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:

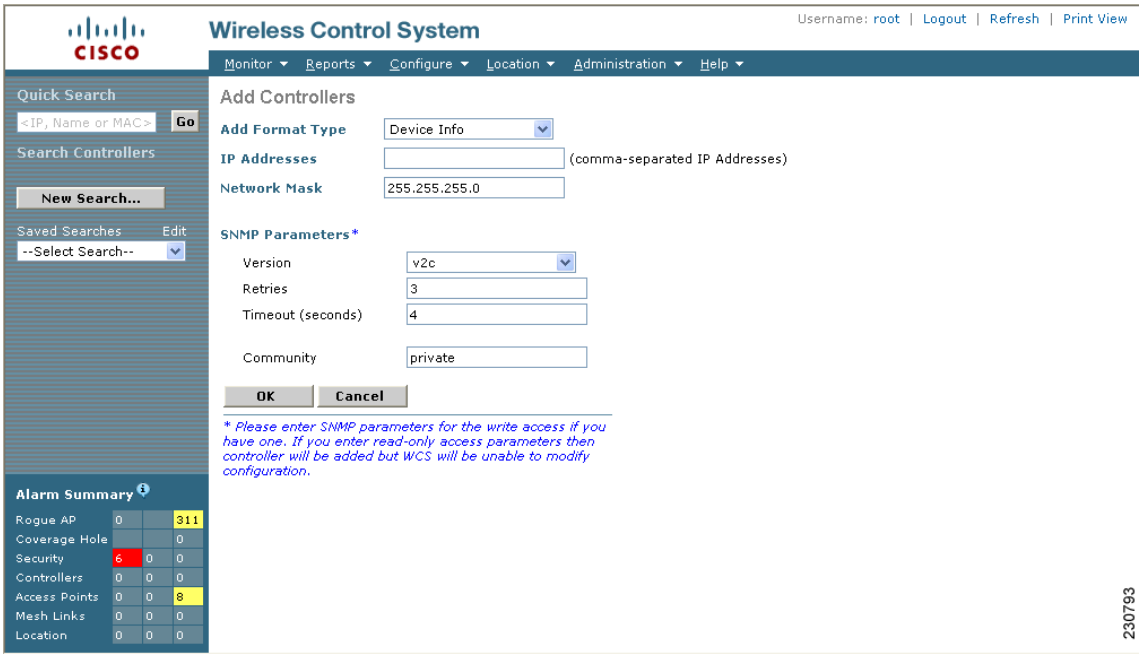
Adding Controllers

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 10-1).

Figure 10-1 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.

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.

Step 5 Click **OK**.

Setting Multiple Country Codes

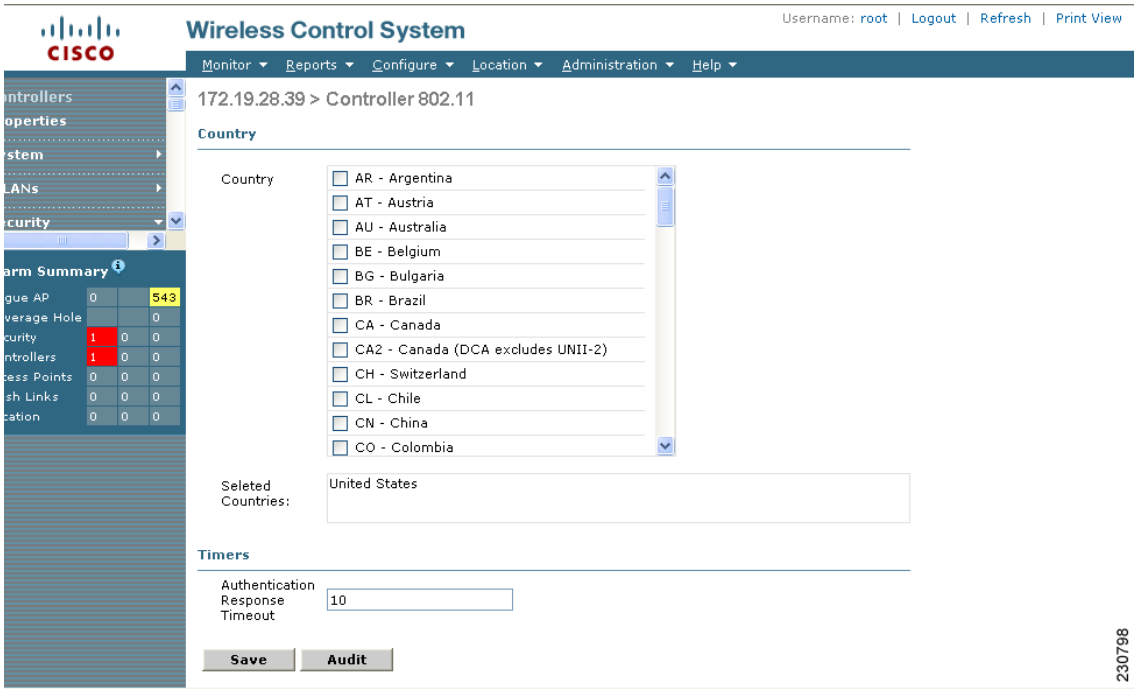
To set multiple country support for a single controller(s) that is not part of a mobility group, follow the steps below.

