- Configuring IGMP Snooping, page 10-12
- Configuring AP Timers, page 10-13
- Configuring Controller WLANs, page 10-13
- Configuring AAA General Parameters, page 10-27
- Setting Multiple Country Codes, page 10-28
- Searching Controllers, page 10-32
- Managing User Authentication Order, page 10-33
- Viewing Audit Status (for Controllers), page 10-34
- Viewing Latest Network Audit Report, page 10-36
- Configuring 802.3 Bridging, page 10-37
- Pinging a Network Device from a Controller, page 10-38
- Enabling Load-Based CAC for Controllers, page 10-38
- Sending Primary Discovery Requests, page 10-38
- Configuring an RRM Threshold Controller (for 802.11a/n or 802.11b/g/n), page 10-41
- Configuring 40-MHz Channel Bonding, page 10-41
- Configuring EDCA Parameters for Individual Controller, page 10-43
- Configuring SNMPv3, page 10-44
- Viewing All Current Templates, page 10-44
- Configuring NAC Out-of-Band Integration, page 10-45
- Configuring Wired Guest Access, page 10-50
- Using Switch Port Tracing, page 10-56
- Background Scanning on 1510s in Mesh Networks, page 10-63

- Configuring QoS Profiles, page 10-65

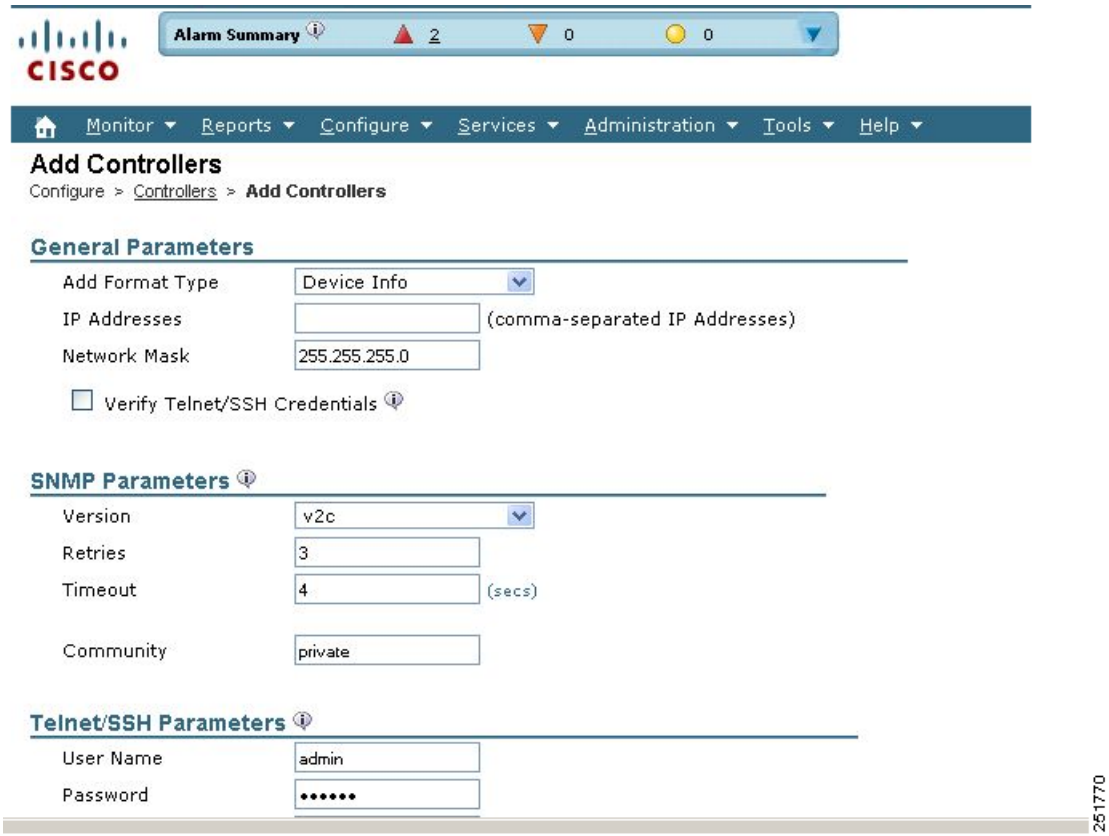
Adding Controllers

You can add controllers one at a time or in batches. Follow these steps to add controllers.

Step 1 Choose **Configure > Controllers**.

Step 2 From the Select a command drop-down list choose **Add Controllers**, and click **Go**. The Add Controller page appears (see Figure 10-1).

Figure 10-1 Add Controller Page



Step 3 Choose one of the following:

If you want to add one controller or use commas to separate multiple controllers, leave the Add Format Type drop-down list at Device Info.

If you want to add multiple controllers by importing a CSV file, choose **File** from the Add Format Type drop-down list. The CSV file allows you to generate your own import file and add the devices you want.

Note When a controller is removed from the system, the associated access points are not removed automatically and therefore remain in the system. These disassociated access points must be removed manually.

Note If you are adding a controller into WCS across a GRE link using IPsec or a lower MTU link with multiple fragments, you may need to adjust the MaxVar Binds PerPDU. If it is set too high, the controller may fail to be added into WCS. To adjust the MaxVarBindsPerPDU setting, do the following: 1) Stop WCS. 2) Go to the location of the Open SnmpParameters.properties file on the server that is running WCS. 3) Edit MaxVarBindsPerPDU to 50 or lower. 4) Restart WCS.

Step 4 If you chose Device Info, enter the IP address of the controller you want to add. If you want to add multiple controllers, use a comma between the string of IP addresses.

Note If a partial byte boundary is used and the IP address appears to be broadcast (without regard to the partial byte boundary), there is a limitation on adding the controllers into WCS. For example, 10.0.2.255/23 cannot be added but 10.0.2.254/23 can.

If you chose File, click **Browse...** to find the location of the CSV file you want to import.

The sample CSV files are as follows:

Table 10-1 Sample CSV Files

ip_address	snmp_version	snmp_community	network_mask
209.165.200.224	v2	public	255.255.255.224
209.165.200.225	v2	public	255.255.255.224
209.165.200.226	v2	private	255.255.255.224
209.165.200.227	v2	private	255.255.255.224

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmpv2_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- telnet_user_name
- telnet_password
- telnet_retries
- telnet_timeout

Step 5 Select the **Verify Telnet/SSH Credentials** check box if you want this controller to verify Telnet/SSH credentials. You may want to leave this unselected (or disabled) because of the substantial time it takes for discovery of the devices.

Step 6 Use the Version drop-down list to choose v1, v2c, or v3.

Step 7 In the Retries parameter, enter the number of times that attempts are made to discover the controller.

Step 8 Provide the client session timeout value in seconds. This determines the maximum amount of time allowed for a client before it is forced to reauthenticate.

Step 9 In the Community parameter, enter either public or private (for v1 and v2 only).

Note If you go back and later change the community mode, you must perform a refresh config for that controller.

Step 10 Choose None, HMAC-SHA, or HMAC-MD5 (for v3 only) for the authorization type.

Step 11 Enter the authorization password (for v3 only).

Step 12 Enter None, CBC-DES, or CFB-AES-128 (for v3 only) for the privacy type.

Step 13 Enter the privacy password (for v3 only).

Step 14 Enter the Telnet credentials information for the controller. If you chose the File option and added multiple controllers, the information will apply to all specified controllers. If you added controllers from a CSV file, the username and password information is obtained from the CSV file.

Note The Telnet/SSH username must have sufficient privileges to execute commands in CLI templates.

The default username and password is admin.

Step 15 Enter the retries and timeout values. The default retries number is 3, and the default retry timeout is 1 minute.

Step 16 Click **OK**.

Note If you fail to add a device to WCS, and if the error message ‘Sparse table not supported' occurs, verify that WCS and WLC versions are compatible and retry. For information on compatible versions, see http://www.cisco.com/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html.

Note When a controller is added to the WCS, the WCS acts as a TRAP receiver and the following traps are enabled on the controller: 802.11 Disassociation, 802.11 Deauthentication, and 802.11 Authenticated.

Downloading Software to Controllers

Both File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) are supported for uploading and downloading files to and from WCS. In previous software releases, only TFTP was supported.

- Download Software (FTP)
- Download Software (TFTP)
- Configure IPaddr > Upload Configuration/Logs from Controller

Download Software (FTP)

To download software to a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 From the Select a command drop-down list, choose **Download Software (FTP)**.

Step 4 Click **Go**.

Note Software can also be downloaded by choosing **Configure > Controllers > *IPaddr* > System > Commands > Upload/Download Commands > Download Software**.

The IP address of the controller and its current status appears in the **Download Software to Controller** page.

Step 5 Select the download type.

Note The pre-download option is displayed only when all selected controllers are using the version 7.0.x.x or later.

- Now—Executes the download software operation immediately. If you select this option, proceed with Step 7.

  Note After the download is successful, reboot the controllers to enable the new software.

- Scheduled—Specify the scheduled download options.
  - Schedule download to controller—Select this check box to schedule download software to controller.
  - Pre-download software to APs—Select this check box to schedule the pre-download software to APs. The APs download the image and then reboot when the controller reboots.

    Note To see Image Predownload status per AP, enable the task in the**Administration > Background Task > AP Image Predownload Task** page, and run an AP Image Predownload report from the Report Launch Pad.

Step 6 If you selected the Scheduled option under Download type, enter the Schedule Details.

- Task Name—Enter a Scheduled Task Name to identify this scheduled software download task.
- Reboot Type—Indicates whether the reboot type is manual, automatic, or scheduled.

Note Reboot Type Automatic can be set when the only Download software to controller option is selected.

- Download date/time—Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists.
- Reboot date/time—This option appears only if you select the reboot type as "Scheduled". Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date to reboot the controller. Choose the time from the hours and minutes drop-down lists.

Note Schedule enough time (at least 30mins) between Download and Reboot so that all APs can complete the software pre-download.

Note If any one of the AP is in pre-download progress state at the time of scheduled reboot, the controller will not reboot. In such a case, wait for the pre-download to finish for all the APs and reboot the controller manually.

- Notification (Optional)—Enter the e-mail address of recipient to send notifications via e-mail.

Note To receive email notifications, configure the WCS mail server in **Administration > Settings > Mail Server Configuration** page.

Step 7 Enter the FTP credentials including username, password, and port.

Step 8 In the **File is located on** parameter, click either the **Local machine** or **FTP Server**.

Note If you choose FTP Server, choose **Default Server** or **New** from the Server Name drop-down list.

Note The software files are uploaded to the FTP directory specified during the install.

Step 9 Specify the local file name or click **Browse** to navigate to the appropriate file.

Note If you chose FTP Server previously, specify the server filename.

Step 10 Click **Download**.

Note If the transfer times out for some reason, you can choose the FTP server option in the **File is located** on parameter; the server filename is populated and retried.

Download Software (TFTP)

To download software to a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 In the Select a command drop-down list, choose **Download Software (TFTP)**.

Step 4 Click **Go**.

Note Software can also be downloaded from **Configure > Controllers > *IPaddr* > System > Commands > Upload/Download Commands > Download Software**.

The IP address of the controller and its current status are displayed in the Download Software to Controller page.

Step 5 Select the download type.

Note The pre-download option is displayed only when all selected controllers are using the version 7.0.x.x or later.

- Now—Executes the download software operation immediately. If you select this option, proceed with Step 7.

  Note After the download is successful, reboot the controllers to enable the new software.

- Scheduled—Specify the scheduled download options.
  - Download software to controller—Select this option to schedule download software to controller.
  - Pre-download software to APs—Select this option to schedule the pre-download software to APs. The APs download the image and then reboot when the controller reboots.

    Note To see Image Predownload status per AP, enable the task in the **Administration > Background Task > AP Image Predownload Task** page, and run an AP Image Predownload report from the Report Launch Pad.

Step 6 If you selected the Scheduled option under Download type, enter the Schedule Detail.

- Task Name—Enter a Scheduled Task Name to identify this scheduled software download task.
- Reboot Type—Indicates whether the reboot type is manual, automatic, or scheduled.

  Note Reboot Type **Automatic** can be set when only Download software to controller option is selected.

- Download date/time—Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Choose the time from the hours and minutes drop-down lists.

- Reboot date/time—This option appears only if you select the reboot type as "Scheduled". Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date to reboot the controller. Choose the time from the hours and minutes drop-down lists.

  Note Schedule enough time (at least 30 minutes) between Download and Reboot so that all APs can complete the software pre-download.

  Note If any one of the AP is in pre-download progress state at the time of scheduled reboot, the controller will not reboot. In such a case, wait for the pre-download to finish for all the APs and reboot the controller manually.

- Notification (Optional)—Enter the e-mail address of recipient to send notifications via e-mail.

  Note To receive email notifications, configure the WCS mail server in the **Administration > Settings > Mail Server Configuration** page.

Step 7 From the File is located on parameter, choose **Local machine** or **TFTP server**.

Note If you choose TFTP server, select the Default Server or add a New server using the Server Name drop-down list.

Step 8 From the Maximum Retries parameter, enter the maximum number of tries the controller should attempt to download the software.

Step 9 In the Timeout parameter, enter the maximum amount of time (in seconds) before the controller times out while attempting to download the software.

Note The software files are uploaded to the TFTP directory specified during the install.

Step 10 Specify the local file name or click **Browse** to navigate to the appropriate file.

Note If you selected TFTP server previously, specify the Server File Name.

Step 11 Click **Download**.

Tip If the transfer times out for some reason, you can choose the TFTP server option in the File is located on parameter; the Server File Name is populated and retried.

Configure *IPaddr* > Upload Configuration/Logs from Controller

To upload files from the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address under the IP address column.

Step 3 From the left sidebar menu, choose **System > Commands**.

Step 4 Select the **FTP** or **TFTP** radio button.

Note Both File Transfer Protocol (FTP) and Trivial Transfer Protocol (TFTP) are supported for uploading and downloading files to and from WCS. In previous software releases, only TFTP was supported.

Step 5 From the Upload/Download Commands drop-down list, choose **Upload File from Controller**.

Step 6 Click **Go** to access this page.

- FTP Credentials Information—Enter the FTP username, password, and port if you selected the FTP radio button previously.
- TFTP or FTP Server Information:
  - Server Name—From the drop-down list, choose **Default Server** or **New**.
  - IP Address—IP address of the controller. This is automatically populated if the default server is selected.
  - File Type—Select from configuration, event log, message log, trap log, crash file, signature files, or PAC.
  - Enter the Upload to File from /(root)/wcs-tftp/ or /(root)/wcs-ftp/ filename.
  - Select whether or not Cisco WCS saves before backing up the configuration.

Note The Cisco WCS uses an integral TFTP and FTP server. This means that third-party TFTP and FTP servers cannot run on the same workstation as the Cisco WCS, because the Cisco WCS and the third-party servers use the same communication port.

Step 7 Click **OK**. The selected file will be uploaded to your TFTP or FTP server and named what you entered in the File Name text box.

Discovering Templates from Controllers

When prompted, WCS can search for associated templates for a controller and show the results.

Step 1 Choose **Configure > Controller**.

Step 2 Choose a desired controller by clicking the check box in front of the IP Address column.

Step 3 From the Select a command drop-down list, choose **Discover Templates from Controller**, and click **Go**.

A warning message confirms that the template discovery refreshes the configuration from the controller first.

The results page shows the template name, number, and template type.

Note The templates that are discovered do not retrieve management/local user passwords.

Displaying Templates Applied to Controller

When prompted, WCS can display a list of templates applied to controllers and show the details for each template.

Step 1 Choose **Configure > Controller**.

Step 2 Choose a desired controller by clicking the check box in front of the IP Address column.

Step 3 From the Select a command drop-down list, choose **Templates Applied to Controller**, and click **Go**.

The template name, template type, the date last saved, and the applied time are shown.

Configuring Controllers and Switches

Configuring DHCP Scopes

Follow these steps to configure DHCP scopes on the controller through WCS. Controllers have built-in DHCP relay agents. However, when network administrators desire network segments that do not have a separate DHCP server, the controller have built-in DHCP scopes that assign IP addresses and subnet masks to wireless clients. 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. After 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 the controller's management interface. You can configure up to 16 DHCP scopes using the controller GUI or CLI. At least one DHCP server must be configured on either the interface associated with the WLAN or with the WLAN itself.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the desired controller from the IP Address column.

Step 3 Choose **System > DHCP Scopes**. In the DHCP Scopes page you can add, delete, or make modifications to an existing proxy.

Step 4 In the Lease Time text box, enter the amount of time (between 0 and 65535 seconds) that an IP address is granted to a client.

Step 5 Enter the network served by this DHCP scope. This IP address is used by the management interface with the netmask (as configured in Step 6) applied.

Step 6 Enter the subnet mask assigned to all wireless clients.

