CHAPTER 9

Configuring Controllers and Access Points

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

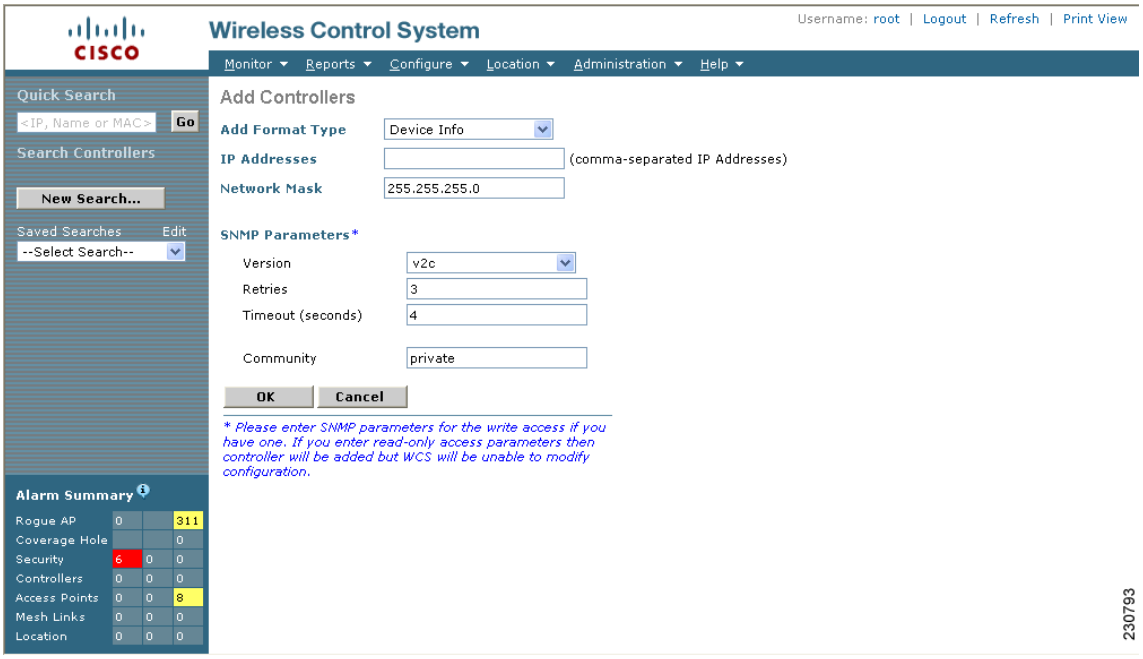
Adding Controllers

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 menu choose **Add Controllers** and click **GO**. The Add Controller window appears (see Figure 9-1).

Figure 9-1 Add Controller Window



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 menu at Device Info.

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

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 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.

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

Step 5 Click **OK**.

Setting Multiple Country Codes

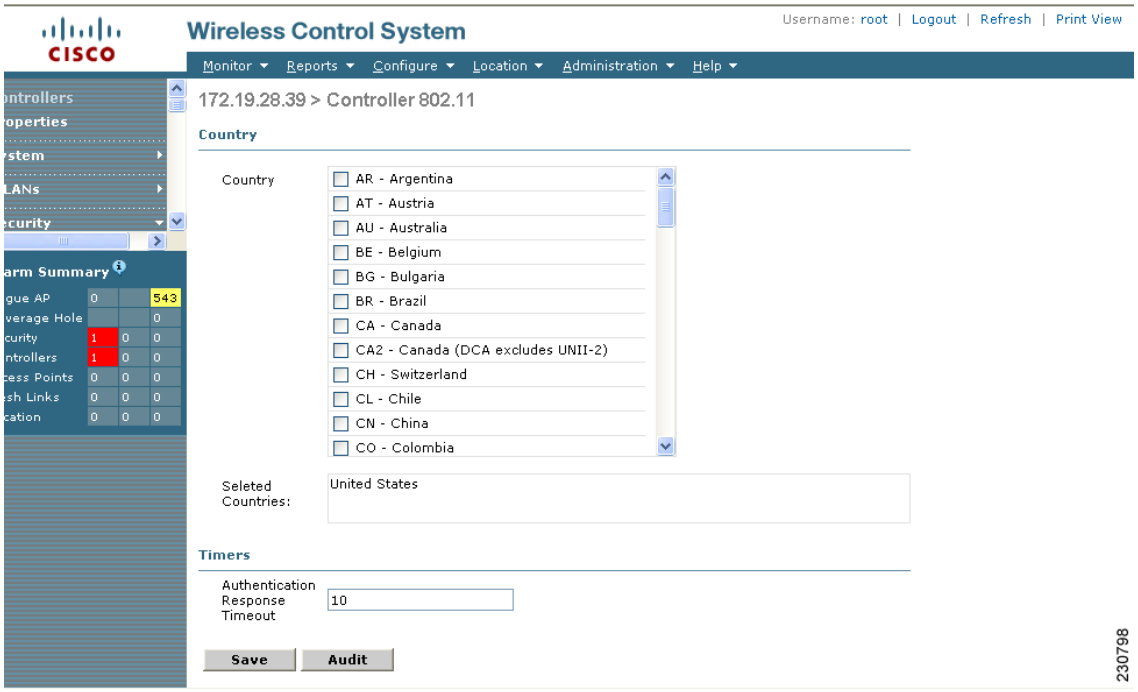
To set multiple country support for a single controller(s) that is not part of a mobility group, follow the steps below.

Step 1 Choose **Configure > Controllers**.

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

Step 3 Select **802.11 > General** from the left sidebar menu. The Controller 802.11 window appears (see Figure 9-2).

Figure 9-2 Controller 802.11



Step 4 Click the check box to choose which country you want to add. 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/warp/public/779/smbiz/wireless/approvals.html.

