CHAPTER 9

Configuring Devices

This chapter describes how to configure devices in the NCS database. It contains the following sections:

Configuring Controllers

This section describes how to configure controllers in the NCS database.

Choose **Configure > Controllers** to access the following:

- A summary of all controllers in the NCS database.
- The ability to add, remove, and reboot selected controllers.
- The ability to download software from the NCS server to selected controllers.
- The ability to save the current configuration to nonvolatile (Flash) memory on selected controllers.
- The ability to view audit reports for selected controllers.

The controllers data table contains the following columns:

- Check box—Select the applicable controller.
- IP Address—Local network IP address of the controller .
  - Click the title to sort the list items.

  - Click a list item to display parameters for that IP address. See the "Viewing Controllers Properties, page 9-23".
  - Click the icon to the right of the IP address to launch the controller Web user interface in a new browser window.

- Device Name—Indicates the name of the controller. Click the **Controller Name** link to sort the list by controller name.
- Device Type—Click to sort by type. Based on the series, device types are grouped. For example:
  - WLC2100—21xx Series Wireless LAN Controllers
  - 2500—25xx Series Wireless LAN Controllers
  - 4400—44xx Series Wireless LAN Controllers
  - 5500—55xx Series Wireless LAN Controllers
  - 7500—75xx Series Wireless LAN Controllers
  - WiSM—WiSM (slot number, port number)
  - WiSM2—WiSM2 (slot number, port number)
- Location—Indicates the location of the controller.
- Software Version—The operating system release.version.dot.maintenance number of the code currently running on the controller.
- Mobility Group Name—Name of the mobility or WPS group.
- Reachability Status—Reachable or not reachable.

Note Reachability status is updated based on the last execution information of the Device Status background task. For updating the current status, choose **Administration > Background Tasks**, and choose **Execute Now** from the Select a command drop-down list.

- Audit Status
  - Not Available—No audit occurred on this switch.
  - Identical—No configuration differences were discovered.
  - Mismatch—Configuration differences were discovered.

  Click the **Audit Status** link to access the audit report. In the Audit Report page, choose **Audit Now** from the Select a command drop-down list to run a new audit for this controller. See the "Understanding the Controller Audit Report, page 9-3" for more information on audit reports.

Note Audit status is updated based on the last execution information of either the Configuration Sync background task or the Audit Now option located in the Controllers page. To get the current status, either choose **Administration > Background Tasks** and choose **Execute Now** or **Audit Now** from the Select a command drop-down list.

Note Use the Search feature to search for a specific controller. See the "Using the Search Feature" section on page 2-33 for more information.

This section contains the following topics:

Understanding the Controller Audit Report

The Controller Audit Report displays the following information depending on the type of audit selected in **Administration > Settings > Audit** and on which parameters the audit is performed:

- Applied template discrepancies (Template Based Audit only)
- Config group template discrepancies (Template Based Audit only)
- Total enforcements for config groups with background audit enabled (Template Based Audit only)
  - If the total enforcement count is greater than zero, this number appears as a link. Click the link to view a list of the enforcements made from NCS.
- Failed for config groups with background audit enabled (Template Based Audit only)
  - If the failed enforcement count is greater than zero, this number appears as a link. Click the link to view the failures returned from the device.
- Other NCS discrepancies

Note The controller audit report indicates if the audit was performed on all parameters or on a selected set of parameters.

Note See the "Configuring an Audit" section on page 15-78 for more in depth information on the two types of audits and how to manage specific parameters for the audit.

A current Controller Audit Report can be accessed in the **Configure > Controllers** page by clicking a value in the Audit Status column.

You can audit a controller by choosing **Audit Now** from the Select a command drop-down list in the **Configure > Controllers** page (See the "Using the Audit Now Feature" section on page 9-20 for more information) or by clicking **Audit Now** in the Controller Audit Report.

Adding Controllers

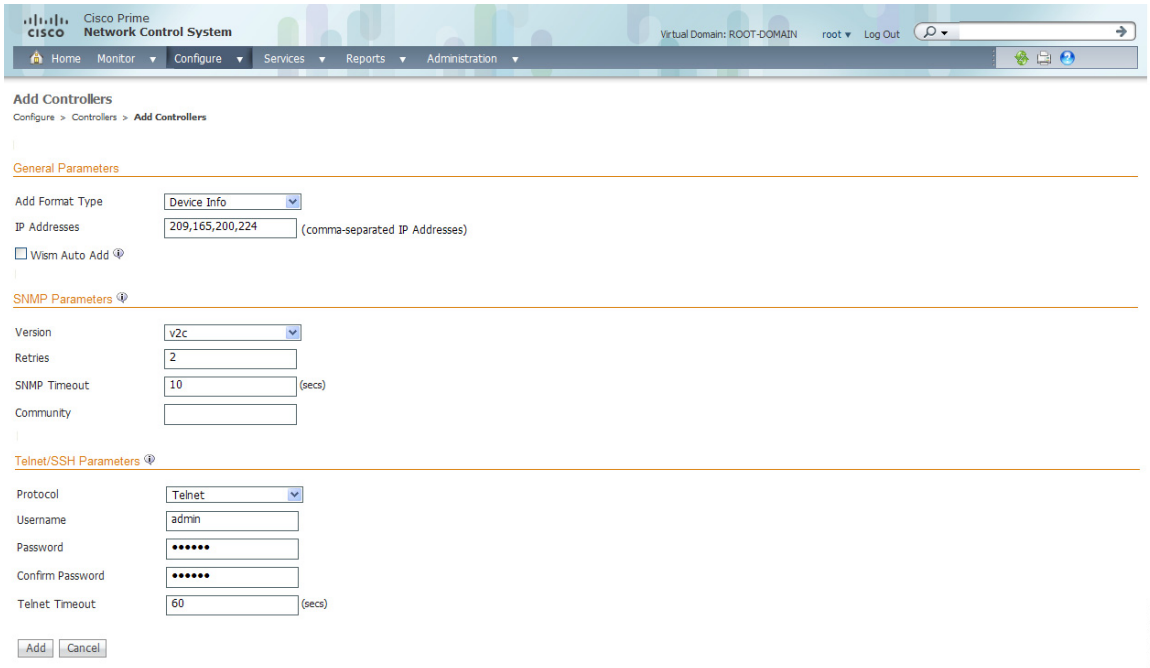
You can add controllers one at a time or in batches.

To add controllers, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 From the Select a command drop-down list, choose **Add Controllers**, and click **Go**. The Add Controller page appears (see Figure 9-1).

Figure 9-1 Add Controller Page



Step 3 Choose one of the following:

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

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

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

Note If you are adding a controller into NCS across a GRE link using IPsec or a lower MTU link with multiple fragments, you may need to adjust the Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU. If it is set too high, the controller may fail to be added into NCS. To adjust the Maximum VarBinds per Get PDU or Maximum VarBinds per Set PDU, do the following: Stop NCS, choose Administration > Settings > SNMP Settings, and edit the Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU values to 50 or lower.

Note If you reduce the Maximum VarBinds per Get PDU or Maximum VarBinds per Set PDU value, applying the configurations to the device might fail.

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 NCS. For example, 10.0.2.255/23 cannot be added but 10.0.2.254/23 can.

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

The first row of the CSV file is used to describe the columns included. The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory. The following example shows a sample CSV file.

```
ip_address,network_mask,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmp
v3_auth_password,snmpv3_privacy_type,snmpv3_privacy_password,snmp_retries,snmp_timeout,pro
tocol,telnet_username,telnet_password,enable_password,telnet_timeout
209.165.200.225,255.255.255.224,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
209.165.200.226,255.255.255.224,v2,public,,,,,3,10,,cisco,cisco,cisco,60
209.165.200.227,255.255.255.224,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
```

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries

- snmp_timeout
- protocol
- telnet_username
- telnet_password
- enable_password
- telnet_timeout

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

Step 6 Use the Version drop-down list to choose v1, v2, or v3.

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

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

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

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

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

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

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

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

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

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

The default username and password is admin.

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

Step 16 Click **OK**.

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

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

Note To update the credentials of multiple controllers in a bulk, choose Bulk Update Controllers from the Select a command drop-down list. The Bulk Update Controllers page appears. You can choose a CSV file. The CSV file contains a list of controllers to be updated, one controller per line. Each line is a comma separated list of controller attributes. The first line describes the attributes included. The IP address attribute is mandatory. For details, see the NCS Configuration Guide.

Bulk Update of Controller Credentials

You can update multiple controllers credentials by importing a CSV file.

To update controller(s) information in a bulk, follow these steps:

Step 1 Choose **Configure > Controllers**.

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

Step 3 From the Select a command drop-down list, choose **Bulk Update Controller**. The Bulk Update Controller page appears.

Step 4 Click **Choose File** to select a CSV file, and then find the location of the CSV file you want to import.

Step 5 Click **Update and Sync**.

Sample CSV File for the Bulk Update of Controller Credentials

The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory. The following example shows a sample CSV file.

```
ip_address,network_mask,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmp
v3_auth_password,snmpv3_privacy_type,snmpv3_privacy_password,snmp_retries,snmp_timeout,pro
tocol,telnet_username,telnet_password,enable_password,telnet_timeout
209.165.200.225,255.255.255.224,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
209.165.200.226,255.255.255.224,v2,public,,,,,3,10,,cisco,cisco,cisco,60
209.165.200.227,255.255.255.224,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
```

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name

- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- protocol
- telnet_username
- telnet_password
- enable_password
- telnet_timeout

Removing Controllers from NCS

To remove a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

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

Step 3 From the Select a command drop-down list, choose **Remove Controllers**.

Step 4 Click **Go**.

Step 5 Click **OK** in the pop-up dialog box to confirm the deletion.

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

Rebooting Controllers

To reboot a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

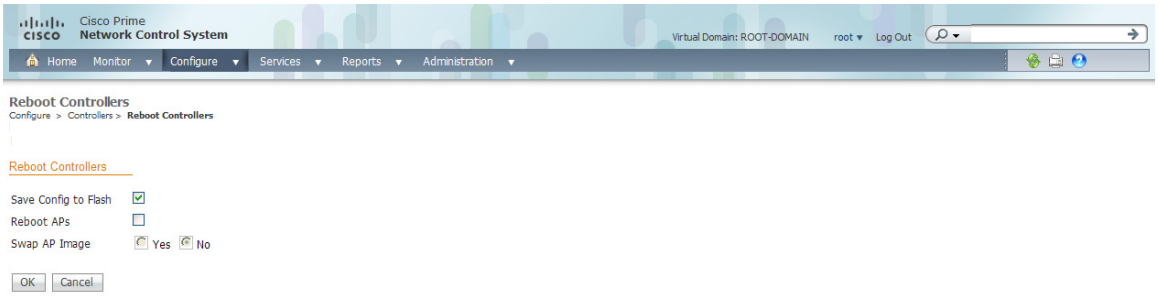
Step 2 Select the check box(es) of the applicable controller(s).

Step 3 From the Select a command drop-down list, choose **Reboot Controllers**.

Step 4 Click **Go**. The Reboot Controllers page appears (see Figure 9-2).

Note Save the current controller configuration prior to rebooting.

Figure 9-2 Reboot Controllers Page



Step 5 Select the Reboot Controller options that must be applied.

- Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
- Reboot APs—Select the check box to enable a reboot of the access point after making any other updates.
- Swap AP Image—Indicates whether or not to reboot controllers and APs by swapping AP images. This could be either Yes or No.

Note Options are disabled unless the Reboot APs check box is selected

Step 6 Click **OK** to reboot the Controller with optional configuration selected.

Downloading Software to Controllers

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

This section contains the following topics:

Download Software (FTP)

To download software to a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

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

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

Step 4 Click **Go**.

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

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

Step 5 Select the download type.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 10 Click **Download**.

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

Download Software (TFTP)

To download software to a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

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

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

Step 4 Click **Go**.

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

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

Step 5 Select the download type.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 11 Click **Download**.

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

Configure *IPaddr* Upload Configuration/Logs from Controller

To upload files from the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

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

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

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

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

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

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

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

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

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

Downloading IDS Signatures

To download Intrusion Detection System (IDS) signature files to a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

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

Step 3 From the Select a command drop-down list, choose **Download IDS Signatures**.

Step 4 Click **Go**.

Note IDS signature files can also be downloaded from Configure > Controllers > IPaddr > System > Commands > Upload/Download Commands > Download IDS Signatures.

In the Download IDS Signatures to Controller page, the controller IP address and its current status appears.

Step 5 Copy the signature file (*.sig) to the default directory on your TFTP server.

Step 6 In the File is located on parameter, select the **Local machine** radio button.

Note If you know the filename and path relative to the server root directory, you can also select the **TFTP server** radio button.

Step 7 In the Maximum Retries text box, enter the maximum number of tries the controller should attempt to download the signature file.

Step 8 In the Timeout text box, enter the maximum amount of time (in seconds) before the controller times out while attempting to download the signature file.

Note The signature files are uploaded to the c:\tftp directory.

Step 9 Specify the local file name or click **Browse** to navigate to the appropriate file. The controller uses this local file name as a base name and adds ***_custom.sgi*** as a suffix.

Note If you chose TFTP server previously, specify the server file name.

Step 10 Click **Download**.

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

Note The local machine option initiates a two-step operation. First, the local file is copied from the administrator workstation to NCS own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the NCS server TFTP directory, and the downloaded web page now automatically populates the filename.

Downloading a Customized WebAuthentication Bundle to a Controller

To download customized web authentication bundle to a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

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

Step 3 From the Select a command drop-down list, choose **Download Customized WebAuth**.

Step 4 Click **Go**.

Note A customized web authentication bundle can also be downloaded from Configure > Controllers > IPaddr > System > Commands > Upload/Download Commands > Download Customized Web Auth.

In the Download Customized WebAuth bundle to Controller page, the controller IP address and its current status appears.

Step 5 Select the **Local machine** radio button in the File is located on parameter.

Note If you know the file name and path relative to the server root directory, you can also select the **TFTP server** radio button.

Note For a local machine download, either .zip or .tar file options exists but the NCS does the conversion of .zip to .tar automatically. If you choose a TFTP server download, only .tar files are specified.

Step 6 In the Maximum Retries text box, enter the maximum number of tries the controller should attempt to download the file.

Step 7 In the Timeout text box, enter the maximum amount of time (in seconds) before the controller times out while attempting to download the file.

Note The NCS Server Files In parameter specifies where the NCS server files are located.

Step 8 Specify the local file name or click **Browse** to navigate to the appropriate file. The controller uses this local file name as a base name and adds *_custom.sgi* as a suffix.

Step 9 Click **Download**.

Tip If the transfer times out for some reason, you can select the **TFTP server** radio button in the File is located on parameter; the server file name is populated and retried.

Step 10 The local machine option initiates a two-step operation. First, the local file is copied from the administrator workstation to NCS own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the NCS server TFTP directory, and the downloaded web page now automatically populates the filename.

Step 11 After completing the download, you are directed to a new page and are able to authenticate.

Downloading a Vendor Device Certificate

Each wireless device (controller, access point, and client) has its own device certificate. If you wish to use your own vendor-specific device certificate, it must be downloaded to the controller.

To download a vendor device certificate to a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 You can download the certificate in one of two ways:

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

b. From the Select a command drop-down list, choose **Download Vendor Device Certificate**.

c. Click **Go**.

-or-

a. Click the IP address of the desired controller.

b. Choose **System > Commands** from the left sidebar menu.

c. From the Upload/Download Commands drop-down list, choose **Download Vendor Device Certificate**.

d. Click **Go**.

Step 3 In the Certificate Password text box, enter the password used to protect the certificate.

Step 4 Re-enter the password in the Confirm Password text box.

Step 5 In the File is located on parameter, select the **Local machine** or **TFTP server** radio button.

Note If the certificate is located on the TFTP server, enter the Server File Name. If it is located on the local machine, enter the local file name by clicking **Browse**.

Step 6 Enter the TFTP server name in the Server Name parameter. The default is the NCS server.

Step 7 Enter the server IP address.

Step 8 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 9 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 10 In the Local File Name text box, enter the directory path of the certificate.

Step 11 In the Server File Name text box, enter the name of the certificate.

Step 12 Click **Download**.

Downloading a Vendor CA Certificate

Controllers and access points have a certificate authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate may be used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you wish to use your own vendor-specific CA certificate, it must be downloaded to the controller.

To download a vendor CA certificate to the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 You can download the certificate in one of two ways:

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

b. From the Select a command drop-down list, choose **Download Vendor CA Certificate**.

c. Click **Go**.

-or-

a. Click the IP address of the desired controller.

b. Choose **System > Commands** from the left sidebar menu.

c. From the Upload/Download Commands drop-down list, choose **Download Vendor CA Certificate**.

d. Click **Go**.

Step 3 In the File is located on parameter, Select the **Local machine** or **TFTP server** radio button.

Note If the certificate is located on the TFTP server, enter the server file name. If it is located on the local machine, enter the local file name by clicking the **Browse** button.

Step 4 Enter the TFTP server name in the Server Name text box. The default is the NCS server.

Step 5 Enter the server IP address.

Step 6 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 7 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 8 In the Local File Name text box, enter the directory path of the certificate.

Step 9 In the Server File Name text box, enter the name of the certificate.

Step 10 Click **OK**.

Saving the Configuration to Flash

To save the configuration to flash memory, follow these steps:

Step 1 Choose **Configure > Controllers**.

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

Step 3 From the Select a command drop-down list, choose **Save Config to Flash**.

Step 4 Click **Go**.

Refreshing the Configuration from the Controller

To refresh the configuration from the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

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

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

Step 4 Click **Go**.

Step 5 At the **Configuration Change** prompt, select the **Retain** or **Delete** radio button.

Step 6 Click **Go**.

Discovering Templates from the Controller

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

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

The following rules apply for template discovery:

- Template Discovery discovers templates that are not found in NCS.
- Existing templates are not discovered.

To discover current templates, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box of the controller for which you want to discover templates.

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

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

Note You can choose the **Enabling this option will create association between discovered templates and the device listed above check box** so that discovered templates will be associated to the configuration on the device and will be shown as applied on that controller.

Note Template discovery refreshes configuration from the controller prior to discovering templates. Click **OK** in the warning dialog box to continue with the discovery.

Updating Credentials in NCS

To update SNMP/Telnet credential details in NCS for multiple controllers, there is no configuration available. To perform this mass update, you need to go to each device and update the SNMP and Telnet credentials.

To update the SNMP/Telnet credentials, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box for each controller to which you want to update SNMP/Telenet credentials.

Step 3 From the **Select a command** drop-down list, choose **Update Credentials in NCS**. The Update Credentials in NCS page appears.

Step 4 Select the **SNMP Parameters** check box and specify the following parameters:

Note SNMP write access parameters are needed for modifying controller configuration. With read-only access parameters, configuration can only be displayed.

- Version—Choose from v1, v2, or v3.
- Retries—Indicates the number of controller discovery attempts.
- Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The valid range is 2 to 90 seconds. The default is 2 seconds.
- Community—Public or Private.
- Verify SNMP Credentials—Select this check box to verify SNMP credentials.

Step 5 Select the **Telnet/SSH Parameters** check box and specify the following parameters:

- User Name—Enter the user name.
- Password/Confirm Password—Enter and confirm the password.
- Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The valid range is 2 to 90 seconds. The default is 60 seconds.

Viewing Templates Applied to a Controller

You can view all templates currently applied to a specific controller.

Note Only templates applied in this partition are displayed.

To view applied templates, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box for the applicable controller.

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

Step 4 Click **Go**. The Templates Applied to a Controller page displays each applied template name, template type, the date the template was last saved, and the date the template was last applied.

Note Click the template name link to view the template details. See “Using Templates” for more information.

Using the Audit Now Feature

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

Note A current Controller Audit Report can be accessed in the Configure > Controllers page by clicking a value in the Audit Status column.

To audit a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Select the check box for the applicable controller.

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

Step 4 Click **Go**.

Step 5 Click **OK** in the pop-up dialog box if you want to remove the template associations from configuration objects in the database as well as template associations for this controller from associated config groups (Template based audit only).

The Audit Report displays:

- Device Name
- Time of Audit
- Audit Status
- Applied and Config Group Template Discrepancies information including:
  - Template type (template name)
  - Template application method
  - Audit status (For example, mismatch, identical)
  - Template attribute
  - Value in NCS
  - Value in Controller
- Other NCS Discrepancies including:
  - Configuration type (name)
  - Audit Status (For example, mismatch, identical)
  - Attribute
  - Value in NCS
  - 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. Choose Config Groups > General for more information on enabling the background audit.
- Failed Enforcements for Config Groups with background audit enabled—Click the link to view a list of failure details (including the reason for the failure) returned by the device. See "Config Groups > General" for more information on enabling the background audit (ConfigAuditSet).
- Restore NCS Values to Controller or Refresh Config from Controller—If there are config differences found as a result of the audit, you can either click **Restore NCS Values to controller** or **Refresh Config from controller** to bring the NCS configuration in sync with the controller.
  - Choose **Restore NCS Values to Controller** to push the discrepancies to the device.

– Choose **Refresh config from controller** to pick up the device for this configuration from the device.

Note Templates are not refreshed as a result of clicking Refresh Config from Controller.

Viewing the 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 list, choose **View Latest Network Configuration Audit Report**.

Step 4 Click **Go**.

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

Note Use the General and Schedule tabs to revise Audit Report parameters. See "Configuration Audit Report" section for more information.

Command Buttons

- Save—Click to save changes made to the current parameters.
- Save and Run—Click to save the changes to the current parameters and run the report.
- Run Now—Click to run the audit report based on existing parameters.
- Export Now—Click to export the report results. The supported export formats is PDF and CSV.
- Cancel—Click to cancel any changes made to the existing 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 on the Reports menu, but this report is interactive and per controller.

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

Configuring Existing Controllers

This section contains the following topics:

Viewing Controllers Properties

To view the properties for current controllers, 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 **Properties > Settings**. The following parameters appear:

- General Parameters:
  - Name—Name assigned to the controller.
  - Type—Controller type.
  - Restore on Cold Start Trap—Select to enable a restore on a cold start trap.
  - Auto Refresh on Save Config Trap—Select to enable an automatic refresh on a Save Config trap.
  - Trap Destination Port—Read-only.
  - Software Version—Read-only.
  - Location—Location of the controller.

  - Contact—The contact person for this controller.
  - Most Recent Backup—The date and time of the most recent backup.
  - Save Before Backup—Select to enable a save before backup.
- SNMP Parameters:

Note SNMP write access parameters are needed for modifying controller configuration. With read-only access parameters, configuration can only be displayed.

  - Version—Choose from v1, v2, or v3.
  - Retries—Indicates the number of controller discovery attempts.
  - Timeout (seconds)—Client Session timeout. Sets the maximum amount of time allowed a client before it is forced to reauthenticate.
  - Community—Public or Private.
  - Access Mode—Read Write

Note Community settings only apply to v1 and v2.

  - User Name—Enter a username.
  - Auth. Type—Choose an authentication type from the drop-down list or choose **None**.
  - Auth. Password—Enter an authentication password.
  - Privacy Type—Choose a privacy type from the drop-down list or choose **None**.
  - Privacy Password—Enter a privacy password.

Note User Name, Auth. Type, Auth. Password, Privacy Type, and Privacy Password only display for v3.

- Telnet/SSH Parameters:
  - User Name—Enter the user name. (Default username is admin.)

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

  - Password/Confirm Password—Enter and confirm the password. (Default password is admin.)
  - Retries—Indicate the number of allowed retry attempts. The default is three.
  - Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The default is 60 seconds.

Note Default values are used if the Telnet/SSH parameters are left blank.

Step 4 If you made changes to this controller properties, click **OK** to confirm the changes, **Reset** to return to the previous or default settings, or **Cancel** to return to the Configure > Controllers page without making any changes to these settings.

Configuring Controller System Parameters

This section describes how to configure the controller system parameters and includes the following topics:

Managing General System Properties for Controllers

To view the general system parameters for a current controller, 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**. The following parameters appear:

- 802.3x Flow Control Mode—Disable or enable. See the ""802.3x Flow Control" section on page 9-29" for more information.
- 802.3 Bridging—Disable or enable. See the ""Configuring 802.3 Bridging" section on page 9-29" for more information.
- Web Radius Authentication—Choose PAP, CHAP, or MD5-CHAP.
  - PAP—Password Authentication Protocol. Authentication method where user information (username and password) is transmitted in clear text.