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 10-2).

Figure 10-2 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/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**.

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 10-1 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 10-1 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)

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

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

To audit a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the check box for the applicable controller.

Step 3 From the Select a command drop-down menu, choose **Audit Now.**

Step 4 Click **GO**.

Step 5 When you perform the Refresh values from controller action from the View Audit Status page, a confirmation is shown.

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 (i.e, 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 8-17 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 8-17 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 following sections are displayed if the audit is selected to be a basic audit:

Config WCS discrepancies

- 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 8-17 for more information on enforcing configurations.

– If you choose *Refresh Config from Controller*, a Refresh Config window appears displaying 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.

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 WLCs.

Note On the Refresh Config window, 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 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. The Audit Details display the config differences, if applicable.

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.

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 Priority drop-down, choose **Enabled**.

To then 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 menu, choose the applicable priority (Low, Medium, High, Critical).

Note The default priority is Low.

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 menu and click **GO**.

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

WCS displays the Ping Results window, 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 window.

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 11-61.

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

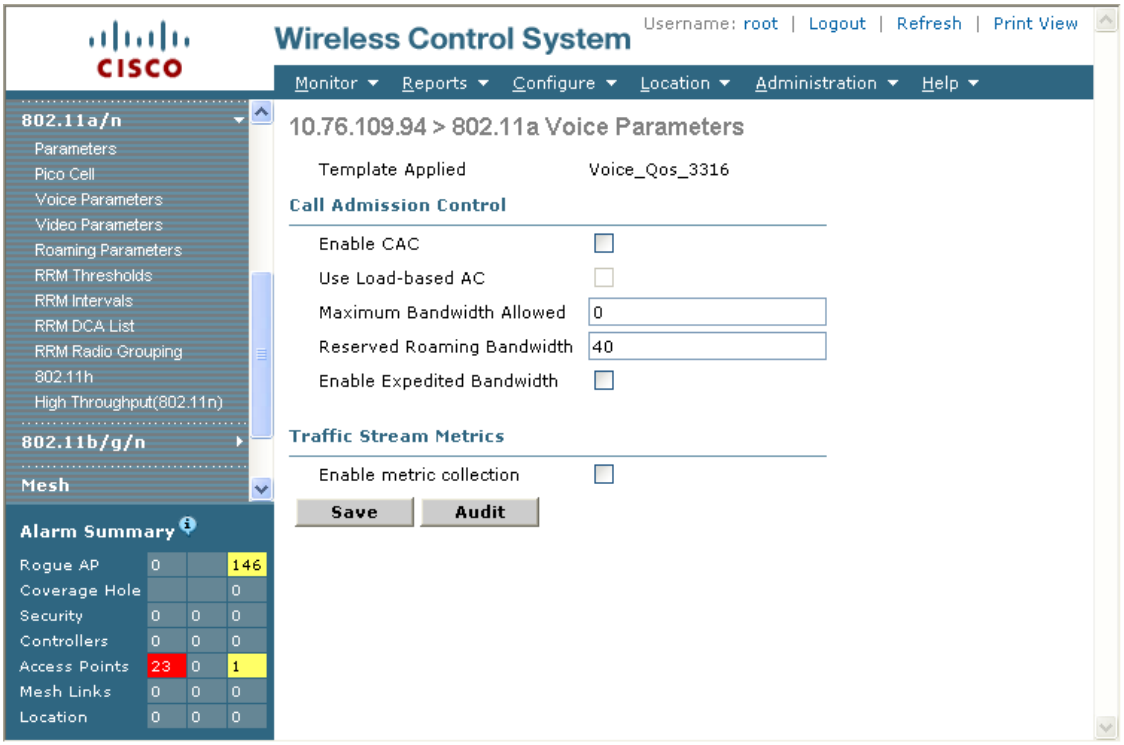
Step 1 Click **Configure > Controllers**.

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 10-3).