Step 7 In the Pool Start and End Addresses fields, enter the IP address of the optional router(s) connecting the controllers. Each router must have a DHCP-forwarding client, which allows a single controller to serve the clients of multiple controllers.

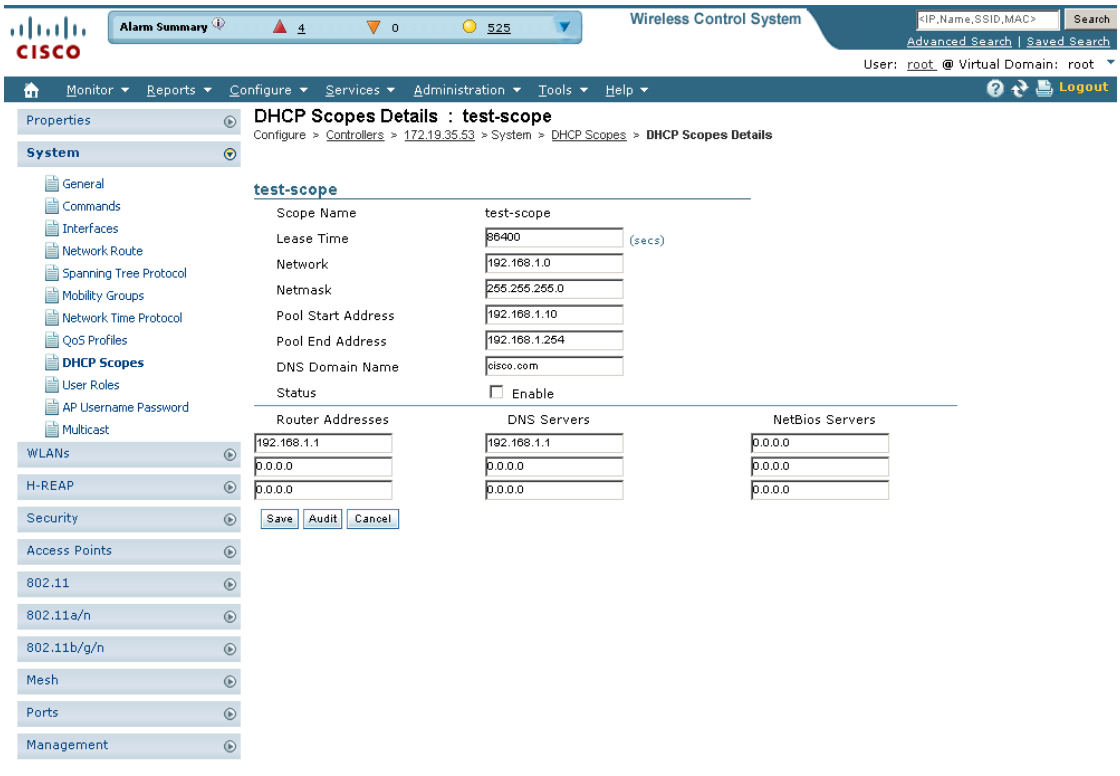
Step 8 Choose to enable or disable this DHCP scope at the Status drop-down list.

Step 9 At the Router Address parameter, enter which IP addresses are already in use and should therefore be excluded. For example, you should enter the IP address of your company's router. In doing so, this IP address will be blocked from use by another client.

Step 10 (Optional) Enter the IP address of the 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 11 (Optional) Enter the IP address of the Microsoft Network Basic Input Output System (NetBIOS) name server(s), such as a Windows Internet Naming Service (WINS) server.

Figure 10-2 DHCP Scope Details Page



Step 12 Click **Save**.

Configuring DHCP Proxy

To configure DHCP (Dynamic Host Configuration Protocol) information for a controller, follow these steps. Controllers have built-in DHCP relay agents. However, if network administrators desire network segments that do not have a separate DHCP server, refer to the "Configuring Controllers and Switches" section on page 10-10. If configured, a controller acts as a DHCP proxy for all DHCP requests received from device access points and clients.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the desired controller from the IP Address column.

Step 3 Choose **System > DHCP**.

Step 4 Choose one of the following options from the DHCP Option 82 Remote ID Field Format drop-down list to specify the format of the DHCP option 82 payload:

- AP-MAC—Adds the MAC address of the access point to the DHCP option 82 payload. If chosen, the Remote ID is set as <AP-MAC>.
- AP-MAC-SSID—Adds the MAC address and SSID of the access point to the DHCP option 82 payload. If chosen, the RemoteID is set as MAP-MAC>:<SSID>.

Step 5 To enable DHCP Proxy, click the check box.

Note When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself.

Step 6 Click **Save**.

Configuring IGMP Snooping

WCS provides an option to configure IGMP snooping and timeout values on the controller. Access points subscribe to the LWAPP multicast group using IGMP. Follow these steps to configure IGMP snooping.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose a desired controller.

Step 3 Choose **System > Multicast** from the left sidebar menu.

Step 4 The Ethernet Multicast Support drop-down is defaulted to disable. If you choose Unicast, the controller unicasts every multicast packet to all access point associated to the controller. This method is not the most efficient, but it may be required for networks that do not support multicasting. If you choose Multicast, the controller sends multicast packets to an LWAPP multicast group. This method reduces the overhead on the controller processor and shifts the work of packet replication to your network.

Step 5 If you choose Multicast, you must enter a group address.

Step 6 Choose **Enable** at the Multicast Mobility Mode drop-down list to change the IGMP snooping status or to set the IGMP timeout. When IGMP snooping is enabled, the controller gathers IGMP reports from the clients and then sends each access point a list of the clients listening to any multicast group. The access point then forwards the multicast packets only to those clients.

Step 7 When the timeout expires, the controller sends a query to all WLANs. Those clients which are listening in the multicast group send a packet back to the controller.

Step 8 If you enable the Multicast Mobility Mode, you must enter a Mobility Group Multicast Address. Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco-manufactured equipment. A device enabled with CDP sends out periodic interface updates to a multicast address to make itself known to neighboring devices.

Configuring AP Timers

Some advanced timer configuration for HREAP and local mode is available for the controller on WCS. Follow these steps to configure the advanced timers and reduce failure detection time.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose to which controller you want to set timer configuration.

Step 3 From the left sidebar menu, choose **System > AP Timers**. The AP Timers page appears.

Note This option is available only for controllers with version 6.0 or later.

Step 4 Click **Local Mode** or **HREAP**.

Step 5 To reduce the failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller. You can then enter a value between 1 and 10 seconds.

Note The 5500 series controller accepts an AP fast heartbeat timer value (local or HREAP mode) in the range of 10 to 15.

Step 6 Click **Save**.

Configuring Controller WLANs

Since controllers can support 512 WLAN configurations, WCS provides an effective way to enable or disable multiple WLANs at a specified time for a given controller. Follow these steps to view a summary of the wireless local access networks (WLANs) that you have configured on your network.

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **WLANs > WLAN Configuration**. The Configure WLAN Summary page appears (see Figure 10-3). This WLAN Configuration page contains the values found in Table 10-2.

Figure 10-3 WLAN Configuration Summary Page

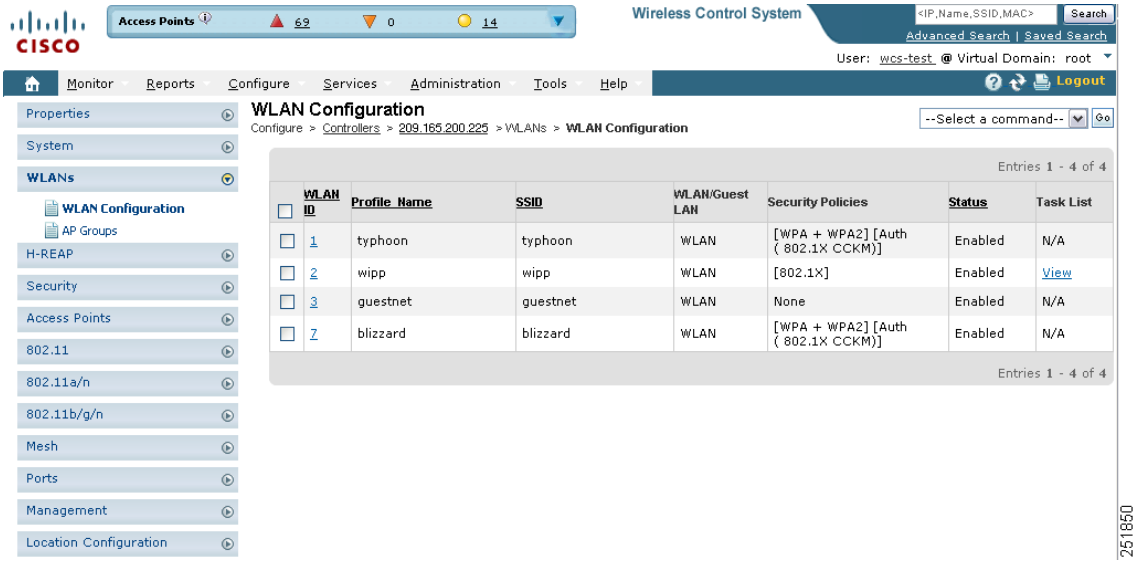


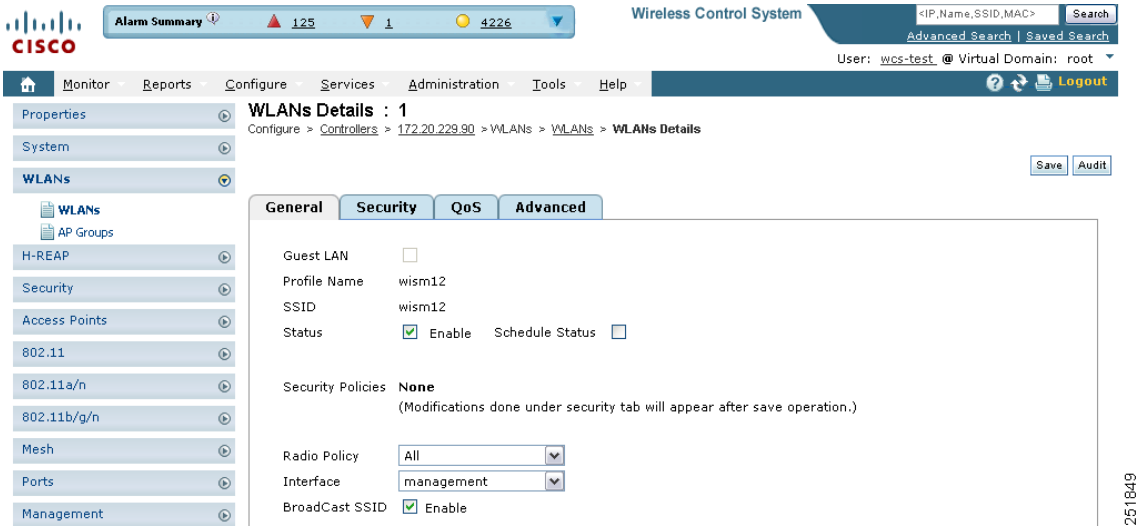
Table 10-2 WLAN Configuration Summary Page

Parameter	Description
Check box	Select the WLAN for deletion. Click **Delete WLANs** from the Select a command drop-down list.
WLAN ID	Identification number of the WLAN.
Profile Name	User-defined profile name specified when creating the WLAN template. Profile Name is the WLAN name.
SSID	Service Set Identifier being broadcast by.
WLAN/Guest LAN	Specifies if it is a WLAN or guest LAN.
Security Policies	Security policies enabled on the WLAN.
Status	Status of the WLAN is either enabled or disabled.
Task List	If a task is scheduled in Configure > Scheduled Configuration Tasks, you have a link to view the scheduled configuration task.

Viewing WLAN Details

To view WLAN details, choose **WLANs**. The WLAN Details page appears (see Figure 10-4).

Figure 10-4 WLAN Details Page



Use the tabs (General, Security, QoS, and Advanced) to view or edit parameters for the WLAN.

- General Tab
- Security Tab
- QoS Tab
- Advanced Tab

General Tab

The General tab includes the following information:

Note Depending on the WLAN template used for this controller, these parameters may or may not be available.

- Guest LAN—Indicates whether or not this WLAN is a Guest LAN.
- Profile Name
- SSID
- Status—Select the Enabled check box to enable this WLAN.

  Note To configure a start time for the WLAN status to be enabled, select the **Schedule Status** check box. Select the hours and minutes from the drop-down lists. Click the calendar icon to select the applicable date.

- Schedule Status
- Security Policies—Identifies the security policies set using the Security tab (includes security policies such as None, 802.1X, Static WEP, Static WEP-802.1X, WPA+WPA2, and CKIP). Changes to the security policies appear in this section after the page is saved.
- Radio Policy—Choose from the drop-down list.

  - All, 802.11a only, 802.11g only, 802.11b/g only, 802.11a/g only.
- Interface—Select from the drop-down list.
- Broadcast SSID—Click the check box to enable.
- Egress Interface—Select the name of the applicable interface. This WLAN provides a path out of the controller for wired guest client traffic.

Note If you only have one controller in the configuration, choose **Management** from the Egress Interface drop-down list.

- Ingress Interface—Select the applicable VLAN from the drop-down list. This interface provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Security Tab

The Security tab includes three additional tabs: Layer 2, Layer 3, and AAA Servers.

Layer 2 Security

Use the Layer 2 Security drop-down list to choose between None, 802.1x, Static WEP, Cranite, Static WEP-802.1x, WPA1+WPA2, and CKIP. These parameters are described in the Table 10-3.

MAC Filtering—Select the check box if you want to filter clients by MAC address.

Table 10-3 Layer 2 Security Options

Parameter	Description
None	No Layer 2 security selected.
802.1x	802.11 Data Encryption: • Type—WEP • Key Size—40, 104, or 128 bits.
Static WEP	802.11 Data Encryption: • Type • Key Size—not set, 40, 104, or 128 bits. • Key Index—1 to 4. • Encryption Key • Encryption Key Format—ASCII or HEX. • Allowed Shared Key Authentication—Select the check box to enable.
Cranite	Configure the WLAN to use the FIPS140-2 compliant Cranite Wireless Wall Software Suite, which uses AES encryption and VPN tunnels to encrypt and verify all data frames carried by the Cisco Wireless LAN Solution.

Table 10-3 Layer 2 Security Options (continued)

Parameter	Description
Static WEP-802.1X	Use this setting to enable both Static WEP and 802.1X policies. If this option is selected, static WEP and 802.1X parameters are displayed at the bottom of the page. Static WEP encryption parameters: • 802.11 Data Encryption – Type – Key Size—not set, 40, 104, or 128 bits. – Key Index—1 to 4. – Encryption Key – Encryption Key Format—ASCII or HEX. • Allowed Shared Key Authentication—Select the check box to enable.
	802.1X parameters: • 802.11 Data Encryption – Type – Key Size—40, 104, or 128 bits.

Table 10-3 Layer 2 Security Options (continued)

Parameter	Description
WPA+WPA2	Use this setting to enable WPA, WPA2, or both. WPA enables Wi-Fi Protected Access with TKIP-MIC Data Encryption or AES. When WPA+WPA2 is selected, you can use Cisco's Centralized Key Management (CCKM) authentication key management, which allows fast exchange when a client roams from one access point to another. When WPA+WPA2 is selected as the Layer 2 security policy and Pre-Shared Key is enabled, neither CCKM or 802.1X can be enabled; although, both CCKM and 802.1X can be enabled at the same time. WPA+WPA2 parameters: • WPA1—Select the check box to enable. • WPA2—Select the check box to enable. Authentication Key Management: • 802.1X—Select the check box to enable. • CCKM—Select the check box to enable. • PSK—Select the check box to enable.
CKIP	Cisco Key Integrity Protocol. A Cisco access point advertises support for CKIP in beacon and probe response packets. CKIP can be configured only when Aironet IE is enabled on the WAN. **Note** CKIP is not supported on 10xx access points. CKIP parameters: • 802.11 Data Encryption – Type – Key Size—not set, 40, 104, or 128 bits. – Key Index—1 to 4. – Encryption Key – Encryption Key Format—ASCII or HEX. • MMH Mode—Select the check box to enable. • Key Permutation—Select the check box to enable.

Layer 3 Security

Use the Layer 3 Security drop-down list to choose between None, VPN Pass Through, and IPsec (Internet Protocol Security). The page parameters change according to the selection you make.

Note Depending on the type of WLAN, the Layer 3 parameters may or may not be available.

Note If you choose VPN pass through, you must enter the VPN gateway address.

Note IPsec is a suite of protocols for securing IP communications by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for establishing cryptographic keys.

Web Policy—Select the check box to specify policies such as authentication, pass through, or conditional web redirect. This section also allows you to enable guest users to view customized login pages.

Note If you choose Pass Through, the Email Input check box appears. Select this check box if you want users to be prompted for their email addresses when attempting to connect to the network.