  - CHAP—Challenge Handshake Authentication Protocol. Authentication method where user information is encrypted for transmission.
  - MD5-CHAP—Message Digest 5 Challenge Handshake Authentication Protocol. With MD5, passwords are hashed using the Message Digest 5 algorithm.

- AP Primary Discovery Timeout—Enter a value between 30 and 3600 seconds.

  The access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry in the list. When configured, the primary discovery request timer specifies the amount of time that a controller has to respond to the discovery request of the access point before the access point assumes that the controller cannot be joined and waits for a discovery response from the next controller in the list.

- CAPWAP Transport Mode—Layer 3 or Layer 2. See the "Lightweight Access Point Protocol Transport Mode, page 9-29" for more information.
- Current LWAPP Operating Mode—Automatically populated.
- Broadcast Forwarding—Disable or enable.
- LAG Mode—Choose **Disable** if you want to disable LAG.

  Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances access points transparently to the user.

  Note LAG is disabled by default on the Cisco 5500 and 4400 series controllers but enabled by default on the Cisco WiSM and the controller in the Catalyst 3750G Integrated Wireless LAN Controller Switch.

  See the "Link Aggregation" section on page 9-31 for more information.

- Ethernet Multicast Support
  - Disable—Select to disable multicast support on the controller.
  - Unicast—Select if the controller, upon receiving a multicast packet, forwards the packets to all the associated access points.

    Note H-REAP supports only unicast mode.

  - Multicast—Select to enable multicast support on the controller.
- Aggressive Load Balancing—Disable or enable. See the ""Aggressive Load Balancing" section on page 9-30" for more information on load balancing.
- Peer to Peer Blocking Mode
  - Disable—Same-subnet clients communicate through the controller.
  - Enable—Same-subnet clients communicate through a higher-level router.
- Over Air Provision AP Mode—Disable or enable.

Over-the-air provisioning (OTAP) is supported by Cisco 5500 and 4400 series controllers. If this feature is enabled on the controller, all associated access points transmit wireless CAPWAP or LWAPP neighbor messages, and new access points receive the controller IP address from these messages. This feature is disabled by default and should remain disabled when all access points are installed.

Note Disabling OTAP on the controller does not disable it on the access point. OTAP cannot be disabled on the access point.

Note You can find additional information about OTAP at this URL: http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a008093d74a.shtml

- AP Fallback—Disable or enable.

  Note Enabling AP Fallback causes an access point which lost a primary controller connection to automatically return to service when the primary controller returns.

- AP Failover Priority—Disable or enable.

  Note To configure failover priority settings for access points, you must first enable the AP Failover Priority feature. See the "AP Failover Priority" section on page 9-28 for more information.

- AppleTalk Bridging—Disable or enable.
- Fast SSID change—Disable or enable.

  When fast SSID changing is enabled, the controller allows clients to move between SSIDs. When the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID. When fast SSID changing is disabled, the controller enforces a delay before clients are allowed to move to a new SSID.

  Note If enabled, the client connects instantly to the controller between SSIDs without having appreciable loss of connectivity.

- Master Controller Mode—Disable or enable.

  Note Because the master controller is normally not used in a deployed network, the master controller setting is automatically disabled upon reboot or OS code upgrade.

- Wireless Management—Disable or enable. See the "Wireless Management" section on page 9-31 for more information.
- Symmetric Tunneling Mode

- ACL Counters—Disable or enable. The number of hits are displayed in the ACL Rule page. See the "Configuring Access Control Lists" section on page 9-98 or the "Configure IPaddr > Access Control List > listname Rules" section on page 9-98 for more information.
- Multicast Mobility Mode—Disable or enable. See the ""Setting the Mobility Scalability Parameters" section on page 9-52" for more information.
- Default Mobility Domain Name—Enter domain name.
- Mobility Anchor Group Keep Alive Interval—Enter the amount of delay time allowed between tries for a client attempting to join another access point. See the ""Mobility Anchor Group Keep Alive Interval" section on page 9-31" for more information.

Tip When you hover your mouse cursor over the parameter text box, the valid range for that field appears.

- Mobility Anchor Group Keep Alive Retries—Enter number of allowable retries.

Tip When you hover your mouse cursor over the parameter text box, the valid range for that field appears.

- RF Network Name—Enter network name.
- User Idle Timeout (seconds)—Enter timeout in seconds.
- ARP Timeout (seconds)—Enter timeout in seconds.

AP Failover Priority

When a controller fails, the backup controller configured for the access point suddenly receives a number of Discovery and Join requests. If the controller becomes overloaded, it may reject some of the access points.

By assigning failover priority to an access point, you have some control over which access points are rejected. When the backup controller is overloaded, join requests of access points configured with a higher priority levels take precedence over lower-priority access points.

To configure failover priority settings for access points, you must first enable the AP Failover Priority feature.

To enable the AP Failover Priority feature, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

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

Step 4 From the AP Failover Priority drop-down, select **Enabled**.

To configure an access point failover priority, follow these steps:

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

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

Note The default priority is Low.

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.

To configure 802.3 bridging using NCS release 4.1 or later, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

Step 3 Choose **System > General** to access the General page.

Step 4 From the 802.3 Bridging drop-down list, choose **Enable** to enable 802.3 bridging on your controller or **Disable** to disable this feature. The default value is Disable.

Step 5 Click **Save** to confirm your changes.

802.3x Flow Control

Flow control is a technique for ensuring that a transmitting entity, such as a modem, does not overwhelm a receiving entity with data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend the transmission until the data in the buffers has been processed.

By default, flow control is disabled. You can only enable a Cisco switch to receive PAUSE frames but not to send them.

Lightweight Access Point Protocol Transport Mode

Lightweight Access Point Protocol transport mode indicates the communications layer between controllers and access points. Selections are Layer 2 or Layer 3.

To convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 lightweight access point transport mode using the NCS user interface, follow these steps:

Note Cisco IOS-based lightweight access points do not support Layer 2 lightweight access point mode. These access points can only be run with Layer 3.

Note This procedure causes your access points to go offline until the controller reboots and the associated access points reassociate to the controller.

Step 1 Make sure that all controllers and access points are on the same subnet.

Note You must configure the controllers and associated access points to operate in Layer 2 mode before completing the conversion.

Step 2 Log into the NCS user interface. Then follow these steps to change the lightweight access point transport mode from Layer 3 to Layer 2:

a. Choose **Configure > Controllers**.

b. Click the IP address of the applicable controller.

c. Choose **System > General** to access the General page.

d. Change lightweight access point transport mode to Layer2 and click **Save**.

e. If NCS displays the following message, click **OK**:

```
Please reboot the system for the CAPWAP Mode change to take effect.
```

Step 3 To restart NCS, follow these steps:

a. Choose **System > Commands**.

b. From the Administrative Commands drop-down list, choose **Save Config To Flash**, and click **Go** to save the changed configuration to the controller.

c. Click **OK** to continue.

d. From the Administrative Commands drop-down list, choose **Reboot**, and click **Go** to reboot the controller.

e. Click **OK** to confirm the save and reboot.

Step 4 After the controller reboots, follow these steps to verify that the CAPWAP transport mode is now Layer 2:

a. Choose **Configure> Controllers**.

b. Click the IP address of the applicable controller.

c. Verify that the current CAPWAP transport mode is Layer2 from the general drop-down list.

You have completed the CAPWAP transport mode conversion from Layer 3 to Layer 2. The operating system software now controls all communications between controllers and access points on the same subnet.

Aggressive Load Balancing

In routing, load balancing refers to the capability of a router to distribute traffic over all its network ports that are the same distance from the destination address. Good load-balancing algorithms use both line speed and reliability information. Load balancing increases the use of network segments, thus increasing effective network bandwidth.

Aggressive load balancing actively balances the load between the mobile clients and their associated access points.

Link Aggregation

Link aggregation allows you to reduce the number of IP addresses needed to configure the ports on your controller by grouping all the physical ports and creating a link aggregation group (LAG). In a 4402 model, two ports are combined to form a LAG whereas in a 4404 model, all four ports are combined to form a LAG.

If LAG is enabled on a controller, the following configuration changes occur:

- Any dynamic interfaces that you have created are deleted. This is done to prevent configuration inconsistencies in the interface database.
- Interfaces cannot be created with the "Dynamic AP Manager" flag set.

Note You cannot create more than one LAG on a controller.

The advantages of creating a LAG include:

- Assurance that, if one of the links goes down, the traffic is moved to the other links in the LAG. As long as one of the physical ports is working, the system remains functional.
- No need to configure separate backup ports for each interface.
- Multiple AP-manager interfaces are not required because only one logical port is visible to the application.

Note When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.

Tip When you hover your mouse over the parameter text box, the valid range for that field appears.

Wireless Management

Because of IPSec operation, management via wireless is only available to operators logging in across WPA, Static WEP, or VPN Pass Through WLANs. Wireless management is not available to clients attempting to log in via an IPSec WLAN.

Mobility Anchor Group Keep Alive Interval

Indicate the delay between tries for clients attempting to join another access point. This decreases the time it takes for a client to join another access point following a controller failure because the failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

Tip When you hover your mouse over the parameter text box, the valid range for that field appears.

Configuring Controller System Commands

To view the System Command parameters for current controllers, 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 > Commands**. The following parameters appear:

- Administrative
  - Reboot—This command enables you to confirm the restart of your controller after saving your configuration changes. Open and confirm a new session and log into the controller to avoid loosing a system connection.
  - Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
  - Reset to Factory Default—Choose this command to return the controller to its original settings. See the "Restoring Factory Defaults" section on page 9-33 for more information.
  - Ping From Controller—Send a ping to a network element. This pop-up dialog box allows you to tell the controller to send a ping request to a specified IP address. This is useful for determining if there is connectivity between the controller and a particular IP station. If you click **OK**, three pings are sent and the results of the ping are displayed in the pop-up. If a reply to the ping is not received, it will show No Reply Received from IP xxx.xxx.xxx.xxx, otherwise it shows Reply received from IP xxx.xxx.xxx.xxx: (send count =3, receive count = n).
- Configuration
  - Audit Config—See the "Viewing the Latest Network Audit Report" section on page 9-22.
  - Refresh Config From Controller—See the "Refreshing the Configuration from the Controller" section on page 9-18.
  - Restore Config To Controller—Choose this command to restore the configuration from the NCS database to the controller.
  - Set System Time—See the "Setting Controller Time and Date" section on page 9-34.
- Upload/Download Commands

Note Select the **FTP** or **TFTP** radio button. Both File Transfer Protocol (FTP) and Trivial Transfer Protocol (TFTP) are supported for uploading and downloading files to and from NCS. In previous software releases, only TFTP was supported.

  - Upload File from Controller—See the "Uploading Configuration/Logs from Controllers" section on page 9-34.
  - Download Config—See the "Downloading Configurations to Controllers" section on page 9-35.
  - Download Software—Choose this command to download software to the selected controller or all controllers in the selected groups after you have a configuration group established. See the "Downloading Software to a Controller" section on page 9-35.
  - Download Web Auth Cert—Choose this command to access the Download Web Auth Certificate to Controller page. See the "Downloading a Web Admin Certificate to a Controller" section on page 9-36.
  - Download Web Admin Cert—Choose this command to access the Download Web Admin Certificate to Controller page. See the "Downloading a Web Admin Certificate to a Controller" section on page 9-36.

  - Download IDS Signatures—Choose this command to download customized signatures to the standard signature file currently on the controller. See the "Downloading Signature Files" section on page 9-106 for more information.
  - Download Customized Web Auth—Choose this command to download a customized Web authentication page to the controller. A customized web page is created to establish a username and password for user web access. See the "Downloading a Customized WebAuthentication Bundle to a Controller" section on page 9-15.
  - Download Vendor Device Certificate—Choose this command to download your own vendor-specific device certificate to the controller to replace the current wireless device certificate. See the "Downloading a Vendor Device Certificate" section on page 9-16.
  - Download Vendor CA Certificate—Choose this command to download your own vendor-specific certificate authority (CA) to the controller to replace the current CA. See the "Downloading a Vendor CA Certificate" section on page 9-17.
- RRM Commands
  - RRM 802.11a/n Reset—Resets Remote Radio Management for 802.11a/n Cisco Radios.
  - 802.11b/g/n Reset—Resets Remote Radio Management for 802.11b/g/n Cisco Radios.
  - 802.11a/n Channel Update—Updates access point dynamic channel algorithm for 802.11a/n Cisco Radios.
  - 802.11b/g/n Channel Update—Updates access point dynamic channel algorithm for 802.11b/g/n Cisco Radios.
  - 802.11a/n Power Update—Updates access point dynamic transmit power algorithm for 802.11a/n Cisco Radios.
  - 802.11b/g/n Power Update—Updates access point dynamic transmit power algorithm for 802.11b/g/n Cisco Radios.

Restoring Factory Defaults

Choose **Configure > Controllers**, and click an IP address in the IP Address column. From the left sidebar menu, choose **System > Commands**, and from the Administrative Commands drop-down list, choose **Reset to Factory Default**, and click **Go** to access this page.

This command enables you to reset the controller configuration to the factory default. This overwrites all applied and saved configuration parameters. You are prompted for confirmation to re-initialize your controller.

All configuration data files are deleted, and upon reboot, the controller is restored to its original non-configured state. This will remove all IP configuration, and you will need a serial connection to restore its base configuration.

Note After confirming configuration removal, you must reboot the controller and select the "Reboot Without Saving" option.

Setting Controller Time and Date

Choose **Configure > Controllers**, and click an IP address under the IP Address column. From the left sidebar menu, choose **System > Commands**, and from the Configuration Commands drop-down list choose **Set System Time**, and click **Go** to access this page.

Use this command to manually set the current time and date on the controller. To use a Network Time Server to set or refresh the current time, see the "Configuring an NTP Server Template" section on page 11-10 page. The following parameters appear:

- Current Time—Shows the time currently being used by the system.
- Month/Day/Year—Choose the month/day/year from the drop-down list.
- Hour/Minutes/Seconds—Choose the hour/minutes/seconds from the drop-down list.
- Delta (hours)—Enter the positive or negative hour offset from GMT (Greenwich Mean Time).
- Delta (minutes)—Enter the positive or negative minute offset from GMT.
- Daylight Savings—Select to enable Daylight Savings Time.

Command Buttons

- Set Date and Time
- Set Time Zone
- Cancel

Uploading Configuration/Logs from Controllers

To upload files from the controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

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

Step 4 From the Upload/Download Commands drop-down list, choose **Upload File from Controller**.

Step 5 Click **Go** to access this page.

Use this command to upload files from your controller to a local TFTP (Trivial File Transfer Protocol) server. The following parameter appears:

- IP Address—IP address of the controller.
- Status—Upload NOT_INITIATED, or other state.
- Enter the TFTP server name, or New and the new TFTP server name.
- Verify and/or enter the IP Address of the TFTP server.
- Select the file type—Configuration file, Event Log, Message Log, Trap Log, Crash File.
- Enter the Upload to File from /(root)/NCS-tftp/ filename.
- Choose whether or not Cisco NCS saves before backing up the configuration.

Step 6 Click **OK**. The selected file will be uploaded to your TFTP server and named what you entered in the File Name text box.

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

Downloading Configurations to Controllers

To download configuration files, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

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

Step 4 From the Upload/Download Commands drop-down list, choose **Download Config**.

Step 5 Click **Go** to access this page.

Use this command to download and install a configuration file to your controller from a local TFTP (Trivial File Transfer Protocol) server. The following parameters appear:

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

- IP Address—IP address of the controller.
- Status—Status of the certificate, for example, NOT_INITIATED.

TFTP Servers

- Server Name—Choose Default Server or New from the drop-down list. When you choose New, type in the IP address.
- Server Address—IP address of the server.
- Maximum Retries—How many times to retry if the download fails.
- Timeout—How long to allow between retries.
- File Name—Enter or choose the filename to download by clicking the Browse button.

Downloading Software to a Controller

To download software, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

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

Step 4 From the Upload/Download Commands drop-down list, choose **Download Software**.

Step 5 Click **Go** to access this page.

Use this command to download and install a new Operating System software to your controller from a local TFTP (Trivial File Transfer Protocol) server.

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

- IP Address—IP address of the controller to receive the software.
- Current Software Version—The software version currently running on the controller.
- Status—Status of the software, for example, NOT_INITIATED.
- TFTP Server on Cisco NCS System—Select the check box enable the built-in Cisco NCS TFTP server.
- Server IP Address—When you have disabled the built-in Cisco NCS TFTP server, IP Address of the TFTP server to send the software to the controller.
- Maximum Retries—Maximum number of unsuccessful attempts before the download is abandoned.
- Timeout—Maximum number of seconds before the download is abandoned.
- File Name—Enter or select the filename to download using the Browse button.

Downloading a Web Admin Certificate to a Controller

To download a Web Admin Certificate, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

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

Step 4 From the Upload/Download Commands drop-down list, choose **Download WEB Admin Cert**.

Step 5 Click **Go** to access this page.

This page enables you to download a web administration certificate to the controller. The following parameters appear:

Caution Each certificate has a variable-length embedded RSA Key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a certificate authority (such as the Microsoft CA), Make sure the RSA key embedded in the certificate is at least 768 Bits.

- IP Address—IP address of the controller to receive the certificate.
- Status—Status of the certificate, for example, NOT_INITIATED.

TFTP Servers

- Server Name—Use the drop-down list to choose the Default Server or New. When you select New, type in the IP address.
- Server Address—IP address of the server.

- Maximum Retries—Maximum number of times each download operation can be attempted.
- Timeout (seconds)—The amount of time allowed for each download operation.
- File Name—File name of the certificate.
- Password—Password to access the certificate.

Downloading IDS Signatures

To download a IDS Signature, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

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

Step 4 From the Upload/Download Commands drop-down list, choose **Download IDS Signatures**.

Step 5 Click **Go** to access this page.

Use this command to download IDS (Intrusion Detection System) signature files from your controller to a local TFTP (Trivial File Transfer Protocol) server. The following parameters appear:

- IP Address—IP address of the controller.
- Status—Download NOT_INITIATED, TRANSFER_SUCCESSFUL or other state.

Downloading a Customized Web Auth Bundle to a Controller

To download a customized Web authentication page to the controller, follow these steps:

Step 1 Choose **Configure > Controllers**

Step 2 Click an IP address in the IP Address column.

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

Step 4 From the Upload/Download Commands drop-down list, choose **Download Customized Web Auth**.

The following parameters appear:

- IP Address—IP address of the controller to receive the bundle.
- Status—State of download: NOT_INITIATED, TRANSFER_SUCCESSFUL, TRANSFER_FAILED, NOT_RESPONDING.

Before downloading the customized Web authentication bundle, follow these steps:

Step 1 Click the indicated link to download the example login.tar bundle file from the server.

The link is the highlighted word “here” near the bottom of the page.

Step 2 Edit the login.html file and save it as a .tar or .zip file.

Step 3 Download the .tar or .zip file to the controller.

The file contains the pages and image files required for the Web authentication display.

Note The controller accepts a .tar or .zip file of up to 1 MB in size. The 1 MB limit includes the total size of uncompressed files in the bundle.

TFTP Servers

To set up one or more TFTP servers, configure the following parameters:

- File is located on—Choose **Local machine** or **TFTP server**. The default is local machine (NCS internal server).
- Server Name—Use the drop-down list to choose one of the following:
  - New—Set up a new server. Enter the server name and IP address in the text boxes provided.
  - Default Server—server name (editable) IP address (read-only) are automatically added.
- Server IP Address—IP address of the server.
- Maximum Retries—Maximum number of unsuccessful attempts before the download is abandoned.
- Timeout—Maximum number of seconds before the download is abandoned.
- NCS Server Files In—C:\tftp or other specified file directory on the local machine.
- Local File Name—Filename of the Web authentication bundle on the local machine. Click **Browse** to locate the file.
- Server File Name—Filename on a remote TFTP server.

When completed, these fields and settings are repopulated in the page and do not need to be entered again.

Command Buttons

- OK—The file is downloaded from the local machine or TFTP server with the name shown in the File Name text box.
- Cancel

Configuring Controller System Interfaces

This section describes how to configure controller system interfaces and includes the following topics:

To view existing interfaces, 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 > Interfaces**. The following parameters appear:

- Check box—Select the dynamic interface for deletion. Choose **Delete Dynamic Interfaces** from the Select a command drop-down list.
- Interface Name—User-defined name for this interface (For example, Management, Service-Port, Virtual).
- VLAN Identifier—VLAN identifier between 0 (untagged) and 4096, or N/A.
- Quarantine—Select the check box if the interface has a quarantine VLAN ID configured on it.
- IP Address—IP address of this interface.
- Interface Type—Static (Management, AP-Manager, Service-Port, and Virtual interfaces) or Dynamic (operator-defined interfaces).
- AP Management Status—Displays the status of AP Management interfaces. The parameters include Enabled, Disabled, and N/A.

Adding an Interface

To add an interface, 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 > Interfaces**.

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

Step 5 Enter the necessary parameters:

- Interface Name—User-defined name for this interface (Management, Service-Port, Virtual, and VLAN n).
- Wired Interface—Select the check box to mark the interface as wired.
- Interface Address
  - VLAN Identifier—1 through 4096, or 0 = untagged.
  - Quarantine—Enable/disable to quarantine a VLAN. Select the check box to enable.
  - IP Address—IP address of the interface.
  - Gateway—Gateway address of the interface.
- Physical Information
  - Port Number—The port that is used by the interface.
  - Primary Port Number (active)—The port that is currently used by the interface.
  - Secondary Port Number—The port that is used by the interface when the primary port is down.

Note Primary and secondary port numbers are only present in Cisco 4400 Series Wireless LAN Controllers.

Note The secondary port is used when the primary port shuts down. When the primary port is reactivated, the Cisco 4400 Series Wireless LAN Controller transfers the interfaces back to the primary port.

  - AP Management—Select to enable access point management.
- DHCP Information
  - Primary DHCP Server—IP address of the primary DHCP server.
  - Secondary DHCP Server—IP address of the secondary DHCP server.
- Access Control List—User-defined ACL name (or none).

Viewing Current Interface Details

To view details for a current interface, 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 > Interfaces**.

Step 4 Select the Interface Name for the applicable interface. The Interface Details page opens.

Step 5 View or edit the following interface parameters:

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

- Interface Address
  - VLAN Identifier—1 through 4096, or 0 = untagged.
  - Guest LAN
  - Quarantine—Enable/disable to quarantine a VLAN. Select the check box to enable.
  - IP Address—IP address of the interface.
  - Gateway—Gateway address of the interface.
- Physical Information
  - Primary Port Number (active)—The port that is currently used by the interface.
  - Secondary Port Number—The port that is used by the interface when the primary port is down.

Note Primary and secondary port numbers are only present in Cisco 4400 Series Wireless LAN Controllers.

Note The secondary port is used when the primary port shuts down. When the primary port is reactivated, the Cisco 4400 Series Wireless LAN Controller transfers the interfaces back to the primary port.

  - AP Management—Select to enable access point management.
- DHCP Information
  - Primary DHCP Server—IP address of the primary DHCP server.
  - Secondary DHCP Server—IP address of the secondary DHCP server.
- Access Control List
  - ACL Name—User-defined name of the access control list (or none).

Step 6 Click **Save** to confirm any changes made. Click **Audit** to audit the device values.

Deleting a Dynamic Interface

To delete a dynamic interface, 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 > Interfaces**.

Step 4 Select the check box of the dynamic interface that you want to delete.

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

Step 6 Click **OK** to confirm the deletion.

Note The dynamic interface cannot be deleted if it is been assigned to interface group.

Configuring Controller System Interface Groups

This section describes how to configure controller system interface groups and introduces the following topics:

Adding an Interface Group

To add an interface group, 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 > Interface Groups**.

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

Step 5 Enter the necessary parameters:

- Name—User-defined name for this interface group (group1, group2).
- Interface Group Type—Select/deselect to quarantine a VLAN.
- Description—(Optional) Description for the Interface group.

Step 6 Click **Add**.

The Interface dialog box appears.

Step 7 Select the interfaces that you want to add to the group and click **OK**.

To remove an Interface from the Interface group, from the Interface Group page, select the Interface and click **Remove**.