Figure 10-3 802.11a/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

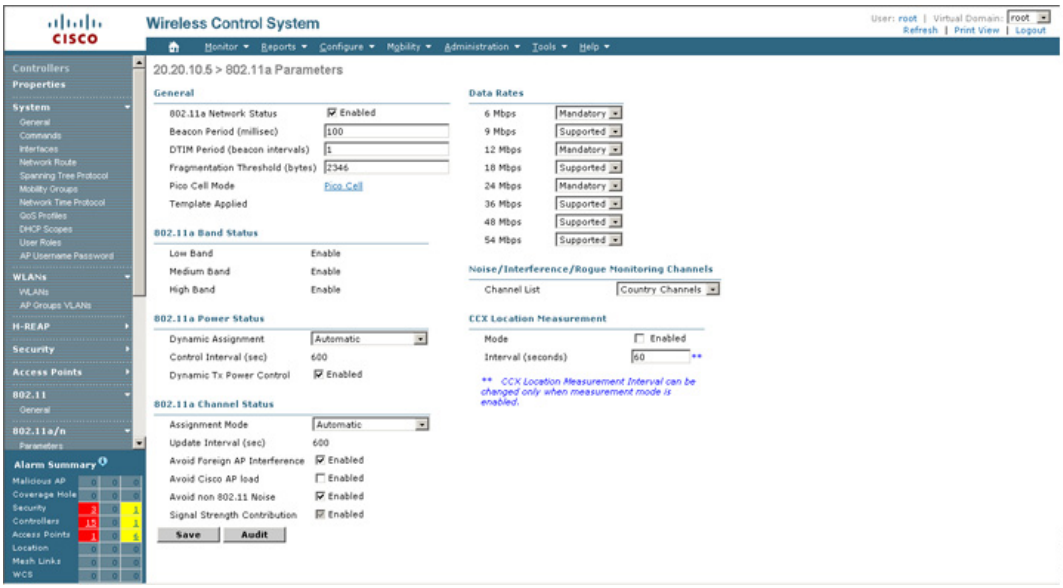
To optimize a controller to support high density, you need to enable pico cell mode v2. A method to mitigate the inter-cell contention problem in high-density networks is to adjust the access point and client receiver sensitivity, CCA sensitivity, and transmit power parameters in a relatively cooperative 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 Applying Controller Templates, page 11-79. 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 From the left sidebar menu, choose **802.11a/n > Parameters** or **802.11b/g/n > Parameters**. The window as shown in Figure 10-4 appears. Ensure that the 802.11a/n (or 802.11b/g/n) Network Status check box is not enabled.

Figure 10-4 Pico Cell Parameter



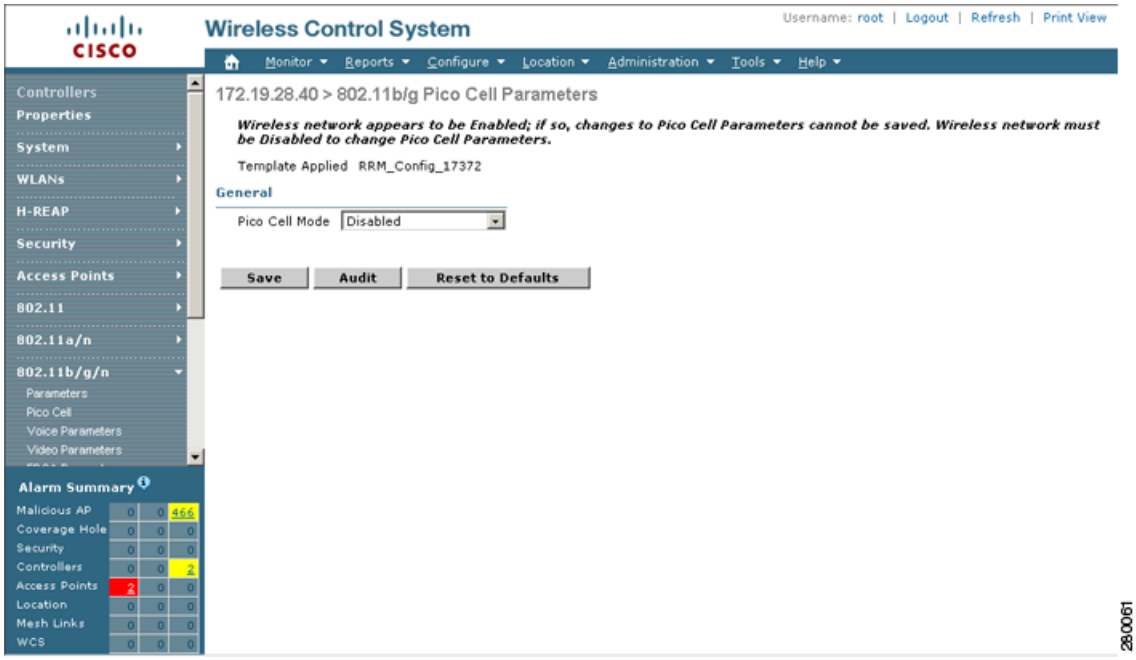
Step 3 In the General portion of this window, you see a Pico Cell Mode parameter. Click **Enable**.