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

Step 6 Click **Save**.

Searching Controllers

Use the controls in the left sidebar to create and save custom searches:

- **New Search** drop-down menu: Opens the Search Controllers window. Use the Search Controllers window to configure, run, and save searches.
- **Saved Searches** drop-down menu: Lists the saved custom searches. To open a saved search, choose it from the Saved Searches list.
- **Edit Link**: Opens the Edit Saved Searches window. You can delete saved searches in the Edit Saved Searches window.

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

- Search for controller by— Choose all controllers, IP address, or controller name.
- Select a Network— Choose all networks or an individual network.
- Save Search— Check the Save Search check box and enter a name in the Save Search text field to save the search in the Saved Searches drop-down list.
- Search by 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 window. The range is 10 to 100 items per window. The default is 20.

After you click **GO**, the controller search results appear:

Table 9-1 Search Results

Parameter	Options
IP Address	Local network IP address of the controller management interface. Clicking the title toggles from ascending to descending order. Clicking an IP address in the list displays a summary of the controller details.
WCS	User-defined WCS name.
Controller Name	Clicking the title toggles from ascending to descending order.
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 from ascending to descending order.

Table 9-1 Search Results

Parameter	Options
Mobility Group Name	Name of the controller or WPS group.
Reachability Status	Reachable or Unreachable. Clicking the title toggles from ascending to descending order.

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 authentication using the local database fails, the controller uses the next type of server.

Step 5 Click **Save**.

Viewing Audit Status (for Controllers)

An Audit Status column on the Configure > Controllers window shows audit status for each of the controllers based on the last audit. You can also view the network audit report for the selected controllers. The report shows the time of the audit, the IP address of the selected controller, and the synchronization status.

Step 1 Choose **Configure > Controllers**.

Step 2 You can view the latest audit report in one of two ways:

Check the check boxes of the controllers for which you want audit reports. Choose **Audit Now** from the Select a command drop-down list and click **GO**. This method shows the report from the network audit task and not an on-demand audit per controller.

or

Click the Audit Status column value to go to 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 If you mouse over the Audit Status column value, the time of the last audit is displayed.

The Audit Report displays the device name, configuration name, time of audit, audit status for each configuration (mismatch or identical), attribute for each configuration (AP Group Name, IP address), value in WCS, and value in controller.

To run an on-demand audit report, select for which controller you want to run the report and choose **Audit Now** from the Select a command drop-down menu. 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.

Step 3 If configuration differences are found as a result of the audit, you can either restore WCS values on the controller or refresh controller values to synchronize WCS with the controller. Choose **Restore WCS Values** or **Refresh Controller Values**.

Note If you choose to refresh the controller values, you receive a Refresh Config window with two options for "Configuration if present on WCS but not on device, do you wish to:"

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 WCS matches the most recent configuration you are refreshing from WLCs.

Note When WCS does a Refresh Config, 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.

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 menu, choose **View Latest Network Audit Report**.

Step 4 Click **GO**.

The Audit Summary displays the time of the audit, the IP address of the selected controller, and the audit status. If any configuration differences exist, they are shown in the details.

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

Note From 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 menu. 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.

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 10-57.

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

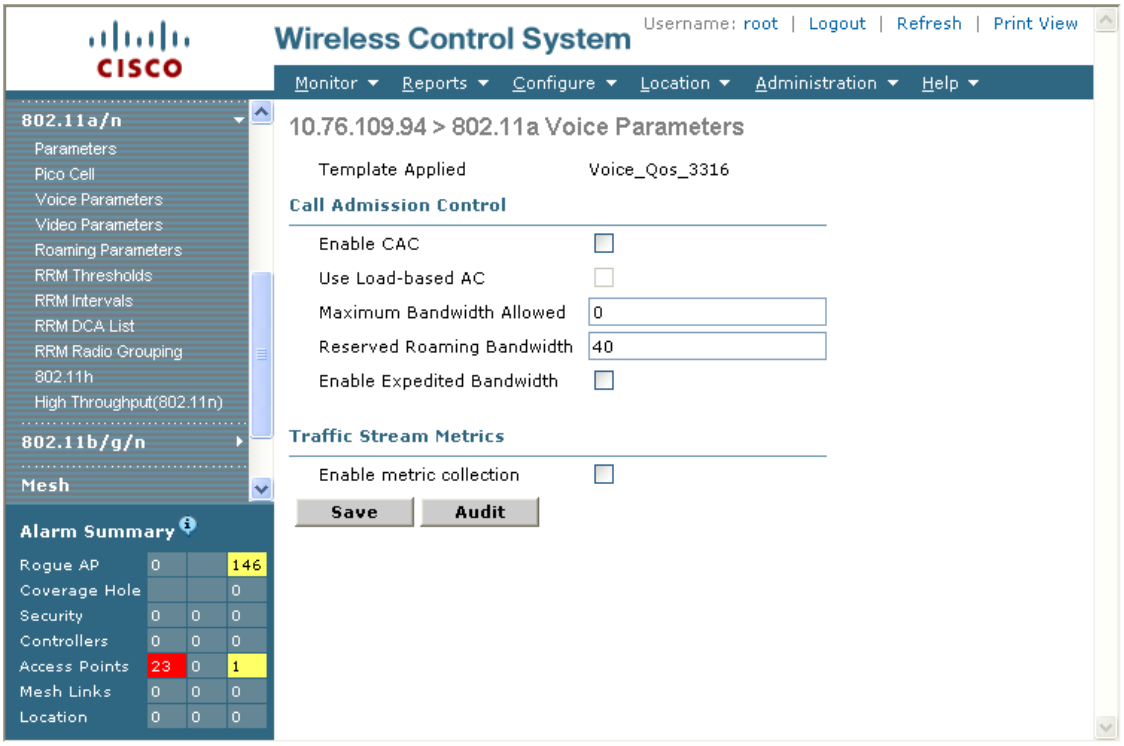
Step 1 Click **Configure > Controllers**.