Step 8 Once you are done with adding the interfaces, in the Interface Group page, click any of these buttons:

- **Save** to confirm any changes made.
- **Audit** to audit the device values.
- **Cancel** to discard the changes.

Note

- The number of interfaces that could be added to an interface group depends upon the type of the controller.
- Guest LAN interfaces cannot be part of interface groups.
- An Interface group name must be different from the Interface name.

Deleting an Interface Group

To delete an interface group, 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 > Interface Groups**.

Step 4 Select the check box of the interface group that you want to delete.

Step 5 From the Select a command drop-down list, choose **Delete Interface Group,** and click **Go**.

Step 6 Click **OK** to confirm the deletion.

Note

- The Interface Group cannot be deleted if it has been assigned to WLAN(s).
- The Interface Group cannot be deleted if it has been assigned to AP Group(s).
- The Interface Group cannot be deleted if it has been assigned to Foreign Controller Mapping for the WLAN(s).

- The Interface Group Template cannot be deleted if it has been assigned to WLAN Template(s).
- The Interface Group Template cannot be deleted if it has been assigned to AP Group Template(s).
- You cannot enable/disable quarantine for an interface if it has been assigned to an interface group.

Viewing Interface Groups

To view existing interface groups, 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 > Interface Groups**. The following parameters appear:

- Name—User-defined name for the interface group (For example, group1, group2).
- Description—(Optional) Description for the Interface Group.
- Interfaces—Count of the number of interfaces belonging to the group.

Step 4 Click the Interface group name link.

The Interface Groups Details page appears with the Interface group details as well as the details of the Interfaces that form part of that particular Interface group.

NAC 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).

For more information on NAC Out-of-Band Integration, see the applicable section in the *Cisco Network Control System Configuration Guide*.

- Guidelines for Using SNMP NAC, page 9-43
- Configuring NAC Out-of-Band Integration (SNMP NAC), page 9-44

Guidelines for Using SNMP NAC

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

Note See the Cisco NAC appliance configuration guides for configuration instructions: http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html.

Guidelines for Using RADIUS NAC

Follow these guidelines when using RADIUS NAC:

- RADIUS NAC is available only for WLAN with 802.1x/WPA/WPA2 Layer 2 security.
- RADIUS NAC cannot be enabled when HREAP local switching is enabled.
- AAA override should be enabled to configure RADIUS NAC.

Configuring NAC Out-of-Band Integration (SNMP NAC)

To configure SNMP NAC out-of-band integration, follow these steps:

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 it in the IP Address column.

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

d. Choose **Add Interface** from the Select a command drop-down list.

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

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

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

Note We recommend 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 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. Choose **WLANs > WLAN** from the left sidebar menu.

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

c. If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the **click here** link to create a new template. For more information on setting up the template, see the "Configuring Wired Guest Access" section on page 9-46 section.

d. Click the **Advanced** tab.

e. To configure SNMP NAC support for this WLAN or guest LAN, select **SNMP NAC** from the NAC Stage drop-down list. To disable SNMP NAC support, select **None** from the NAC Stage drop-down list, 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, follow these steps:

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

Note AP Groups (for 5.2 and later controllers) is referred to as **AP Group VLANs** for controllers prior to 5.2.

b. Click the name of the desired AP group.

c. From the Interface Name drop-down list, choose the quarantine enabled interface.

d. To configure SNMP NAC support for this AP group, select **SNMP NAC** from the Nac State drop-down list. To disable NAC out-of-band support, select **None** from the Nac State drop-down list, 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. Choose **Monitor > Clients** to open the Clients. 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, invalid, or quarantine in the Security Information section.

Configuring Wired Guest Access

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

Like wireless guest user accounts, wired guest access ports are added to the network using the Lobby Ambassador feature. See the "Configuring a Guest Account" section on page 15-86.

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, see the "Configuring a Guest Account" section on page 15-86.

To configure and enable wired guest user access on the network, follow these steps:

Step 1 To configure a dynamic interface for wired guest user access, choose **Configure > Controllers** and after IP address, choose **System > Interfaces**.

Step 2 Choose **Add Interface** from the Select a command drop-down list, and click **Go**.

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

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

Step 5 Enter the primary and secondary port number.

Step 6 Click **Save**. You are now ready to create a wired LAN for guest access.

Step 7 To configure a wired LAN for guest user access, choose **WLANs > WLAN configuration** from the left sidebar menu.

Step 8 Choose **Add a WLAN** from the Select a command drop-down list, and click **Go**.

Step 9 If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the **click here** link to create a new template.

Step 10 In the **WLAN > New Template general** page, enter a name in the Profile Name text box that identifies the guest LAN. Do not use any spaces in the name entered.

Step 11 Select the **Enabled** check box for the WLAN Status parameter.

Step 12 From the Ingress Interface drop-down list, choose the VLAN that you created in Step 3. This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 13 From the Egress Interface drop-down list, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.

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

Step 14 Choose **Security > Layer 3** tab to modify the default security policy (web authentication) or to assign WLAN specific web authentication (login, logout, login failure) pages and the server source.

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

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

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

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

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

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

These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files. For specifics on downloading custom pages, see the "Downloading a Customized WebAuthentication Bundle to a Controller" section on page 9-15.

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

You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA pane. To do so, continue with Step 17.

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

Step 15 If you selected External as the Web Authentication Type in Step 15, choose **Security > AAA** and choose up to three RADIUS and LDAP servers using the drop-down lists.

Step 16 Click **Save**.

Step 17 Repeat this process if a second (anchor) controller is being used in the network.

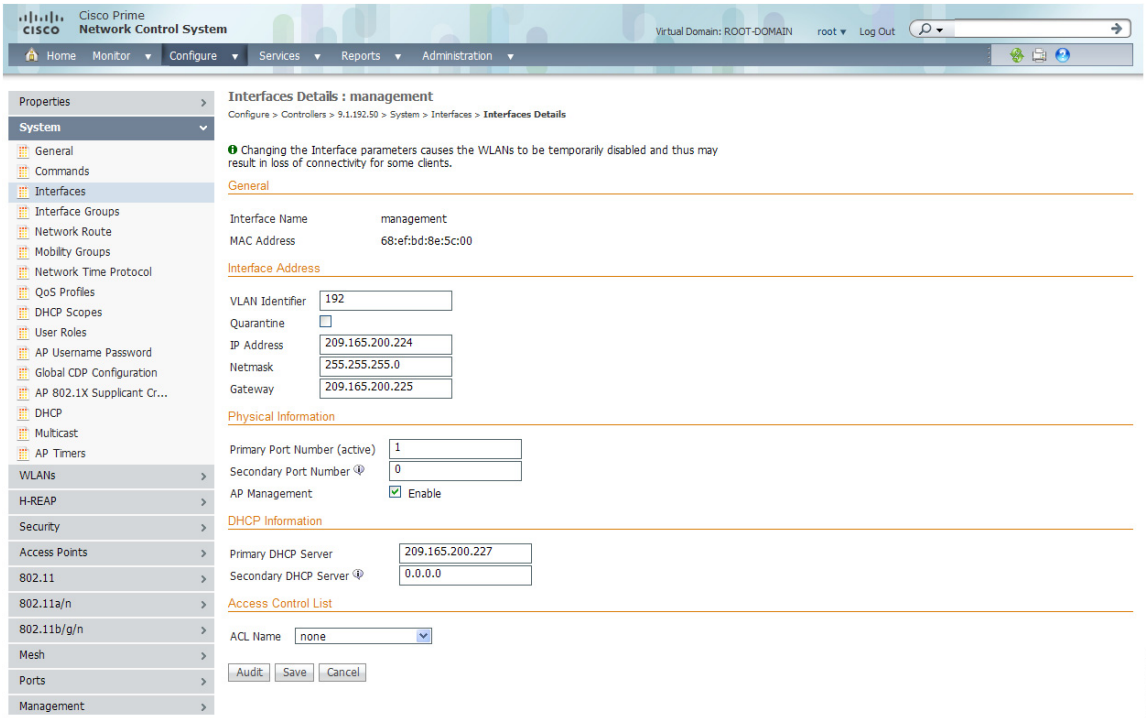
Creating an Ingress Interface

To create an Ingress interface, follow these step:

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

Step 2 Click an interface name. The Interfaces Details : New Config page appears (see Figure 9-3).

Figure 9-3 Interfaces Details : New Config Page



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

Step 4 Enter a VLAN identifier for the new interface.

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

Step 6 Enter the primary and secondary port numbers.

Step 7 Click **Save**.

Creating an Egress Interface

To create an Egress interface, follow these steps:

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

Step 2 Click an interface name. The Interfaces Details : New Config page appears (see Figure 9-3).

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

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

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

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

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

Step 7 Enter the primary and secondary port numbers.

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

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

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

Configuring Controller Network Routes

The Network Route page enables you to add a route to the controller service port. This route allows you to direct all Service Port traffic to the designated management IP address.

- Viewing Existing Network Routes, page 9-49
- Adding a Network Route, page 9-49

Viewing Existing Network Routes

To view existing network routes, 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 > Network Route**. The following parameters appear:

- IP Address—The IP address of the network route.
- IP Netmask—Network mask of the route.
- Gateway IP Address—Gateway IP address of the network route.

Adding a Network Route

To add a network route, 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 > Network Route**.

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

Step 5 Click **Go**.

Step 6 Enter the IP address, IP Netmask, and Gateway IP address information.

Step 7 Click **Save**.

Configuring Controller Spanning Tree Protocol Parameters

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

To view or manage current STP parameters, 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 > Spanning Tree Protocol**. The Spanning Tree Protocol page displays the following parameters:

- Protocol Spec—The current protocol specification.
- Admin Status—Check this check box to enable.
- Priority—The numerical priority number of the ideal switch.
- Maximum Age (seconds)—The amount of time (in seconds) before the received protocol information recorded for a port is discarded.
- Hello Time (seconds)—Determines how often (in seconds) the switch broadcasts its hello message to other switches.
- Forward Delay (seconds)—The time spent (in seconds) by a port in the learning/listening states of the switches.

Configuring Controller Mobility Groups

By creating a mobility group, you can enable multiple network controllers to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers can share the context and state of client devices and controller loading information. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

Note If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.

- Setting the Mobility Scalability Parameters, page 9-52

Messaging Among Mobility Groups

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers:

- There can be up to 72 members in the list with up to 24 in the same mobility group.
- The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it.
- In NCS and controller software release 5.0, the controller uses multicast mode to send the Mobile Announce messages. This allows the controller to send only one copy of the message to the network, which delivers it to the multicast group containing all the mobility members.

Note For more information regarding mobility groups, see the *Cisco Network Control System Configuration Guide*.

Mobility Group Prerequisites

Before you add controllers to a mobility group, you must verify that the following requirements have been met for all controllers that are to be included in the group:

- All controllers must be configured for the same CAPWAP transport mode (Layer 2 or Layer 3).
- IP connectivity must exist between the management interfaces of all devices.
- All controllers must be configured with the same mobility group name.
- All devices must be configured with the same virtual interface IP address.
- Availability of MAC and IP addresses of each controller to be included in the mobility group (to configure the controllers with the MAC address and IP address of all the other mobility group members).

Viewing Current Mobility Group Members

To view current mobility group members, 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 > Mobility Groups**.

Note To delete a group member, select a check box for the applicable group member, choose **Delete Group Members**, and click **Go**.

Adding Mobility Group Members from a List of Controllers

To add a mobility group member from a list of existing controllers, 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 > Mobility Groups**.

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

Step 5 Click **Go**.

Step 6 Select the check box(es) for the controller to be added to the mobility group.

Step 7 Click **Save**.

Manually Adding Mobility Group Members

If no controllers were found to add to the mobility group, you can add members manually. To manually add members to the mobility group, follow these steps:

Step 1 Click the **click here** link from the Mobility Group Member details page.

Step 2 In the Member MAC Address text box, enter the MAC address of the controller to be added.

Step 3 In the Member IP Address text box, enter the management interface IP address of the controller to be added.

Note If you are configuring the mobility group in a network where Network Address Translation (NAT) is enabled, enter the IP address sent to the controller from the NAT device rather than the controller management interface IP address. Otherwise, mobility fails among controllers in the mobility group.

Step 4 Enter the multicast group IP address to be used for multicast mobility messages in the Multicast Address text box. The local mobility member group address must be the same as the local controller group address.

Step 5 In the Group Name text box, enter the name of the mobility group.

Step 6 Click **Save**.

Step 7 Repeat the Steps 1 through 6 for the remaining WLC devices.

Setting the Mobility Scalability Parameters

Note Mobility Groups must be configured prior to setting the mobility scalability parameters.

To set the mobility message parameters, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose an IP address of a controller whose software version is 5.0 or later.

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

Step 4 At the Multicast Mobility Mode parameter, specify if you want to enable or disable the ability for the controller to use multicast mode to send Mobile Announce messages to mobility members.

Step 5 If you enabled multicast messaging by setting multicast mobility mode to enabled, you must enter the group IP address at the Mobility Group Multicast-address parameter to begin multicast mobility messaging. You must configure this IP address for the local mobility group but it is optional for other groups within the mobility list. If you do not configure the IP address for other (non-local) groups, the controllers use unicast mode to send mobility messages to those members.

Step 6 Click **Save**.

Configuring Controller Network Time Protocol

To add a new NTP Server, 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 > Network Time Protocol**.

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

Step 5 Click **Go**.

Step 6 From the Select a template to apply to this controller drop-down list, select the applicable template to apply to this controller.

Command Buttons

- Apply
- Cancel

To create a New Template for NTP Servers, use the **click here** link to access the template creation page (Configure NTP Servers > New Template).

NTP general parameters include:

- Template Name—Enter the new NTP Template name.

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Server Address—Enter the NTP server IP address.
- No. of Controllers Applied To—Number of controllers to which this template is applied (read-only).

Background Scanning on 1510s in Mesh Networks

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

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

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

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

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

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

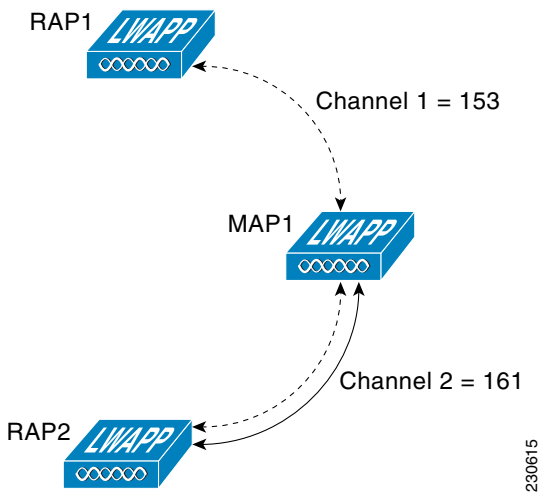
Note In the EMEA regulatory domain, locating neighbors on other channels might take longer given DFS requirements.

Background Scanning Scenarios

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

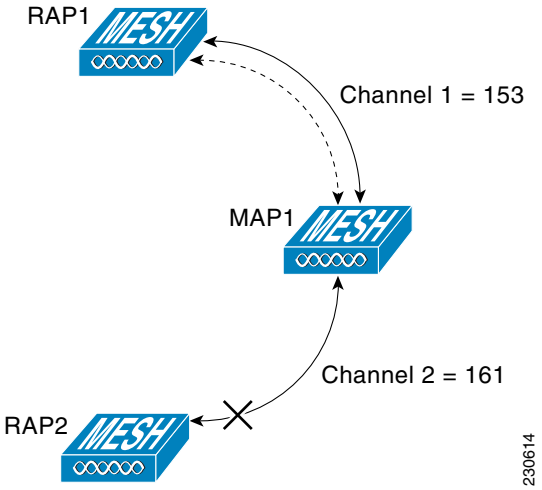
In Figure 9-4, when the mesh access point (MAP1) initially comes up, it is aware of both root access points (RAP1 and RAP2) as possible parents. It chooses RAP2 as its parent because the route through RAP2 is better in terms of hops, SNR, and so on. After the link is established, background scanning (once enabled) continuously monitors all channels in search of a more optimal path and parent. RAP2 continues to act as parent for MAP1 and communicates on channel 2 until either the link goes down or a more optimal path is located on another channel.

Figure 9-4 Mesh Access Point (MAP1) Selects a Parent



In Figure 9-5, the link between MAP1 and RAP2 is lost. Data from ongoing background scanning identifies RAP1 and channel 1 as the next best parent and communication path for MAP1 so that link is established immediately without the need for additional scanning after the link to RAP2 goes down.

Figure 9-5 Background Scanning Identifies a New Parent



Enabling Background Scanning

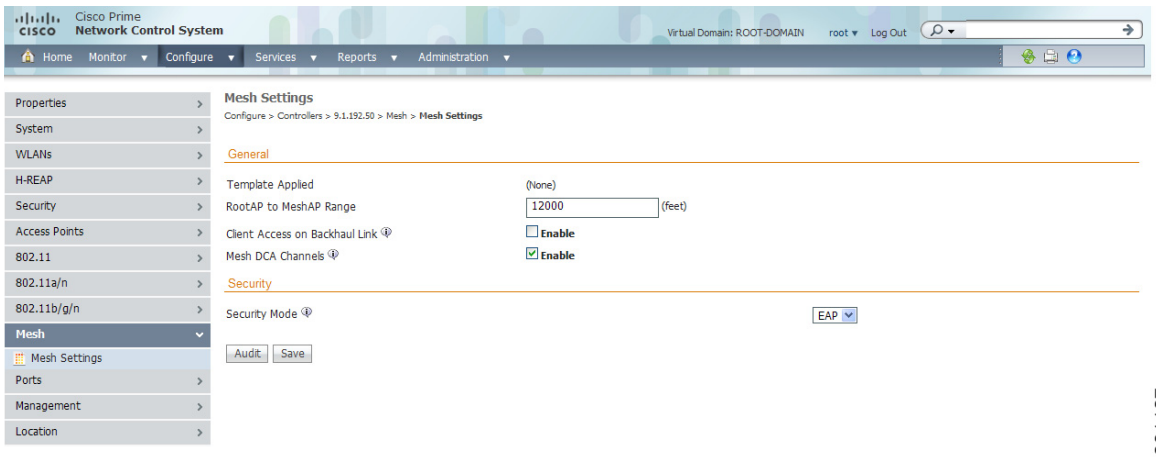
To enable background scanning on an AP1510 RAP or MAP, follow these steps:

Step 1 Click **Configure > Controllers**.

Note You can also enable this on the Controllers template. See the "Configuring Mesh Templates" section on page 11-114.

Step 2 Choose **Mesh > Mesh Settings** from the left sidebar menu. The Mesh Settings page appears (see Figure 9-6).

Figure 9-6 Mesh Settings Page



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

Step 4 Click **Save**.

Configuring Controller QoS Profiles

To make modifications to the quality of service profiles, 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 > QoS Profiles**. The following parameters appear:

- Bronze—For Background
- Gold—For Video Applications
- Platinum—For Voice Applications
- Silver—For Best Effort

Step 4 Click the applicable profile to view or edit profile parameters.

Step 5 Set the following values in the Per-User Bandwidth Contracts section (all have a default of 0 or Off):

- Average Data Rate—The average data rate for non-UDP traffic.
- Burst Data Rate—The peak data rate for non-UDP traffic.
- Average Real-time Rate—The average data rate for UDP traffic.
- Burst Real-time Rate—The peak data rate for UDP traffic.

Step 6 Set the following values for the Over-the-Air QoS section:

- Maximum QoS RF Usage Per AP (%)—The maximum air bandwidth available to clients. The default is 100%.
- QoS Queue Depth—The depth of queue for a class of client. The packets with a greater value are dropped at the access point.

Step 7 Set the following values in the Wired QoS Protocol section:

- Wired QoS Protocol—Choose **802.1P** to activate 802.1P priority tags or **None** to deactivate 802.1P priority tags.

Step 8 Click **Save**.

Configuring Controller DHCP Scopes

Viewing Current DHCP Scopes

To view current DHCP (Dynamic Host Configuration Protocol) scopes, 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 > DHCP Scopes**.

The following DHCP Scopes information appears:

- Pool Address
- Lease Time
- Status

Adding a New DHCP Scope

To add a new DHCP Scope, 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 > DHCP Scopes**.

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

Step 5 Enter the following information:

- Scope Name
- Lease Time (in seconds)
- Network
- Netmask
- Pool Start Address
- Pool End Address
- DNS Domain Name
- Status
- Router Addresses—Enter which IP addresses are already in use and should therefore be excluded. For example, you should enter the IP address of your company router. In doing so, this IP address will be blocked from use by another client.
- DNS Servers—Enter the IP address of the DNS server(s). Each DNS server must be able to update a client DNS entry to match the IP address assigned by this DHCP scope.
- NetBios Servers—Enter the IP address of the Microsoft Network Basic Input Output System (NetBIOS) name server(s), such as a Windows Internet Naming Service (WINS) server.

Step 6 Click **Save**.

Configuring Controller User Roles

- Viewing Current Local Net User Roles, page 9-58
- Adding a New Local Net User Role, page 9-58

Viewing Current Local Net User Roles

To view current local net user roles, 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 > User Roles**.

The following Local Net User Role parameters appear:

- Template Name

Note Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

- Role Name
- Average Data Rate—The average data rate for non-UDP traffic.
- Burst Data Rate—The peak data rate for non-UDP traffic.
- Average Real-time Rate—The average data rate for UDP traffic.
- Burst Real-time Rate—The peak data rate for UDP traffic.

Step 4 Click a Template Name to view the User Role details.

Adding a New Local Net User Role

To add a new local net user role, 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 > User Roles**.

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

Step 5 Select a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

Note To create a new template for local net user roles, click the **click here** link to access the template creation page. See the "Configuring User Roles Controller Templates" section on page 11-11 for more information about User Role templates.

Configuring a Global Access Point Password

The AP Username Password page enables you to set a global password that all access points inherit as they join a controller. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis. See the "Configuring AP Configuration Templates" section on page 11-127 to view where the global password is displayed and how it can be overridden on a per-access point basis.

Also in controller software release 5.0, after an access point joins the controller, the access point enables console port security and you are prompted for your username and password whenever you log into the access point console port. When you log in, you are in non-privileged mode and you must enter the enable password in order to use the privileged mode.

To establish a global username and password, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address of a controller with a version of 5.0 or later.

Step 3 From the left sidebar menu, choose **System > AP Username Password**.

Step 4 Enter the username and password that you want to be inherited by all access points that join the controller.

Note For Cisco IOS access points, you must also enter and confirm an enable password.

Step 5 Click **Save**.

Configuring Global CDP

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

Note CDP is enabled on the bridge's Ethernet and radio ports by default.

Note Global Interface CDP Configuration will be applied to only the APs with CDP enabled at AP level.

To configure a Global CDP, perform the following steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the IP address of the desired controller.

Step 3 From the left sidebar menu, choose **System > Global CDP Configuration** from the left sidebar menu. The Global CDP Configuration page appears.

Step 4 In the Global CDP portion of the page, specify the following parameters:

- CDP on controller—Choose enable or disable CDP on the controller.

Note This configuration cannot be applied on WISM2 controllers.

- Global CDP on APs—Choose to enable or disable CDP on the access points.
- Refresh-time Interval (seconds)—At the Refresh Time Interval parameter, enter the time in seconds at which CDP messages are generated. The default is 60.
- Holdtime (seconds)—Enter the time in seconds before the CDP neighbor entry expires. The default is 180.
- CDP Advertisement Version—Enter which version of the CDP protocol to use. The default is v1.

Step 5 In the CDP for Ethernet Interfaces portion of the page, select the slots of Ethernet interfaces for which you want to enable CDP.

Note CDP for Ethernet Interfaces fields are supported for controller version 7.0.110.2 onwards.

Step 6 In the CDP for Radio Interfaces portion of the page, select the slots of Radio interfaces for which you want to enable CDP.

Note CDP for Radio Interfaces fields are supported for controller version 7.0.110.2 onwards.

Step 7 Click **Save**.

Configuring AP 802.1X Supplicant Credentials

You can configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning. You can set global authentication settings that all access points inherit as they join the controller. This includes all access points that are currently joined to the controller and any that join in the future.

If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point. See the "Configuring Access Point Details" section on page 9-164 for more information.

To enable global supplicant credentials, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the IP address of the desired controller.