Note Pico cell mode cannot be enabled while Aggressive Load Balancing is enabled on the controller.

Step 4 Click **Save**.

Step 5 Choose **802.11a/n > Pico Cell** or **802.11b/g/n > Pico Cell** from the left sidebar menu. The Pico Cell Parameters screen appears (see Figure 10-5).

Figure 10-5 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 6 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 7 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 8 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 9 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 10 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 11 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 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:

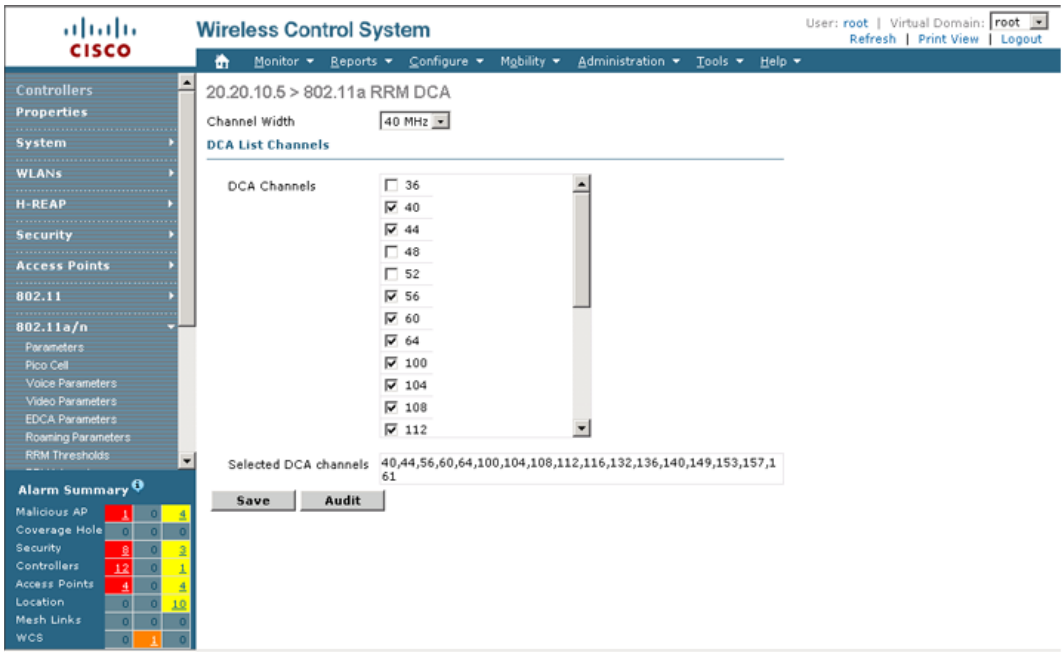
Step 1 Choose **Configure > Controllers**.

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 window appears (see Figure 10-6).

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 10-6 802.11a/n RRM DCA Window



Step 4 From the Channel Width drop-down menu, 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 Choose the check box(es) for the applicable DCA channel(s). The selected channels are listed in the **Selected DCA channels** text box.

Step 6 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 11-63 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 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**.

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 menu, choose **Discover Templates from Controller**.

Step 4 Click **GO**. The Discover Templates window displays the number of discovered templates and each template's name.

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

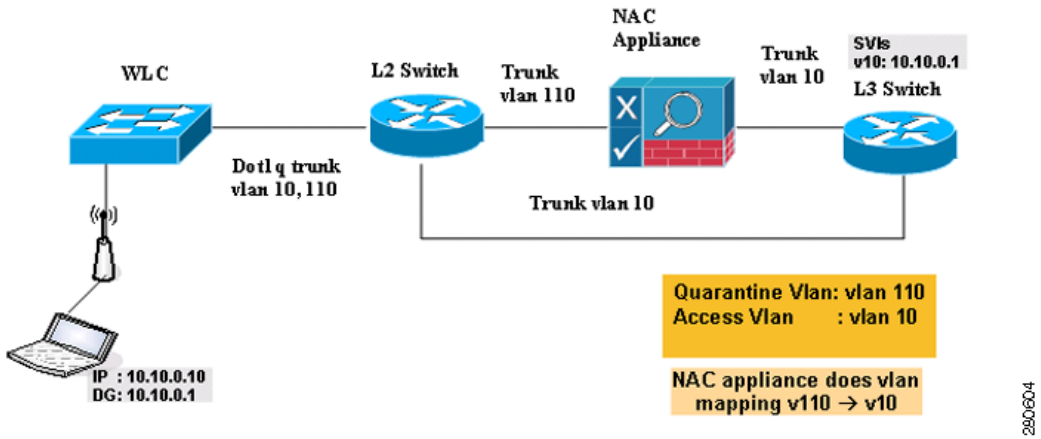
Configuring NAC Out-of-Band Integration

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 10-7 provides an example of NAC out-of-band integration.