To allow guest users to view customized login pages, follow these steps:

Step 1 Unselect the **Global WebAuth Configuration** check box.

Step 2 Select the **Web Auth Type** from the drop-down list on the Security > Layer 3 tab.

- Default Internal—The guest user receives the default login page.
- Customized WebAuth—Customized login pages can be downloaded from the Upload/Download Commands page. See "Downloading a Customized Web Authentication Page" section on page 12-67 for more information.
  - Select **Web Auth Login Page**, **Web Auth Login Failure Page**, or **Web Auth Logout Page** from the drop-down lists.
  - Select **None** from any of the drop-down lists if you do not want to display a customized page for that option.
- External—The guest user is redirected to an external login page. Enter the login page URL in the External Web Auth URL text box.

Note If External is selected, you can select up to three RADIUS and LDAP servers from the Security > AAA page. See "AAA Servers" for more information.

AAA Servers

Select RADIUS and LDAP servers to override use of default servers on the current WLAN.

- RADIUS Servers—Use the drop-down lists to choose authentication and accounting servers. With this selection, the default RADIUS server for the specified WLAN overrides the RADIUS server that is configured for the network. If all three RADIUS servers are configured for a particular WLAN, server 1 has the highest priority and so on.
- LDAP Servers—If no LDAP servers are chosen from the drop-down lists, WCS uses the default LDAP server order from the database.
- Local EAP Authorization—Allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the back-end system becomes disrupted or the external authentication server fails.

  Select the check box to enable if you have an EAP profile configured. Select the profile from the drop-down list.
- Allow AAA Override—When enabled, if a client has conflicting AAA and controller WLAN authentication parameters, client authentication is performed by the AAA server.

  As part of this authentication, the operating system moves clients from the default Cisco WLAN solution to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, or WPA operation).

  In all cases, the operating system also uses QoS and ACL provided by the AAA server as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as *identity networking*.)

  When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is only performed by the AAA server if the controller WLANs do not contain any client-specific authentication parameters.

QoS Tab

- Quality of Service (QoS)—From the drop-down list, select Platinum (voice), Gold (video), Silver (best effort), or Bronze (background).
  - Services such as VoIP should be set to gold. Non-discriminating services such as text messaging can be set to bronze.
- WMM Parameters
  - WMM Policy—Choose Disabled, Allowed (to allow clients to communicate with the WLAN), or Required (to make it mandatory for clients to have WMM enabled for communication).
  - 7920 AP CAC—Select the check box to enable support on Cisco 7920 phones.
  - 7920 Client CAC—Select the check box to enable WLAN support for older versions of the software on 7920 phones. The CAC limit is set on the access point for newer versions of software.

Advanced Tab

- H-REAP Local Switching—Select the check box to enable Hybrid REAP local switching. When enabled, the H-REAP access point handles client authentication and switches client packets locally. See the "Configuring Hybrid REAP" section on page 15-4 for more information.

Note H-REAP local switching applies only to Cisco 1130/1240/1250 series access points. It is not supported with L2TP, PPTP, CRANITE, and FORTRESS authentications. It does not apply to WLAN IDs 9-16.

- Session Timeout (secs)—Set the maximum time a client session can continue before re-authentication.
- Aironet IE—Select the check box to enable support for Aironet information elements (IEs) for this WLAN.
  - 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 association request.
- IPv6—Select the check box to enable IPv6.

Note Layer 3 security must be set to None for IPv6 to be enabled.

- Diagnostic Channel—Click to enable the diagnostics. When enabled, clients can connect to this WLAN for diagnostic purposes.

Note The results of the diagnostic tests are stored in the SNMP table, and WCS polls these tables to display the results.

- Override Interface ACL—Select a defined access control list (ACL) from the drop-down list. When the ACL is selected, the WLAN associates the ACL to the WLAN.

Note Selecting an ACL is optional, and the default is None.

For more information, see the "Configuring Access Control List Templates" section on page 12-69.

- Peer to Peer Blocking—From the drop-down list, select Disable, Drop, or Forward-Up Stream.
  - This option allows users to configure peer-to-peer blocking for individual clients rather than universally for all WLAN clients.
- Client Exclusion—Select the check box to enable automatic client exclusion. If it is enabled, set the timeout value in seconds for disabled client machines.
  - Client machines are excluded by MAC address, and their status can be observed.
  - A timeout setting of 0 indicates that administrative control is required in order to re-enable the client.

Note When session timeout is not set, the excluded client remains and will not time out from the excluded state. It does not imply that the exclusion feature is disabled.

- Media Session Snooping—Click to enable Media Session Snooping. This feature enables access points to detect the establishment, termination, and failure of voice calls and then report them to the controller and WCS. It can be enabled or disabled for each WLAN.

When media session snooping is enabled, the access point radios advertise this WLAN snoop for Session Initiation Protocol (SIP) voice packets. Any packets destined to or originating from port number 5060 are considered for further inspection. The access point tracks whether Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, already on an active call, or in the process of ending a call and then notify the controller of any major call events.

- NAC Support—Select the **NAC Support** check box to enable it. SIP errors that are discovered generate traps that appear on the client troubleshooting and alarms screens. 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. See the "Configuring NAC Out-of-Band Integration" section on page 10-45 for more information.
- Passive Client—If the check box is selected, it enables passive clients on your WLAN.

  Passive clients are wireless devices like scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information during association with an access point. As a result, when passive clients are used, the controller will never know the IP address unless they use DHCP.

  Wireless LAN controllers currently act as a proxy for ARP requests. On receiving an ARP request, the controller responds with an ARP response instead of passing the request directly to the client. This has two advantages:

  - The upstream device that sends out the ARP request to the client cannot know where the client is located.
  - Reserves power for battery-operated devices like mobile phones and printers as they do not need to respond to every ARP request.

  Because the wireless controller does not have any IP-related information about passive clients, it cannot respond to any ARP requests. The current behavior does not allow the transfer of ARP requests to passive clients. Therefore, any application that tries to access a passive client will fail.

  This feature enables ARP requests and responses to be exchanged between wired and wireless clients on a per-VLAN/WLAN basis. This feature enables the user to mark a desired WLAN for presence of proxy ARP thereby enabling the controller to pass the ARP requests until the client gets to RUN state.

  Note This feature is supported only on the 5500 and 2100 series controllers.

- DTIM Period (in beacon intervals)—For 802.11a/n and 802.11b/g/n, specify the frequency of the DTIM packet sent in the wireless medium. This period can be configured for every WLAN (except guest WLAN) on all version 6.0 and above controllers.
- DHCP
  - DHCP Server—Select the check box to override the DHCP server, and enter the IP address of the DHCP server.

    Note For some WLAN configurations, this setting is required.

  - DHCP Addr. Assignment—If you select the Required check box, clients connected to this WLAN will get an IP address from the default DHCP server.
- Management Frame Protection (MFP)

- MFP Signature Generation—If the check box is selected, it enables signature generation for the 802.11 management frames transmitted by an access point associated with this WLAN. With signature generation, changes to the transmitted management frames by an intruder are detected and reported.
- MFP Client Protection—From the drop-down list, choose **Optional**, **Disabled**, or **Required** for individual WLAN configurations.
- MFP Version—Displays the Management Frame Protection version.

Note Client-side MFP is available only for those WLANs configured to support CCXv5 (or later) clients. In addition, WPA1 must first be configured.

Adding a WLAN

To add a WLAN, follow these steps:

Step 1 Choose **Configure > Controllers**.

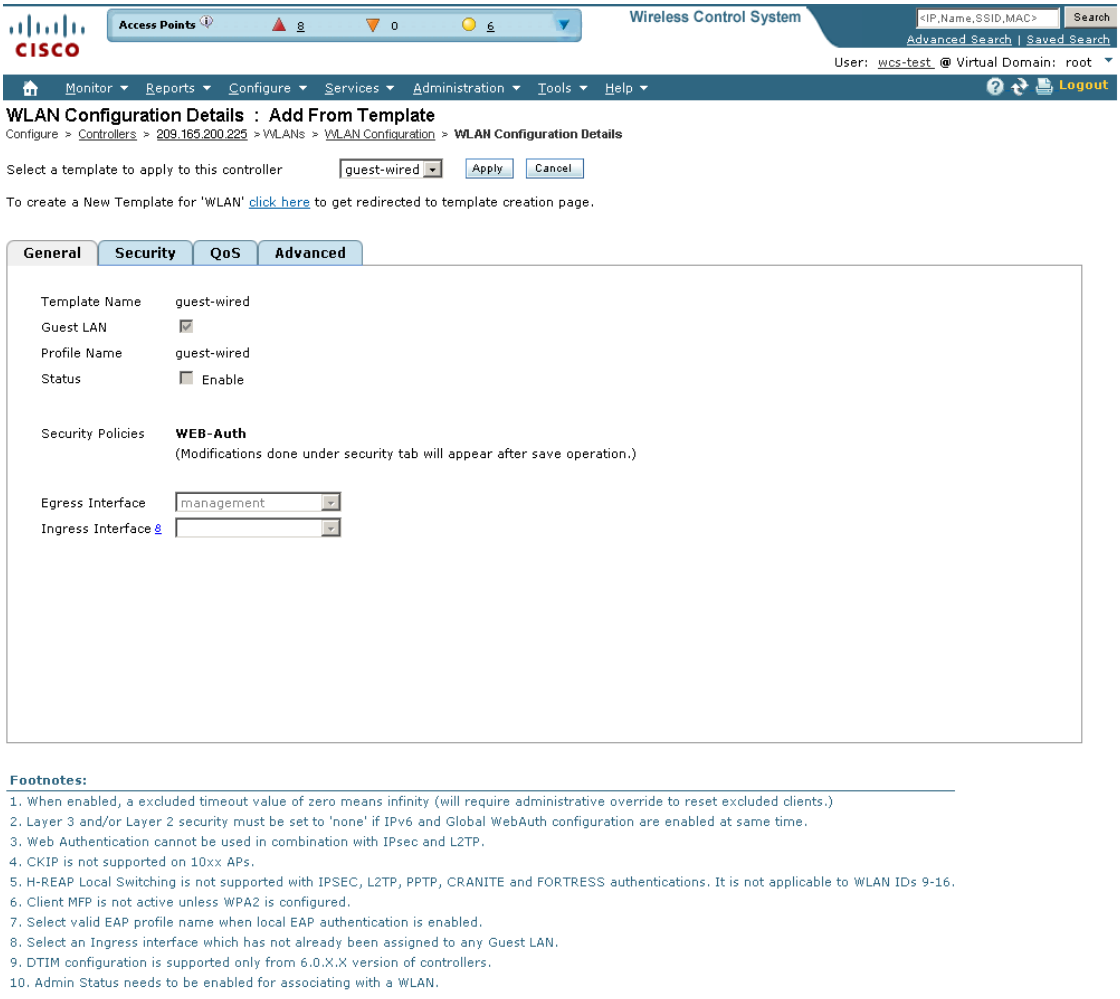
Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, select **WLANs > WLAN Configuration**.

Step 4 From the Select a command drop-down list, choose **Add a WLAN**.

Step 5 Click **Go** to open the WLAN Details: Add from Template page (see Figure 10-5).

Figure 10-5 WLAN Details: Add From Template Page



Step 6 Choose a template from the Select a template to apply to this controller drop-down list.

Step 7 Click **Apply**.

Note To create a new template for WLANs, use the click here link in this page or choose **Configure > Controller Template Launch Pad > WLANs > WLAN**.

Deleting a WLAN

To delete a WLAN, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, choose **WLANs > WLAN Configuration**.

Step 4 Select the check boxes of the WLANs that you want to delete.

Step 5 From the Select a command drop-down list, choose **Delete a WLAN**.

Step 6 Click **Go**.

Step 7 Click **OK** to confirm the deletion.

Managing WLAN Status Schedules

WCS enables you to change the status of more than one WLAN at a time on a given controller. You can select multiple WLANs and select the date and time for that status change to take place.

To schedule multiple WLANs for a status change, follow these steps:

Step 1 Choose **Configure > Controllers**.

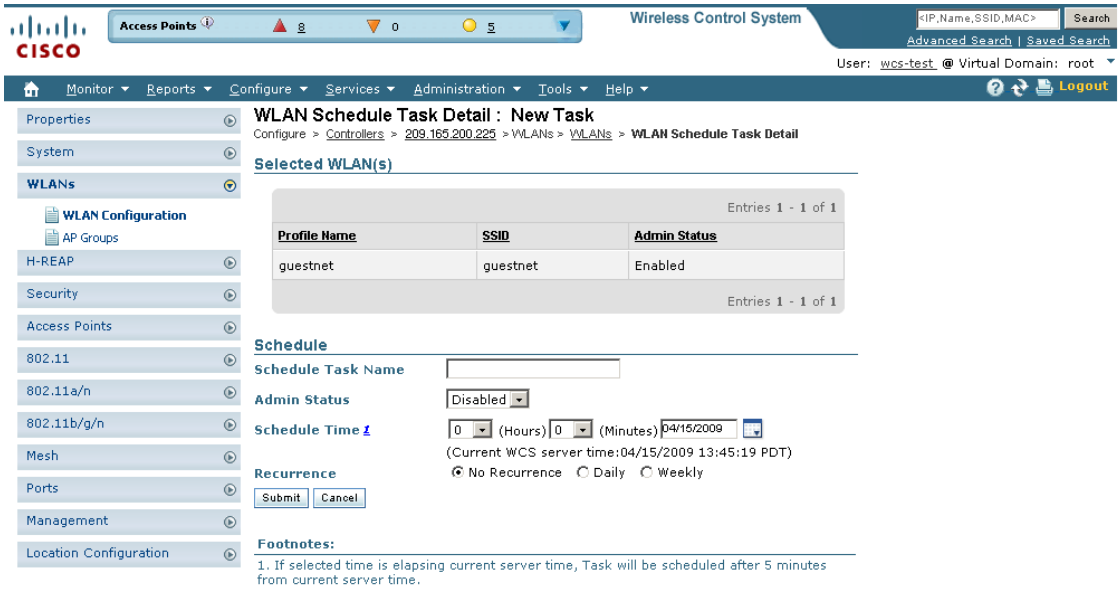
Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, select **WLANs > WLAN Configuration**.

Step 4 Select the check boxes of the WLANs that you want to schedule for a status change.

Step 5 From the Select a command drop-down list, choose **Schedule Status** to open the WLAN Schedule Task Detail page (see Figure 10-6).

Figure 10-6 WLAN Schedule Task Detail Page



The selected WLANs are listed at the top of the page.

Step 6 Enter a Scheduled Task Name to identify this status change schedule.

Step 7 Select the new Admin Status (Enabled or Disabled) from the drop-down list.

Step 8 Select the schedule time using the hours and minutes drop-down lists.

Step 9 Click the calendar icon to choose a schedule date or enter the date in the text box (MM/DD/YYYY).

Step 10 Select the appropriate Recurrence radio button to determine the frequency of the status change (Daily, Weekly, or No Recurrence).

Step 11 Click **Submit** to initiate the status change schedule.

Note For more information on the WLAN Configuration Scheduled Task results, see "Viewing WLAN Configuration Scheduled Task Results" section on page 12-124.

Mobility Anchors

Mobility anchors are one or more controllers defined as anchors for the WLAN. Clients (802.11 mobile stations such as a laptop) are always attached to one of the anchors.

This feature can be used to restrict a WLAN to a single subnet, regardless of the client's entry point into the network. In this way, users can access a public or guest WLAN throughout an enterprise but still be restricted to a specific subnet. Guest WLAN can also be used to provide geographical load balancing because WLANs can represent a particular section of a building (such as a lobby, restaurant, and so on).

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EitherIP. The foreign controller decapsulates the packets and forwards them to the client.

Note A 2000 series controller cannot be designated as an anchor for a WLAN. However, a WLAN created on a 2000 series controllers can have a 4100 series controller or a 4400 series controller as its anchor.

Note The L2TP Layer 3 security policies are unavailable for WLANs configured with a mobility anchor.

To view the real time status of mobility anchors for a specific WLAN, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, select **WLANs > WLAN Configuration**.

Step 4 Click a WLAN ID to view the parameters for a specific WLAN.

Step 5 Click the **Advanced** tab.

Step 6 Click the **Mobility Anchors** link. Table 10-4 describes the parameters that are displayed.

Table 10-4 Mobility Anchors

Parameter	Description
Mobility Anchor	Anchor's IP address.
Status	Anchor's current status. For example, reachable or unreachable.

Configuring AAA General Parameters

The Security > AAA > General page allows you to configure the local database entries on a controller. Follow these steps to configure the local database entries:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **Security > AAA > General**.

Step 4 Enter the maximum number of allowed database entries. The valid range is 512 to 2048. This amount becomes effective on the next reboot. The current maximum displays the effective maximum value currently set on the controller.

Configuring Local Network Users

You can store the credentials (username and password) of all the local network users. These credentials are then used to authenticate the users. For example, local EAP may use the local user database as its backend database to retrieve user credentials. You must create a local net user and define a password when logging in as a web authentication client.