Step 3 From the left sidebar menu, choose **System > AP 802.1X Supplicant Credentials**.

Step 4 Select the **Global Supplicant Credentials** check box.

Step 5 Enter the supplicant username.

Step 6 Enter and confirm the applicable password.

Step 7 Click **Save**.

Note Once saved, you can click **Audit** to perform an audit on this controller. See the "Understanding the Controller Audit Report" section on page 9-3 or the "Configuring an Audit" section on page 15-78 for more information.

Configuring Controller DHCP

To configure DHCP (Dynamic Host Configuration Protocol) information for a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the IP address of the desired controller.

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

Step 4 Add or modify the following parameters:

- DHCP Option 82 Remote Id Field Format—Select AP-MAC or AP-MAC-SSID from the drop-down list.

  Note To set format for RemoteID field in DHCP option 82: If 'Ap-Mac' is selected, then set the RemoteID format as <AP-Mac>. If 'Ap-Mac-ssid' is selected, then set the RemoteID format as <AP-Mac>:<SSID>.

- DHCP Proxy—Select the check box to enable DHCP by proxy.

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

Step 5 Enter the DHCP Timeout in seconds after which the DHCP request will time out. The default setting is 5. Allowed values range from 5 to 120 seconds.

Note DHCP Timeout is applicable from the controller version 7.0.114.74 onwards.

Step 6 Click **Save**.

Note Once saved, you can click **Audit** to perform an audit on this controller. See the "Understanding the Controller Audit Report" section on page 9-3 or the "Configuring an Audit" section on page 15-78 for more information.

Configuring Controller Multicast Mode

NCS provides an option to configure IGMP (Internet Group Management Protocol) snooping and timeout values on the controller.

To configure multicast mode and IGMP snooping for a controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the desired controller.

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

Step 4 Choose **Disable**, **Unicast**, or **Multicast** from the Ethernet Multicast Support drop-down list.

Note IGMP Snooping and timeout can be set only if Ethernet Multicast mode is Enabled.

Step 5 If Multicast is selected, enter the multicast group IP address.

Step 6 Select the Enable Global Multicast Mode check box to make the multicast mode available globally.

Step 7 Select to enable IGMP Snooping.

Step 8 Choose **Enable** from the Multicast Mobility Mode drop-down list to change the IGMP snooping status or to set the IGMP timeout. When IGMP snooping is enabled, the controller gathers IGMP reports from the clients and then sends each access point a list of the clients listening to any multicast group. The access point then forwards the multicast packets only to those clients.

The timeout interval has a range of 3 to 300 and a default value of 60. When the timeout expires, the controller sends a query to all WLANs. Those clients which are listening in the multicast group then send a packet back to the controller.

Step 9 If you enabled the Multicast Mobility Mode, enter the mobility group multicast address.

Step 10 Select the Multicast Direct feature check box to enable videos to be streamed over a wireless network.

Step 11 Specify the Session Banner information, which is the error information sent to the client if the client is denied or dropped from a Media Stream.

a. State—Select the check box to activate the Session Banner. If not activated, the Session Banner is not sent to the client.

b. URL—A web address reported to the client

c. Email—An email address reported to the client

d. Phone—A telephone number reported to the client

e. Note—A note reported to the client

Note All Media Streams on a Controller share this configuration.

Step 12 Click **Save**.

Note Once saved, you can click **Audit** to perform an audit on this controller. See the "Understanding the Controller Audit Report" section on page 9-3 or the "Configuring an Audit" section on page 15-78 for more information.

Configuring Access Point Timer Settings

Advanced timer configuration for HREAP and local mode is available for the controller on NCS.

Note This feature is only supported on Release 6.0 controllers and later.

Configuring Advanced Timers

To configure the advanced timers, follow these steps:

Step 1 Choose **Configure > Controllers**.

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

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

Step 4 Select the applicable access point mode (Local mode or HREAP mode).

Step 5 See the "Access Point Timer Settings for Local Mode" section on page 9-63 or the "Access Point Timer Settings for HREAP Mode" section on page 9-63 for more information on each mode configuration.

Access Point Timer Settings for Local Mode

To reduce the failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller. You can then enter a value between 10 and 15 seconds.

Access Point Timer Settings for HREAP Mode

Once selected, you can configure the HREAP timeout value. Select the **AP Primary Discovery Timeout** check box to enable the timeout value. Enter a value between 30 and 3600 seconds.

Note 5500 series controllers accept access point fast heartbeat timer values in the range of 10-15. All other controller models support a range of 1-10.

Configuring Controller WLANs

Since controllers can support 512 WLAN configurations, NCS provides an effective way to enable or disable multiple WLANs at a specified time for a given controller.

To view a summary of the wireless local access networks (WLANs) that you have configured on your network, 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 **WLANs > WLAN Configuration**. The Configure WLAN Summary page appears (see Figure 9-7). This WLAN Configuration page contains the values found in Table 9-1.

Figure 9-7 WLAN Configuration Summary Page

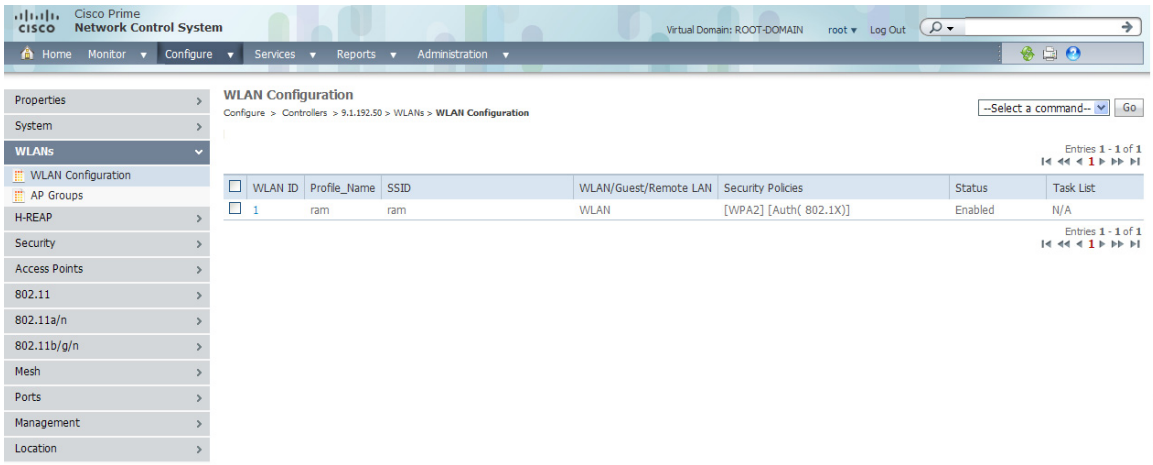


Table 9-1 WLAN Configuration Summary Page

Parameter	Description
Check box	Select the WLAN for deletion. Click **Delete WLANs** from the Select a command drop-down list.
WLAN ID	Identification number of the WLAN.
Profile Name	User-defined profile name specified when creating the WLAN template. Profile Name is the WLAN name.
SSID	Service Set Identifier being broadcast by.
WLAN/Guest LAN	Specifies if it is a WLAN or guest LAN.
Security Policies	Security policies enabled on the WLAN.

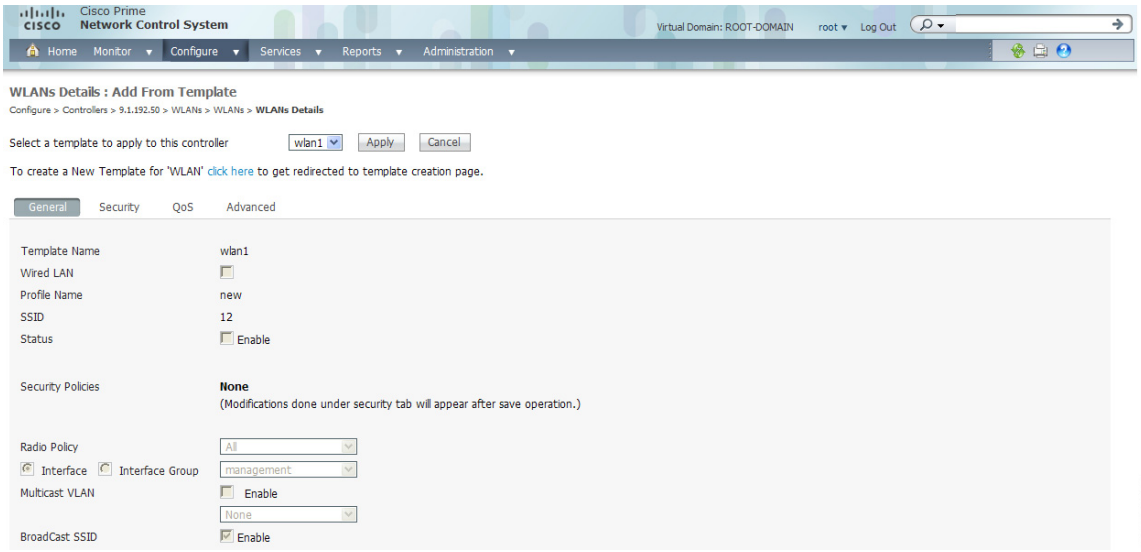
Table 9-1 WLAN Configuration Summary Page (continued)

Parameter	Description
Status	Status of the WLAN is either enabled or disabled.
Task List	If a task is scheduled in Configure > Scheduled Configuration Tasks, you have a link to view the scheduled configuration task.

Viewing WLAN Details

To view WLAN details, choose **WLANs**. The WLAN Details page appears (see Figure 9-8).

Figure 9-8 WLAN Details Page



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

- General Tab, page 9-65
- Security Tab, page 9-66
- QoS Tab, page 9-70
- Advanced Tab, page 9-70

General Tab

The General tab includes the following information:

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

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

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

- Schedule Status
- Security Policies—Identifies the security policies set using the Security tab (includes security policies such as None, 802.1X, Static WEP, Static WEP-802.1X, WPA+WPA2, and CKIP). Changes to the security policies appear in this section after the page is saved.
- Radio Policy—Choose from the drop-down list.
  - All, 802.11a only, 802.11g only, 802.11b/g only, 802.11a/g only.
- Interface/Interface Group—Select from the drop-down list.
- Broadcast SSID—Select the check box to enable.
- Egress Interface—Select the name of the applicable interface. This WLAN provides a path out of the controller for wired guest client traffic.

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

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

Security Tab

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

Layer 2 Security

Use the Layer 2 Security drop-down list to choose between None, 802.1x, Static WEP, Cranite, Static WEP-802.1x, WPA1+WPA2, and CKIP. These parameters are described in the Table 9-2.

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

Table 9-2 Layer 2 Security Options

Parameter	Description
None	No Layer 2 security selected.
802.1x	802.11 Data Encryption: • Type—WEP • Key Size—40, 104, or 128 bits.

Table 9-2 Layer 2 Security Options (continued)

Parameter	Description
Static WEP	802.11 Data Encryption: • Type • Key Size—not set, 40, 104, or 128 bits. • Key Index—1 to 4. • Encryption Key • Encryption Key Format—ASCII or HEX. • Allowed Shared Key Authentication—Select the check box to enable.
Cranite	Configure the WLAN to use the FIPS140-2 compliant Cranite Wireless Wall Software Suite, which uses AES encryption and VPN tunnels to encrypt and verify all data frames carried by the Cisco Wireless LAN Solution.
Static WEP-802.1X	Use this setting to enable both Static WEP and 802.1X policies. If this option is selected, static WEP and 802.1X parameters are displayed at the bottom of the page. Static WEP encryption parameters: • 802.11 Data Encryption – Type – Key Size—not set, 40, 104, or 128 bits. – Key Index—1 to 4. – Encryption Key – Encryption Key Format—ASCII or HEX. • Allowed Shared Key Authentication—Select the check box to enable.
	802.1X parameters: • 802.11 Data Encryption – Type – Key Size—40, 104, or 128 bits.

Table 9-2 Layer 2 Security Options (continued)

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

Layer 3 Security

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

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

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

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

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

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

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

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

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

- Default Internal—The guest user receives the default login page.
- Customized WebAuth—Customized login pages can be downloaded from the Upload/Download Commands page. See the "Downloading a Customized Web Authentication Page" section on page 11-66 for more information.
  - Select **Web Auth Login Page**, **Web Auth Login Failure Page**, or **Web Auth Logout Page** from the drop-down lists.
  - Select **None** from any of the drop-down lists if you do not want to display a customized page for that option.
- External—The guest user is redirected to an external login page. Enter the login page URL in the External Web Auth URL text box.

Note If External is selected, you can select up to three RADIUS and LDAP servers from the Security > AAA page. See the "AAA Servers" section on page 9-70 for more information.

AAA Servers

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

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

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

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

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

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

QoS Tab

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

Advanced Tab

- H-REAP Local Switching—Select the check box to enable Hybrid REAP local switching. When enabled, the H-REAP access point handles client authentication and switches client packets locally. See the "Configuring Hybrid REAP" section on page 12-4 for more information.

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

- Enable H-REAP local authentication by selecting the **H-REAP Local Auth** check box.

  Local authentication is useful where you cannot maintain the criteria a remote office setup of minimum bandwidth of 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local switching, the authentication capabilities are present in the access point itself. Thus local authentication reduces the latency requirements of the branch office.

  Note Local authentication can only be enabled on the WLAN of a HREAP AP that is in local switching mode.

  Local authentication is not supported in the following scenarios:

  - Guest Authentication cannot be performed on a HREAP local authentication enabled WLAN.
  - RRM information is not available at the controller for the hybrid REAP local authentication enabled WLAN.
  - Local radius is not supported.
  - Once the client has been authenticated, roaming will only be supported after the WLC and the other hybrid REAPs in the group are updated with the client information.
- Session Timeout (secs)—Set the maximum time a client session can continue before re-authentication.
- Aironet IE—Select the check box to enable support for Aironet information elements (IEs) for this WLAN.
  - If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the association request.
- IPv6—Select the check box to enable IPv6.

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

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

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

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

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

For more information, see the "Configuring an Access Control List Template" section on page 11-69.

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

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

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

  When media session snooping is enabled, the access point radios advertise this WLAN snoop for Session Initiation Protocol (SIP) voice packets. Any packets destined to or originating from port number 5060 are considered for further inspection. The access point tracks whether Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, already on an active call, or in the process of ending a call and then notify the controller of any major call events.
- NAC State—From the **NAC State** drop-down list, choose **SNMP NAC** or **Radius NAC**. SIP errors that are discovered generate traps that appear on the client troubleshooting and alarms screens. The controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing. See the "NAC Integration" section on page 9-43 for more information.
- Passive Client—If the check box is selected, it enables passive clients on your WLAN.

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

  Wireless LAN controllers currently act as a proxy for ARP requests. On receiving an ARP request, the controller responds with an ARP response instead of passing the request directly to the client. This has two advantages:
  - The upstream device that sends out the ARP request to the client cannot know where the client is located.
  - Reserves power for battery-operated devices like mobile phones and printers as they do not need to respond to every ARP request.

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

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

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

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

    Note For some WLAN configurations, this setting is required.

  - DHCP Addr. Assignment—If you select the Required check box, clients connected to this WLAN will get an IP address from the default DHCP server.
- Management Frame Protection (MFP)
  - MFP Signature Generation—If the check box is selected, it enables signature generation for the 802.11 management frames transmitted by an access point associated with this WLAN. With signature generation, changes to the transmitted management frames by an intruder are detected and reported.
  - MFP Client Protection—From the drop-down list, choose **Optional**, **Disabled**, or **Required** for individual WLAN configurations.
  - MFP Version—Displays the Management Frame Protection version.

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

- Foreign Controller Mapping—Click this link to configure foreign controller mappings. This will take you to the Foreign Controller configuration page. In this configuration page, choose a foreign controller from the Foreign Controller drop-down list and choose an interface or interface group from the Interface/Interface Group drop-down list. After choosing the required options, click **Add** to complete the adding of a foreign controller.

Adding a WLAN

To add a WLAN, follow these steps:

Step 1 Choose **Configure > Controllers**.

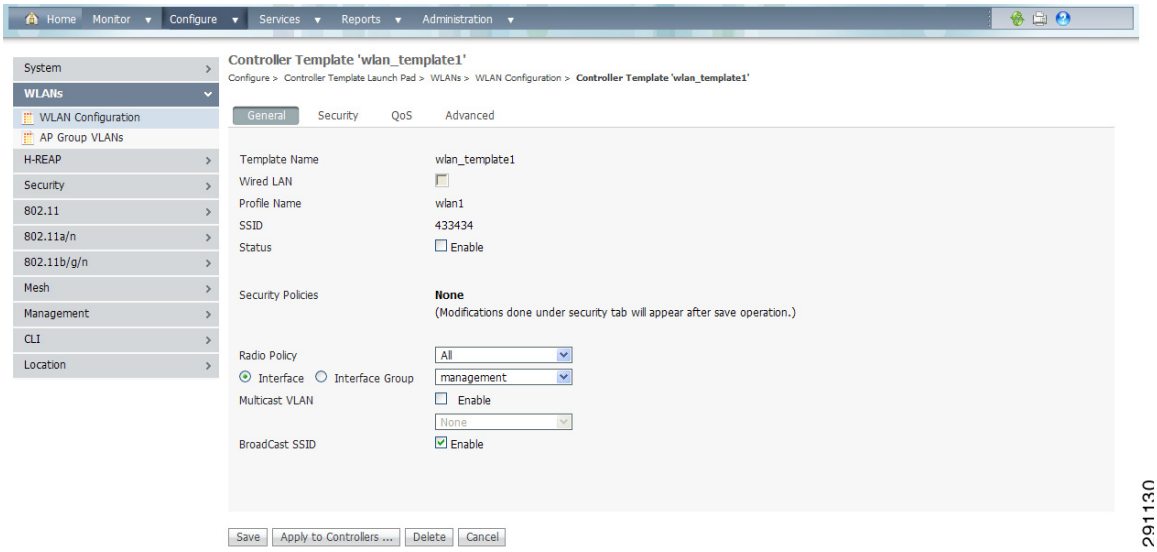
Step 2 Click the IP address of the appropriate controller.

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

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

Step 5 Click **Go** to open the WLAN Details: Add from Template page (see Figure 9-9).

Figure 9-9 WLAN Details: Add From Template Page



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

Step 7 Click **Apply**.

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

Deleting a WLAN

To delete a WLAN, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller.

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

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

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

Step 6 Click **Go**.

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

Managing WLAN Status Schedules

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

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

Step 1 Choose **Configure > Controllers**.

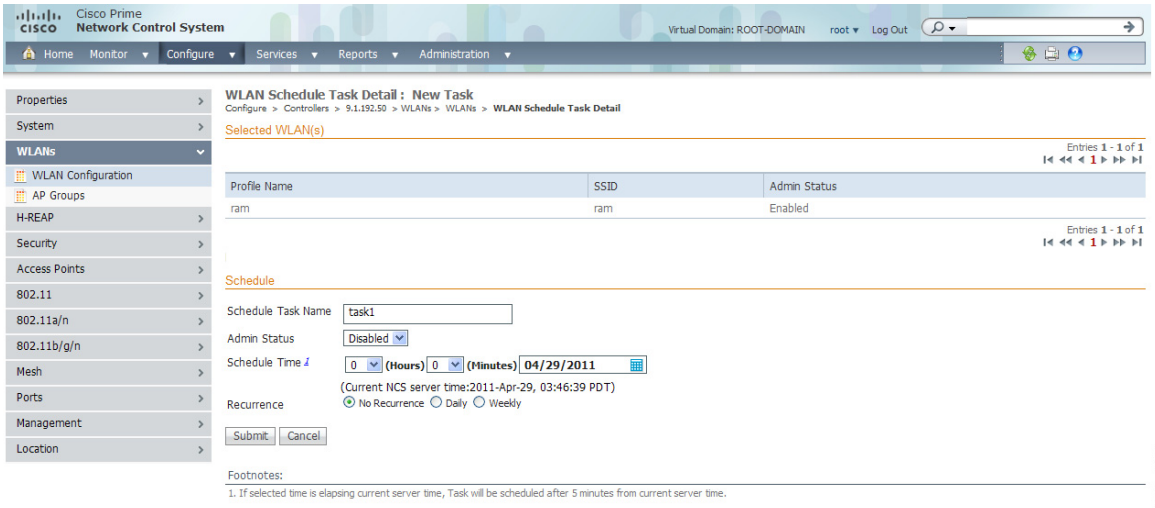
Step 2 Click the IP address of the appropriate controller.

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

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

Step 5 From the Select a command drop-down list, choose **Schedule Status** to open the WLAN Schedule Task Detail page (see Figure 9-10).

Figure 9-10 WLAN Schedule Task Detail Page



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

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

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

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

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

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

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

Note For more information on the WLAN Configuration Scheduled Task results, see the "Viewing WLAN Configuration Scheduled Task Results" section on page 9-215.

Mobility Anchors

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

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

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

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

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

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

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

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller.

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

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

Step 5 Click the **Advanced** tab.

Step 6 Click the **Mobility Anchors** link. Table 9-3 describes the parameters that are displayed.

Table 9-3 Mobility Anchors

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

Configuring WLANs AP Groups

Site-specific VLANs or AP groups limit the broadcast domains to a minimum by segmenting a WLAN into different broadcast domains. Benefits of this include more effective management of load balancing and bandwidth allocation.

To open this page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **WLAN > AP Groups**.

This page displays a summary of the AP groups configured on your network. From here you can add, remove, or view details of an AP group. Click the AP group name on the Access Points tab to view or edit its access point(s). Click the **WLAN Profiles** tab to view, edit, add, or delete WLAN profiles.

Adding Access Point Groups

To add a new access point group, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **WLAN > AP Groups**.

Note AP Groups (for 5.2 and later controllers) is referred to as AP Group VLANs for controllers prior to 5.2.

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

Step 5 Click **Go**.

In the AP Groups details page, you can add access points and WLAN profiles to this access point group.

Step 6 Enter a name and group description for the access point group.

Note The group description is optional.

Step 7 To add access points to the group, follow these steps:

a. Click the **Access Points** tab.

b. Click **Add**. The access point page displays parameters for available access points. Click the access point name to view or edit parameters for one of the available access points.

c. Select the check box(es) of the access point(s) you want to add.

d. Click **Select**.

Step 8 To add a WLAN profile to this group, follow these steps:

a. Click the **WLAN Profiles** tab.

Note Each access point is limited to sixteen WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.

Note The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).

Note OfficeExtend access points are limited to fifteen WLAN profiles because one is reserved as the personal or local SSID for the OfficeExtend access point.

Step 9 Enter a WLAN profile name or choose one from the WLAN Profile Name drop-down list.

Step 10 Choose the interface or interface group from the Interface/Interface Group drop-down list.

Note For more information about configuring interfaces, see the ""Configuring Controller System Interfaces" section on page 9-38."

Step 11 Select the **NAC Override** check box, if applicable. NAC override is disabled by default.

Step 12 When access points and WLAN profiles are added, click **Save**.

Note After saving, use the edit icon from the WLAN Profiles tab to edit WLAN profile information.

Note Changing the WLAN-interface mapping in an AP Group will remove the local VLAN mapping for HREAP APs in this group. These mappings will need to be reconfigured after applying this change.

Deleting Access Point Groups

To delete an access point group, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **WLAN > AP Groups**.

Step 4 Select the check box(es) of the access point group(s) that you want to delete.

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

Step 6 Click **OK** to confirm the deletion.

Auditing Access Point Groups

You can audit the access point group to determine if the NCS and device values differ.

To audit an access point group, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **WLAN > AP Groups**.

Step 4 Click the name of the access point group that you want to audit.

Note Click **Audit** located at the bottom of the page.

Configuring Hybrid REAP Parameters

Hybrid REAP enables customers to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. There is no deployment restriction on the number of hybrid-REAP access points per location. The hybrid-REAP access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller.

- Configuring H-REAP AP Groups, page 9-79
- Auditing an H-REAP Group, page 9-81

Configuring H-REAP AP Groups

To view a list of existing H-REAP AP groups, 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 **H-REAP > H-REAP AP Groups**. The H-REAP AP Groups page opens.

- Group Name—The name of the H-REAP AP group. Click the group name to view its details.

Note Use the check box to select a group for deletion.