Figure 10-7 NAC Out-of-Band Integration



In Figure 10-7, 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 Refer to Chapter 13 for more information on hybrid REAP.

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

Note Refer to the Cisco NAC appliance configuration guides for configuration instructions: http://www.cisco.com/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:

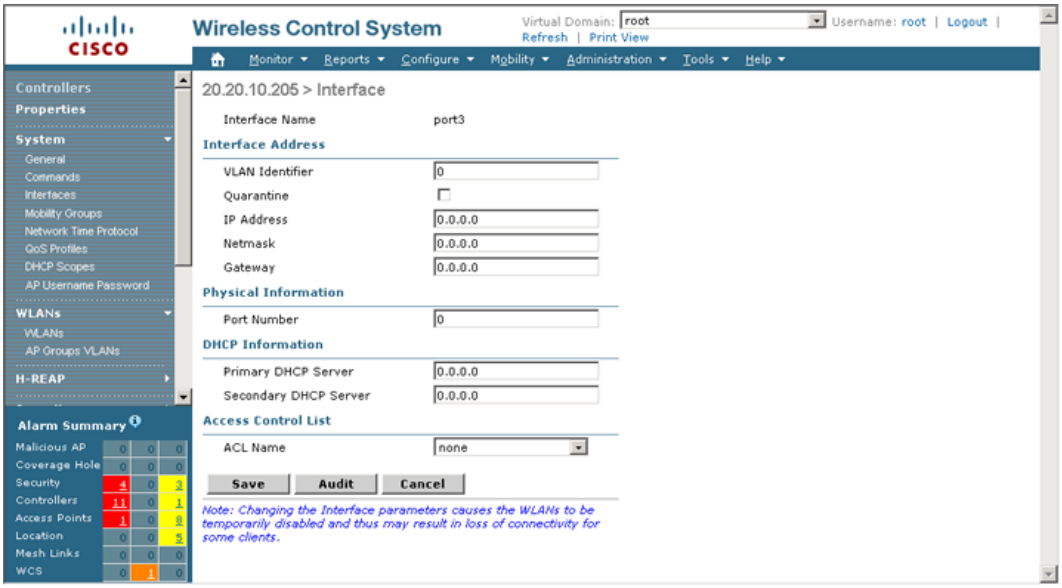
a. Choose **Configure > Controller**.

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 menu. The Interface window appears (see Figure 10-8).

Figure 10-8 Interface Window



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

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

g. Check 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.

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

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

j. 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 > WLANs** from the left sidebar menu.

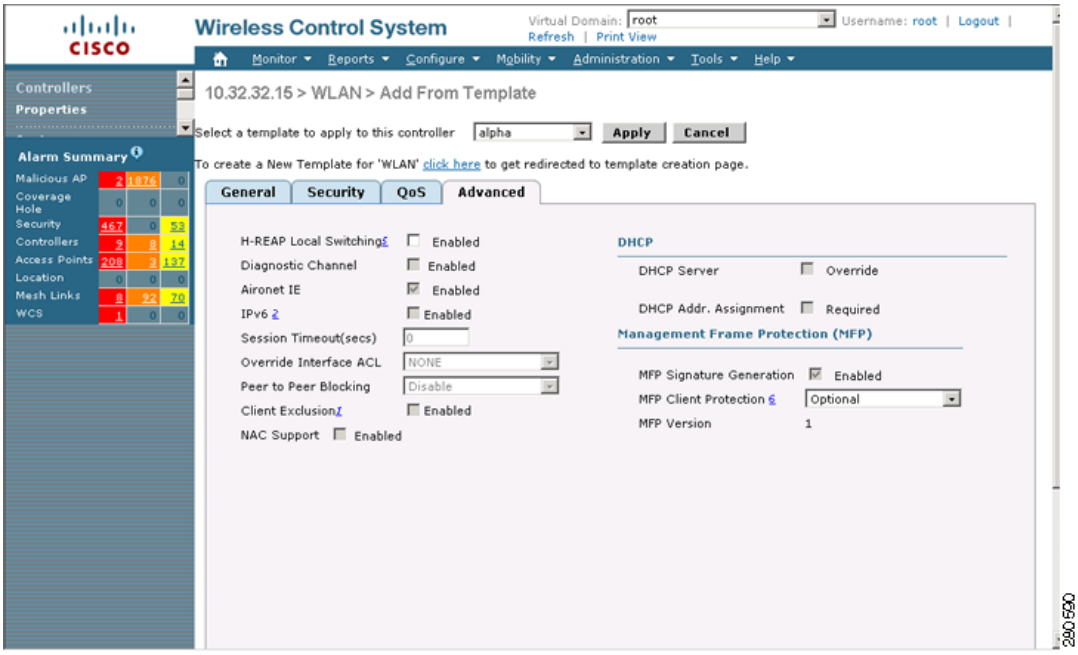
b. Choose **Add WLAN** from the Select a command drop-down menu and click **GO**.