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 9-3).

Figure 9-3 802.11a/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**.

Enabling High Density

The high density deployments are enabled with Cisco Unified Wireless Network software release 4.1 in conjunction with the Cisco and Intel Business Class Suite Version 2 initiative.

The high density networking feature is designed for large, multi-cell high density wireless networks in which it can be challenging to populate a site with a large number of lightweight access points to manage the cumulative bandwidth load while diminishing the contention between access points and still maintaining quality of service. To optimize RF channel capacity and improve network performance, the high density (or pico cell) mode parameters are introduced.

With this feature you can manually configure the transmit power, receiver sensitivity thresholds, and clear channel assessment sensitivity threshold of Intel client devices and Cisco Aironet lightweight access points in order to create optimal high-density deployments. When a client that supports high density associates to an access point with high-density enabled, they exchange specific 802.11 information element s (IEs) that instruct the client to adhere to the access point's advertised received sensitivity threshold, CCA sensitivity threshold, and transmit power levels. These three parameters reduce the effective cell size by adjusting the received signal strength before an access point and client consider the channel accessible for the transfer of packets. When all access points and clients raise the signal standard in this way throughout a high density area, access points can be deployed closer together, minimizing interference with each other and managing environmental and distant rogue signals.

Note High density is off by default. There are deployment risks involved if you change from the predetermined values. Do not attempt to configure pico cell functionality within your wireless LAN without the advice of Cisco technical support. Non-standard installation is not supported.

Along with these configuration changes, you can further optimize the pico cell deployment as follows:

Requirements

High density has the following restrictions:

- Only Cisco lightweight access points (except the AP1030 and 1500 series mesh access points) and the Intel PRO/Wireless 3945ABG and Intel Wireless WiFi Link 4965AGN clients are supported.
- Only 802.11a/n networks with high density deployments are supported.

Note Cisco recommends the use of high density only in new WLAN deployments in which all clients and lightweight access points support the high-density feature.

Optimizing the Controller to Support High Density

To optimize a controller to support high density, you need to enable pico cell mode v2. A method to mitigate the inter-cell contention problem in high-density networks is to adjust the access point and client receiver sensitivity, CCA sensitivity, and transmit power parameters in a relatively cooperative manner. By adjusting these variables, the effective cell size can be reduced, not by lowering the transmit power but by increasing the necessary received power before an access point and client consider the channel sufficiently clear for packet transfer. These similar values can be set in the Controller Templates portion of the GUI. Refer to Adding Controller Templates, page 10-1. Follow these steps to configure high density.

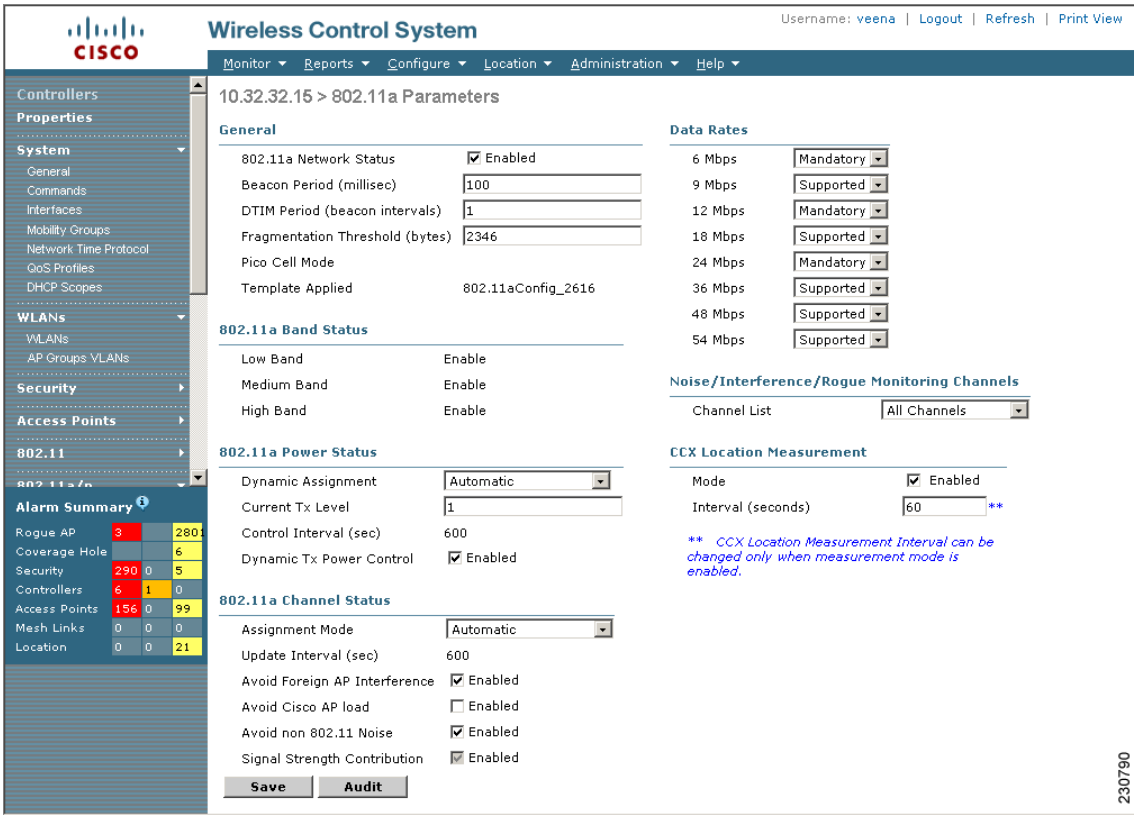
Note If you enable pico cell, the default values for auto RF adjust according to the values suggested for Intel 3945ABG clients. The transmit power is set to 10 dBm, CCA sensitivity threshold to -65 dBm, and receiver sensitivity threshold to -65 dBm.