Configuring a H-REAP AP Group

To configure a hybrid-REAP access point group, 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 **H-REAP > H-REAP AP Groups**.

Step 4 From the Select a command drop-down list, click **Add H-REAP AP Group** to open the H-REAP AP Group > Add From Template pane.

Step 5 Select a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

Note To make modifications to an existing H-REAP AP Group, click the existing group in the Group Name column of the H-REAP AP Group page.
To delete an existing group, select the check box of the group you want to remove, and choose **Delete H-REAP AP Group** from the Select a command drop-down list.

Step 7 Configure the following H-REAP AP Group parameters:

- General tab
  - Template Name—The name of the template applied to this controller.
  - Primary Radius—From the drop-down list, choose the primary radius authentication server present on the controller.

    Note If a RADIUS authentication server is not present on the controller, the NCS configured RADIUS server does not apply.

    Note You must configure the RADIUS server configuration on the controller before you apply H-REAP RADIUS server configuration from NCS.

  - Secondary Radius—From the drop-down list, choose the secondary radius authentication server present on the controller.

    Note If a RADIUS authentication server is not present on the controller, the NCS configured RADIUS server does not apply.

- H-REAP AP tab
  - Ethernet MAC—Check this check box H-REAP AP to apply to the H-REAP group.

    Note An AP Ethernet MAC address cannot exist in more than one H-REAP group on the same controller. The controller will not allow you to set an AP Ethernet MAC in a hybrid-REAP group if it is already present in another H-REAP group.

- Add AP—Click to add an additional H-REAP AP (present in the NCS) to an existing H-REAP group.

Step 8 If you want to enable local authentication for a hybrid-REAP group, click the **H-REAP Configuration** tab.

Note Make sure that the Primary RADIUS Server and Secondary RADIUS Server parameters are set to **None** on the General tab.

Step 9 Select the **H-REAP Local Authentication Enable** check box to enable local authentication for this hybrid-REAP group. The default value is unseelcted.

Step 10 To allow a hybrid-REAP access point to authenticate clients using LEAP, select the **LEAP** check box. Otherwise, to allow a hybrid-REAP access point to authenticate clients using EAP-FAST, select the **EAP-FAST** check box.

Step 11 Perform one of the following, depending on how you want protected access credentials (PACs) to be provisioned:

- To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the EAP=FAST Key text box. The key must be 32 hexadecimal characters.
- To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the **Ignore Server Key** check box.

Step 12 In the EAP-FAST Authority ID text box, enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.

Step 13 In the EAP-FAST Authority Info text box, enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.

Step 14 In the EAP-FAST PAC Timeout text box, specify a PAC timeout value by entering the number of seconds for the PAC to remain visible in the edit text box. The valid range is 2 to 4095 seconds.

Note To see if an individual access point belongs to a hybrid-REAP group, click the **Users configured in the group** link. It advances you to the H-REAP AP Group page which shows the names of the groups and the access points that belong in it.

Auditing an H-REAP Group

If the H-REAP configuration changes over a period of time either on NCS or the controller, you can audit the configuration. The changes are visible in subsequent pages. You can specify to refresh NCS or the controller to synchronize the configuration.

Configuring Security Parameters

- Configuring Controller File Encryption, page 9-82
- Configure Controllers > IPaddr > Security > AAA, page 9-82
- Configure Controllers > IPaddr > Security > Local EAP, page 9-93
- Configuring User Login Policies, page 9-97

Configuring Controller File Encryption

To configure a controller file encryption, 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 **Security > File Encryption**. File encryption ensures that data is encrypted when you upload or download the controller configuration file from a TFTP server.

File Encryption parameters include:

- File Encryption—If this option is enabled, the data in the controller configuration file is encrypted when it is uploaded or downloaded through the TFTP server.
- Encryption Key—A text string of exactly 16 characters.
- Confirm Encryption Key—Enter the encryption key.

Configure Controllers > *IPaddr* > Security > AAA

This section describes how to configure controller security AAA parameters and contains the following topics:

Configuring AAA General Parameters

The General page allows you to configure the local database entries on a controller.

To configure the local database entries, 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 **Security > AAA > General**.

Step 4 Enter the maximum number of allowed database entries. This amount becomes effective on the next reboot. The valid range is 512 - 2048.

Configuring AAA RADIUS Auth Servers

To view a summary of existing RADIUS authentication servers, 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 **Security > AAA > RADIUS Auth Servers**. The following RADIUS Auth Servers parameters appear:

- Server Index—Access priority number for the RADIUS server (display only). Click to go to Configure IPaddr > RADIUS Authentication Server.
- Server Address—IP address of the RADIUS server (read-only).
- Port Number—Controller port number (read-only).
- Admin Status—Enable or Disable.
- Network User—Enable or Disable.
- Management User—Enable or Disable.

Adding an Authentication Server

To add an authentication server, 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 **Security > AAA > RADIUS Auth Servers**.

Step 4 From the Select a command drop-down list, choose **Add Auth Server** to open the Radius Authentication Server > Add From Template page.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

Note To create a new template for Radius authentication servers, choose **Configure > Controller Templates > Security > RADIUS Auth Servers**.

Configuring AAA RADIUS Acct Servers

To view a summary of existing RADIUS accounting servers, 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 **Security > AAA > RADIUS Acct Servers**. RADIUS Acct Server parameters include the following:

- Server Index—Access priority number for the RADIUS server (read-only). Click to open the Radius Acct Servers Details page.

  Note To edit or audit the current accounting server parameters, click the Server Index for the applicable accounting server.

- Server Address—IP address of the RADIUS server (read-only).
- Port Number—Controller port number (read-only).
- Admin Status—Enable or Disable.
- Network User—Enable or Disable.

Command Buttons

- Save
- Audit

Adding an Accounting Server

To add an accounting server, 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 **Security > AAA > RADIUS Acct Servers**.

Step 4 From the Select a command drop-down list, choose **Add Acct Server** to open the Radius Acct Servers Details > Add From Template page.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 From the drop-down list, choose a controller to apply to this template.

Step 7 Click **Apply**.

Note To create a new template for Radius accounting servers, choose **Configure > Controller Templates Launch Pad > Security > RADIUS Acct Servers**.

Deleting an Accounting Server

To delete an accounting server, 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 **Security > AAA > RADIUS Acct Servers**.

Step 4 Select the check box(es) for the applicable accounting server(s).

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

Step 6 Click **Go**.

Step 7 Click **OK** in the pop-up dialog box to confirm the deletion.

Configuring AAA RADIUS Fallback Parameters

To configure RADIUS fallback parameters, 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 **Security > AAA > RADIUS Fallback**.

Step 4 Add or modify the following parameters:

- RADIUS FallbackMode
- Username
- Time Interval

Step 5 Click **Save**.

Note Click **Audit** to check the present configuration status of NCS and the controller.

Configuring AAA LDAP Servers

This page enables you to add and delete LDAP servers to this controller.

To access the LDAP Servers page, 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 **Security > AAA > LDAP Servers**.

This page displays LDAP servers currently used by this controller and contains the following parameters:

- Check box—Select the check box to choose an LDAP server for deletion.
- Server Index—A number assigned to identify the LDAP server.

Note Click the index number to go the LDAP server configuration page.

- Server Address—The LDAP server IP address.
- Port Number—The port number used to communicate with the LDAP server.
- Admin Status—Server template status.

  Indicates if use of the LDAP server template is enabled o disabled.

Note If the title of a column is a link, click it to toggle between ascending and descending order.

Note NCS now supports LDAP configuration for both an anonymous or authenticated bind. For more information, see the "Configuring New LDAP Bind Requests" section on page 9-87.

LDAP Servers Select a command Drop-Down List Options

Adding LDAP Server

To add a LDAP Server, 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 **Security > AAA > LDAP Servers**.

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

Step 5 Click **Go**.

Deleting LDAP Servers

To delete the LDAP Server, 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 **Security > AAA > LDAP Servers**.

Step 4 Select the check box(es) of the LDAP servers that you want to delete.

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

Step 6 Click **Go**.

Configuring New LDAP Bind Requests

NCS now supports LDAP configuration for both an anonymous or authenticated bind. A bind is a socket opening that performs a lookup.

To configure LDAP bind requests, follow these steps:

Step 1 Choose **Configure > Controller**.

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

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

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

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

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

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

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

Step 9 Click **Save**.

Configuring AAA TACACS+ Servers

This page enables you to add and delete TACACS+ servers to this controller.

To access the TACACS+ Servers page, 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 **Security > AAA > TACACS+ Servers**.

This page displays TACACS+ servers currently used by this controller and contains the following parameters:

- Check box—Select the check box to choose a TACACS+ server for deletion.
- Server Type—The TACACS+ server type.
- Displays Accounting, Authorization, or Authentication.
- Server Index—A number assigned to identify the TACACS+ server and set its use priority.
- Click the index number to go the TACACS+ server configuration page.
- Server Address—The TACACS+ server IP address.
- Port Number—The port number used to communicate with the TACACS+ server.
- Admin Status—Server template status.

  Indicates if use of the TACACS+ server template is enabled.

If the title of a column is a link, click it to toggle between ascending and descending order.

The Select a command drop-down list has the following options:

- Add TACACS+ Server—Choose this option, then click **Go** to add a TACACS+ server to the controller.
- Delete TACACS+ Servers—Choose this option, then click **Go** to delete all TACACS+ servers with a selected check box from the controller.

Configuring AAA Local Net Users

This page provides a summary of the existing local network user controllers for clients who are allowed to access a specific WLAN. This is an administrative bypass of the RADIUS authentication process. Layer 3 Web Authentication must be enabled. The client information is passed to the RADIUS authentication server first, and if the client information does not match a RADIUS database entry, this local database is polled. Clients located in this database are granted access to network services if the RADIUS authentication fails or does not exist.

- Adding a Local Net User, page 9-88
- Deleting a Local Net User, page 9-89

To view existing local network users, 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 **Security > AAA > Local Net Users**. The Local Net Users page displays the following local net user parameters:

- Username—User-defined identification.
- WLAN ID—Any WLAN ID, 1 through 16; 0 for all WLANs; 17 for third-party WLAN that this local net user is allowed to access.
- Description—Optional user-defined description.

Adding a Local Net User

To add a local net user, 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 **Security > AAA > Local Net Users**.

Step 4 From the Select a command drop-down list, choose **Add Local Net User** to open the **Local Net User > Add From Template** page.

Step 5 Select a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

Note To create a new template for local net users, choose **Configure > Controller Templates > Security > Local Net Users**. See the "Configuring a Local Network Users Template" section on page 11-55 for more information.

Deleting a Local Net User

To delete a local net user, 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 **Security > AAA > Local Net Users**.

Step 4 Select the check box(es) for the applicable local net user(s).

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

Step 6 Click **Go**.

Step 7 Click **OK** in the dialog box to confirm the deletion.

Configuring AAA MAC Filtering

This page enables you to view MAC Filter parameter information.

Note You cannot use MAC address in the broadcast range.

To access the MAC Filtering page, 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 **Security > AAA > MAC Filtering**. The MAC Filtering page displays the following parameters:

- MAC Filter Parameters

  - RADIUS Compatibility Mode—User-defined RADIUS server compatibility: Cisco ACS, FreeRADIUS, or Other.
  - MAC Delimiter—The MAC delimiters can be Colon (xx:xx:xx:xx:xx:xx), Hyphen (xx-xx-xx-xx-xx-xx), Single Hyphen (xxxxxx-xxxxxx), or No Delimiter (xxxxxxxxxxxx), as required by the RADIUS server.
- MAC Filters
  - MAC Address—Client MAC address. Click to open Configure *IPaddr* > MAC Filter.
  - WLAN ID—1 through 16, 17 = Third-party AP WLAN, or 0 = all WLANs.
  - Interface—Displays the associated Interface Name.
  - Description—Displays an optional user-defined description.

Step 4 From the Select a command drop-down list, choose **Add MAC Filters** to add a MAC Filter, **Delete MAC Filters** to delete the template(s), or **Edit MAC Filter** Parameters to edit the MAC Filters.

Step 5 Click **Go**.

Configuring AAA AP/MSE Authorization

The AP/MSE Authorization page displays the access point policies and the list of authorized access points along with the type of certificate that an access point uses for authorization.

Note You cannot use MAC address in the broadcast range.

To access the AP/MSE Authorization page, 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 **Security > AAA > AP/MSE Authorization**. The AP/MSE Authorization page displays the following parameters:

- AP Policies
  - Authorize APs—Enabled or Disabled.
  - Accept SSC-APs—Enabled or Disabled.
- AP/MSE Authorization
  - AP/MSE Base Radio MAC Address—The MAC address of the authorized access point.

    Note Click the AP/MSE Base Radio MAC Address to view AP/MSE Authorization details.

  - Type
  - Certificate Type—MIC or SSC.
  - Key Hash—The 40-hex long SHA1 key hash.

Note The key hash is displayed only if the certificate type is SSC.

Command Buttons

- Add AP/MSE Auth Entry—Select this command, and click **Go**. See the "Configuring an Access Point or MSE Authorization Template" section on page 11-59.
- Delete AP/MSE Auth Entries—Select one or more access points, select this command, and click **Go** to delete the selected access point from the AP authorization list.
- Edit AP Policies—Select this command, and click **Go**. See the "Editing AP Policies" section on page 9-91.

Editing AP Policies

To edit AP/MSE Authorization access point policies, 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 **Security > AAA > AP/MSE Authorization**.

Step 4 In Edit AP Policies page, edit the following parameters, if necessary:

- Authorize APs—Select the check box to enable access point authorization.
- Accept SSC-APs—Select the check box to enable the acceptance of SSE access points.

Step 5 Click **Save** to confirm the changes, **Audit** to perform an audit on these device values, or **Cancel** to close this page with no changes.

Configuring AAA Web Auth Configuration

The Web Auth Configuration page enables the user to configure the Web auth configuration type. If the type is configured as customized, the user downloaded web auth replaces the controller-provided internal web auth page.

To access the Web Auth Configuration page, 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 **Security > AAA > Web Auth Configuration**.

Step 4 In the Web Authentication page, choose the Web Auth Type from the drop-down list. Web auth options include a default internal web page, a customized web authentication page, or an external web page.

Step 5 Configure the web auth parameters depending on the type chosen:

- Default Internal

  - Logo Display—Enable or disable logo display.
  - Web Auth Page Title—Title displayed on web authentication page.
  - Web Auth Page Message—Message displayed on web authentication page.
  - Custom Redirect URL—URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user would be directed to the company home page.

- Customized Web Auth

  You have the option of downloading an example login page and customizing the page. If you are using a customized web authentication page, it is necessary to download the example login.tar bundle file from the server, edit the login.html file and save it as either a .tar or .zip file, then download the .tar or .zip file to the controller.

  Click the preview image to download this sample login page as a TAR. After editing the HTML you may click here to redirect to the Download Web Auth page. See the "Downloading a Customized WebAuthentication Bundle to a Controller" section on page 9-15 for more information.

- External
  - External Redirect URL—Location of the login.html on an external server on the network.

    If there are not any External Web Auth servers configured, you have the option of configuring one.

    No external Web Auth server(s) configured. Click here to configure External Web Auth Servers.

Note To configure an External Web server template, see the "Configuring an External Web Auth Server Template" section on page 11-67.

Command Buttons

- Save—Save the current settings to the controller.
- Audit—Check the present configuration status of NCS and the controller.

Configuring AAA Password Policy

This page enables you to determine your password policy.

To make modifications to an existing password policy, follow these steps:

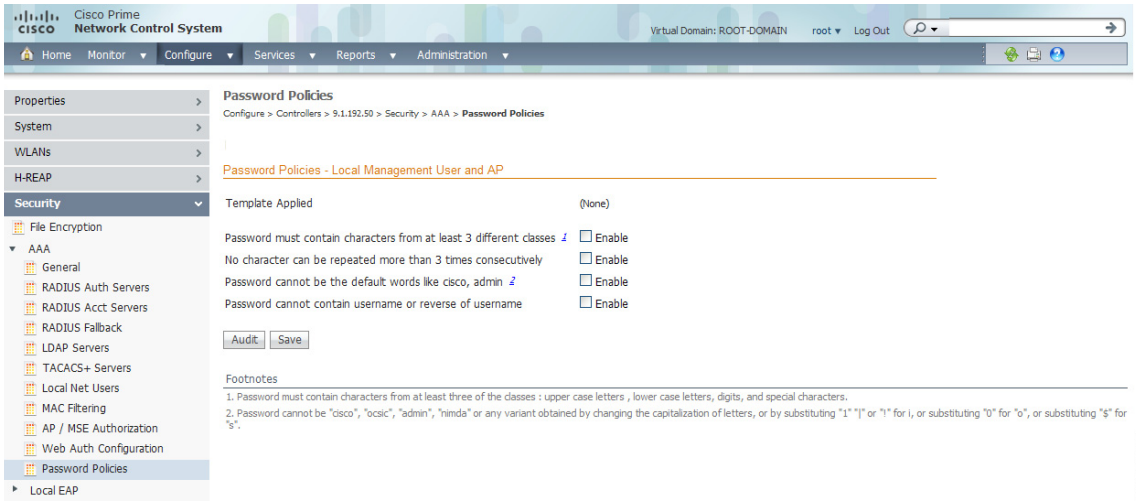
Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

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

Step 4 Modify the password policy parameters as appropriate (see Figure 9-11).

Figure 9-11 Password Policy



Step 5 Click **Save**.

Note If you disable password policy options, you will see a "'Disabling the strong password check(s) will be a security risk as it allows weak passwords" message.

Configure Controllers > *IPaddr* > Security > Local EAP

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.

When you enable local EAP, the controller serves as the authentication server and the local user database, making it independent of an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users.

Configuring Local EAP General Parameters

This page allows you to specify a timeout value for local EAP. You can then add a template with this timeout value or make changes to an existing template.

Note If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

To specify a timeout value for local EAP, 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 **Security > Local EAP > General - Local EAP**.

Step 4 Enter the Local Auth Active Timeout in the Local Auth Active Timeout text box (in seconds).

Note Local Auth Active Timeout refers to the timeout period during which Local EAP will always be used after all Radius servers are failed.

Step 5 The following values should be adjusted if you are using EAP-FAST, manual password entry, one-time password, or 7920/7921 phones.

Note You must increase the 802.1x timeout values on the controller (default=2 seconds) for the client to obtain the PAC using automatic provisioning. We recommend the default timeout on the Cisco ACS server of 20 seconds.

- Local EAP Identify Request Timeout =1 (in seconds)
- Local EAP Identity Request Maximum Retries=20 (in seconds)
- Local EAP Dynamic Wep Key Index=0
- Local EAP Request Timeout=20 (in seconds)
- Local EAP Request Maximum Retries=2
- EAPOL-Key Timeout=1000 (in milli-seconds)
- EAPOL-Key Max Retries=2
- Max-Login Ignore Identity Response

Note Roaming fails if these values are not set the same across multiple controllers.

Step 6 Click **Save**.

Command Buttons

- Save—Click to save the current template.
- Apply to Controllers—Click to apply the current template to controllers. In the Apply to Controllers page, choose the applicable controllers, and click **OK**.
- Delete—Click to delete the current template. If the template is currently applied to controllers, click **OK** to confirm that you want to remove the template from the selected controllers to which it is applied.
- Cancel—Click to cancel the current template creation or changes to the current template.

Configuring Local EAP Profiles

This page allows you to apply a template for a local EAP profile or make modifications to an existing template.

Note The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with PACs are not supported for use with the LDAP backend database.

- Viewing Existing Local EAP Profiles, page 9-95
- Adding a Local Net User, page 9-95

Viewing Existing Local EAP Profiles

To view existing local EAP profiles, 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 **Security > Local EAP > Local EAP Profiles**. The Local EAP Profiles page displays the following parameters:

- EAP Profile Name—User-defined identification.
- LEAP—Authentication type that leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. A username and password are used to perform mutual authentication with the RADIUS server through the access point.
- EAP-FAST—Authentication type (Flexible Authentication via Secure Tunneling) that uses a three-phased tunnel authentication process to provide advanced 802.1x EAP mutual authentication. A username, password, and PAC (protected access credential) are used to perform mutual authentication with the RADIUS server through the access point.
- TLS—Authentication type that uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It requires a client certificate for authentication.
- PEAP—Protected Extensible Authentication Protocol.

Adding a Local Net User

To add a local EAP profile, 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 **Security > Local EAP > Local EAP Profile**.

Step 4 From the **Select a command** drop-down list, choose **Add Local EAP Profile** to open the Local EAP Profile > Add From Template page.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click **Apply**.

Note To create a new template for local EAP profiles, choose **Configure > Controller Templates > Security > Local EAP Profiles**.

Configuring Local EAP General EAP-FAST Parameters

This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1x EAP mutual authentication. A username, password, and PAC are used to perform mutual authentication with the RADIUS server through the access point.

To set EAP-FAST Parameters, 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 **Security > Local EAP > EAP-FAST Parameters**.

Step 4 Enter the following parameters:

- Time to live for the PAC—The number of days for the PAC to remain viable. The valid range is 1 to 1000 days; the default setting is ten days.
- Authority ID—The authority identifier of the local EAP-FAST server in hexidecimal characters. You can enter up to 32 hexadecimal characters but it must be an even number of characters.
- Authority Info—The authority identifier of the local EAP-FAST server in text format.
- Server Key—The key (in hexadecimal characters) used to encrypt and decrypt PACs.
- Confirm Server Key—Verify the correct Server Key by re-typing it.
- Anonymous Provision—Select the check box to enable anonymous provisioning.

Note This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If this feature is disabled, PACs must be manually provisioned.

Step 5 Click **Save**.

Configuring Local EAP General Network Users Priority

To specify the order that LDAP and local databases use to retrieve user credential information, 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 **Security > Local EAP > Network Users Priority**.

Step 4 Use the left and right pointing arrows to include or exclude network credentials in the right-most list.

Step 5 Use the up and down buttons to determine the order credentials are attempted.

Step 6 Click **Save**.

Configuring User Login Policies

To configure the user login policies, 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 **Security > User Login Policies**.

Step 4 Enter the maximum number of concurrent logins allowed for a single username.

Step 5 Click **Save**.

Managing Manually Disabled Clients

The Disabled Clients page enables you to view excluded (blacklisted) client information.

Clients who fail to authenticate three times when attempting to associate are automatically blocked, or excluded, from further association attempts for an operator-defined timeout. After the Excluded timeout, the client is allowed to retry authentication until it associates or fails authentication and is excluded again.

Note You cannot use MAC address in the broadcast range.

To access the Manually Disabled Clients page, 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 **Security > Manually Disabled Clients**. The Manually Disabled Clients page displays the following parameters:

- MAC Address—Disabled Client MAC addresses. Click a list item to edit the disabled client description.
- Description—Optional description of disabled client.

Manually Disabled Clients Select a command Drop-Down List Options

- Add Manually Disabled Client—Select this command, and click **Go**. See the "Configuring a Manually Disabled Client Template" section on page 11-61.
- Delete Manually Disabled Clients—Select the applicable controller check box, select this command, and click **Go**.

Configuring Access Control Lists

The Access Control Lists page displays access control lists (ACLs) available for this controller. It also enables you to add a new rule or edit an existing rule in an applied access control list.

To access the Access Control Lists page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the applicable IP address under the IP Address column.

Step 3 From the left sidebar menu, choose **Security > Access Control Lists**.

- Check box—Use the check box to select one or more ACLs for deletion.
- ACL Name—User-defined name of this template. Click an ACL item to view its parameters. See the "Configure IPaddr > Access Control List > listname Rules" section on page 9-98.

Configure *IPaddr* > Access Control List > *listname* Rules

This page displays current access control list (ACL) rules applied to this access control list.

To access the Access Control Lists Rules page, follow these steps:

Step 1 Choose **Configure > Controllers**.

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

Step 3 From the left sidebar menu, choose **Security > Access Control Lists**.

Step 4 Click an ACL name.

- Check box—Select to delete access control list rules.
- Seq#—The operator can define up to 64 Rules for each ACL. The Rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if Rules 1 through 4 are already defined and you add Rule 29, it will be added as Rule 5.

Note If you add or change a Sequence number, operating system adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have Sequence numbers 1 through 7 defined and change number 7 to 5, operating system automatically reassigns Sequence 6 to 7 and Sequence 5 to 6.