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 menu. 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 10-23.

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

d. Click the **Advanced** Tab (see Figure 10-9).

Figure 10-9 WLAN > Add From Template Window



e. To configure NAC out-of-band support for this WLAN or guest LAN, check the **NAC Support** check box. To disable NAC out-of-band support, leave the check box unchecked, 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 VLANs** in the left sidebar menu to open the AP Groups VLANs page.

b. Click the name of the desired AP group.

c. From the Interface Name drop-down box, choose the quarantine-enabled VLAN.

d. To configure NAC out-of-band support for this AP group VLAN, check the **NAC Support** check box. To disable NAC out-of-band support, leave the check box unchecked, which is the default value.

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

Step 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. Click the MAC address of the desired client to open the Clients > Detail page. The NAC state appears as access or quarantine under the Security Information section (see Figure 10-10).

Figure 10-10 Monitor > Client Window

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.

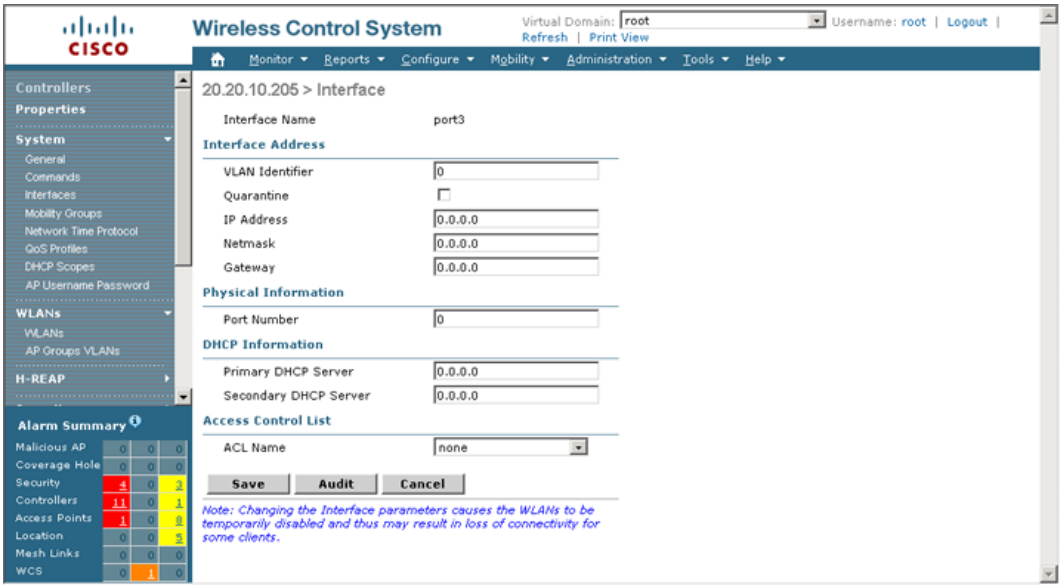
If two controllers are being used, the controller (foreign) that receives the wired guest traffic from the switch then forwards the wired guest traffic to an anchor controller that is also configured for wired guest access. After successful hand off of the wired guest traffic to the anchor controller, 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.

To create dynamic interfaces for wired guest user access, click **Configure > Controllers** and after choosing a particular IP address, choose **System > Interfaces**. 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 10-24 and the "Creating an Egress Interface" section on page 10-25 before continuing to "Creating a Wired LAN for Guest Access" section on page 10-25. Both the Ingress and Egress Interfaces use the screen as shown in Figure 10-11.

Figure 10-11 Interfaces Summary Window



Creating an Ingress Interface

Follow these steps to create an Ingress interface.

Step 1 Choose **Add Interface** from the Select a command drop-down menu and click **GO**.

Step 2 In the Interface Name field, enter a name for this interface, such as guestinterface.

Step 3 Enter a VLAN ID for the new interface.

Step 4 Check the **Guest LAN** check box.

Step 5 Enter the primary and secondary port numbers.

Step 6 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 menu and click **GO**.

Step 2 In the Interface Name field, enter a name for this interface, such as quarantine.

Step 3 In the VLAN Identifier field, enter a non-zero value for the access VLAN ID, such as 10.

Step 4 Check 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 5 Enter the IP address, netmask, and default gateway.

Step 6 Enter the primary and secondary port numbers.

Step 7 Provide an IP address for the primary and secondary DHCP server.

Step 8 Configure any remaining fields for this interface and click **Save**.