Step 1 Choose **Configure > Controllers**.

Step 2 Go to **802.11a/n > Parameters** and ensure that the 802.11a/n Network Status check box is not enabled.

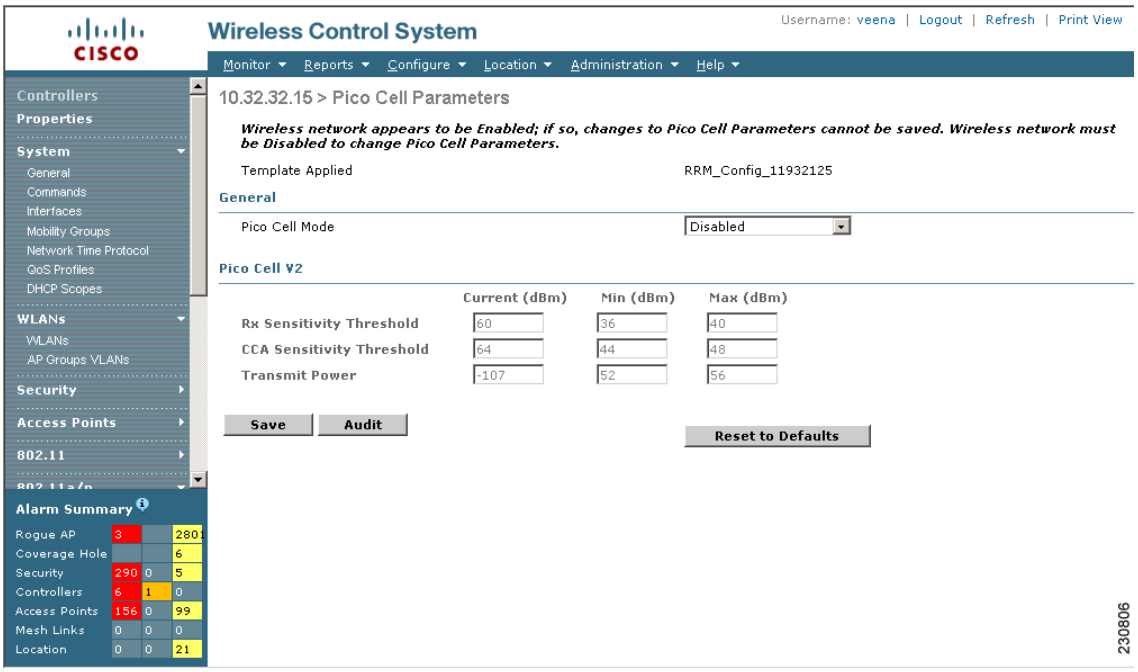
Step 3 From the left sidebar menu, choose **802.11a/n > Parameters**. The window as shown in Figure 9-4 appears.

Figure 9-4 Pico Cell Parameter



Step 4 In the General portion of this window, you see a Pico Cell Mode parameter. If you hover around this parameter click the link that appears, the window shown in Figure 9-5 appears. You can also get to this window by directly choosing **802.11a/n > Pico Cell** from the left sidebar menu.

Figure 9-5 Pico Cell Parameters Window



Note If the Pico Cell Mode parameter is set to Disabled or V1, the Pico Cell V2 parameters are grayed out.

Step 5 From the Pico Cell Mode drop-down menu, choose **V2**. By choosing V2, the high-density parameters for the access point and clients share the same values and make communication symmetrical. This selection also allows you to enter values for Rx sensitivity, CCA sensitivity, and transmit power, although the defaulted minimum and maximum values represent the Cisco recommended values for most networks.

Note Choose V1 only if you are using a legacy Airespace branded product acquired prior to their acquisition by Cisco. Cisco recommends that you choose V2 if you want to enable pico cell mode.

Step 6 Set the Rx sensitivity threshold based on the desired receiver sensitivity for 802.11a/n radios. The Current column shows what is currently set on the access point and clients, and the Min and Max columns show the range to which the access points and clients should adapt. The valid ranges for Current, Min, and Max columns are -127 to 127 dBm. The defaults are -65 dBm (current), -127 dBm (Min), and 127 dBm (Max). Receiver signal strength values outside of this range are blocked.

Step 7 Set the CCA sensitivity threshold based on when the access point or client considers the channel clear enough for activity. The Current column shows what is currently set on the access point and clients, and the Min and Max columns show the range to which the access points and clients should adapt. The valid ranges for Current, Min, and Max columns are -127 to 127 dBm. The defaults are -65 dBm (current), -127 dBm (Min), and 127 dBm (Max). CCA values outside of this range are blocked.

Step 8 Specify the transmit power of the radio that will be used by the client. The valid ranges for Current, Min, and Max columns are -127 to 127 dBm. The defaults are 10 dBm (current), 0 dBm (Min), and 17 dBm (Max).

Step 9 Click **Save** to save these values. Click **Audit** to see a comparison of how WCS configuration matches up with controller configurations. Before choosing **Reset to Defaults**, you must turn off the 802.11a/n network.

Step 10 Return to **802.11a/n > Parameters** and check the 802.11a /n Network Status check box to turn the network back on.

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 s the General page.

Step 3 From the 802.3 Bridging drop-down menu, 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.

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 > Controller**.

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 Thresholds, Load Thresholds, Other Thresholds, and Noise/Interference/Rogue Monitoring Channels.

Note When the Coverage Thresholds Min SNR Level (dB) parameter is adjusted, the value of the Signal Strength (dB) automatically reflects this change. The Signal Strength (dB) parameter provides information regarding what the target range of coverage thresholds is when adjusting the SNR value.