- Action—Permit, Deny.
- Source IP/Mask—Source IP address and mask.
- Destination IP/Mask—Destination IP address and mask.
- Protocol—Protocol to use for this ACL:
  - Any—All protocols
  - TCP—Transmission Control Protocol
  - UDP—User Datagram Protocol
  - ICMP—Internet Control Message Protocol
  - ESP—IP Encapsulating Security Payload

  - AH—Authentication Header
  - GRE—Generic Routing Encapsulation
  - IP—Internet Protocol
  - Eth Over IP—Ethernet over Internet Protocol
  - Other Port OSPF—Open Shortest Path First
  - Other—Any other IANA protocol (http://www.iana.org/)

  If TCP or UDP is selected, Source Port and Dest Port parameters appear:

  - Source Port—Source Port. Can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
  - Dest Port—Destination port. If TCP or UDP is selected, can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.

- DSCP (Differentiated Services Code Point)—Any, or 0 through 255.
- Direction—Any, Inbound (from client) or Outbound (to client).

To add a new ACL rule, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Access Control Lists**.

Step 4 Click an ACL Name.

Step 5 Click an applicable **Seq#,** or choose **Add New Rule** to access this page.

Configuring CPU Access Control Lists

Access control lists (ACL) can be applied to the controller CPU to control traffic to the CPU.

The Access Control Lists Rules page displays the name of the CPU access control list template applied to the chosen controller.

To access the Access Control Lists Rules page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click a controller IP address.

Step 3 From the left sidebar menu, choose **Security > CPU Access Control Lists**.

Step 4 Select the **Enable CPU ACL** check box to enable the CPU ACL.

If this check box is selected, the following parameters are available:

- ACL Name—Choose the ACL to use from the ACL Name drop-down list.
- CPU ACL Mode—Choose which data traffic direction this CPU ACL list controls.

The choices include: The wired side of the data traffic, the wireless side of the data traffic, or both wired and wireless.

Configuring the IDS Sensor List

When the sensors identify an attack, they alert the controller to shun the offending client. When you add a new IDS (Intrusion Detection System) sensor, you register the controller with that IDS sensor so that the sensor can send shunned client reports to the controller. The controller also polls the sensor periodically.

To view IDS sensors, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > IDS Sensor Lists**.

The IDS Sensor page lists all IDS sensors that have been configured for this controller. Click an IP address to view details for a specific IDS sensor.

Configuring CA Certificates

A CA certificate is a digital certificate issued by one certificate authority (CA) for another certification CA.

- Importing a CA Certificate, page 9-100
- Pasting a CA Certificate Directly, page 9-100

Importing a CA Certificate

To import a CA certificate from a file, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > IP Sec Certificates > CA Certificate**.

Step 4 Click **Browse** to navigate to the applicable certificate file.

Step 5 Click **Open**.

Step 6 Click **Save**.

Pasting a CA Certificate Directly

To paste a CA certificate directly, follow these steps:

Step 1 Copy the CA certificate to your computer clipboard.

Step 2 Choose **Configure > Controllers**.

Step 3 Click an applicable IP address.

Step 4 From the left sidebar menu, choose **Security > IP Sec Certificates > CA Certificate**.

Step 5 Select the **Paste** check box.

Step 6 Paste the certificate directly into the text box.

Step 7 Click **Save**.

Configuring ID Certificates

This page lists the existing network ID certificates by certificate name. An ID certificate can be used by web server operators to ensure secure server operation. This section contains the following topics:

Importing a ID Certificate

To import an ID certificate from a file, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > IP Sec Certificates > ID Certificate**.

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

Step 5 Click **Go**.

Step 6 Enter the Name and Password.

Step 7 Click **Browse** to navigate to the applicable certificate file.

Step 8 Click **Open**.

Step 9 Click **Save**.

Pasting an ID Certificate

To paste an ID certificate directly, follow these steps:

Step 1 Copy the ID certificate to your computer clipboard.

Step 2 Choose **Configure > Controllers**.

Step 3 Click an applicable IP address.

Step 4 From the left sidebar menu, choose **Security > IP Sec Certificates > ID Certificate**.

Step 5 From the Select a command drop-down list, choose **Add Certificate**.

Step 6 Click **Go**.

Step 7 Enter the Name and Password.

Step 8 Select the **Paste** check box.

Step 9 Paste the certificate directly into the text box.

Step 10 Click **Save**.

Note ID certificates are available only if the controller is running Cisco Unified Wireless Network Software Version 3.2 or higher.

Note To delete a certificate, select it, choose **Delete Certificates** from the Select a command drop-down list, and click **Go**.

Configure Controllers > *IPaddr* > Security > Web Auth Certificate

This page enables you to download a web authorization certificate or regenerate the internally-generated web auth certificate.

To access the Web Auth Certificate page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Web Auth Certificate**.

Caution Each certificate has a variable-length embedded RSA Key. The RSA key can vary from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a certificate authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 Bits.

- Download Web Auth Certificate—Click to access the Download Web Auth Certificate to Controller page. See the "Download Web Auth or Web Admin Certificate to Controller" section on page 9-148 for additional information.

Command Buttons

- Regenerate Cert—Regenerate the internally-generated web auth certificate.

Configuring Wireless Protection Policies

This section describes the wireless protection policy configurations and introduces the following topics:

- Configuring Custom Signatures, page 9-109
- Configuring AP Authentication and MFP, page 9-109

Configuring Rogue Policies

This page enables you to set up policies for rogue access points.

To access the Rogue Policies page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Rogue Policies**. The following parameters appear:

- Rogue Location Discovery Protocol—RLDP determines whether or not the rogue is connected to the enterprise wired network. Choose one of the following from the drop-down list:
  - Disable—Disables RLDP on all access points. This is the default value.
  - All APs—Enables RLDP on all access points.
  - Monitor Mode APs—Enables RLDP only on access points in monitor mode.

Note Make sure that rogue detection is enabled on the desired access points. Rogue detection is enabled by default for all access points joined to a controller (except for OfficeExtend access points). However, in NCS software Release 6.0 or later, you can enable or disable rogue detection for individual access points by selecting or unselecting the **Rogue Detection** check box in the Access Point Details page. See the "Configuring Access Points" section on page 9-151 for more information.

Note Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

- Rogue APs
  - Expiration Timeout for Rogue AP and Rogue Client Entries (seconds)—Enter the number of seconds after which the rogue access point and client entries expire and are removed from the list.

    The valid range is 240 to 3600 seconds and the default value is 1200 seconds.

    Note If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.

- Rogue Clients
  - Validate rogue clients against AAA—Select the check box to use the AAA server or local database to validate if rogue clients are valid clients. The default value is unselected.

– Detect and report Adhoc networks—Select the check box to enable ad-hoc rogue detection and reporting. The default value is selected.

Command Buttons

- Save—Save the changes made to the client exclusion policies and return to the previous page.
- Audit—Compare the NCS values with those used on the controller.

Configuring Rogue AP Rules

This page enables you to view and edit current Rogue AP Rules.

To access the Rogue AP Rules page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Rogue AP Rules**. The Rogue AP Rules displays the Rogue AP Rules, the rule types (Malicious or Friendly), and the rule sequence.

Step 4 Click a Rogue AP Rule to view or edit its details. See the "Configuring a Rogue AP Rules Template" section on page 11-78 for more information.

Configuring Client Exclusion Policies

This page enables you to set, enable, or disable the client exclusion policies applied to the controller.

To access the Client Exclusion Policies page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Client Exclusion Policies**. The following parameters appear:

- Excessive 802.11a Association Failures—If enabled, clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
- Excessive 802.11a Authentication Failures—If enabled, clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
- Excessive 802.11x Authentication Failures—If enabled, clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
- Excessive 802.11 Web Authentication Failures—If enabled, clients are excluded on the fourth web authentication attempt, after three consecutive failures.
- IP Theft Or Reuse—If enabled, clients are excluded if the IP address is already assigned to another device.

Step 4 Click **Save** to save the changes made to the client exclusion policies and return to the previous page or click **Audit** to compare the NCS values with those used on the controller.

Configuring IDS Signatures

You can configure *IDS* Signatures, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, an appropriate mitigation action is initiated.

Cisco supports 17 standard signatures on the controller as shown on the Standard Signatures and Custom Signatures pages. For more information on these IDS Signatures, see the *Cisco Network Control System Configuration Guide*.

- Configuring Controller Standard Signature Parameters, page 9-105
- Configuring Custom Signatures, page 9-109
- Configuring AP Authentication and MFP, page 9-109

Configuring Controller Standard Signature Parameters

The Standard Signature Parameters page shows the list of Cisco-supplied signatures that are currently on the controller. This section contains the following topics:

- Downloading Signature Files, page 9-106
- Uploading Signature Files, page 9-106
- Global Settings for Standard and Custom Signatures, page 9-107

To access the Standard Signatures page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Standard Signatures**. This page displays the following parameters:

- Precedence—The order in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. For example:
  - None—No action is taken.
  - Report—Report the detection.
- State—Enabled or Disabled.
- Description—A more detailed description of the type of attack the signature is trying to detect.

Note Click a signature Name to view individual parameters and to enable or disable the signature.

Downloading Signature Files

To download a signature file, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Standard Signatures** or **Security > Wireless Protection Policies > Custom Signatures**.

Step 4 From the **Select a command** drop-down list, choose **Download Signature Files**.

Note This function can also be accessed by choosing **System > Commands > Upload/Download Commands > Download IDS Signatures**.

Step 5 Click **Go**.

Step 6 Copy the signature file (*.sig) to the default directory on your TFTP server.

Step 7 Choose **Local Machine** from the File is Located On. If you know the filename and path relative to the server root directory, you can also choose **TFTP server**.

Step 8 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries.

Step 9 Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout.

Step 10 The signature files are uploaded to the c:\tftp directory. Specify the local file name in that directory or click the **Browse** button to navigate to it. A "revision" line in the signature file specifies whether the file is a Cisco-provided standard signature file or a site-tailored custom signature file (custom signature files must always have revision=custom).

Note If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On parameter, and the server file name will be populated for you and retried. The local machine option initiates a two-step operation. First, the local file is copied from the administrator workstation to NCS own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the NCS server TFTP directory, and the downloaded web page now automatically populates the filename.

Step 11 Click **OK**.

Uploading Signature Files

To upload a signature file from the controller, follow these steps:

Step 1 Obtain a signature file from Cisco (hereafter called a standard signature file). You can also create your own signature file (hereafter called a custom signature file) by following "Downloading Signature Files" section on page 9-106.

Step 2 Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the signature download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port cannot be routed.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port cannot be routed.
- A third-party TFTP server cannot run on the same computer as the Cisco NCS because NCS built-in TFTP server and third-party TFTP server use the same communication port.

Step 3 Choose **Configure > Controllers**.

Step 4 Click an applicable IP address.

Step 5 From the left sidebar menu, choose **Security > Wireless Protection Policies > Standard Signatures** or **Security > Wireless Protection Policies > Custom Signatures**.

Step 6 From the Select a command drop-down list, choose **Upload Signature Files from controller**.

Note This function can also be accessed by choosing **Security > Custom Signatures > Select a command > Upload Signature Files from controller** or **System > Commands > Upload/Download Commands > Upload File from Controller**.

Step 7 Specify the TFTP server name being used for the transfer.

Step 8 If the TFTP server is new, enter the TFTP IP address in the **Server IP Address** parameter.

Step 9 Choose **Signature Files** from the File Type drop-down list.

Step 10 The signature files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory at the Upload to File parameter (this parameter only shows if the Server Name is the default server). The controller uses this local file name as a base name and then adds _std.sig as a suffix for standard signature files and _custom.sig as a suffix for custom signature files.

Step 11 Click **OK**.

Global Settings for Standard and Custom Signatures

This command enables all signatures that were individually selected as enabled. If this text box remains unselected, all files will be disabled, even those that were previously enabled. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.

To enable all standard and custom signatures currently on the controller, follow these steps:

Step 1 From the Select a command drop-down list, choose **Edit Signature Parameters**.

Step 2 Click **Go**.

Step 3 Select the **Enable Check for All Standard and Custom Signatures** check box.

Step 4 Click **Save**.

To enable or disable an individual signature, follow these steps:

Step 1 Click an applicable Name for the type of attack you want to enable or disable.

The Standard Signature parameters page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. The following parameters are displayed in both the signature page and the detailed signature page:

- Precedence—The order, or precedence, in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Description—A more detailed description of the type of attack that the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. One possibility is *None*, where no action is taken, and another is *Report*, to report the detection.
- Frequency—The signature frequency or the number of matching packets per interval that must be identified at the detecting access point level before an attack is detected. The range is 1 to 32,000 packets per interval and the default value is 50 packets per interval.
- Quiet Time—The length of time (in seconds) after which no attacks have been detected at the individual access point level, and the alarm can stop. This time appears only if the MAC information is all or both. The range is 60 to 32,000 seconds and the default value is 300 seconds.
- MAC Information—Whether the signature is to be tracked per network or per MAC address or both at the detecting access point level.
- MAC Frequency—The signature MAC frequency or the number of matching packets per interval that must be identified at the controller level before an attack is detected. The range is 1 to 32,000 packets per interval and the default value is 30 packets per interval.
- Interval—Enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds and the default value is 1 second.
- Enable—Select this check box to enable this signature to detect security attacks or unselect it to disable this signature.
- Signature Patterns—The pattern that is being used to detect a security attack.

Step 2 From the Enable drop-down list, choose **Yes**. Because you are downloading a customized signature, you should enable the files named with the _custom.sgi and disable the standard signature with the same name but differing suffix. For example, if you are customizing broadcast probe flood, you want to disable broadcast probe flood in the standard signatures but enable it in custom signatures.

Step 3 Click **Save**.

Configuring Custom Signatures

The Custom Signature page shows the list of customer-supplied signatures that are currently on the controller.

- Downloading Signature Files, page 9-106
- Uploading Signature Files, page 9-106
- Global Settings for Standard and Custom Signatures, page 9-107

To access the Custom Signatures page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > Custom Signatures**. This page displays the following parameters:

- Precedence—The order in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. For example:
  - None—No action is taken.
  - Report—Report the detection.
- State—Enabled or Disabled.
- Description—A more detailed description of the type of attack the signature is trying to detect.

Note Click a signature Name to view individual parameters and to enable or disable the signature.

Configuring AP Authentication and MFP

This page enables you to set the access point authentication policy.

To access the AP Authentication and MFP (Management Frame Protection) page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Security > Wireless Protection Policies > AP Authentication and MFP**.

- RF Network Name—Not an editable text box. The RF Network Name entered in the general parameters page (See Configure *IPaddr* > General) is displayed here.
- Protection Type—From the drop-down list, select one of the following authentication policies:
  - None—No access point authentication policy.
  - AP Authentication—Apply authentication policy.

  - MFP—Apply Management Frame Protection. See the "Monitoring Management Frame Protection" section on page 5-19 for more information.

- Alarm Trigger Threshold—(Appears only when AP Authentication is selected as the Protection Type). Set the number of hits to be ignored from an alien access point before raising an alarm.

  The valid range is from 1 to 255. The default value is 255.

Command Buttons

- Save
- Audit

Configuring Cisco Access Points

You can use the Configure > Controllers page to view and configure Cisco access points for a specific controller.

To access the Cisco APs page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Access Points > Cisco APs**. The Cisco APs page opens and displays the following parameters:

- AP Name—Click an access point name to view or configure access point details.
- Base Radio MAC
- Admin Status
- AP Mode
- Software Version
- Primary Controller Name

Step 4 Click an access point name to view or configure the access point details. The displayed information may vary depending on the access point type.

Note See the "Configuring Access Points" section on page 9-151 for more detailed information.

Command Buttons

- Save—Save the current settings.
- Audit—Discover the present status of this access point.

Sniffer feature

When the sniffer feature is enabled on an access point, the access point functions as a sniffer and captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. The packets contain information on timestamp, signal strength, packet size, and so on.

Note The sniffer feature can be enabled only if you are running AiroPeek, which is a third-party network analyzer software that supports decoding of data packets. For more information on AiroPeek, see the following URL: www.wildpackets.com/products/airopeek/overview

Prerequisites for Using the Sniffer Feature

Before using the sniffer feature, you must have completed the following:

- Configured an access point in sniffer mode at the remote site. For information on how to configure an access point in sniffer mode, see AP mode in Configuring an AP in Sniffer Mode Using the Web User Interface.
- Installed AiroPeek version 2.05 or later on a Windows XP machine.

Note You must be a WildPackets Maintenance Member to download the following dll files. See the following URL:

https://wpdn.wildpackets.com/view_submission.php?id=30

- Copied the following dll files:
  - socket.dll file to the Plugins folder (Example: C:\ProgramFiles\WildPackets\AiroPeek\Plugins)
  - socketres.dll file to the PluginRes folder (Example:C:\ProgramFiles\WildPackets\AiroPeek\1033\PluginRes)

Configuring AiroPeek on the Remote Machine

To configure AiroPeek on the remote machine, follow these steps:

Step 1 Start the AiroPeek application and click **Options** on the Tools tab.

Step 2 Click **Analysis Module** in the Options page.

Step 3 Right-click inside the page and select **Disable All** option.

Step 4 Find the Cisco remote module column and enable it. Click **OK** to save the changes.

Step 5 Click **New capture** to bring up the capture option page.

Step 6 Choose the remote Cisco adapter and from the list of adapter modules.

Step 7 Expand it to locate the new remote adapter option. Double-click it to open a new page, enter a name in the text box provided and enter the controller management interface IP in the IP address column.

Step 8 Click **OK**. The new adapter will be added to the remote Cisco adapter.

Step 9 Select the new adapter for remote airopeek capture using the access point.

Step 10 Click **start socket capture** in the capture page to start the remote capture process.

Step 11 Go to the controller CLI, bring up an access point, and set it to sniffer mode by entering **config ap mode sniffer <ap-name>**.

The access point will reboot and come up in sniffer mode.

Configuring an AP in Sniffer Mode Using the Web User Interface

To configure an AP in Sniffer Mode using the web user interface, follow these steps:

Step 1 Choose **Configure > Access Points**, then click an item under AP Name list to navigate to this pane.

Step 2 In General parameters, set the AP mode to Sniffer using the drop-down list, and click **Apply**.

Step 3 Select a Protocol (802.11a/802.11b/g) under Radio Interfaces. This will open the configuration page.

Step 4 Select the **Sniff** check box to bring up the Sniff parameters. Select the channel to be sniffed and enter the IP address of the server (The remote machine running AiroPeek).

Step 5 Click **Save** to save the changes.

Configuring 802.11 Parameters

Configuring General Parameters for an 802.11 Controller

This page enables you to edit country selection and timer information on a 802.11 controller. To access this page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11 > General**. The page opens and displays the following parameters:

- Country
  - Country—Countries and the protocols allowed.

    Note The maximum number of countries that you can select is 20.

  - Selected Countries—Displays countries currently selected.
- Timers

– Authentication Response Timeout—Configures 802.11 authentication response timeout in seconds.

Setting Multiple Country Codes

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

Step 1 Choose **Configure > Controllers**.

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

Step 3 Choose **802.11 > General** from the left sidebar menu.

Step 4 Select 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 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 regulatory domain. For a complete list of country codes supported per product, see 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**.

Configuring Aggressive Load Balancing

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

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

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

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

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

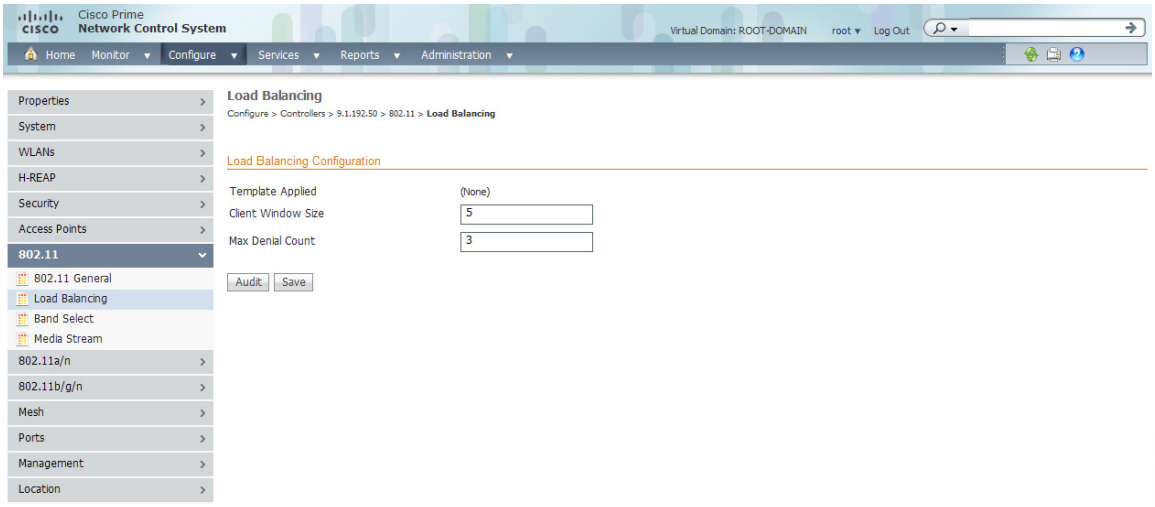
To configure aggressive load balancing, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the controller that you need to configure.

Step 3 Choose **802.11 > Load Balancing** from the left sidebar menu. The load balancing page appears (see Figure 9-12).

Figure 9-12 Load Balancing



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

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

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

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

Step 6 Click **Save**.

Step 7 To enable or disable aggressive load balancing on specific WLANs, browse to the WLAN Configuration page, and click the **Advanced** tab. For instructions on using the WLAN Configuration page, see the "Configuring Controller WLANs" section on page 9-64.

Configuring Band Selection

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

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

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

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

Guidelines for Using Band Selection

Follow these guidelines when using band selection:

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

Configuration Steps

To configure band selection, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the controller that you need to configure.

Step 3 Choose **802.11 > Band Select** from the left sidebar menu. The band select page appears (see Figure 9-13).

Figure 9-13 Band Select

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

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

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

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

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

Step 9 Click **Save**.

Step 10 To enable or disable band selection on specific WLANs, browse to the WLAN Configuration page and click the **Advanced** tab. For instructions on using the WLAN Configuration page, see the "Configuring Controller WLANs" section on page 9-64.

Configuring 802.11 Media Parameters

To configure the media parameters for 802.11, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the applicable IP address.

Step 3 From the left sidebar menu, choose **802.11 > Media Stream**.

Step 4 In the Media Stream Configuration section, specify the following parameters

- Media Stream Name

- Multicast Destination Start IP—Start IP address of the media stream to be multicast
- Multicast Destination End IP—End IP address of the media stream to be multicast
- Maximum Expected Bandwidth—Maximum bandwidth that a media stream can use

Step 5 In the Resource Reservation Control (RRC) Parameters group box, specify the following parameters:

- Average Packet Size—Average packet size that a media stream can use.
- RRC Periodical Update—Resource Reservation Control calculations that are updated periodically; if disabled, RRC calculations are done only once when a client joins a media stream.
- RRC Priority—Priority of RRC with the highest at 1 and the lowest at 8.
- Traffic Profile Violation—Appears if the stream is dropped or put in the best effort queue if the stream violates the QoS video profile.
- Policy—Appears if the media stream is admitted or denied.

Step 6 Click **Save**.

Configuring 802.11a/n Parameters

This section contains the following topics:

Configuring 802.11a/n General Parameters

To view 802.11a/n parameters for a specific controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n Parameters** to view the following parameters:

- General
  - 802.11a/n Network Status—Select the check box to enable.

  - Beacon Period—The amount of time between beacons. The valid range is from 100 to 600 milliseconds.
  - DTIM Period—The number of beacon intervals that may elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field is 0.
  - Fragmentation Threshold (in bytes)—The size at which packets are fragmented. Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
  - Template Applied
- 802.11a/n Band Status
  - Low, Medium, and High Bands (read-only).
- 802.11a/n Power Status
  - Dynamic Assessment—Automatic, On Demand, or Disabled.
  - Current Tx Level—Range includes: 1 (maximum power allowed per country code setting), 2 (50% power), 3 (25% power), 4 (6.25 to 12.5% power), and 5 (0.195 to 6.25% power).

Note The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.