Step 1 Choose **Configure > Controllers**.

Step 2 From the left sidebar menu choose **Security > AAA > Local Net Users**.

Step 3 If you keep Import from File enabled, you need to enter a file path or click the Browse button to navigate to the file path. Then continue to Step 11. If you disable the import, continue to Step 5.

Note You can only import a.csv file. Any other file formats are not supported.

The first row in the file is the header. The data in the header is not read by the Cisco WCS. The header can either be blank or filled. The Cisco WCS reads data from the second row onwards.

Step 4 Enter a username and password.It is mandatory to fill the Username and Password text boxes in all the rows.

Step 5 Enter a profile. The Profile column if left blank (or filled in with *any profile*) means a client on any profile can use this account.

Step 6 Enter a description of the profile.

Step 7 Use the drop-down list to choose the SSID which this local user is applied to or choose the *any SSID* option.

Step 8 Enter a user-defined description of this interface. Skip to Step10.

Step 9 If you want to override the existing template parameter, click to enable this parameter.

Step 10 Click Save.

Configuring New LDAP Bind Requests

WCS now supports LDAP configuration for both an anonymous or authenticated bind. A bind is a socket opening that performs a lookup. Follow these steps to configure LDAP bind requests.

Step 1 Choose **Configure > Controllers**.

Step 2 From the left sidebar menu choose **Security > AAA > LDAP Servers**.

Step 3 From the Bind Type drop-down list, choose **Authenticated** or **Anonymous**. If you choose Authenticated, you must enter a bind username and password as well.

Step 4 In the Server User Base DN text box, enter the distinguished name of the subtree in the LDAP server that contains a list of all the users.

Step 5 In the Server User Attribute text box, enter the attribute that contains the username in the LDAP server.

Step 6 In the Server User Type text box, enter the ObjectType attribute that identifies the user.

Step 7 In the Retransmit Timeout text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Step 8 Select the **Admin Status** check box if you want the LDAP server to have administrative privileges.

Step 9 Click **Save**.

Setting Multiple Country Codes

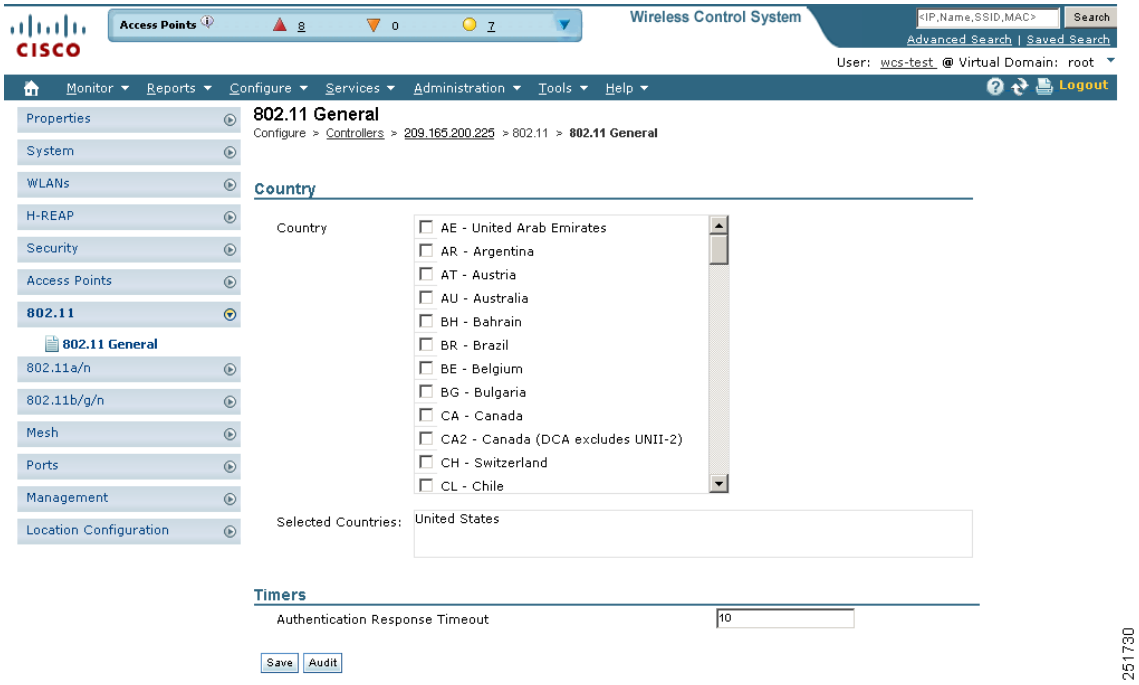
To set multiple country support for a single controllers that is not part of a mobility group, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the controller for which you are adding countries.

Step 3 Choose **802.11 > General** from the left sidebar menu. The Controller 802.11 page appears (see Figure 10-7).

Figure 10-7 Controller 802.11



Step 4 Select the check box to choose a country. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that it complies with your country's regulations.

Note Access points may not operate properly if they are not designed for use in your country of operation. For example, an access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Australia. Always be sure to purchase access points that match your country's regulatory domain. For a complete list of country codes supported per product, refer to:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html.

Step 5 Enter the time in seconds after which the authentication response will timeout.

Step 6 Click **Save**.

Configuring Aggressive Load Balancing

Enabling aggressive load balancing on the controller allows lightweight access points to load balance wireless clients across access points.

Note Clients are load balanced between access points on the same controller. Load balancing does not occur between access points on different controllers.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. This code indicates whether the access point can accept any more associations. If the access point is too busy, the client attempts to associate to a different access point in the area. The system determines if an access point is relatively more busy than its neighbor access points that are also accessible to the client.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing page, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it would be allowed to assciate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

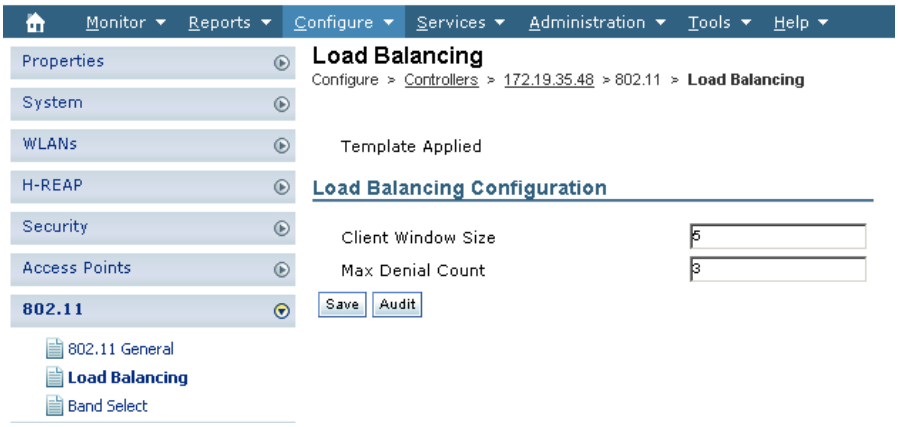
Follow these steps to configure aggressive load balancing:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the controller that you need to configure.

Step 3 Choose **802.11 > Load Balancing** from the left sidebar menu. The load balancing page appears (see Figure 10-8).

Figure 10-8 Load Balancing



Step 4 Enter a value between 1 and 20 for the client page size. The page size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing page + client associations on AP with lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client page size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

Step 5 Enter a value between 0 and 10 for the max denial count. The denial count sets the maximum number of association denials during load balancing.

Step 6 Click **Save**.

Step 7 To enable or disable aggressive load balancing on specific WLANs, browse to the WLAN Configuration page, and click the **Advanced** tab. For instructions on using the WLAN Configuration page, see the "Configuring Controller WLANs" section on page 10-13.

Configuring Band Selection

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three non-overlapping channels. To combat these sources of interference and improve overall network performance, you can configure band selection on the controller.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

You can enable band selection globally on a controller, or you can enable or disable band selection for a particular WLAN, which is useful if you want to disable it for a select group of clients (such as time-sensitive voice clients).

Note Band-selection-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

Guidelines for Using Band Selection

Follow these guidelines when using band selection:

- Band selection can be used only with Cisco Aironet 1140 and 1250 series access points.
- Band selection operates only on access points that are connected to a controller. A hybrid-REAP access point without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.
- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.

Configuration Steps

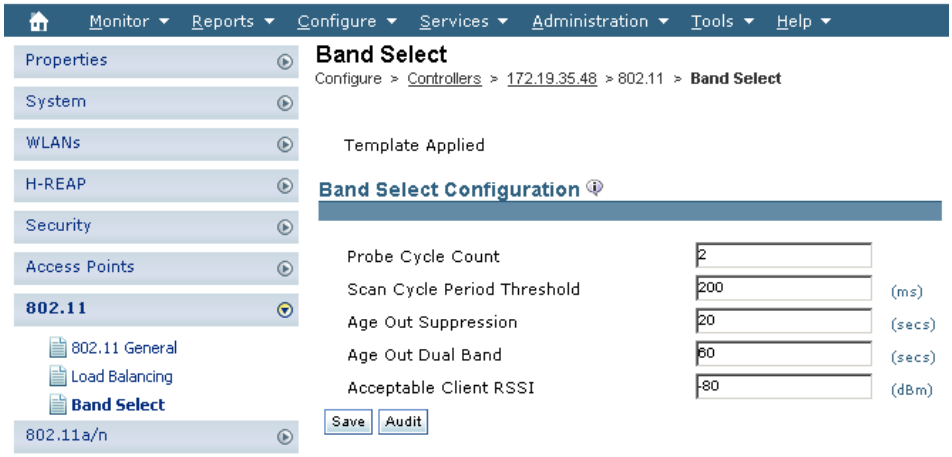
Follow these steps to configure band selection:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the controller that you need to configure.

Step 3 Choose **802.11 > Band Select** from the left sidebar menu. The band select page appears (see Figure 10-9).

Figure 10-9 Band Select



Step 4 Enter a value between 1 and 10 for the probe cycle count. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 5 Enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.

Step 6 Enter a value between 10 and 200 seconds for the age out suppression parameter. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 7 Enter a value between 10 and 300 seconds for the age out dual band parameter. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 8 Enter a value between –20 and –90 dBm for the acceptable client RSSI parameter. This parameter sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Step 9 Click **Save**.

Step 10 To enable or disable band selection on specific WLANs, browse to the WLAN Configuration page and click the **Advanced** tab. For instructions on using the WLAN Configuration page, see the "Configuring Controller WLANs" section on page 10-13.

Searching Controllers

The enhanced WCS Search feature provides easy access to advanced search options and saved searches. You can access the search options from any page within WCS making it easy to search for a device or SSID.

The Search function is located in the top right section of the WCS window. See the "Using the Search Feature" section on page 2-31 for more information on using the search feature.

- Quick Search: For a quick search, you can enter a partial or complete IP address, MAC address, name, or SSID for clients, alarms, access points, controllers, maps, tags, or rogue clients.

- Advanced Search: An advanced search allows you to search for a device based on a variety of categories and filters.
- Saved Searches: Lists the saved custom searches. To open a saved search, choose it from the Saved Searches list.

You can configure the following parameters in the Search Controllers page:

- Search for controller by— Choose all controllers, IP address, or controller name.
- Select a Network— Choose all networks or an individual network.
- Audit Status— Search by audit status of the following:
  - Not Available: Audit status is not available.
  - Identical: No configuration differences found during last audit.
  - Mismatch: Configuration differences were found between WCS and controller during last audit.
- Items per page—Choose the number of found items to display on the search results page. The range is 10 to 100 items per page. The default is 20.

When you click **New Search**, the controller search results appear:

Table 10-5 Search Results

Parameter	Options
IP Address	Local network IP address of the controller management interface. Clicking the title toggles the order from ascending to descending. Clicking an IP address in the list displays a summary of the controller details.
Controller Name	Clicking the title toggles the order from ascending to descending.
Type	Type of controller. For example, Cisco 2000 Series, Cisco 4100 Series, or Cisco 4400 Series.
Location	The geographical location (such as campus or building). Clicking the title toggles the order from ascending to descending.
Mobility Group Name	Name of the controller or WPS group.
Reachability Status	Reachable or Unreachable. Clicking the title toggles the order from ascending to descending.
AP Count	The number of access points associated with this controller.

Managing User Authentication Order

You can control the order in which authentication servers are used to authenticate a controller's management users.

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address.

Step 3 From the left sidebar menu, choose **Management > Authentication Priority**.

Step 4 The local database is searched first. Choose either **RADIUS** or **TACACS+** for the next search. If you do not want the local database searched first, choose **Second**. If authentication using the local database fails, the controller uses the next type of server.

Step 5 Click **Save**.

Viewing Audit Status (for Controllers)

You can audit a controller by choosing **Audit Now** from the Select a command drop-down list in the Configure > Controllers page or by clicking **Audit Now** directly from the Controller Audit Report.

Note A current Controller Audit Report can be viewed in the Configure > Controllers page by choosing an object from the Audit Status column.

To audit a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box for the appropriate controller. From the Select a command drop-down list, choose **Audit Now**.

Step 3 Click **Go**.

A confirmation appears after you perform the controller actions from the View Audit Status page.

The Audit Report displays the following:

- Device Name
- Time of Audit
- Audit Status
- Applied and Config Group Template Discrepancies occur because of applied templates. The config group templates are listed, and the information includes the following:
  - Template type (template name)
  - Template application method
  - Audit status (such as mismatch, identical)
  - Template attribute
  - Value in WCS
  - Value in Controller
- Config WCS Discrepancies occur because of configuration objects in the WCS database. The current WLC configuration is listed, and the information includes the following:
  - Configuration type (name)
  - Audit Status (for example, mismatch, identical)
  - Attribute
  - Value in WCS

  - Value in Controller

- Total enforcements for config groups with background audit enabled—If discrepancies are found during the audit in regards to the config groups enabled for background audit and if the enforcement is enabled, this section lists the enforcements made during the controller audit. See the "Creating Config Groups" section on page 8-19 for more information on enabling the background audit.
- Failed Enforcements for Config Groups with background audit enabled—Check the link to view a list of failure details (including the reason for the failure) returned by the device. See the "Creating Config Groups" section on page 8-19 for more information on enabling the background audit.

Note The following sections are displayed if the audit selected is a template-based audit:

Applied and Config Group Template Discrepancies
Total enforcements for config groups with background audit enabled
Failed enforcements for config groups with background audit enabled
Config WCS discrepancies

The Config WCS discrepancies section is displayed if the audit is selected to be a basic audit.

- Restore WCS Values to Controller or Refresh Config from Controller—If the audit reveals configuration differences, you can either restore WCS values on the controller or refresh controller values. Choose **Restore WCS Values to Controller** or **Refresh Config from Controller**.
  - If you choose Restore WCS Values to Controller, all of the WCS values are enforced on the controller in an attempt to resolve the discrepancies on the device. All of the applied templates and the templates that are part of the config group are applied to this controller (for template based audit). If the audit done is a basic audit, the configuration objects in WCS database are enforced on the controller.

Note Template discrepancies can be resolved by enforcing WCS templates on the device. See the "Creating Config Groups" section on page 8-19 for more information on enforcing configurations.

  - If you choose Refresh Config from Controller, a Refresh Config page opens and shows the following message: "Configuration is present on WCS but not on device, do you wish to:" Choose one of the following options, and click **Go** to confirm your selection.

    You should choose Refresh Config from Controller after an upgrade of software to ensure that the AP timers configuration is visible.

    Retain—The WCS refreshes the configuration from the controller but will not delete any devices or configurations that no longer exist in the controller configuration. For example, if the WCS database shows an AP1, but that access point is no longer present in the controller configuration, WCS will not delete AP1 from its database.

    Delete—WCS deletes the configuration of the controller from its database and retrieves a new configuration from the controller. Delete is the recommended option so that WCS matches the most recent configuration you are refreshing from WLC.

Note In the Refresh Config page, only the configuration objects for this controller in the WCS database are updated. Upon refresh, the WCS templates are not updated.

Viewing Latest Network Audit Report

The Network Audit Report shows the time of the audit, the IP address of the selected controller, and the synchronization status. The Applied and Config Group Template Discrepancies, Total Enforcements for Config Groups with Background Audit Enabled, and Failed Enforcements for Config Groups with Background Audit Enabled sections have data only if the network audit was run as a template based audit.

Note This method shows the report from the network audit task and not an on-demand audit per controller.

To view the latest network audit report for the selected controllers, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box for the applicable controller.

Step 3 From the Select a command drop-down list, choose **View Latest Network Configuration Audit Report**.

Step 4 Click **Go**.

The Audit Summary displays the time of the audit, the IP address of any selected controller, and the audit status. The Audit Details page displays the configuration differences, if applicable.

You can use the General and Schedule tabs to revise the Audit Report parameters.