Step 5 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. Refer to the "Configuring EDCA Parameters through a Controller Template" section on page 10-59 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 Select the **EDCA Profile** from the drop-down menu.

Note Profiles 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 Click the **Enable Streaming MAC** check box to enable this feature.

Note Only enable Streaming MAC if all clients on the network are WMM compliant.

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. 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 menu.

Step 3 On the SNMP Parameters portion of the window, choose **v3** from the Version drop-down menu.

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 menu, 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**.

Autonomous to LWAPP Migration Support

The autonomous to LWAPP migration support feature provides a common application (WCS) from which you can perform basic monitoring of IOS access points along with current LWAPP access points. The following autonomous access points are supported:

- Cisco Aironet 1100 Access Point
- Cisco Aironet 1130 Access Point
- Cisco Aironet 1200 Access Point
- Cisco Aironet 1240 Access Point
- Cisco Aironet 1240 Access Point
- Cisco Aironet 1310 Bridge
- Cisco Aironet 1410 Bridge

You may also choose to convert IOS access points to LWAPP.

From WCS, the following functions are available when managing IOS access points:

- Adding IOS access points
- Configuring IOS access points
- Viewing current IOS access points from the Monitor > Access Points page (see Monitoring Access Points for more information)
- Adding and viewing IOS access points from the Monitor > Maps page (see Maps for more information)
- Monitoring associated alarms
- Performing an autonomous access point background task
  - Checks the status of IOS access points managed by WCS.
  - Generates a critical alarm when an unreachable IOS access point is detected.
  - See Background Task for more information
- Running reports on IOS access points
  - See Reports > Inventory Reports and Reports > Client Reports > Client Count for more information
- Supporting IOS access points in Work Group Bridge (WGB) mode
- Migrating IOS access points to LWAPP access points

Adding IOS Access Points to WCS

From WCS, the following methods are available for adding IOS access points:

- Add IOS access points by Device information (IP addresses and credentials).
- Add IOS access points by CSV file.

Adding IOS Access Points by Device Information

IOS access points can be added to WCS by device information using comma-separated IP addresses and credentials.

To add IOS access points using device information, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 From the Select a command drop-down menu, choose **Add Autonomous APs**.

Step 3 Click **GO**.

Step 4 Select **Device Info** from the Add Format Type drop-down list.

Step 5 Enter comma-separated IP addresses of IOS access points.

Step 6 Enter the SNMP parameters including version number, number of retries, and timeout in seconds.

Step 7 Enter Telnet credentials for migration (optional).

Note The Telnet credentials are required to convert the access points from autonomous to unified.

Note If the autonomous access point already exists, WCS updates the credentials (SNMP and Telnet) to the existing device.

Step 8 Click **OK**.

Adding Autonomous Access Points by CSV File

Autonomous access points can be added to WCS using a CSV file exported from WLSE.

To add autonomous access points using a CSV file, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 From the **Select a Command** drop-down menu, choose **Add Autonomous APs**.

Step 3 Click **GO**.

Step 4 Select **File** from the **Add Format Type** drop-down list.

Step 5 Enter or browse to the applicable CSV file.

Note The CSV file has the same format as Adding Controllers but includes additional (optional) columns such as telnet_username, telnet_password, and enable_password.

Step 6 Click **OK**.

To remove an autonomous access point from WCS:

Step 1 Select the checkbox(es) of the appropriate access point(s).

Step 2 Select **Remove APs** from the **Select a Command** drop-down list.

Viewing Autonomous Access Points in WCS

Once added, the autonomous access points can be viewed on the **Monitor > Access Points** page.

Click the autonomous access point to view more detailed information such as:

- Operational status of the access points
- Key attributes including radio information, channel, power, and number of clients on the radio
- CDP neighbored information

The autonomous access points can also be viewed in **Monitor > Maps**.

They can be added to a floor area by choosing **Monitor Maps > <floor area>** and selecting **Add Access Points** from the **Select a Command** drop-down list**.**

Work Group Bridge (WGB) Mode

Wireless Group Bridge (WGB) mode is a special mode where an autonomous access point functions as a wireless client and connects to an LWAPP access point. The WGB and its wired clients are listed as client in WCS.

Choose **Monitor > WGBs** to view a list of all WCS clients that are in WGBs. Click a **User** to view detailed information regarding a specific WGB and its wired clients.

Note The WCS provides WGB client information for the autonomous access point whether or not it is managed by the WCS. If the WGB access point is also managed by the WCS, WCS provides basic monitoring funtions for the access point similar to other autonomous access points.

Autonomous Access Point to LWAPP Access Point Migration

To make a transition from an Autonomous solution to a Unified architecture, autonomous access points must be converted to LWAPP access points. The migration utility is available from the **Configure > Migration Templates** page where existing templates are listed.

From the **Select a command** drop-down list, the following functions can be performed:

- Add Template—Allows you to provide necessary information for migration.
- Delete Templates—Allows you to delete a current template.
- View Migration Report—Allows you to view information such as AP address, migration status, timestamp, and a link to detailed logs.
- View Current Status—Allows you to view the progress of the current migration (updated every three seconds).

Note When migrating an already-managed autonomous access point to LWAPP, its location and antenna information is migrated as well. You do not need to re-input the information. WCS automatically removes the autonomous access point after migration.

Adding/Modifying a Migration Template

To add a new template, select **Add Template** from the **Select a command** drop-down list.

To modify an existing template, click the template name from the summary list.

Enter or modify the following migration parameters:

General

- Template Name—User-defined name of this migration template.
- Description—Brief description to help you identify the migration template.

Upgrade Options

- DHCP Support—Ensures that after the conversion every access point gets an IP from the DHCP server.
- Retain AP HostName—Allows you to retain the same hostname for this access point.
- Migrate over WANLink—Increases the default timeouts for the CLI commands executed on the access point.
- DNS Address
- Domain Name

Controller Details

Note Ensures that the access point authorization information (SSC) can be configured on this controller and the converted access points can join.