  - Control Interval—In seconds (read-only).
  - Dynamic Treatment Power Control—Select the check box to enable.
- 802.11a/n Channel Status
  - Assignment Mode—Automatic, On Demand, or Disabled.
  - Update Interval—In seconds.
  - Avoid Foreign AP Interference—Enable to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels.
  - Avoid Cisco AP load—Enable to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points.
  - Avoid non 802.11 Noise—Enable to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Disable this parameter to have RRM ignore this interference.
  - Signal Strength Contribution—Not configurable.
  - Avoid Persistent Non-WiFi interface
- Data Rates
  - Ranges between 6 Mbps and 54 Mbps—Supported, Mandatory, or Disabled.
- Noise/Interference/Rogue Monitoring Channels.
  - Channel List—All Channels, Country Channels, DCA Channels.

Note Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation from a set of managed devices connected to the controller.

- CCX Location Measurement—When enabled, it enhances the location accuracy of clients.
  - Mode—Select the check box to enable.

– Interval—In seconds.

Note The CCX Location Measurement Interval can be changed only when measurement mode is enabled.

Command Buttons

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

Configuring 802.11a/n RRM Thresholds

To configure a 802.11a/n RRM threshold controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/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 will be when adjusting the SNR value.

Step 5 Click **Save**.

Configuring 802.11a/n RRM Intervals

To configure 802.11a/n or 802.11b/g/n RRM intervals for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

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

Note The default for the following four RRM interval parameters is 300 seconds.

Step 4 Enter at which interval you want strength measurements taken for each access point.

Step 5 Enter at which interval you want noise and interference measurements taken for each access point.

Step 6 Enter at which interval you want load measurements taken for each access point.

Step 7 Enter at which interval you want coverage measurements taken for each access point.

Step 8 Click **Save**.

Configuring 802.11a/n RRM Transmit Power Control

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the access points' transmit power according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases an access point's power in response to changes in the RF environment. In most instances TPC will seek to lower an access point's power to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from Coverage Hole Detection, explained below. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To configure 802.11a/n or 802.11b/g/n RRM TPC, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n-RRM > TPC**.

Step 4 Configure the following TPC parameters:

- Template Applied—The name of the template applied to this controller.
- Dynamic Assignment—At the Dynamic Assignment drop-down list, choose one of three modes:
  - Automatic - The transmit power is periodically updated for all access points that permit this operation.
  - On Demand - Transmit power is updated when the Assign Now button is selected.
  - Disabled - No dynamic transmit power assignments occur, and values are set to their global default.
- Maximum Power Assignment—Indicates the maximum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Minimum Power Assignment—Indicates the minimum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Dynamic Tx Power Control—Determine if you want to enable Dynamic Tx Power Control.
- Transmitted Power Threshold—Enter a transmitted power threshold between -50 and -80.
- Control Interval—In seconds (read-only).

Step 5 Click **Save**.

Configuring 802.11a/n RRM Dynamic Channel Allocation

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

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

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

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

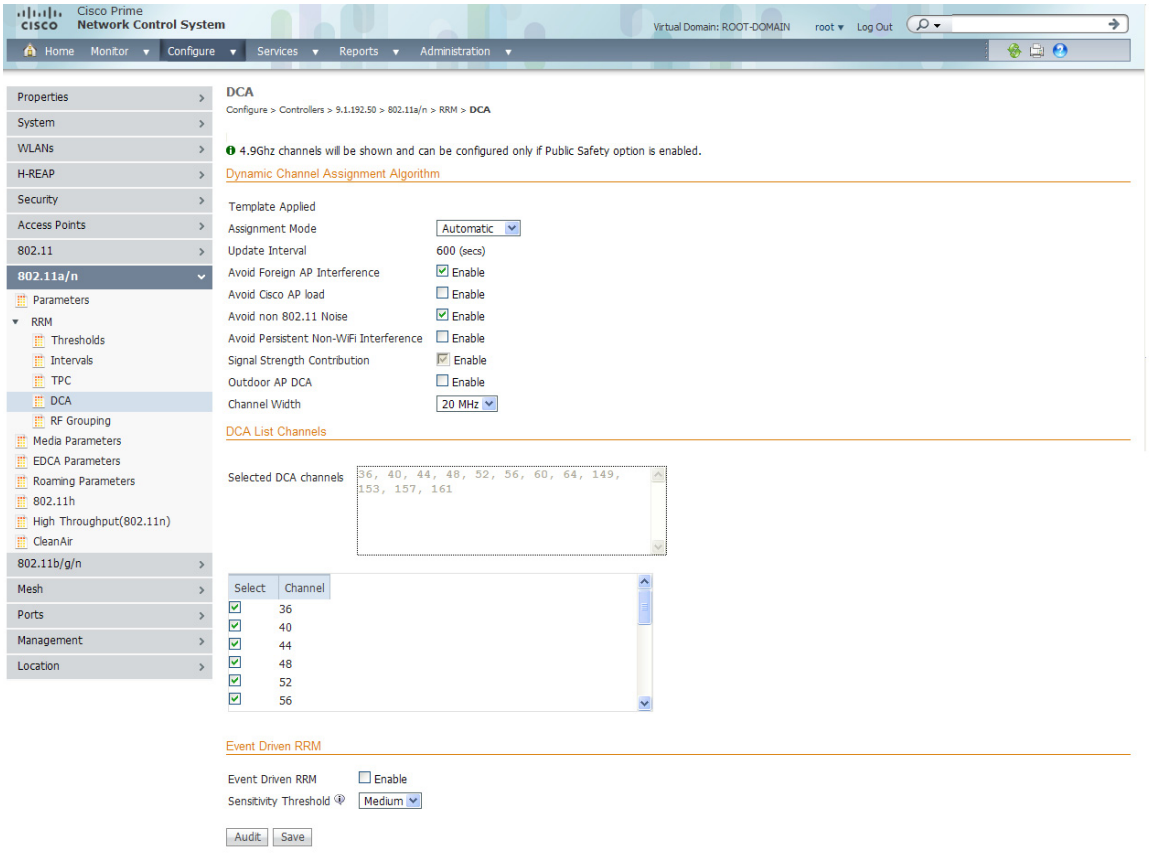
Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the appropriate controller.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM DCA**. The 802.11a/n RRM DCA page appears (see Figure 9-14).

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 9-14 802.11a/n RRM DCA Page



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

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

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

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

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

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

Step 7 Click **Save**.

Configuring 802.11a/n RRM Radio Grouping

To configure 802.11a/n or 802.11b/g/n RRM Radio Grouping for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > RRM > RF Grouping**.

Step 4 Choose a grouping mode from the drop-down list. The following parameters appear:

- Automatic—Allows you to activate the automatic RRM Grouping Algorithm. This is the default mode.
- Off—Allows you to deactivate the automatic grouping.
- Leader—Allows you to assign members to the group.

Step 5 Choose a group update interval (secs) from the drop-down list. When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm will also run when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 600 seconds.

Step 6 In the Group Members group box, click **Add >**. The selected controller moves from the Available Controllers to the RF Group Members list.

Note The RF Group Members group box appears only when the grouping mode is set to Leader.

Note The maximum number of controllers that can be added to a RF Group is 20.

Step 7 Click **Save**.

Configuring 802.11a/n Media Parameters

To configure the media parameters for 802.11a/n, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > Media Parameters**.

Step 4 In the **Voice** tab, specify the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.

  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.

- CAC Method—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.

  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.

- Maximum Bandwidth Allowed—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.

- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.

- Expedited Bandwidth—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.

  You must have an expedited bandwidth that is CCXv5 compliant so that a TSPEC request is given higher priority.

- SIP CAC—Select the check box to enable SIP CAC.

  SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- SIP Codec—Specify the codec name you want to use on this radio. The available options are G.711, G.729, and User Defined.

- SIP Call Bandwidth—Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This parameter can be configured only when the SIP Codec selected is User Defined.

- SIP Sample Interval—Specify the sample interval in milliseconds that the codec must operate in.

- Max Voice Calls per Radio—Specify the maximum number of voice calls that can be made per Radio.

- Max Roaming Reserved Calls per Radio—Specify the maximum number roaming calls that can be reserved per Radio.

Note The Max Voice Calls per Radio and Max Roaming Reserved Calls per Radio options are available only if the CAC Method is specified as Static and SIP CAC is enabled.

- Metric Collection—Select the check box to enable metric collection.

  Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which 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 interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Step 5 On the **Video** tab, specify the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.
- Maximum Bandwidth Allowed—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
- Unicast Video Redirect—Select the **Unicast Video Redirect** check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
- Client Minimum Phy Rate—Specify the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
- Multicast Direct Enable—Select the **Multicast Direct Enable** check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
- Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.
- Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.
- Best Effort QOS Admission—Select the Best Effort QOS Admission check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used.

Note If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Step 6 In the **General** tab, specify the following parameter:

- Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Step 7 Click **Save**.

Note SIPs are available only on the following controllers: 4400, 5500 and on for the following access points: 1240, 1130, and 11n.

Command Buttons

- Save—Save the changes made.

- Audit—Compare the NCS values with those used on the controller.

Configuring 802.11a/n EDCA Parameters

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.

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

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

Step 4 Choose the EDCA Profile from the drop-down list.

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 Select 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 802.11a/n Roaming Parameters

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11a/n > Roaming Parameters**.

Step 4 From the Mode drop-down list, choose **Default values** or **Custom values**.

- Default values—The default values (read-only) are automatically displayed in the text boxes.
- Custom values—Activates the text boxes to enable editing of the roaming parameters.

Step 5 In the Minimum RSSI text box, enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point.

- Range**:** -80 to -90 dBm
- Default**:** -85 dBm

Note If the client average received signal power dips below this threshold, reliable communication is typically impossible; clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

Step 6 In the Hysteresis text box, enter a value to indicate how strong the signal strength of a neighboring access point must for the client to roam to it.

This parameter is intended to reduce the amount of "ping ponging" between access points if the client is physically located on or near the border between two access points.

- Range**:** 2 to 4 dB
- Default**:** 3 dB

Step 7 In the Adaptive Scan Threshold text box, enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time.

This parameter provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.

- Range**:** -70 to -77 dB
- Default**:** -72 dB

Step 8 In the Transition Time text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

- Range**:** 1 to 10 seconds
- Default**:** 5 seconds

Step 9 Click **Save**.

Configuring 802.11a/n 802.11h Parameters

To configure 802.11h parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

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

Step 4 Select the **power constraint** check box to enable TPC.

Step 5 Select the **channel announcement** check box to enable channel announcement. Channel announcement is a method in which the access point announces when it is switching to a new channel and the new channel number.

Step 6 Click **Save**.

Configuring 802.11a/n High Throughput (802.11n) Parameters

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

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

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

Step 4 Select the **802.11n Network Status Enabled** check box to enable high throughput.

Step 5 In the MCS (Data Rate) Settings, choose which level of data rate you want supported. MCS is modulation coding schemes which are similar to 802.11a data rate. As a default, 20 MHz and short guarded interval is used.

Note When you select the Supported check box, the chosen numbers appear in the Selected MCS Indexes page.

Step 6 Click **Save**.

Configuring 802.11a/n CleanAir Parameters

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

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

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

- CleanAir—Select the check box to enable CleanAir functionality on the 802.11 a/n network, or unselect to disable CleanAir functionality. The default value is selected.
- Reporting Configuration—Use the parameters in this section to configure the interferer devices you want to include for your reports.
  - Report—Select the **report interferers** check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.
  - Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect text box and any that do not need to be detected appear in the Interferers to Ignore text box. Use the > and < buttons to move interference sources between these two text boxes. By default, all interference sources are detected.
- Alarm Configuration—This section enables you to configure triggering of air quality alarms.
  - Air Quality Alarm—Select the **Air Quality Alarm** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature. The default value is selected.

  - Air Quality Alarm Threshold—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.
  - Interferers For Security Alarm—Select the **Interferers For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is selected.
  - Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms text box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms text box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.
- Event Driven RRM—To trigger spectrum event-driven Radio Resource Management (RRM) to run when a CleanAir-enabled access point detects a significant level of interference, follow these steps:
  - Event Driven RRM—Displays the current status of spectrum event-driven RRM.
  - Sensitivity Threshold—If Event Driven RRM is enabled, this text box displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Command Buttons

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

Configuring 802.11b/g/n Parameters

This section contains the following topics:

Configuring 802.11b/g/n General Parameters

To view 802.11b/g/n parameters for a specific controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11b/g/n Parameters** to view the following parameters:

- General
  - 802.11b/g Network Status—Select the check box to enable.
  - 802.11g Support—Select the check box to enable.
  - Beacon Period—In milliseconds.
  - DTIM Period—The number of beacon intervals that may elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field is 0.
  - Fragmentation Threshold—In bytes.
  - Short Preamble—Select the check box to enable.
  - Template Applied
- 802.11a/n Power Status
  - Dynamic Assessment—Automatic, On Demand, or Disabled.
  - Current Tx Level
  - Control Interval—In seconds (Read-only).
  - Dynamic Treatment Power Control—Select the check box to enable.
- 802.11a/n Channel Status
  - Assignment Mode—Automatic, On Demand, or Disabled.
  - Update Interval—In seconds.
  - Avoid Foreign AP Interference—Select the check box to enable.
  - Avoid Cisco AP load—Select the check box to enable.
  - Avoid non 802.11 Noise—Select the check box to enable.
  - Signal Strength Contribution—Select the check box to enable.
- Data Rates
  - Ranges between 1 Mbps and 54 Mbps—Supported, Mandatory, or Disabled.
- Noise/Interference/Rogue Monitoring Channels
  - Channel List—All Channels, Country Channels, DCA Channels.
- CCX Location Measurement
  - Mode—Select the check box to enable.
  - Interval—In seconds.

Note The CCX Location Measurement Interval can be changed only when measurement mode is enabled.

Command Buttons

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

Configuring 802.11b/g/n RRM Thresholds

To configure a 802.11b/g/n RRM threshold controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **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 will be when adjusting the SNR value.

Step 5 Click **Save**.

Configuring 802.11b/g/n RRM Intervals

To configure 802.11a/n or 802.11b/g/n RRM intervals for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

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

Note The default for the following four RRM interval parameters is 300 seconds.

Step 4 Enter at which interval you want strength measurements taken for each access point.

Step 5 Enter at which interval you want noise and interference measurements taken for each access point.

Step 6 Enter at which interval you want load measurements taken for each access point.

Step 7 Enter at which interval you want coverage measurements taken for each access point.

Step 8 Click **Save**.

Configuring 802.11b/g/n RRM Transmit Power Control

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the access points' transmit power according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases an access point's power in response to changes in the RF environment. In most instances TPC will seek to lower an access point's power to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from Coverage Hole Detection, explained below. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To configure 802.11b/g/n RRM TPC, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11b/g/n-RRM > TPC**.

Step 4 Configure the following TPC parameters:

- Template Applied—The name of the template applied to this controller.
- Dynamic Assignment—At the Dynamic Assignment drop-down list, choose one of three modes:
  - Automatic - The transmit power is periodically updated for all access points that permit this operation.
  - On Demand - Transmit power is updated when the Assign Now button is selected.
  - Disabled - No dynamic transmit power assignments occur, and values are set to their global default.
- Maximum Power Assignment—Indicates the maximum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Minimum Power Assignment—Indicates the minimum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Dynamic Tx Power Control—Determine if you want to enable Dynamic Tx Power Control.
- Transmitted Power Threshold—Enter a transmitted power threshold between -50 and -80.
- Control Interval—In seconds (read-only).

Step 5 Click **Save**.

Configuring 802.11b/g/n RRM DCA

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

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11b/g/n-RRM > DCA**.

Step 4 Select the check box(es) for the applicable DCA channel(s). The selected channels are listed in the Selected DCA channels text box.

Step 5 Enable or disable event-driven Radio Resource Management (RRM). Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference, follow these steps:

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

Step 6 Click **Save**.

Configuring 802.11b/g/n RRM Radio Grouping

To configure 802.11a/n or 802.11b/g/n RRM Radio Grouping for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **802.11b/g/n > RRM > RF Grouping**.

Step 4 Choose a grouping mode from the drop-down list. The following parameters appear:

- Automatic—Allows you to activate the automatic RRM Grouping Algorithm. This is the default mode.
- Off—Allows you to deactivate the automatic grouping.
- Leader—Allows you to assign members to the group.

Step 5 Choose a group update interval (secs) from the drop-down list. When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm will also run when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 600 seconds.

Step 6 Under the Group Members group box, click **Add >**. The selected controller moves from the Available Controllers to the RF Group Members list.

Note The RF Group Members group box appears only when the grouping mode is set to Leader.

Note The maximum number of controllers that can be added to a RF Group is 20.

Step 7 Click **Save**.

Configuring 802.11b/g/n Media Parameters

To configure the media parameters for 802.11b/g/n, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the applicable IP address.

Step 3 From the left sidebar menu, choose **802.11b/g/n > Media Parameters**.

Step 4 In the Voice tab, specify the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.

  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.

- CAC Method—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.

  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.

- Maximum Bandwidth Allowed—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.

- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.

- Expedited Bandwidth—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.

  You must have an expedited bandwidth that is CCXv5 compliant so that a TSPEC request is given higher priority.

- SIP CAC—Select the check box to enable SIP CAC.

SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- SIP Codec—Specify the codec name you want to use on this radio. The available options are G.711, G.729, and User Defined.
- SIP Call Bandwidth—Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This parameter can be configured only when the SIP Codec selected is User Defined.
- SIP Sample Interval—Specify the sample interval in milliseconds that the codec must operate in.
- Max Voice Calls per Radio—Indicates the maximum number of voice calls that can be made per Radio.

Note You cannot set the value of Max Voice Calls per Radio. This is automatically calculated based on the selected CAC method, Max BW allowed, and Roaming Bandwidth.

- Max Roaming Reserved Calls per Radio—Indicates the maximum number roaming calls that can be reserved per Radio.

Note The Max Voice Calls per Radio and Max Roaming Reserved Calls per Radio options are available only if the CAC Method is specified as Static and SIP CAC is enabled.

- Metric Collection—Select the check box to enable metric collection.

  Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which 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 interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Step 5 In the **Video** tab, specify the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.
- Maximum Bandwidth—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
- Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
- Unicast Video Redirect—Select the **Unicast Video Redirect** check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
- Client Minimum Phy Rate—Specify the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
- Multicast Direct Enable—Select the **Multicast Direct Enable** check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
- Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.
- Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.
- Best Effort QOS Admission—Select the **Best Effort QOS Admission** check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used.

Note If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Step 6 In the **General** tab, specify the following parameter:

- Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Step 7 Click **Save**.

Note SIPs are available only on the following controllers: 4400, 5500 and on for the following access points: 1240, 1130, and 11n.

Command Buttons

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

Configuring 802.11b/g/n EDCA Parameters

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.

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

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

Step 4 Choose the EDCA Profile from the drop-down list.

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 Select 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 802.11b/g/n Roaming Parameters

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

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

Step 4 From the Mode drop-down list, choose **Default values** or **Custom values**.

- Default values—The default values (read-only) are automatically displayed in the text boxes.
- Custom values—Activates the text boxes to enable editing of the roaming parameters.

Step 5 In the Minimum RSSI text box, enter a value for the minimum received signal strength indicator (RSSI) required for the client to associate to an access point.

- Range**:** -80 to -90 dBm
- Default**:** -85 dBm

Note If the client average received signal power dips below this threshold, reliable communication is typically impossible; clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

Step 6 In the Hysteresis text box, enter a value to indicate how strong the signal strength of a neighboring access point must be in order for the client to roam to it.

This parameter is intended to reduce the amount of "ping ponging" between access points if the client is physically located on or near the border between two access points.

- Range**:** 2 to 4 dB
- Default**:** 3 dB

Step 7 In the Adaptive Scan Threshold text box, enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time.

This parameter provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.

- Range**:** -70 to -77 dB
- Default**:** -72 dB

Step 8 In the Transition Time text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

- Range**:** 1 to 10 seconds
- Default**:** 5 seconds

Step 9 Click **Save**.

Configuring 802.11b/g/n High Throughput (802.11n) Parameters

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

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

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

Step 4 Select the **802.11n Network Status Enabled** check box to enable high throughput.

Step 5 In the MCS (Data Rate) Settings, choose which level of data rate you want supported. MCS is modulation coding schemes which are similar to 802.11a data rate. As a default, 20 MHz and short guarded interval is used.

Note When you select the Supported check box, the chosen numbers appear in the Selected MCS Indexes page.

Step 6 Click **Save**.

Configuring 802.11b/g/n CleanAir Parameters

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

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

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

- CleanAir—Select the check box to enable CleanAir functionality on the 802.11b/g/n network, or unselect to prevent the controller from detecting spectrum interference. The default value is selected.
- Reporting Configuration—Use the parameters in this section to configure the interferer devices you want to include for your reports.
  - Report—Select the **report interferers** check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.
  - Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect text box and any that do not need to be detected appear in the Interferers to Ignore text box. Use the > and < buttons to move interference sources between these two text boxes. By default, all interference sources are detected.
- Alarm Configuration—This section enables you to configure triggering of air quality alarms.
  - Air Quality Alarm—Select the **Air Quality Alarm** check box to enable the triggering of air quality alarms, or unselect the text box to disable this feature. The default value is selected.

  - Air Quality Alarm Threshold—If you selected the **Air Quality Alarm** check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.
  - Interferers For Security Alarm—Select the **Interferers For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is selected.
  - Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms text box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms text box. Use the **>** and **<** buttons to move interference sources between these two text boxes. By default, all interference sources trigger interferer alarms.

- Event Driven RRM—To trigger spectrum event-driven Radio Resource Management (RRM) to run when a CleanAir-enabled access point detects a significant level of interference, use the following parameters:
  - Event Driven RRM—Displays the current status of spectrum event-driven RRM.
  - Sensitivity Threshold—If Event Driven RRM is enabled, this text box displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Allocation (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Command Buttons

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

Configuring Mesh Parameters

To configure Mesh parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Mesh > Mesh Settings**.

Step 4 View or edit the following mesh parameters:

- RootAP to MeshAP Range (150 - 13200 ft)—By default, this value is 12,000 feet. You can enter a value between 150 and 132,000 feet. Enter the optimum distance (in feet) that should exist between the root access point and the mesh access point. This global parameter applies to all access points when they join the controller and all existing access points in the network.

- Client Access on Backhaul Link—Enabling this feature lets mesh access points associate with 802.11a wireless clients over the 802.11a backhaul. This client association is in addition to the existing communication on the 802.11a backhaul between the root and mesh access points. This feature is only applicable to access points with two radios. For more information, see the "Client Access on 1524SB Dual Backhaul" section on page 9-140.

Note Changing Backhaul Client Access reboots all mesh access points.

- Mesh DCA Channels—Enable or disable. This option is disabled by default. Enable this option to enable backhaul channel deselection on the Controller using the DCA channel list. Any change to the channels in the Controller DCA list is pushed to the associated access points. This option is only applicable for 1524SB mesh access points. For more information on this feature, see the "Backhaul Channel Deselection Using NCS" section on page 9-141.
- Background Scanning—Select the **Background Scanning** check box to enable background scanning or unselect it to disable the feature. The default value is disabled. Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents.
- Security Mode—Choose **EAP** (Extensible Authentication Protocol) or PSK (Pre-Shared Key) from the Security Mode drop-down list.

Note Changing Security reboots all mesh access points.

Step 5 Click **Save**.

Client Access on 1524SB Dual Backhaul

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

The two 802.11a backhaul radios use the same MAC address. There may be instances where the same WLAN maps to the same BSSID in more than one slot.

By default, client access is disabled over both of the backhaul radios.

The following guidelines should be followed for enabling or disabling a radio slot:

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

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

- The Controller command-line interface (CLI)
- The Controller Graphical User Interface (GUI)
- The NCS GUI. For more information, see the "Configuring Client Access using NCS - GUI" section on page 9-141.

Note The procedure for configuring client access using the CLI and GUI is documented in the *Controller Configuration Guide*.

Configuring Client Access using NCS - GUI

To configure client access on the two backhaul radios, follow these steps:

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

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

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

Step 4 Click **Save**.

A warning message is displayed:

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

Step 5 Click **OK**.

The Universal Client access is configured on both the radios.