Note In the All Controllers page, click the Audit Status column value to view the latest audit details page for the selected controller. This method has similar information as the Network Audit report in the Reports menu, but this report is interactive and per controller.

Note To run an on-demand audit report, select which controller you want to run the report on and choose **Audit Now** from the Select a command drop-down list. If you run an on-demand audit report and configuration differences are detected, you are given the option to retain the existing controller or WCS values.

Configuring 802.3 Bridging

The controller supports 802.3 frames and applications that use them, such as those typically used for cash registers and cash register servers. However, to make these applications work with the controller, the 802.3 frames must be bridged on the controller.

Support for raw 802.3 frames allows the controller to bridge non-IP frames for applications not running over IP. Only this raw 802.3 frame format is currently supported.

You can configure 802.3 bridging using WCS release 4.1 or later. Follow these steps.

Step 1 Click **Configure > Controllers**.

Step 2 Click **System > General** to access the General page.

Step 3 From the 802.3 Bridging drop-down list, choose **Enable** to enable 802.3 bridging on your controller or **Disable** to disable this feature. The default value is Disable.

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

Setting AP Failover Priority

When a controller fails, the backup controller configured for the access point suddenly receives a number of discovery and join requests. This may cause the controller to reach an overloaded point and reject some of the access points.

By assigned priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is overloaded, the higher-priority access points join the backup controller and disjoin the lower priority access points.

To configure priority settings for access points, you must first enable the AP Priority feature. To enable the AP Priority feature, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > General**.

Step 4 From the AP Failover Priority drop-down list, choose **Enable**.

To configure an access point's priority, follow these steps:

Step 1 Choose **Configure > Access Points > <AP Name>**.

Step 2 From the AP Priority drop-down list, choose the applicable priority (Low, Medium, High, Critical).

Note The default priority is Low.

Sending Primary Discovery Requests

The access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry on the list.

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 From the left sidebar menu, choose **System > General**.

Step 4 Select the **AP Primary Discovery Timeout** check box to enable the timeout value. When configured, the primary discovery request timer specifies the amount of time that a controller has to respond to the discovery request of the access point before the access point assumes that the controller cannot be joined and waits for a discovery response from the next controller in the list. Enter a value between 30 and 3600 seconds.

Step 5 Click **Save**.

Pinging a Network Device from a Controller

Follow these steps to ping network devices from a controller.

Step 1 Click **Configure** > **Controllers** to navigate to the All Controllers page.

Step 2 Click the desired IP address to display the IP Address > Controller Properties page.

Step 3 In the sidebar, choose **System > Commands** to display the IP Address > Controller Commands page.

Step 4 Choose **Ping From Controller** from the Administrative Commands drop-down list, and click **Go**.

Step 5 In the Enter an IP Address (x.x.x.x) to Ping page, enter the IP address of the network device that you want the controller to ping, and click **OK**.

WCS displays the Ping Results page, which shows the packets that have been sent and received. Click **Restart** to ping the network device again or click **Close** to stop pinging the network device and exit the Ping Results page.

Enabling Load-Based CAC for Controllers

Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

In load-based CAC, the access point periodically measures and updates the utilization of the RF channel, channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents over-subscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

To enable load-based CAC for a controller template, refer to the "Configuring a Voice Parameter Template (for 802.11a/n or 802.11b/g/n)" section on page 12-86.

To enable load-based CAC for a controller using the WCS web interface, follow these steps.

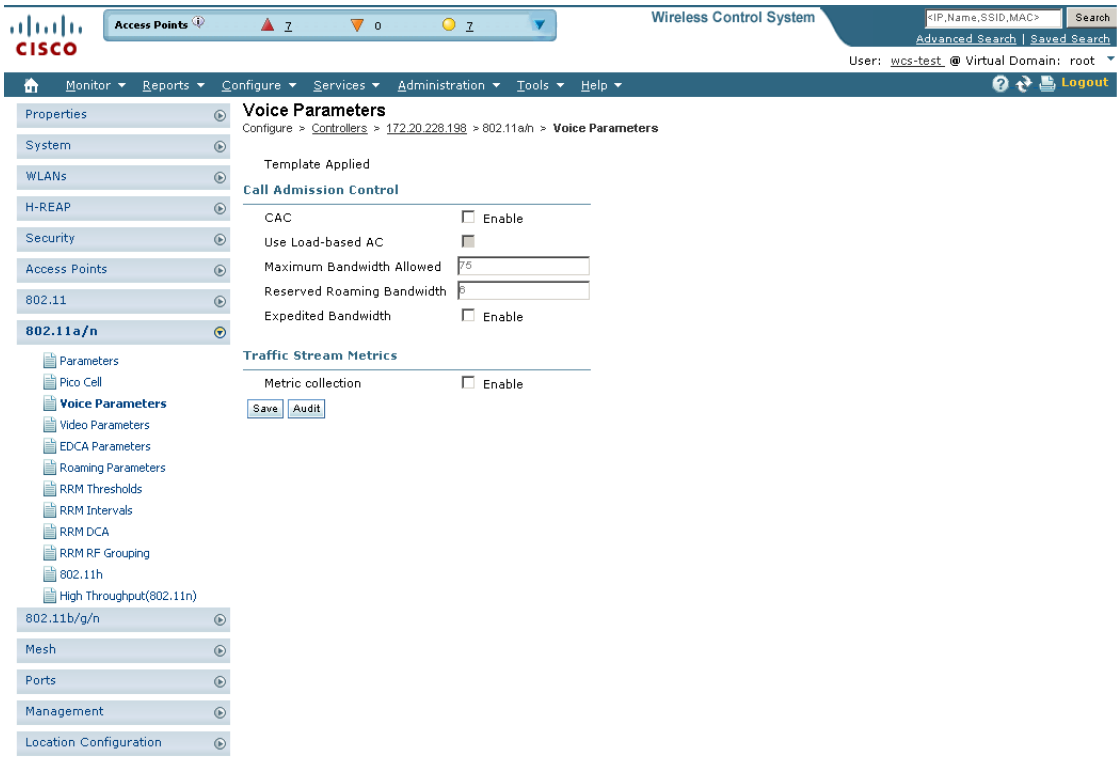
Step 1 Click **Configure > Controllers**.

Step 2 Click the IP address link of the controller.

Step 3 Click **Voice Parameters** under 802.11a/n or 802.11b/g/n.

The 802.11a/n (or 802.11b/g/n) Voice Parameters page appears (see Figure 10-10).

Figure 10-10 802.11a/n Voice Parameters Page



Step 4 Click the check box to enable bandwidth CAC. For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, call admission control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.

Step 5 Determine if you want to enable load-based CAC for this radio band. Doing so incorporates a measurement scheme that considers the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference.

Step 6 Enter the percentage of maximum bandwidth allowed.

Step 7 Enter the percentage of reserved roaming bandwidth.

Step 8 Click the check box if you want to enable expedited bandwidth as an extension of CAC for emergency calls. You must have an expedited bandwidth IE that is Cisco Compatible Extensions (version 5) compliant so that a TSPEC request is given higher priority.

Step 9 Click the check box if you want to enable metric collection. Traffic stream metrics are a series of statistics about VoIP over your wireless LAN, and they inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g/n interfaces from all associated access points. If you are using VoIP or video, enable this feature.

Step 10 Click **Save**.

Configuring CleanAir Parameters (for 802.11a/n or 802.11b/g/n)

To configure 802.11a/n or 802.11b/g/n CleanAir parameters, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, choose **802.11a/n > CleanAir** or **802.11b/g/n > CleanAir** to view the following information:

- CleanAir—Select the check box to enable CleanAir functionality on the 802.11a/n or 802.11b/g/n network, or unselect to disable CleanAir functionality.
- Reporting Configuration—Use the parameters in this section to configure the interferer devices you want to include for your reports.
  - Report—Select the report interferers check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.
  - Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferers to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are detected.
- Alarm Configuration—This section enables you to configure triggering of air quality alarms.
  - Air Quality Alarm—Select the Air Quality Alarm check box to enable the triggering of air quality alarms, or unselect the box to disable this feature. The default value is selected.
  - Air Quality Alarm Threshold—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold field to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.
  - Interferers For Security Alarm—Select the Interferers For Security Alarm check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is selected.
  - Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.
- Event Driven RRM—To trigger spectrum event-driven radio resource management (RRM) to run when a CleanAir-enabled access point detects a significant level of interference, use the following parameters:

- Event Driven RRM—Displays the current status of spectrum event-driven RRM.
- Sensitivity Threshold—If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Command Buttons

- Save—Save the changes made.
- Audit—Compare the WCS values with those used on the controller.

Configuring an RRM Threshold Controller (for 802.11a/n or 802.11b/g/n)

Follow these steps to configure an 802.11a/n or 802.11b/g/n RRM threshold controller.

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller to open the Controller Properties page.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM Thresholds** or **802.11b/g/n > RRM Thresholds**.

Step 4 Make any necessary changes to coverage level thresholds, load thresholds, and thresholds for traps.

Step 5 Click **Save**.

Configuring 40-MHz Channel Bonding

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

Note Choosing a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

To configure 802.11 a/n RRM DCA channels for an individual controller, follow these steps:

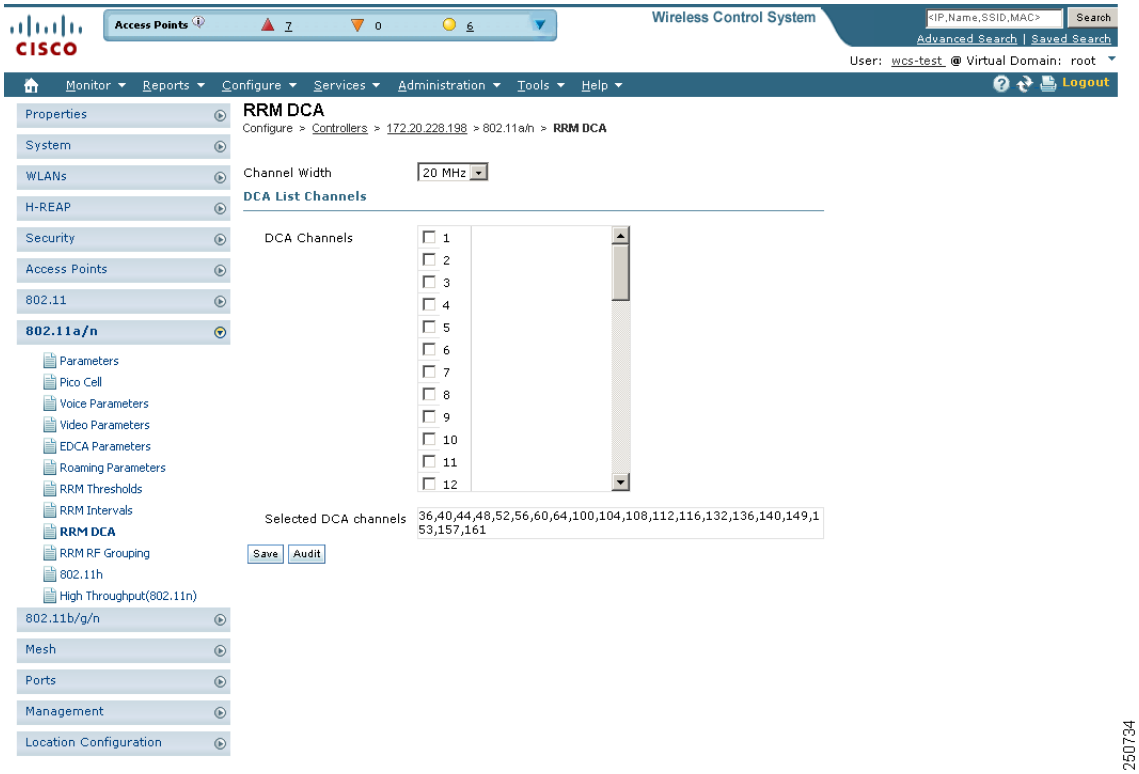
Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM DCA**. The 802.11a/n RRM DCA page appears (see Figure 10-11).

Note You can also configure the channel width on the access point page by choosing **Configure > Access Points** and clicking the **802.11a/n** link in the Radio column. The Current RF Channel Assignment. is provided, and you can choose a Global assignment method or choose Custom to specify a channel.

Figure 10-11 802.11a/n RRM DCA Page



Step 4 From the Channel Width drop-down list, choose **20 MHz** or **40 MHz**. Prior to software release 5.1, 40-MHz channels were only statically configurable. Only radios with 20-MHz channels were supported by DCA. With 40 MHz, radios can achieve higher instantaneous data rates; however, larger bandwidths reduce the number of non-overlapping channels so certain deployments could have reduced overall network throughput.

Note Be cautious about deploying a mix of 20-MHz and 40-MHz devices. The 40-MHz devices have slightly different channel access rules which may negatively impact the 20-MHz devices.

Note To view the channel width for an access point's radio, go to **Monitor > Access Points > <name> > Interfaces** tab. You can also view the channel width and antenna selections by choosing **Configure > Access Points** and clicking on the desired radio in the Radio column.

Step 5 Select the check boxes for the appropriate DCA channels. The selected channels are listed in the Selected DCA channels list.

Step 6 Enable or disable event-driven radio resource management (RRM) using the following parameters. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference.

- Event Driven RRM—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.
- Sensitivity Threshold—If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Step 7 Click **Save**.

Configuring EDCA Parameters for Individual Controller

The EDCA parameters (EDCA profile and Streaming MAC Enable settings) for 802.11a/n and 802.11b/g/n can be configured either by individual controller or through a controller template to improve voice QoS support. See the "Configuring EDCA Parameters through a Controller Template" section on page 12-88 for steps to configure a controller template.

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, do the following:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP Address of the applicable controller.

Step 3 From the left sidebar menu, select **802.11a/n > EDCA Parameters** or **802.11b/g/n > EDCA Parameters**.

Step 4 Choose an EDCA profile from the drop-down list. The choices include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice & Video Optimized. WMM is the default EDCA profile.

Note You must shut down radio interface before configuring EDCA Parameters.

Step 5 Select the **Low Latency MAC** check box to enable this feature.

Note Cisco recommends never to enable Low Latency MAC if serving voice clients.

Configuring SNMPv3

When you are configuring a controller, you can add SNMPv3 settings or change the setting (and any other settings) established from the previously added controller. (If SNMPv3 is enabled on the Ethernet switch, use the Ethernet switch CLI or switch UI to include all the OIDS and use the context option to create a group for each VLAN.) Follow these steps to set the SNMPv3 settings.

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP Address of the applicable controller or choose **Add Controller** from the Select a command drop-down list, and click **Go**.

Step 3 In the SNMP Parameters area of the page, choose **v3** from the Version drop-down list.

Step 4 You can change the retries and timeout values that were established for this controller if desired.

Step 5 In the Privacy Type drop-down list, choose **None, CBC-DES**, or **CFB-AES-128**. AES refers to the Advanced Encryption Standard algorithm established by the National Institute of Standards and Technology (NIST). It is more secure than older DES algorithms. CFB (Cipher Feedback) refers to the method AES uses to encrypt the packets, and 128 refers to the key length (128 bits).

Step 6 Any passwords used to derive encryption keys for algorithms using 128 but must contain a minimum of 12 characters. Enter a privacy password that fits this criteria.

Step 7 Click **OK**.

Viewing All Current Templates

Prior to software release 5.1, templates were detected when a controller was detected, and every configuration found on WCS for a controller had an associated template. Now templates are not automatically detected with controller discovery, and you can specify which WCS configurations you want to have associated templates.

The following rules apply for template discovery:

- Template discovery discovers templates that are not found in WCS.
- Existing templates are not discovered.
- Discovered templates are not associated to the configuration on the device.

Follow these steps to use the Discover Templates from Controller feature:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the check box for the applicable controller.

Step 3 From the Select a command drop-down list, choose **Discover Templates from Controller**.

Step 4 Click **Go**. The Discover Templates page displays the number of discovered templates and name of each template.

Note The configuration from the controller is refreshed if you select this option.

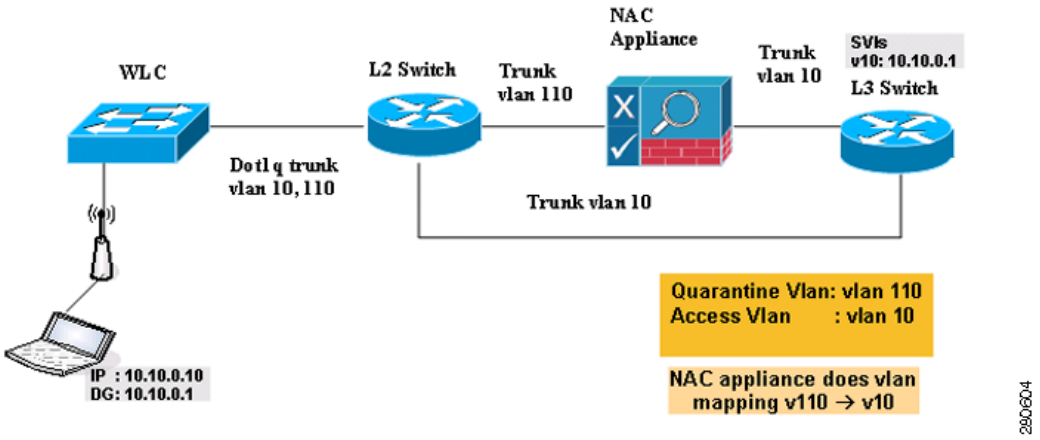
Configuring NAC Out-of-Band Integration

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 WCS 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 WCS software release 5.1, 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 10-12 provides an example of NAC out-of-band integration.