- Controller IP
- User Name
- Password

TFTP Details

- TFTP Server IP

- File Path
- File Name

Once a template is added in WCS, the following additional buttons appear:

- **Select APs**—Selecting this option provides a list of autonomous access points in WCS from which to choose the access points for conversion.
- **Select File**—To provide CSV information for access points intended for conversion.

Configuring Access Points

Choose **Configure > Access Points** to see a summary of all access points in the Cisco WCS database. The summary information includes the following:

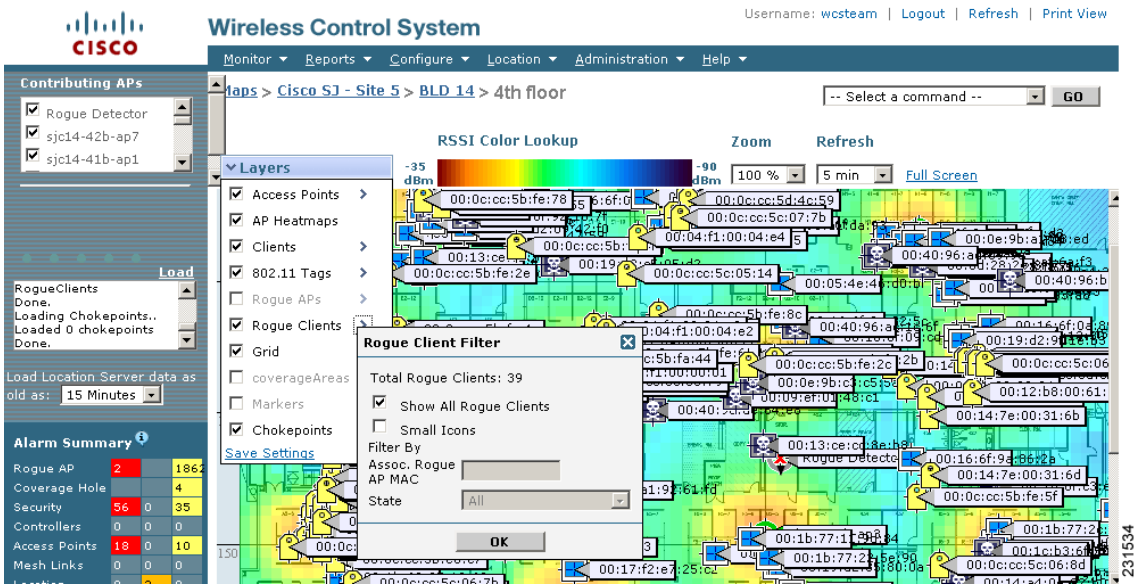
- Ethernet MAC
- IP Address
- Radio
- Map Location
- AP Type
- Controller
- Operation Status
- Alarm Status
- Audit Status

Note If you hover over the Audit Status value, the time of the last audit is displayed.

Step 1 Click the link under AP Name to see detailed information about that access point name. The following window appears (see Figure 9-6).

Figure 9-6 Detailed Access Point Information

.



Note There is no need to add access points to the Cisco WCS database. The operating system software automatically detects and adds an access point to the Cisco WCS database as it associates with existing controllers in the Cisco WCS database.

Some of the parameters on the window are supplied.

- The General portion displays the Ethernet MAC, the Base Radio MAC, and IP Address.
- The Versions portion of the window displays the software and boot version.
- The Inventory Information portion displays the model, IOS version, and serial number and type of the access point, provides which certificate type is required, and determines whether H-REAP mode is supported or not.
- The Radio Interfaces portion provides the current status of the 802.11a/n and 802.11b/g/n radios such as admin status, channel number, power level, antenna mode, antenna diversity, and antenna type.

Follow the steps below to set the configurable parameters.

Step 1 Enter the name assigned to the access point.

Step 2 Use the drop-down menu to choose a country code to establish multiple country support. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that the access point complies with your country's regulations. Consider the following when setting the country code:

- You can configure up to 20 countries per controller.
- Because only one auto-RF engine and one list of available channels exist, configuring multiple countries limits the channels available to auto-RF in the common channels. A common channel is one that is legal in each and every configured country.

- When you configure access points for multiple countries, the auto-RF channels are limited to the highest power level available in every configured country. A particular access point may be set to exceed these limitations (or you may manually set the levels in excess of these limitations), but auto-RF does not automatically choose a non-common channel or raise the power level beyond that available in all countries.

Note Access points may not operate properly if they are not designed for use in your country of operation. For example, an (-A) access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Europe (-E). 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/warp/public/779/smbiz/wireless/approvals.html.

Step 3 If you want to enable the access point for administrative purposes, check the **Enabled** check box.

Step 4 If you click **Enabled** at the AP Static IP check box, a static IP address is always assigned to the access point rather than getting an IP address dynamically upon reboot.

Step 5 Choose the role of the access point from the AP Mode drop-down menu. A reboot is not required after the mode is changed. The available modes are as follows:

- Local — This is the normal operation of the access point and the default AP Mode choice. With this mode, data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration.
- Monitor — This is radio receive only mode and allows the access point to scan all configured channels every 12 seconds. Only deauthentication packets are sent in the air with an access point configured this way. A monitor mode access point detects rogues, but it cannot connect to a suspicious rogue as a client to prepare for the sending of RLDP packets.
- Rogue Detector — In this mode, the access point radio is turned off, and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points expected. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.
- Sniffer Mode — Operating in sniffer mode, the access point captures and forwards all the packets on a particular channel to a remote machine that runs Airopeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run Airopeek, which is a third-party network analyzer software that supports the decoding of data packets. For more information on Airopeek, see http://www.wildpackets.com/products.
- HREAP —Choose **HREAP** from the AP Mode drop-down menu to enable hybrid REAP for up to six access points. The HREAP access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

Step 6 In the Primary, Secondary, and Tertiary Controller fields, you can define the order in which controllers are accessed.