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

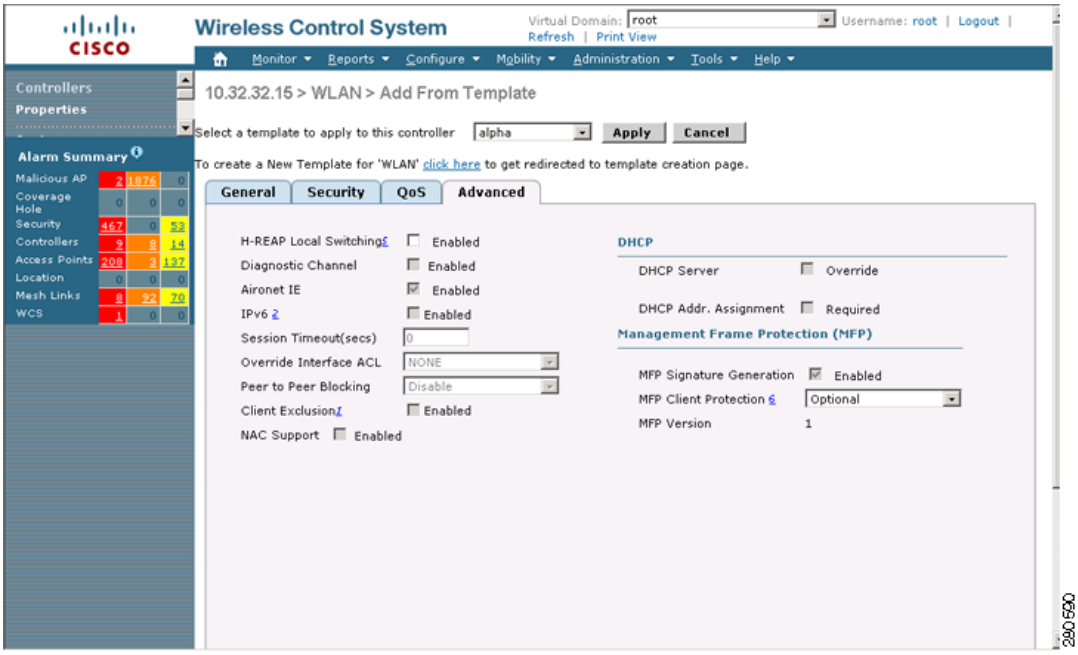
Creating a Wired LAN for Guest Access

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** from the left sidebar menu.

Step 2 Choose **Add WLAN** from the Select a command drop-down menu and click **GO**. The WLAN > Add From Template window appears (see Figure 10-12).

Figure 10-12 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 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 4 At the New Template general tab, enter a name in the Template Name field 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 Check the **Enabled** check box for the WLAN Status parameter.

Step 8 From the Ingress Interface drop-down menu, choose the Ingress interface that you created in the "Creating an Ingress Interface" section on page 10-24. The provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 9 From the Egress Interface drop-down menu, choose the Egress interface that you created in the "Creating an Egress Interface" section on page 10-25. 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 menu.

Step 10 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, check 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. Check 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 windows, uncheck the Global WebAuth Configuration **Enabled** check box.

1. When the Web Auth Type drop-down menu 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 menus 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 menu 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 3-17.

   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 field.

   You can select specific RADIUS or LDAP servers to provide external authentication on the **Security > AAA** panel. To do so, continue with Step 11.

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

Step 11 If you selected External as the Web Authentication Type in Step 10, click **Security > AAA** and select up to three RADIUS and LDAP servers using the drop-down menus.

Step 12 Click **Save**.

Step 13 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 an LWAPP 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 connected to rogue access point information is used to track the switch port to which the rogue access point is connnected 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.