Figure 10-12 NAC Out-of-Band Integration



In Figure 10-12, 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.

Note CCA software release 4.5 or later is required for NAC out-of-band integration.

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.
- 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 See Chapter 15, “Configuring Hybrid REAP” 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 See the Cisco NAC appliance configuration guides for configuration instructions:

  http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Configuring NAC Out-of-Band Integration

Follow these steps to configure NAC out-of-band integration.

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

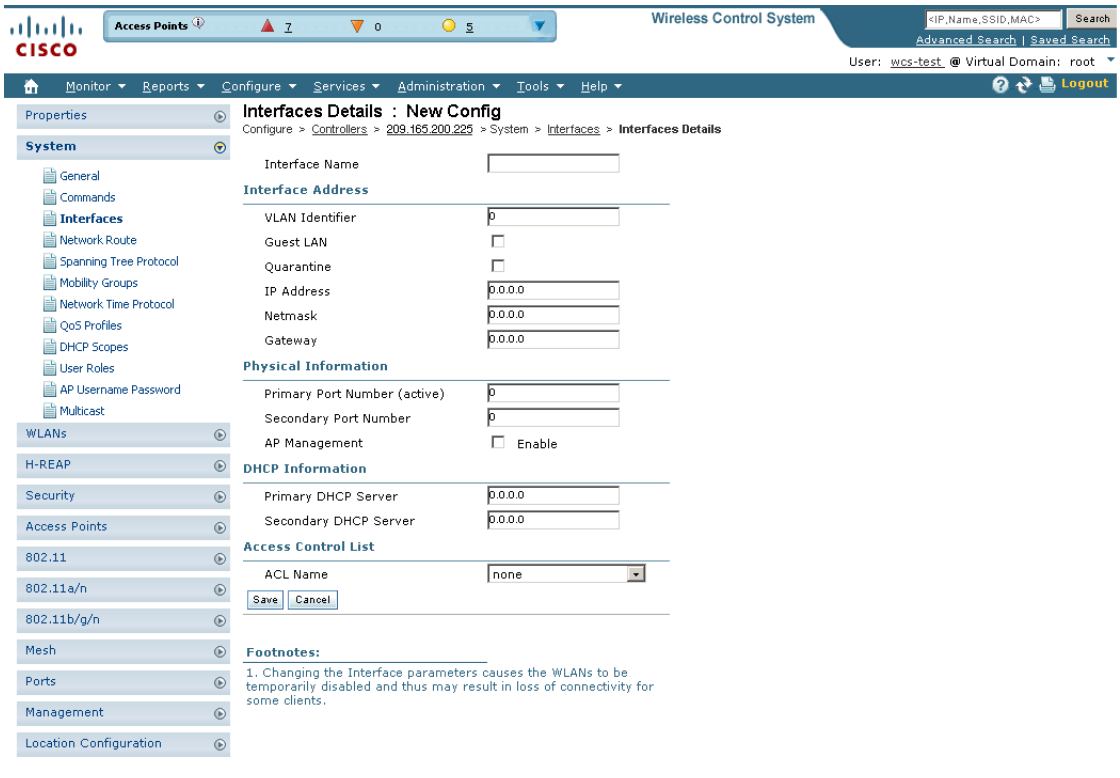
a. Choose **Configure > Controllers**.

b. Choose which controller you are configuring for out-of-band integration by clicking in the IP Address column.

c. Choose **System > Interfaces** from the left sidebar menu.

d. Choose **Add Interface** from the Select a command drop-down list. The Interface page appears (see Figure 10-13).

Figure 10-13 Interface Page



e. In the Interface Name text box, enter a name for this interface, such as “quarantine.”

f. In the VLAN Identifier text box, enter a non-zero value for the access VLAN ID, such as “10.”

g. Click to enable guest LAN.

h. Select the **Quarantine** check box if the interface has a quarantine VLAN ID configured on it.

Note You can have NAC support enabled on the WLAN or Guest WLAN template Advanced tab only for interfaces with quarantine enabled.

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.

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

j. Enter the primary port number.

k. Enter the secondary port number.

l. Select the **AP Management** check box to enable an AP-manager interface. A controller has one or more AP-manager interfaces that are used for all Layer 3 communications between the controller and lightweight access points after the access points have joined the controller.

m. Enter an IP address for the primary and secondary DHCP server.

n. Choose the user-defined name of the access control list (or none) from the drop-down list.

o. Click **Save**. You are now ready to create a NAC-enabled WLAN or guest LAN

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

a. Click **WLANs > WLAN Configuration** from the left sidebar menu.

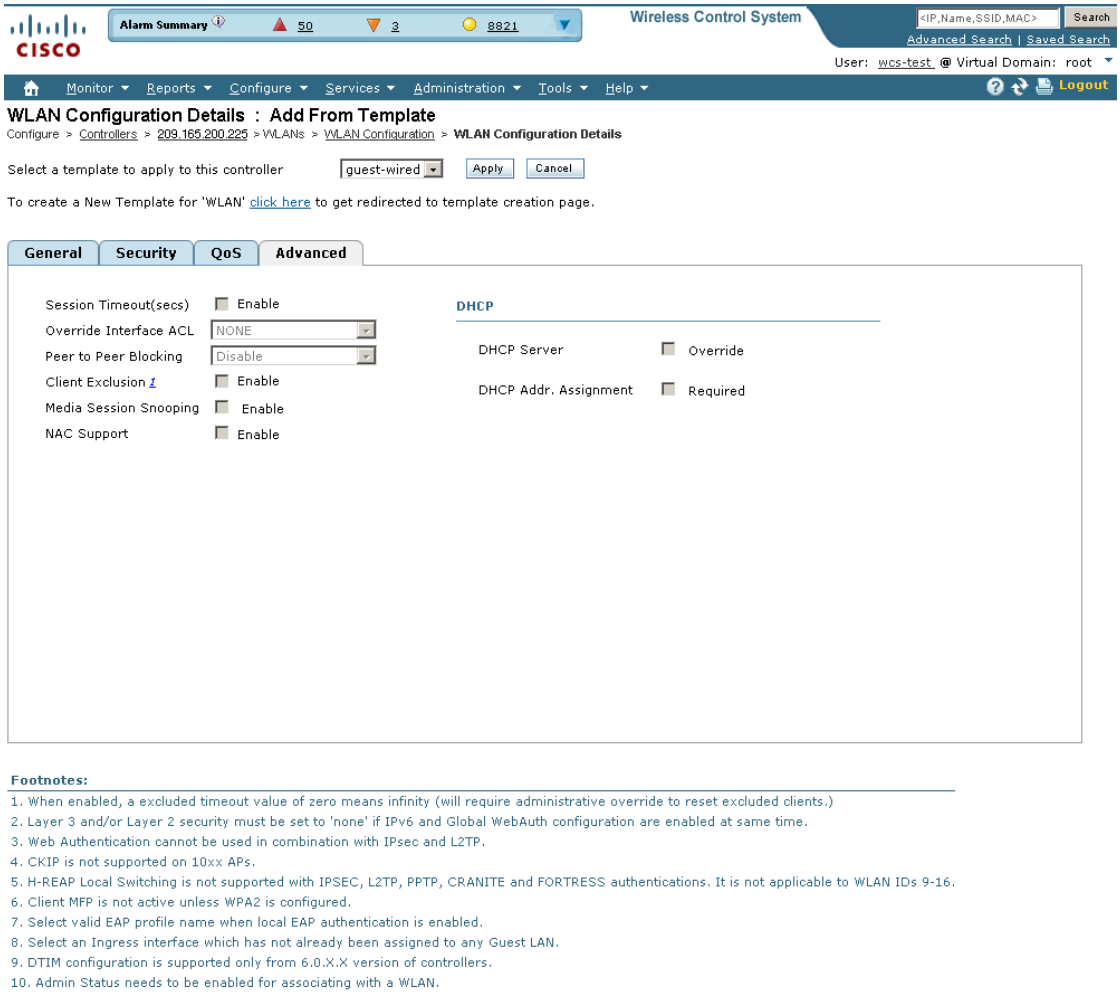
b. Choose **Add WLAN** from the Select a command drop-down list, and click **Go**.

c. If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the **click here** link to create a new template. For more information on setting up the template, refer to the "Configuring Wired Guest Access" section on page 10-50.

Note Ensure that WLAN IDs within the same network match before you forward the WLAN template.

d. Click the **Advanced** Tab (see Figure 10-14).

Figure 10-14 WLAN > Add From Template Page



e. To configure NAC out-of-band support for this WLAN or guest LAN, select the **NAC Support** check box. To disable NAC out-of-band support, leave the check box unselected, which is the default value.

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

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

a. Choose **WLANs > AP Groups** in the left sidebar menu to open the AP Groups page.

b. Click the name of the desired AP group.

c. To change the interface name to a quarantine-enabled VLAN, click the Edit icon.

d. To override NAC, click the Edit icon and click the Disabled check box.

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

Step 4 To see the current state of the client (either Quarantine or Access), follow these steps:

a. Click **Monitor > Clients** to open the Clients page and perform a search for clients.

b. In the client search page, you can specify to search for quarantine or access state.

Configuring Wired Guest Access

Wired Guest Access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room.

Like wireless guest user accounts, wired guest access ports are added to the network using the Lobby Ambassador feature. See the "Creating Guest User Accounts" section on page 7-10.

Wired Guest Access can be configured in a standalone configuration or in a dual controller configuration employing an anchor and foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

Wired Guest Access ports initially terminate on a Layer 2 access switch or switch port which is configured with VLAN interfaces for wired guest access traffic.

The wired guest traffic is then trunked from the access switch to a wireless LAN controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch.

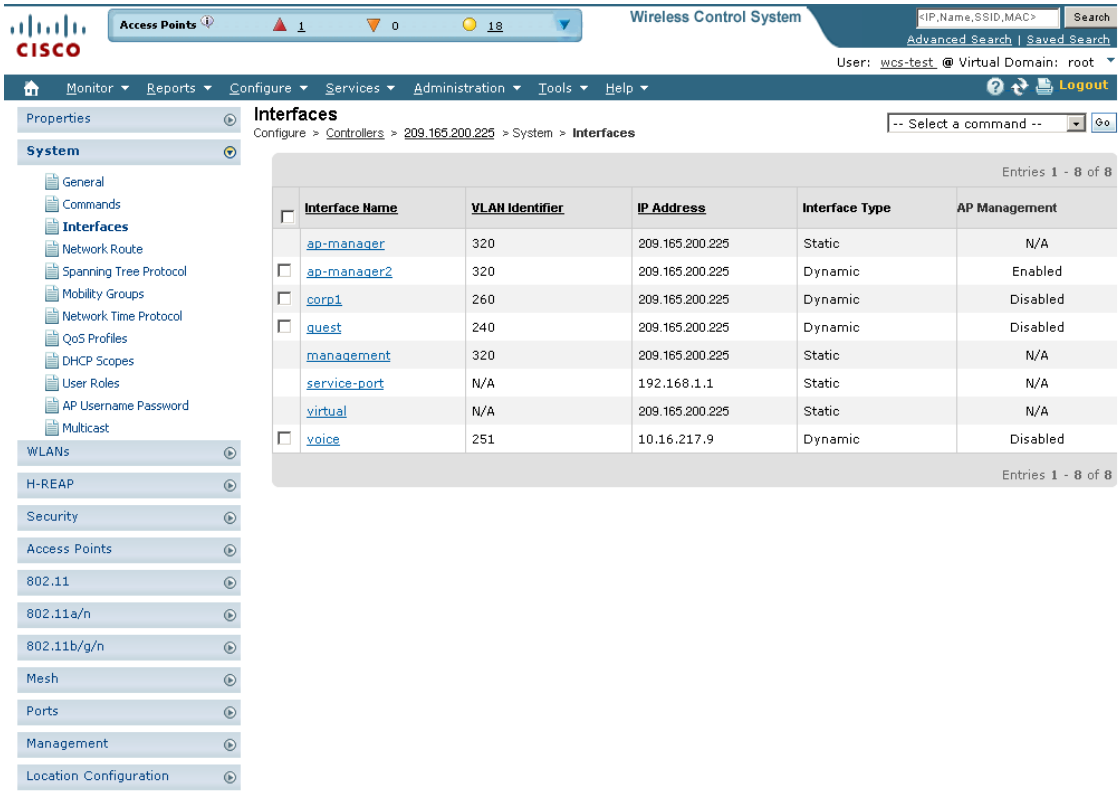
If two controllers are being used, the controller (foreign) that receives the wired guest traffic from the switch then forwards the wired guest traffic to an anchor controller that is also configured for wired guest access. After successful hand off of the wired guest traffic to the anchor controller, a bidirectional Ethernet over IP (EoIP) tunnel is established between the foreign and anchor controllers to handle this traffic.

Note Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

Note You can specify how much bandwidth a wired guest user is allocated in the network by configuring and assigning a role and bandwidth contract. For details on configuring these features, refer to the "Creating Guest User Accounts" section on page 7-10.

To create dynamic interfaces for wired guest user access, click **Configure > Controllers** and after choosing a particular IP address, choose **System > Interfaces**. The Interfaces page appears (see Figure 10-15). Two interfaces should be created: one for Ingress and one for Egress. The Ingress interface provides a path between the wired guest client and the controller by way of a Layer 2 access switch. The Egress interface provides a path out of the controller for the guest client traffic. You must complete the "Creating an Ingress Interface" section on page 10-51 and the "Creating an Egress Interface" section on page 10-52 before continuing to "Configuring DHCP Proxy" section on page 10-11. Both the Ingress and Egress Interfaces use the screen as shown in Figure 10-15.

Figure 10-15 Interfaces Summary Page



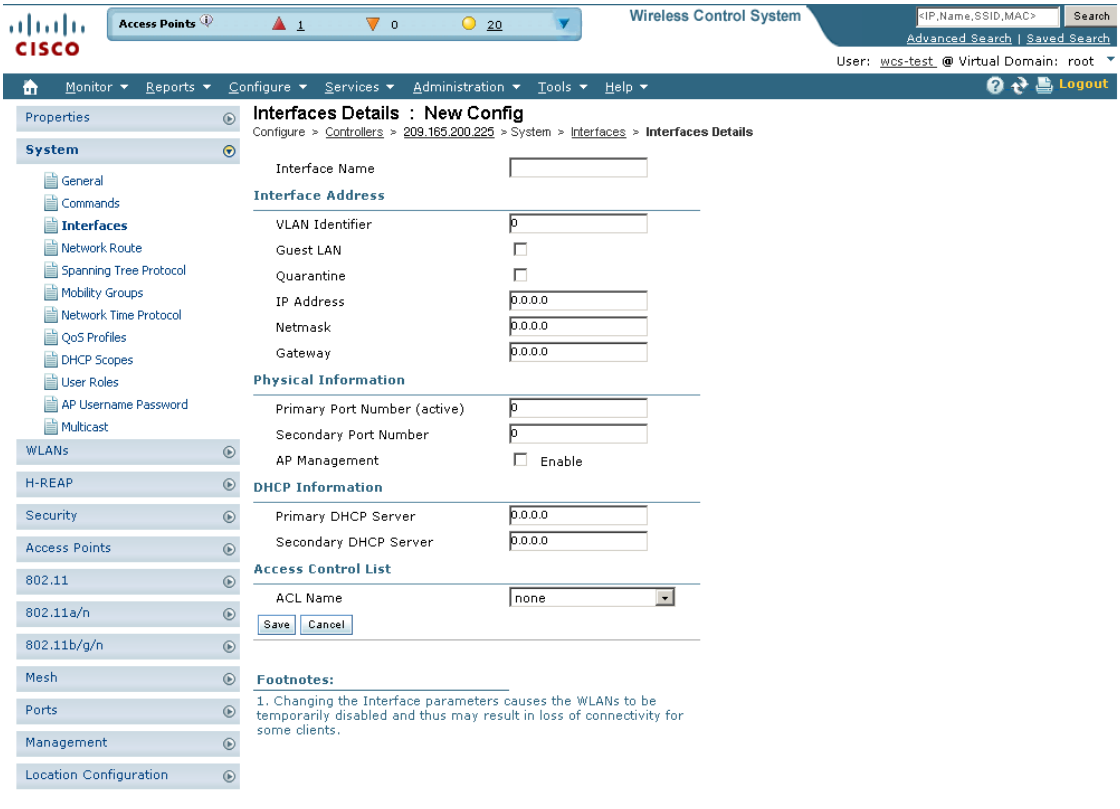
Creating an Ingress Interface

Follow these steps to create an Ingress interface.