Step 7 The AP Group Name drop-down shows all access point group names that have been defined using WLANS > AP Group VLANs, and you can specify whether this access point is tied to any group.

Step 8 Enter a description of the physical location where the access point was placed.

Step 9 In the Stats Collection Period parameter, enter the time in which the access point sends .11 statistics to the controller. The valid range is 0 to 65535 seconds. A value of 0 means statistics should not be sent.

Step 10 Choose Enabled for **Mirror Mode** if you want to duplicate (to another port) all of the traffic originating from or terminating at a single client device or access point. Mirror mode is useful in diagnosing specific network problems but should only be enabled on an unused port since any connections to this port become unresponsive.

Step 11 You can globally configure MFP on a controller. When you do, management frame protection and validation are enabled by default for each joined access point, and access point authentication is automatically disabled. After MFP is globally enabled on a controller, you can disable and re-enable it for individual WLANs and access points.

If you click to enable MFP Frame Validation, three main functions are performed:

- Management frame protection — When management frame protection is enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, and the receiving access points which were configured to detect MFP frames report the discrepancy.
- Management frame validation — When management frame validation is enabled, the access point validates every management frame it receives from other access points in the network. When the originator is configured to transmit MFP frames, the access point ensures that the MIC IE is present and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE, it reports the discrepancy to the network management system. In order to report this discrepancy, the access point must have been configured to transmit MFP frames. Likewise, for the timestamps to operate properly, all controllers must be Network Transfer Protocol (NTP) synchronized.
- Event reporting — The access point notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and reports the results through SNMP traps to alert the network manager.

Step 12 Click the **Cisco Discovery Protocol** check box if you want to enable it. CDP is a device discovery protocol that runs on all Cisco-manufactured equipment, such as routers, bridges, and communication servers. Each device sends periodic messages to a multicast address and listens to the messages that others send in order to learn about neighboring devices. When the device boots, it sends a CDP packet specifying whether the device is inline power enabled so that the requested power can be supplied.

Note Changing access point parameters temporarily disables an access point and might result in loss of connectivity to some clients.

Step 13 Select the role of the mesh access point from the AP Role drop-down menu. The default setting is MAP.

Note An access point in a mesh network functions as either a root access point (RAP) or mesh access point (MAP).

Step 14 Enter the name of the bridge group to which the access point belongs. The name can have up to 10 characters.

Note Bridge groups are used to logically group the mesh access points to avoid two networks on the same channel from communicating with each other.

Note For mesh access points to communicate, they must have the same bridge group name.

Note For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another.

Note For configurations where separate sectors are required, make sure that each RAP and its associated MAPs have separate bridge group names.

The Type parameter displays whether the mesh access point is an indoor or outdoor access point, and the Backhaul Interface parameter displays the access point radio that is being used as the backhaul for the access point.

Step 15 Select the data rate for the backhaul interface from the drop-down menu. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps.

Note This data rate is shared between the mesh access points and is fixed for the whole mesh network.

Note Do NOT change the data rate for a deployed mesh networking solution.

Step 16 Choose the Enable option from the Ethernet Bridging drop-down menu to enable Ethernet bridging for the mesh access point.

Step 17 If you need to perform a hardware reset on this access point, click **Reset AP Now**.

Step 18 If you need to clear the access point configuration and reset all values to the factory default, click **Clear Config**.

Viewing Audit Status (for Access Points)

An Audit Status column on the Configure > Access Points window shows an audit status for each of the access points. You can also view the audit report for the selected access points. The report shows the time of the audit, the IP address of the selected access point, and the synchronization status.

Step 1 Choose **Configure > Access Points**.

Step 2 Click the Audit Status column value to go to the latest audit details page for the selected access point. This report is interactive and per access point.

Note If you hover over the Audit Status column value, the time of the last audit is displayed.

To run an access point on-demand audit report, select the desired access point for which you want to run the report and choose **Audit Now** from the Select a command drop-down menu. In versions prior to 4.1, the audit only spanned the parameters present on the AP Details and AP Interface Details page. In release 4.1, this audit report covers complete access point level auditing. The audit results are stored in the database so that you can view the latest audit reports without having to run another audit.

Note The audit can only be run on an access point that is associated to a controller.

Searching Access Points

Use the controls in the left sidebar to create and save custom searches:

- **New Search** drop-down menu: Opens the Search Access Points window. Use the Search Access Points window to configure, run, and save searches.
- **Saved Searches** drop-down menu: Lists the saved custom searches. To open a saved search, choose it from the Saved Searches list.
- **Edit Link**: Opens the Edit Saved Searches window. You can delete saved searches in the Edit Saved Searches window.

You can configure the following parameters in the Search Access Points window:

- Search By
- Radio Type
- Search in
- Save Search
- Items per page

After you click GO, the access point search results appear:

Table 9-2 Access Point Search Results

Parameter	Options
AP Name	Name assigned to the access point. Click the access point name item to display details.
WCS	WCS name where access point was detected.
Ethernet MAC	MAC address of the access point.
IP Address	IP address of the access point.
Radio	Protocol of the access point is either 802.11a/n or 802.11b/g/n.
Map Location	Campus, building, and floor location.
Controller	IP address of the controller.
Admin Status	Administration site of the access point (Enabled or Disabled).
AP Type	Access point radio frequency type.