Step 1 Choose **Monitor > Security.**

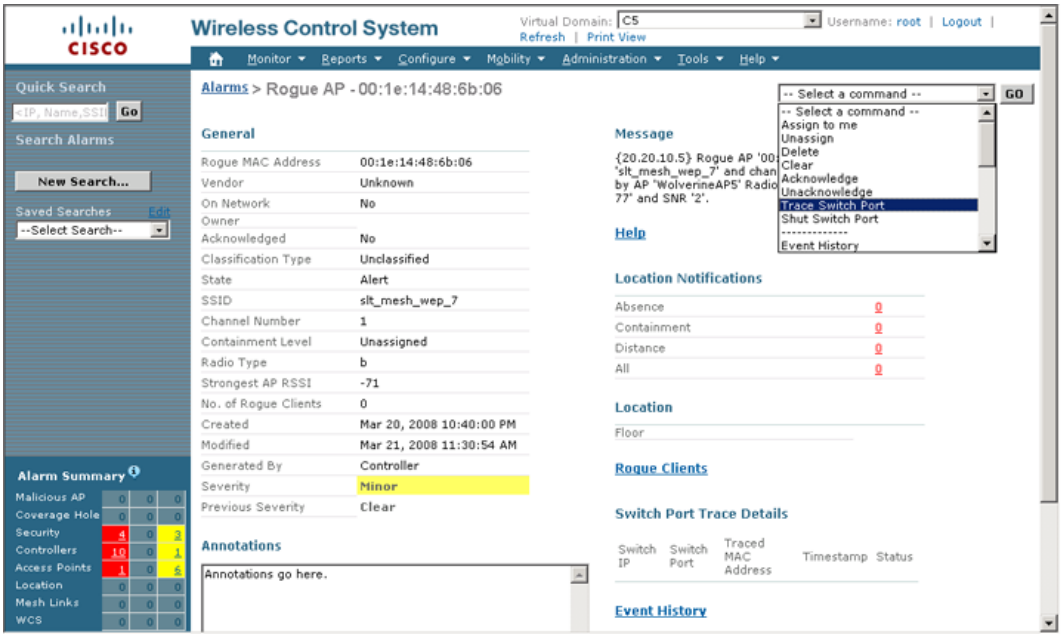
Step 2 Click **View All** in the Rogue APs and Adhoc Rogues section.

Step 3 Choose for which rogue you are setting switch port tracking by clicking the URL in the MAC Address column.

Step 4 From the Select a command drop-down menu, choose **Trace Switch Port** (see Figure 10-13).

Figure 10-13 Trace Switch Port option on the Alarms > Rogue Page

.

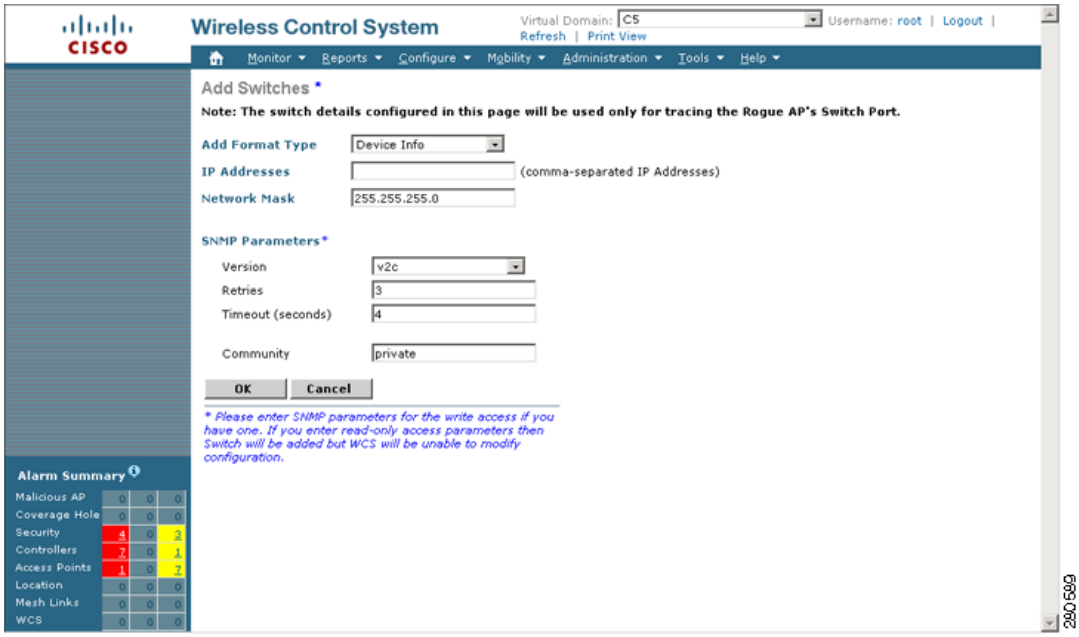


Step 5 When one or more searchable MAC addresses are available, the WCS uses CDP to discover any switches connected up to two hops away from the detecting access point. The MIBs of each CDP discovered switch is examined to see if it contains any of the target MAC addresses. If any of the MAC addresses are found, the corresponding port number is returned and reported as the rogue's switch port.

The SNMP communities for the switches are provided in Configure > Switches (see Figure 10-14).

Figure 10-14 Configure > Switches

.



Step 6 The switch details configured on this page are used only for tracing the rogue access point's switch port. Choose one of the following:

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

If you want to add multiple switches 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.

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 On the SNMP Parameters portion of the window, choose your version choice from the Version drop-down menu.

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.

Step 10 You can change the retries and timeout values that were established for this switch if desired.

Step 11 Enter the community for this switch.

Step 12 Click **OK**.

Removing Switches

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

Shutting Switch Port

You can suppress the switch port to which the rogue access point is connected. From the Alarms Rogue page (shown in Figure 10-13), choose **Shut Switch Port** from the Select a command drop-down menu.

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.