Step 1 Choose **Add Interface** from the Select a command drop-down list, and click **Go**.

Step 2 Click an interface name. The Interfaces Details : New Config page appears (see Figure 10-16).

Figure 10-16 Interfaces Details : New Config Page



Step 3 In the Interface Name text box, enter a name for this interface, such as guestinterface.

Step 4 Enter a VLAN identifier for the new interface.

Step 5 Select the **Guest LAN** check box.

Step 6 Enter the primary and secondary port numbers.

Step 7 Click **Save**.

Creating an Egress Interface

Follow these steps to create an Egress interface.

Step 1 Choose **Add Interface** from the Select a command drop-down list, and click **Go**.

Step 2 Click an interface name. The Interfaces Details : New Config page appears (see Figure 10-16).

Step 3 In the Interface Name text box, enter a name for this interface, such as quarantine.

Step 4 In the VLAN Identifier text box, enter a non-zero value for the access VLAN ID, such as 10.

Step 5 Select the **Quarantine** check box and enter a non-zero value for the quarantine VLAN ID, such as 110.

Note You can have NAC-support enabled on the WLAN or guest WLAN template Advanced tab for interfaces with Quarantine enabled.

Step 6 Enter the IP address, netmask, and default gateway.

Step 7 Enter the primary and secondary port numbers.

Step 8 Provide an IP address for the primary and secondary DHCP server.

Step 9 Configure any remaining fields for this interface and click **Save**.

You are now ready to create a wired LAN for guest access.

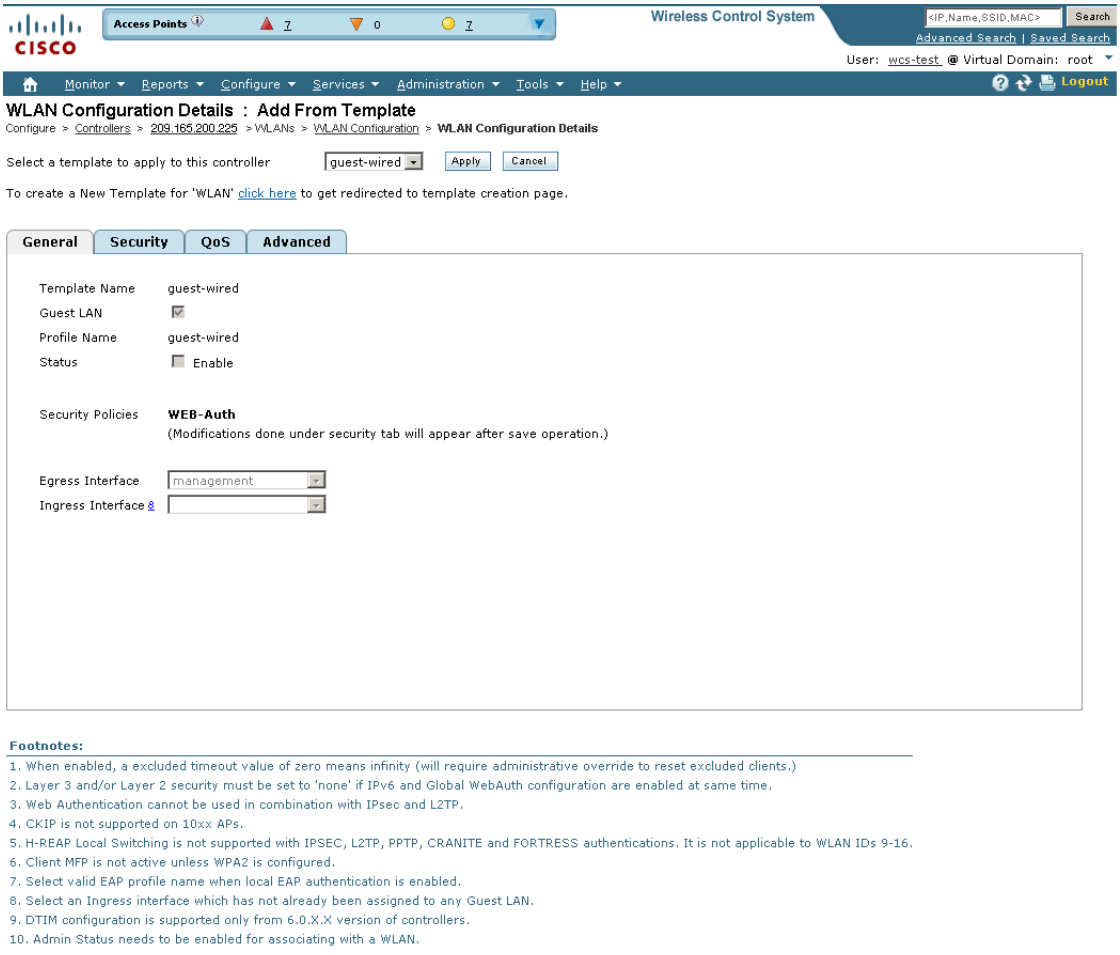
Creating a Wired LAN for Guest Access

Follow these steps to configure and enable wired guest user access on the network.

Step 1 To configure a wired LAN for guest user access, click **WLANs > WLAN Configuration** from the left sidebar menu.

Step 2 Choose **Add a WLAN** from the Select a command drop-down list, and click **Go**. The WLAN > Add From Template page appears (see Figure 10-17).

Figure 10-17 WLAN > Add From Template



Step 3 If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the **click here** link to create a new template.

Note Ensure that WLAN IDs within the same network match before you forward the WLAN template.

Step 4 On the New Template general tab, enter a name in the Template Name text box that identifies the guest LAN. Do not use any spaces in the name entered.

Step 5 Enable the **Guest LAN** check box.

Step 6 Enter the profile name.

Step 7 Select the **Enable** check box for the Status parameter.

Step 8 From the Interface Name drop-down list, choose the desired interface name.

Step 9 From the Egress Interface drop-down list, choose the Egress interface that you created in the "Creating an Egress Interface" section on page 10-52. This provides a path out of the controller for wired guest client traffic.

Note If you have only one controller in the configuration, choose **management** from the Egress Interface drop-down list.

Step 10 From the Ingress Interface drop-down list, choose the Ingress interface that you created in the "Creating an Ingress Interface" section on page 10-51. The provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 11 Click **Security > Layer 3** to modify the default security policy (web authentication) or to assign specific web authentication (login, logout, login failure) pages and the server source.

a. To change the security policy to passthrough, select the **Web Policy** check box and the **Passthrough** option. This option allows users to access the network without entering a username or password.

An Email Input check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

b. To specify custom web authentication pages, unselect the Global WebAuth Configuration **Enable** check box.

1. When the Web Auth Type drop-down list appears, choose one of the following options to define the web login page for the wireless guest users:

Internal—Displays the default web login page for the controller. This is the default value.

Customized—Displays custom web login, login failure, and logout pages. When the customized option is selected, three separate drop-down lists for login, login failure, and logout page selection appear. You do not need to define a customized page for all three of the options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.

These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files. For specifics on downloading custom pages, refer to the "Downloading Customized Web Authentication" section on page 3-48.

External—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA page. To do so, continue with Step 12.

Note The RADIUS and LDAP external servers must be already configured to have selectable options in the Security > AAA page. You can configure these servers in the RADIUS Authentication Servers page, TACACS+ Authentication Servers page, and LDAP Servers page.

Step 12 If you selected External as the Web Authentication Type in Step 11, click **Security > AAA Servers** and select up to three RADIUS and LDAP servers using the drop-down lists.

Step 13 Click **Save**.

Step 14 Repeat this process if a second (anchor) controller is being used in the network.

Using Switch Port Tracing

Currently, WCS provides rogue access point detection by retrieving information from the controller. The rogue access point table is populated with any detected BSSID addresses from any frames that are not present in the neighbor list. At the end of a specified interval, the contents of the rogue table are sent to the controller in a Lightweight Rogue AP Report message. With this method, WCS would simply gather the information received from the controllers; but with software release 5.1, you can now incorporate switch port tracing of wired rogue access point switch port. This enhancement allows you to react to found wired rogue access points and prevent future attacks. The trace information is available only in the WCS log and only for rogue access points, not rogue clients.

Note The rogue client and its rogue access point information is used to track the switch port to which the rogue access point is connected in the network.

Note If you try to set tracing for a friendly or deleted rogue, a warning message appears.

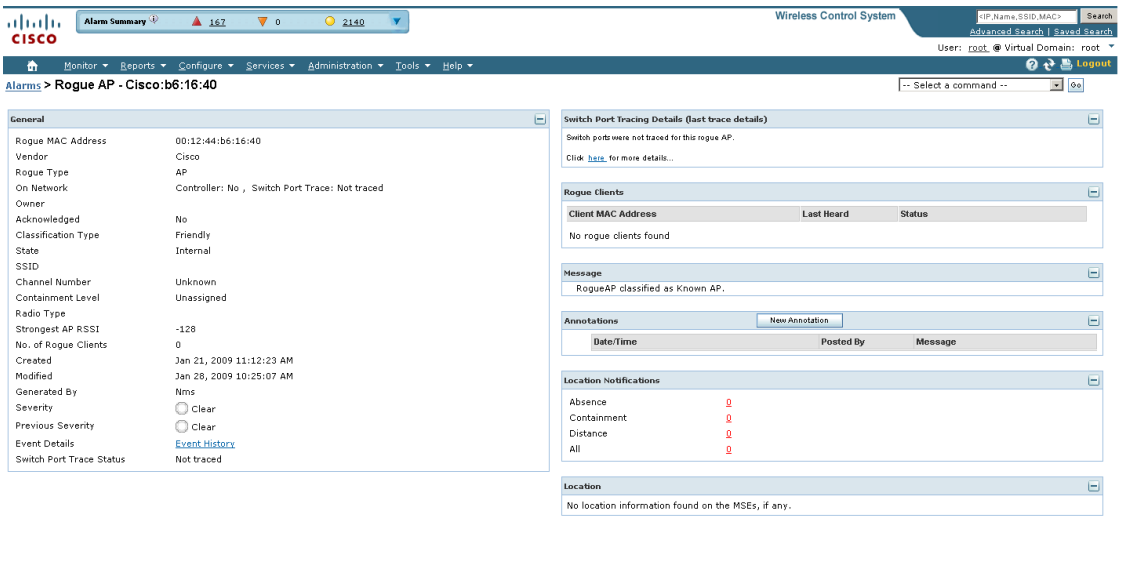
Follow these steps to establish switch port tracing. See the "Switch Port Trace" section on page 18-60 for further information.

Step 1 In the WCS home page, click the **Security** tab.

Step 2 In the Rogue APs and Adhoc Rogues section, click the URL that specifies the number of rogues in the last hour, last 24 hours, or total active.

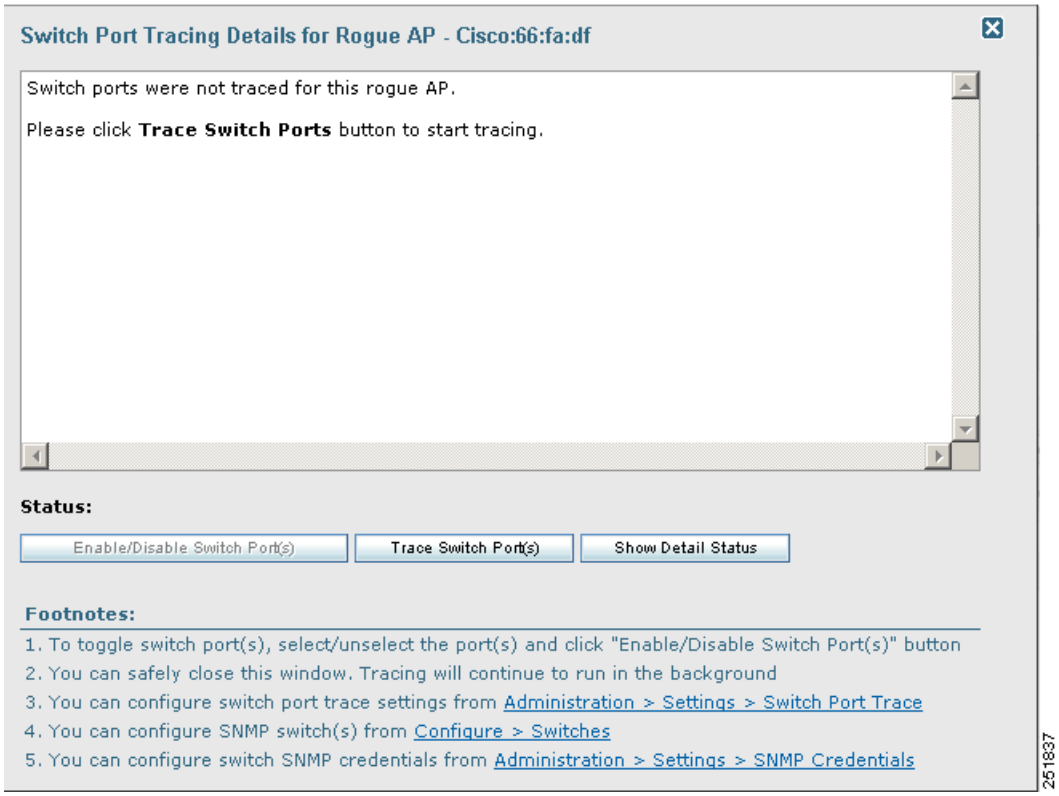
Step 3 Choose the rogue for which you are setting switch port tracking by clicking the URL in the Rogue MAC Address column. The Alarms > Rogue AP details page appears (see Figure 10-18).

Figure 10-18 Trace Switch Port option on the Alarms > Rogue Page



Step 4 In the Switch Port Tracing Details portion of the page, click the **Click here for more details** link. The Switch Port Tracing Details for Rogue AP page appears (see Figure 10-19).

Figure 10-19 Switch Port Tracing Details for Rogue AP Page



This page provides the current port status. The various status types include the following:

- Not traced—Switch port tracing was never executed.
- Failed—Switch port tracing was executed but failed for some reason. The detail status page in the SPT dialog includes more information.
- Traced and detected on network—Switch port tracing was executed, and a rogue access point was found on the wired network. A *yes* status indicates a wired network.
- Traced and wire contained—Switch port tracing was executed, but the switch port to which the rogue access point was connected is disabled. The rogue access point is now wire contained.

From this page, you can start a trace for troubleshooting purposes by clicking **Trace Switch Ports**. You can also enable and then provide the IP address and hop information or disable switch ports.

When one or more searchable MAC addresses are available, the WCS uses CDP to discover any switches connected up to two hops away from the detecting access point. SPT uses the directly connected Ethernet switches of the detecting access points as the seed switches for tracing. The MIBs of each CDP discovered switch are examined to see if they contain any of the target MAC addresses; therefore, it is important that the access point CDP information is enabled and available. If any of the MAC addresses are found, the corresponding port number is returned and reported as the rogue's switch port.

You can view the access point CDP neighbors choosing Monitor > Access Points and the CDP Neighbors tab. No entries signify that CDP is not enabled on the access point.

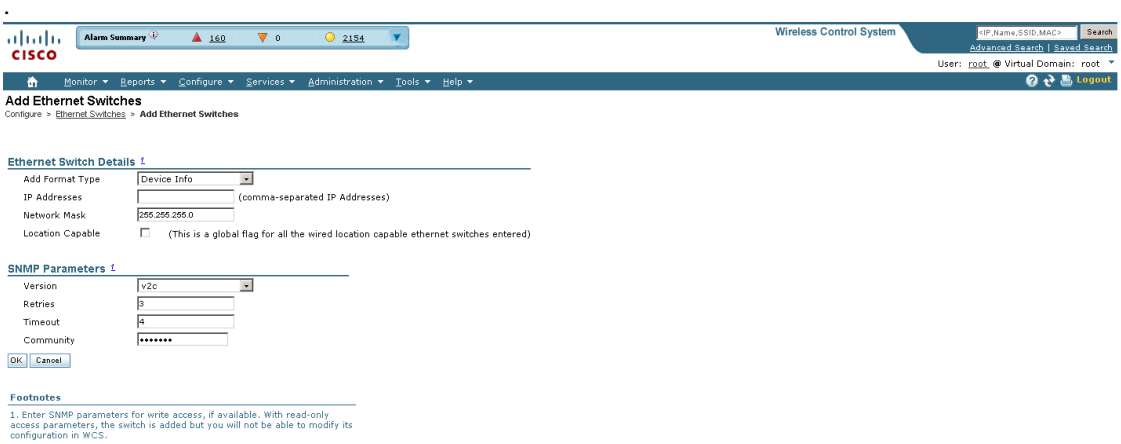
You can configure switch port trace settings by choosing Administration > Settings > Switch Port Trace. See the "Switch Port Trace" section on page 18-60 for more information.