Table 9-2 Access Point Search Results (continued)

Operational Status	Displays the operational status of the Cisco radios (Up or Down).
Alarm Status	Alarms are color coded as follows: • Clear = No Alarm • Red = Critical Alarm • Orange = Major Alarm • Yellow = Minor Alarm

Configuring Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to WCS. This feature allows the WCS to collect, monitor, and archive detailed interferer data from Spectrum Experts in the network.

To configure spectrum experts, choose Configure > Spectrum Experts. This page provides a list of all Spectrum Experts including:

- Hostname—The hostname or IP address of the Spectrum Expert laptop.
- MAC Address— The MAC address of the spectrum sensor card in the laptop.
- Reachability Status— Specifies whether the Spectrum Expert is successfully running and sending information to WCS. The status appears as reachable or unreachable.

Adding a Spectrum Expert

To add a Spectrum Expert, follow these steps:

Step 1 Choose **Configure > Spectrum Experts**.

Step 2 Click **Add a Spectrum Expert**.

Note This link only appears when no spectrum experts are added. You can also access the Add a Spectrum Expert page by choosing Add a Spectrum Expert from the Select a command drop-down menu.

Step 3 Enter the Spectrum Expert's Hostname or IP address. If you use hostname, your spectrum expert must be registered with DNS in order to be added to WCS.

Note To be correctly added as a spectrum expert, the spectrum expert client must be running and configured to communicate to WCS.

Monitoring Spectrum Experts

You also have the option to monitor spectrum experts. Follow these steps to monitor spectrum experts:

Step 1 Choose **Monitor > Spectrum Experts**.

Step 2 From the left sidebar menu, you can access the **Spectrum Experts > Summary** page and the **Interferers > Summary** page.

Spectrum Experts > Summary

The Spectrum Experts Summary page provides a table of the Spectrum Experts added to the system. The table provides the following Spectrum Expert information:

Hostname—Displays the host name or IP address.

Active Interferers—Indicates the current number of interferes being detected by the Spectrum Experts.

Alarms APs—The number of access points seen by the Spectrum Experts that are potentially affected by detected interferers.

Alarms—The number of active interference traps sent by the Spectrum Expert. Click to access the Alarm page that is filtered to the active alarms for this Spectrum Expert.

Reachability Status—Indicates “Reachable” in green if the Spectrum Expert is running and sending data to WCS. Otherwise, indicates “unreachable” in red.

Location—When the Spectrum Expert is a wireless client, a link for location is available. It shows the location of the Spectrum Expert with a red box that shows the effective range.

Interferers > Summary

The Interferers Summary page displays a list of all the interferers detected over a 30-day interval. The table provides the following interferers’ information:

- Interferer ID—An identifier that is unique across different spectrum experts.
- Category—Indicates the category of the interferer. Categories include: Bluetooth, cordless phones, microwave ovens, 802.11 FH, generic: fixed-frequency, jammers, generic: frequency-hopped, generic:continuous, and analog video.
- Type—Active indicates that the interferer is currently being detected by a spectrum expert. Inactive indicates that the interferer is no longer detected by a spectrum expert or the spectrum expert saw that the interferer is no longer reachable by WCS.
- Discover Time—Indicates when the interferer was discovered.
- Affected Channels—Identifies affected channels.
- Number of APs Affected—The number of access points managed by WCS that the spectrum expert detects or the interferers that the spectrum expert detected on the channels of the access point. Only active interferers are shown. If all of the following conditions are met, the access point is labelled as ***affected***:
  - If the access point is managed by WCS.
  - If the spectrum expects detects the access point.
  - If the spectrum expert detects an interferer on the serving channel of the access point.

- Power—Indicated in dBm.
- Duty Cycle—Indicated in percentage. 100% is the worst value.
- Severity—Indicates the severity ranking of the interferer. 100 is the worst case whereas 0 is no interference.

Spectrum Experts Details

The Spectrum Expert Details page provides all interference details from a single Spectrum Expert. This page updates every 20 seconds and gives a real-time look at the remote spectrum expert. This page includes the following items:

- Total Interferer Count—Given from the specific spectrum expert.
- Active Interferers Count Chart—Displays a pie chart that groups interferers by category.
- Active Interferer Count Per Channel—Displays the number of interferers grouped by category on different channels.
- AP List—Provides a list of access points detected by the spectrum expert. These access points are on channels that have active interferers detected.
- Affected Clients List—Provides a list of clients that are currently authenticated to an access point in the access point list.

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. Refer to the "Creating Guest User Accounts" section on page 7-11.

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 7-11.

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

Step 1 To configure a dynamic interface for wired guest user access, click **Configure > Controllers** and after choosing a particular IP address, choose **System > Interfaces**. The Interfaces summary window appears.

Step 2 Choose **Add Interface** from the Select a command drop-down menu and click **GO**.

Step 3 Enter a name and VLAN ID for the new interface.

Step 4 Check the Guest LAN check box.

Step 5 Enter the IP address, netmask, and gateway address for the interface.

Step 6 Enter an IP address address for the primary and secondary DHCP server.

Step 7 Click **Save**. You are now ready to create a wired LAN for guest access.

Step 8 To configure a wired LAN for guest user access, click **WLANs > WLAN** from the left sidebar menu.

Step 9 Choose **Add WLAN** from the Select a command drop-down menu and click **GO**.

Step 10 If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down menu. 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 11 Enter a name in the Profile Name field that identifies the guest LAN. Do not use any spaces in the name entered.

Step 12 Enter a name in the SSID field that identifies the guest LAN. Do not use any spaces in the name entered.

Step 13 Check the **Enabled** check box for the WLAN Status parameter.

Step 14 Web Authentication (web auth) is the default security policy. If you want to change this to web passthrough, choose the Security tab and Layer 3.

Step 15 Choose the authentication method from the drop-down menu. Options are IPSEC, VPN passthrough, and none (open).

Note If you select the VPN Passthrough option, a VPN Gateway Address option appears.

Step 16 Click **Save**.