Note If switch port tracing is taking a long time, adjust the settings in the "SNMP Settings" section on page 18-58.

Click the **Message** link in the Annotations section to re-enable the switch port.

Step 5 If you choose Configure > Ethernet Switches, the SNMP communities for the switches are visible (see Figure 10-20). The switch details configured on this page are used only for tracing the rogue access point's switch port. At this same location you can add a location-capable switch for tracking wired clients by MSE and WCS.

Figure 10-20 Configure > Ethernet Switches



251771

Step 6 Choose one of the following:

- If you want to add one switch or use commas to separate multiple switches, leave the Add Format Type drop-down list at Device Info.
- If you want to add multiple switches by importing a CSV file, choose **File** from the Add Format Type drop-down list. With the CSV file, you can generate your own import file and add the devices you want.

Step 7 If you chose Device Info, enter the IP address of the switch you want to add. If you want to add multiple switches, use a comma between the string of IP addresses.

Step 8 Enter the network mask for the IP address you specified.

Step 9 Select the Location Capable check box if the switch is capable of storing the location information.

Step 10 In the SNMP Parameters portion of the page, choose your version choice from the Version drop-down list.

Note For switch port tracing to be successful in switches configured with SNMP V3, the context for the corresponding VLAN must be configured in the switch. To configure SNMPv on the switch, use the following example:

snmp-server view v3default iso included
snmp-server group v3group v3 auth write v3default snmp-server user <username> <v3group> v3 auth <md5 or sha> <authentication password>

If the switch has VLANs, the following must be configured for each VLAN. Otherwise, switch port tracing will fail:

snmp-server group v3group v3 auth context vlan-1 write v3default snmp-server group v3group v3 auth context vlan-20 write v3default

Step 11 You can change the retries and timeout values that were established for this switch if desired.

Step 12 Enter the community for this switch.

Step 13 Click **OK**.

Troubleshooting New Switch Failure

If adding a new switch fails with the reason "**Not a switch device**", follow these steps to check if switch port tracing is established:

Step 1 Check the new switch in the list of the devices from **SwitchPortTracingUtil.properties** in **C:\Program Files\WCS7.0.x.x\webnms\classes\com\cisco\server\spt** in windows and **opt/WCS7.0.x.x/webnms/classes/com/cisco/server/spt** in linux.

Step 2 Each device supported by WCS is characterized by the OID 1.3.6.1.4.1.9.1.X, where '1.3.6.1.4.1.9.1' is the root OID for 'CiscoProducts' and 'X' is the value specific to the sysObjectID of the switch.

Note WCS does not contain the sysObjectID's for all the Cisco switches, Only some are pre-configured.

Step 3 Check the sysObjectID of the new switch with an SNMP walk to the OID 1.3.6.1.2.1.1.2:

snmpwalk -v <version> -c <community> <switch_IP> .1.3.6.1.2.1.1.2 which should return SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.X where X is a value specific to the new switch.

Step 4 Verify if there is a line 1.3.6.1.4.1.9.1.X in the **SwitchPortTracingUtil.properties** file, where the X indicates the value specific to the new switch obtained from the previous step. If the line is not present, stop the WCS Services, edit the file and insert the line and save the file. Restart the WCS Services. Confirm if the new switch is added to the list of devices in **SwitchPortTracingUtil.properties**.

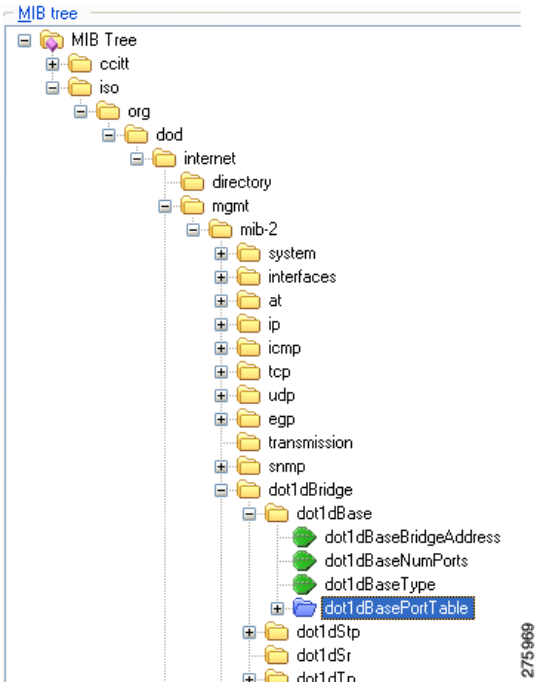
Switch VLANs

Switch Port Trace (SPT) queries the switch CAM table for each VLAN; therefore, the switch must be an unreserved and operational Ethernet VLAN for success of the query. SPT queries vtpVlanTable to determine the VLAN list.

For each VLAN, SPT searches the CAM table for the MAC address. Since CAM tables are stored per VLAN, community string indexing is used to query the switch CAM table. SPT queries dot1dTpFdbTable to get the CAM table entries. In addition to the switch CAM table, SPT also queries the following MIB tables (see Figure 10-21).

Note The switch CAM table must be accessible using community string indexing (such as public@1).

Figure 10-21 MIB Tables



The following MIBs are used by SPT:

Table 10-6 MIBs Used by SPT

MIB	Purpose
vtpVlanTable (CISCO-VTP-MIB)	For VLAN list
dot1dTpFdbTable (BRIDGE MIB)	For query of CAM table entries
dot1dBasePortTable (BRIDGE MIB)	To map base port to ifIndex
ifTable (IF-MIB)	For interface list
ifXTable (IF-MIB)	For interface description (ifAlias)

Table 10-6 MIBs Used by SPT

MIB	Purpose
vlanTrunkPortTable	For trunk port status
cdpCacheTable	For switch CDP neighbors

Removing Switches

You can remove switches by choosing **Configure > Switches** and choosing **Remove Switches** from the Select a command drop-down list.

Shutting a Switch Port

You can suppress the switch port to which the rogue access point is connected. In the Alarms Rogue page (shown in Figure 10-18), choose **Shut Switch Port** from the Select a command drop-down list.

The Alarms page will then show the switch IP address, the switch port, the traced MAC address, the port status, and the timestamp of the suppression.

Client Access on 1524SB Dual Backhaul

The 1524 Serial Backhaul (SB) access point consists of three radio slots. Radios in slot-0 operates in 2.4 GHz frequency band and is used for client access. Radios in slot-1 and slot-2 operate in 5.8 GHz band and are primarily used for backhaul. However, with Universal Client Access feature, client access is also allowed over slot-1 radio and slot-2 radio.

The two 802.11a backhaul radios use the same MAC address. So there maybe instances where same WLAN maps to the same BSSID on more than one slot.

By default Client Access is disabled over both the backhaul radios by default.

The following are the guidelines to be followed for enabling or disabling a radio slot:

- You can enable client access on slot-1 even if client access on slot-2 is disabled.
- You can enable client access on slot-2 only when client access on slot-1 is enabled.
- If you disable client access on slot-1 the client access on slot-2 is automatically disabled.
- All the Mesh Access Points reboot whenever the client access is enabled or disabled.

You can configure client access over both the backhaul radio from either one of the interfaces:

- The Controller Command Line Interface (CLI)
- The Controller Graphical User Interface (GUI)
- The Wireless Control System (WCS) Graphical User Interface (GUI). For more information, see Configuring Client Access using WCS.

Note The procedure for configuring client access using Controller CLI and GUI is documented in the Controller Configuration Guide. See the *Cisco Wireless LAN Controller Configuration Guide* for more information.

Configuring Client Access using WCS

To configure client access on the two backhaul radios:

Step 1 Choose **Configure > Controllers > Controller IP > Mesh > Mesh Settings**.

The Mesh Settings dialog box appears.

Step 2 Select the **Client Access on Backhaul Link** check box to display Extended Backhaul Client Access check box.

Step 3 Select the **Extended Backhaul Client Access** check box if you want to enable extended backhaul client access.

Step 4 Click **Save**.

An alert box is displayed:

```
Enabling client access on both backhaul slots will use same BSSIDs on both the slots.
Changing Backhaul Client Access will reboot all Mesh APs.
```

Step 5 Click **OK**.

The Universal Client access is configured on both the radios.

Backhaul Channel Deselection Using WCS

To configure backhaul channel deselection:

Step 1 You must first configure the Mesh DCA channels flag on the controllers. See Configuring Mesh DCA Flag on Controllers Using WCS for more information.

Step 2 Then change the channel list using config groups. See Changing the Channel List Using Config Groups for more information.

Configuring Mesh DCA Flag on Controllers Using WCS

You can configure the Mesh DCA Channel flag to push each channel change on one or more controllers to all the associated 1524SB access points. To configure this feature, follow these steps:

Step 1 Choose **Configure > Controllers >** *ip address of controller* **> Mesh > Mesh Settings** to configure this flag for a specific controller.

Or

Configure > Controller Template Launch Pad > Mesh > Mesh Settings to configure this flag for a list of controllers.

The Mesh Settings page appears.

Step 2 From the general options, select the **Mesh DCA Channels** option to enable channel selection. This option is unselected by default.

Now the channel changes in the controllers are pushed to the associated 1524SB access points.

Changing the Channel List Using Config Groups

You can use controller config groups to configure backhaul channel deselection. You can create a config group and add the required controllers into the group and use the Country/DCA tab to select or deselect channels for the controllers in that group.

To configure backhaul channel deselection using config groups:

Step 1 Choose **Configure > Controller Config Groups**.

Step 2 Select a config group to view its config group details.

Step 3 In the Config Group detail page, click the **Country/DCA** tab.

Step 4 Select or unselect the channels to select or deselect channels for the config group.

Note You can also configure backhaul channel deselection from controllers. For more information, see the Controller Online Help or *Cisco Wireless LAN Controller Configuration Guide*.

Background Scanning on 1510s in Mesh Networks

Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents. Because the access points are searching on neighboring channels as well as the current channel, the list of optimal alternate paths and parents is greater.

Identifying this information prior to the loss of a parent results in a faster transfer and the best link possible for the access points. Additionally, access points might switch to a new channel if a link on that channel is found to be better than the current channel in terms of fewer hops, stronger signal-to-noise ratio (SNR), and so on.

Background scanning on other channels and data collection from neighbors on those channels are performed on the primary backhaul between two access points:

The primary backhaul for 1510s operate on the 802.11a link.

Background scanning is enabled on a global basis on the access point's associated controller.

Note Latency might increase for voice calls when they are switched to a new channel.

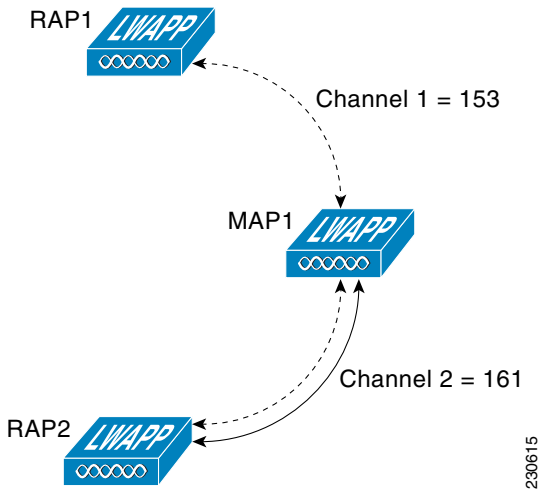
Note In the EMEA regulatory domain, locating neighbors on other channels might take longer given DFS requirements.

Background Scanning Scenarios

A few scenarios are provided below to better illustrate how background scanning operates.

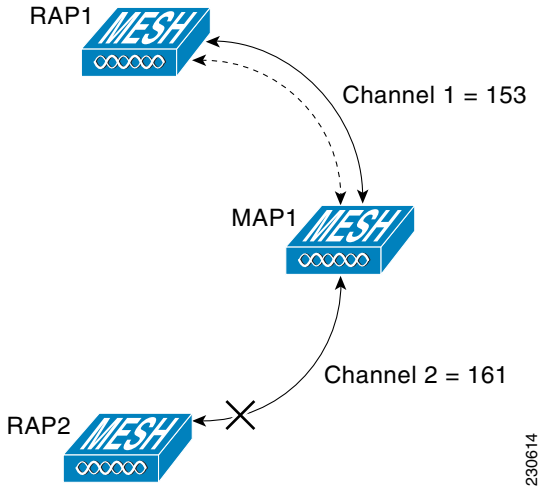
In Figure 10-22, when the mesh access point (MAP1) initially comes up, it is aware of both root access points (RAP1 and RAP2) as possible parents. It chooses RAP2 as its parent because the route through RAP2 is better in terms of hops, SNR, and so on. After the link is established, background scanning (once enabled) continuously monitors all channels in search of a more optimal path and parent. RAP2 continues to act as parent for MAP1 and communicates on channel 2 until either the link goes down or a more optimal path is located on another channel.

Figure 10-22 Mesh Access Point (MAP1) Selects a Parent



In Figure 10-23, the link between MAP1 and RAP2 is lost. Data from ongoing background scanning identifies RAP1 and channel 1 as the next best parent and communication path for MAP1 so that link is established immediately without the need for additional scanning after the link to RAP2 goes down.

Figure 10-23 Background Scanning Identifies a New Parent



Enabling Background Scanning

Follow these steps to enable background scanning on an AP1510 RAP or MAP:

Step 1 Click **Configure > Controllers.**

Note You can also enable this on the Controllers template. See the "Configuring a Mesh Template" section on page 12-98.

Step 2 Choose **Mesh > Mesh Settings** from the left sidebar menu. The Mesh Settings page appears (see Figure 10-24).

Figure 10-24 Mesh Settings Page

Step 3 Select the **Background Scanning** check box to enable background scanning or unselect it to disable the feature. The default value is disabled.

Step 4 Click **Save**.

Configuring QoS Profiles

You can have multiple QoS Profiles on the controller. The 4 default QoS profiles are bronze, silver, gold, and platinum. Follow these steps to modify the existing QoS profiles.

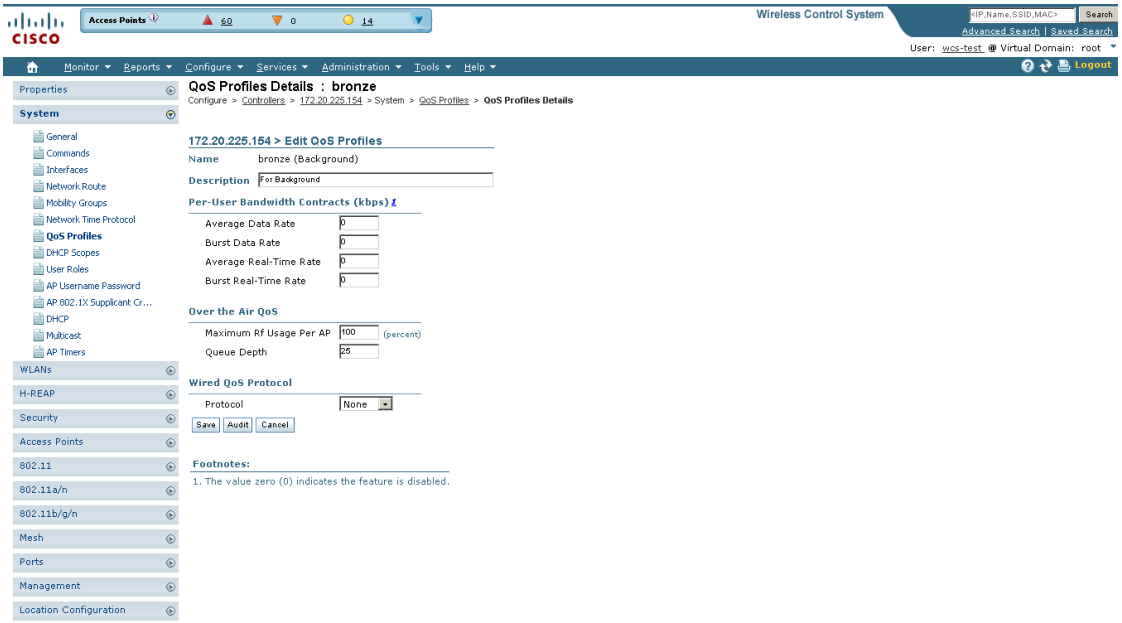
Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the desired controller.

Step 3 Choose **System > QoS Profiles** from the left sidebar menu.

Step 4 Choose the profile you want to modify. The Edit QoS Profiles page appears (see Figure 10-25).

Figure 10-25 QoS Profiles Details Page



251799