Backhaul Channel Deselection Using NCS

To configure backhaul channel deselection, follow these steps:

Step 1 You must first configure the Mesh DCA channels flag on the controllers. See the "Configuring Mesh DCA Channel Flag on Controllers Using NCS" section on page 9-141 for more information.

Step 2 Then change the channel list using config groups. See the "Changing the Channel List Using Config Groups" section on page 9-142 for more information.

Configuring Mesh DCA Channel Flag on Controllers Using NCS

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

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

Or

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

The Mesh Settings page appears.

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

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

Changing the Channel List Using Config Groups

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

To configure backhaul channel deselection using config groups, follow these steps:

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

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

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

Step 4 Select or unselect the channels for the config group.

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

Configuring Port Parameters

To configure Port parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Ports > Port Settings**.

Step 4 Click the applicable Port Number to open the Port Settings Details page. The following parameters display:

- General Parameters:
  - Port Number—Read-only.
  - Admin Status—Choose Enabled or Disabled from the drop-down list.
  - Physical Mode—Choose Auto Negotiate or Full Duplex 1 Gbps.
  - STP Mode—Choose 802.1D, Fast, or Off.
  - Mirror Mode—Choose Enabled or Disabled.
  - Link Traps—Choose Enabled or Disabled.
  - Power Over Ethernet
  - Multicast Application Mode—Select Enabled or Disabled.
- Spanning Tree Protocol Parameters:
  - Priority—The numerical priority number of the ideal switch.

– Path Cost—A value (typically based on hop count, media bandwidth, or other measures) assigned by a network administrator and used to determine the most favorable through an internetwork environment (the lower the cost, the better the path).

Step 5 Choose **Save** or **Audit** for General or Spanning Tree Protocol settings.

Configuring Controllers Management Parameters

Configuring Trap Receivers

This section contains the following topics:

Configuring Trap Receivers for an Individual Controller

To configure trap receivers for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Trap Receivers**.

Step 4 The following parameters are displayed for current trap receivers:

- Template Name—User-defined name of this template.
- IP Address—The IP address of the server.
- Admin Status—Status must be enabled for the SNMP traps to be sent to the receiver.

Step 5 Click a receiver Name to access its details.

Step 6 Select the **Admin Status** check box to enable the trap receiver. Deselect the check box to disable the trap receiver.

Step 7 Click **Save**.

Adding a New Receiver

To add a new receiver, follow these steps:

Step 1 From the Select a command drop-down list, choose **Add Receiver**.

Step 2 Click **Go**.

Step 3 From the Select a template to apply to this controller drop-down list, choose the applicable template to apply to this controller.

Note To create a new template for Trap Receivers, use the **click here** link to access the applicable template creation page.

Step 4 Click **Apply**.

Configuring Trap Control Parameters

To configure trap control parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Trap Control**.

The applied template is identified (if applicable). See the "Configuring Trap Control Templates" section on page 11-116 for more information.

The following traps can be enabled for this controller:

- Miscellaneous Traps
  - SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated.

    Note When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.

  - Link (Port) Up/Down—Link changes status from up or down.
  - Multiple Users—Two users login with the same login ID.
  - Spanning Tree—Spanning Tree traps. See the STP specifications for descriptions of individual parameters.
  - Rogue AP—Whenever a rogue access point is detected this trap will be sent with its MAC Address; When a rogue access point that was detected earlier and it no longer exists this trap is sent.
  - Config Save—Notification sent when the controller configuration is modified.
- Client Related Traps

  - 802.11 Association—The associate notification is sent when the client sends an association frame.
  - 802.11 Disassociation—The disassociate notification is sent when the client sends a disassociation frame.
  - 802.11 Deauthentication—The deauthenticate notification is sent when the client sends a deauthentication frame.
  - 802.11 Failed Authentication—The authenticate failure notification is sent when the client sends an authentication frame with a status code other than 'successful'.
  - 802.11 Failed Association—The associate failure notification is sent when the client sends an association frame with a status code other than 'successful'.
  - Excluded—The associate failure notification is sent when a client is excluded.
- Cisco AP Traps
  - AP Register—Notification sent when an access point associates or disassociates with the controller.
  - AP Interface Up/Down—Notification sent when access point interface (802.11a or 802.11b/g) status goes up or down.
- Auto RF Profile Traps
  - Load Profile—Notification sent when Load Profile state changes between PASS and FAIL.
  - Noise Profile—Notification sent when Noise Profile state changes between PASS and FAIL.
  - Interference Profile—Notification sent when Interference Profile state changes between PASS and FAIL.
  - Coverage Profile—Notification sent when Coverage Profile state changes between PASS and FAIL.
- Auto RF Update Traps
  - Channel Update—Notification sent when access point dynamic channel algorithm is updated.
  - Tx Power Update—Notification sent when access point dynamic transmit power algorithm is updated.
- AAA Traps
  - User Auth Failure—This trap is to inform that a client RADIUS Authentication failure has occurred.
  - RADIUS Server No Response—This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
- IP Security Traps
  - ESP Authentication Failure—IPSec packets with invalid hashes were found in an inbound ESP SA.
  - ESP Replay Failure—IPSec packets with invalid sequence numbers were found in an inbound ESP SA.
  - Invalid SPI—A packet with an unknown SPI was detected from the specified peer with the specified SPI using the specified protocol.
  - IKE Negotiation Failure—An attempt to negotiate a phase 1 IKE SA failed. The notification counts are also sent as part of the trap, along with the current value of the total negotiation error counters.

  - IKE Suite Failure—An attempt to negotiate a phase 2 SA suite for the specified selector failed. The current total failure counts are passed as well as the notification type counts for the notify involved in the failure.
  - Invalid Cookie—ISAKMP packets with invalid cookies were detected from the specified source, intended for the specified destination. The initiator and responder cookies are also sent with the trap.
- 802.11 Security Traps
  - WEP Decrypt Error—Notification sent when the controller detects a WEP decrypting error.
- WPS Traps
  - Rogue Auto Containment—Notification sent when a rogue access point is auto-contained.

Step 4 After selecting the applicable parameters, click **Save**.

Configuring Telnet SSH Parameters

To configure Telnet SSH (Secure Shell) parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Telnet SSH**.

The applied template is identified (if applicable). See the "Configuring Telnet SSH Templates" section on page 11-119 for more information.

The following parameters can be configured:

- Session Timeout—Indicates the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there will be no timeout. May be specified as a number from 0 to 160. The factory default is 5.
- Maximum Sessions—From the drop-down list choose a value from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed.

  Note New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service port.

- Allow New Telnet Sessions—Indicates that new Telnet sessions will not be allowed on the DS Port when set to no. The factory default value is no.

  Note New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service port.

- Allow New SSH Sessions—Indicates that new Secure Shell Telnet sessions will not be allowed when set to no. The factory default value is yes.

Step 4 After configuring the applicable parameters, click **Save**.

Configuring a Syslog for an Individual Controller

To enable a Syslog for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

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

The applied template is identified (if applicable). See the "Configuring Legacy Syslog Templates" section on page 11-120 for more information.

- **Syslog Enabled**—Select the check box to enable the syslog.

Step 4 Click **Save**.

Configuring Multiple Syslog Servers

For version 5.0.148.0 controllers or later, you can configure multiple (up to three) syslog servers on the WLAN controller. With each message logged, the controller sends a copy of the message to each configured syslog host, provided the message has severity greater than or equal to the configured syslog filter severity level.

To enable syslogs for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Multiple Syslog**.

The applied template is identified:

Syslog Server Address—Indicates the server address of the applicable syslog.

Step 4 Click **Save**.

Configuring WEB Admin

This section provides instructions for enabling the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Sockets Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You also have the option of downloading an externally generated certificate.

To enable WEB admin parameters for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Web Admin**.

The following parameters can be configured:

- Web Mode—Choose **Enable** or **Disable** from the drop-down list. When enabled, users can access the controller GUI using *http:ip-address*. The default is Disabled.

  Note Web mode is not a secure connection.

- Secure Web Mode—Choose **Enable** or **Disable** from the drop-down list. When enabled, users can access the controller GUI using *https://ip-address*. The default is Enabled.

  Note Secure web mode is a secure connection.

- Certificate Type
- Download Web Admin Certificate—Click to access the Download Web Admin Certificate to Controller page. See the "Download Web Auth or Web Admin Certificate to Controller" section on page 9-148 for additional information.

  Note The controller must be rebooted for the new Web Admin certificate to take effect.

Command Buttons

- Save
- Audit
- Regenerate Cert

Download Web Auth or Web Admin Certificate to Controller

To download a Web Auth or Web Admin Certificate to the controller, follow these steps:

Step 1 Click the **Download Web Admin Certificate** or **Download Web Auth Certificate** link.

Step 2 In the File is located on parameter, specify Local machine or TFTP server.

Note If the certificate is located on the TFTP server, enter the Server File Name. If it is located on the local machine, enter the Local File Name using the **Browse** button.

Step 3 Enter the TFTP server name in the **Server Name** parameter. The default is the NCS server.

Step 4 Enter the server IP address.

Step 5 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 6 In the Timeout text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 7 In the Local File Name text box, enter the directory path of the certificate.

Step 8 In the Server File Name text box, enter the name of the certificate.

Step 9 Enter the password in the Password text box.

Step 10 Click **OK**.

Configuring Local Management Users

This page lists the names and access privileges of the local management users.

To access the Local Management Users page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable IP address.

Step 3 From the left sidebar menu, choose **Management > Local Management Users**.

Step 4 Click a user name.

- User Name (read-only)—Name of the user.
- Access Level (read-only)—Read Write or Read Only.

Configuring Authentication Priority

In this page, you can control the order in which authentication servers are used to authenticate a controller management users.

To access the Authentication Priority page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an applicable 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**.

Command Buttons

- Save—Save the changes made to the management user authentication order and return to the previous page.
- Audit—Compare the NCS values with those used on the controller.

Configuring Location Configurations

In the Location Configuration page, you can configuration location parameters such as expiration times, notification interval, and other advanced configuration options.

You can set the following general and advanced parameters on the location template:

- General parameters—Enable RFID tag collection, set the location path loss for calibrating or normal (non-calibrating) clients, measurement notification for clients, tags, and rogue access points, set the RSSI expiry timeout value for clients, tags, and rogue access points.
- Advanced parameters–Set the RFID tag data timeout value and enable the location path loss configuration for calibrating client multi-band.

To configure location configurations for an individual controller, follow these steps:

Step 1 Choose **Configure > Controller**.

Step 2 Click an applicable IP address.

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

The Location Configuration page displays two tabs: General and Advanced.

Step 4 Add or modify the General parameters:

- RFID Tag Data Collection—Select the check box to enable the collection of data on tags.

  Before the location server can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command **config rfid status enable** on the controllers.

- Location Path Loss Configuration
  - Calibrating Client—Select the **Enabled** check box to enable calibration for the client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrate clients. Packets are transmitted on all channels. All access points gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic.

    Note To use all radios (802.11a/b/g/n) available, you must enable multiband in the Advanced page.

  - Normal Client—Select the **Enabled** check box to have a non-calibrating client. No S36 requests are transmitted to the client.

    Note S36 and S60 are client drivers compatible with specific Cisco Compatible Extensions. S36 is compatible with CCXv2 or later. S60 is compatible with CCXv4 or later. For details, see http://www.cisco.com/en/US/products/ps9806/products_qanda_item09186a0080af9513.shtml

- Measurement Notification Interval (in secs)
  - Tags, Clients, and Rogue APs/Clients—Allows you to set the NMSP measurement notification interval for clients, tags, and rogues. Specify how many seconds should elapse before notification of the found element (tags, clients, and rogue access points/clients).

    Setting this value on the controller generates an out-of-sync notification which you can view on the Synchronize Servers page. When different measurement intervals exist between a controller and the mobility services engine, the largest interval setting of the two is adopted by the mobility services engine.

    Once this controller is synchronized with the mobility services engine, the new value is set on the mobility services engine.

Note Synchronization to the mobility services engine is required if changes are made to measurement notification interval.

- RSS Expiry Timeout (in secs)
  - For Clients—Enter the number of seconds after which RSSI measurements for normal (non-calibrating) clients should be discarded.
  - For Calibrating Clients—Enter the number of seconds after which RSSI measurements for calibrating clients should be discarded.
  - For Tags—Enter the number of seconds after which RSSI measurements for tags should be discarded.
  - For Rogue APs—Enter the number of seconds after which RSSI measurements for rogue access points should be discarded.

Step 5 Add or modify the Advanced parameters:

- RFID Tag Data Timeout (in secs)—Enter a value (in seconds) to set the RFID tag data timeout setting.
- Location Path Loss Configuration
  - Calibrating Client Multiband—Select the **Enabled** check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enable in the general page.

Note To use all radios (802.11a/b/g/n) available, you must enable multiband.

Step 6 Click **Save**.

Command Buttons

- Save—Save the changes made to the management user authentication order and return to the previous page.
- Audit—Compare the NCS values with those used on the controller.uld be discarded.

Configuring Access Points

This section describes how to configure access points in the Cisco NCS database. This section contains the following topics:

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 a saturation point and reject some of the access points.

By assigning priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is saturated, the higher priority access points are allowed to join the backup controller by disjoining the lower priority access points.

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

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address of the applicable controller.

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

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

To configure an access point's priority, see the "Configuring Access Point Details" section on page 9-164.

Configuring Global Credentials for Access Points

Cisco autonomous access points are shipped from the factory with *Cisco* as the default enable password. This password allows users to log into the non-privileged mode and execute show and debug commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the access point's console port.

In NCS and controller software releases prior to 5.0, you can set the access point enable password only for access points that are currently connected to the controller. In NCS and controller software release 5.0, you can set a global username, password, and enable password that all access points inherit as they join a controller. This includes all access points that are currently joined to the controller and any that join in the future. When you are adding an access point, you can also choose to accept this global

username and password or override it on a per-access point basis and assign a unique username, password, and enable password. See the "Configuring AP Configuration Templates" section on page 11-127 to see where the global password is displayed and how it can be overridden on a per-access point basis.

Also in controller software release 5.0, after an access point joins the controller, the access point enables console port security, and you are prompted for your username and password whenever you log into the access point's console port. When you log in, you are in non-privileged mode, and you must enter the enable password in order to use the privileged mode.

Note These controller software release 5.0 features are supported on all access points that have been converted to lightweight mode, except the 1100 series. VxWorks access points are not supported.

The global credentials that you configure on the controller are retained across controller and access point reboots. They are overwritten only if the access point joins a new controller that is configured with a global username and password. If the new controller is not configured with global credentials, the access point retains the global username and password configured for the first controller.

Note You need to keep careful track of the credentials used by the access points. Otherwise, you might not be able to log into an access point's console port. If necessary, you can clear the access point configuration to return the access point username and password to the default setting.

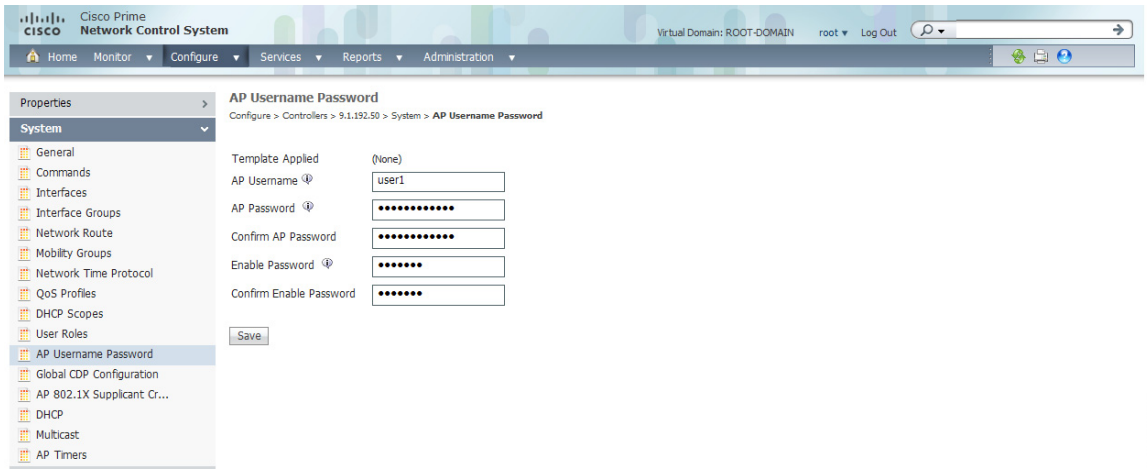
To establish a global username and password, follow these steps:

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

Step 2 Choose an IP address of a controller with software release 5.0 or later or choose an access point associated with software release 5.0 or later.

Step 3 Choose **System > AP Username Password** from the left sidebar menu. The AP Username Password page appears (see Figure 9-15).

Figure 9-15 AP Username Password Page



Step 4 In the AP Username text box, enter the username that is to be inherited by all access points that join the controller.

Step 5 In the AP Password text box, enter the password that is to be inherited by all access points that join the controller. Re-enter in the Confirm AP Password text box.

Step 6 For Cisco autonomous access points, you must also enter and confirm an enable password. In the AP Enable Password text box, enter the enable password that is to be inherited by all access points that join the controller. Re-enter in the Confirm Enable Password text box.

Step 7 Click **Save**.

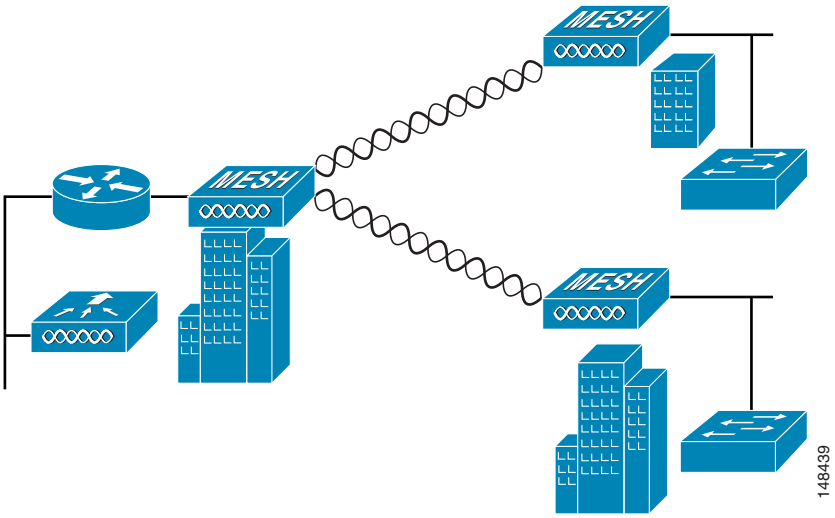
Configuring Ethernet Bridging and Ethernet VLAN Tagging

Ethernet bridging is used in two mesh network scenarios:

1. Point-to-point and point-to-multipoint bridging between MAPs (untagged packets). A typical trunking application might be bridging traffic between buildings within a campus (see Figure 9-16).

Note You do not need to configure VLAN tagging to use Ethernet bridging for point-to-point and point-to-multipoint bridging deployments.

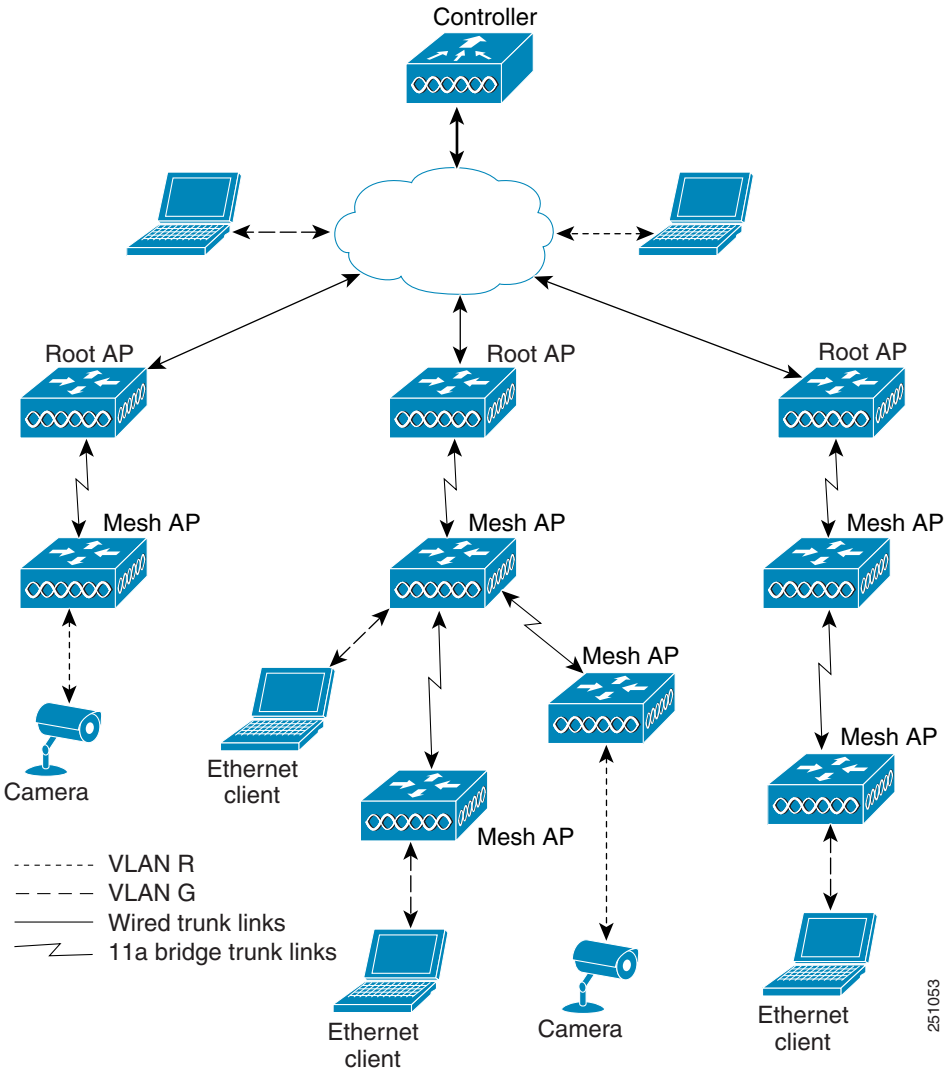
Figure 9-16 Point-to-Multipoint Bridging



2. Ethernet VLAN tagging allows specific application traffic to be segmented within a wireless mesh network and then forwarded (bridged) to a wired LAN (access mode) or bridged to another wireless mesh network (trunk mode).

A typical public safety access application using Ethernet VLAN tagging is placement of video surveillance cameras at various outdoor locations within a city. Each of these video cameras has a wired connection to a MAP. The video of all these cameras is then streamed across the wireless backhaul to a central command station on a wired network (see Figure 9-17).

Figure 9-17 Ethernet VLAN Tagging



Ethernet VLAN Tagging Guidelines

- For security reasons, the Ethernet port on a mesh access point (RAP and MAP) is disabled by default. It is enabled by configuring Ethernet Bridging on the mesh access point port.
- You must enable Ethernet bridging on all the access points in the mesh network to allow Ethernet VLAN Tagging to operate.
- You must set VLAN Mode as non-VLAN transparent (global mesh parameter). See the "Configuring Ethernet Bridging and Ethernet VLAN Tagging" section on page 9-154.
  - VLAN transparent is enabled by default. To set as non-VLAN transparent, you must unselect the VLAN transparent option in the Global Mesh Parameters page.
- VLAN configuration on a mesh access point is only applied if all the uplink mesh access points are able to support that VLAN.

  - If uplink access points are not able to support the VLAN, then the configuration is stored rather than applied.
- VLAN tagging can only be configured on Ethernet interfaces.
  - On 152x mesh access points, use three of the four ports as *secondary Ethernet interfaces*: *port 0-PoE in, port 1-PoE out, and port 3- fiber.* You cannot configure *Port 2 - cable* as a secondary Ethernet interface.
  - In Ethernet VLAN tagging, *port 0-PoE in* on the RAP connects the trunk port of the switch of the wired network. *Port 1-PoE out* on the MAP connects external devices such as video cameras.
- Backhaul interfaces (802.11a radios) act as *primary Ethernet interfaces*. Backhauls function as trunks in the network and carry all VLAN traffic between the wireless and wired network. You are not required to configure the primary Ethernet interface.
- You must configure the switch port in the wired network that is attached to the RAP (*port 0–PoE in*) to accept tagged packets on its trunk port. The RAP forwards all tagged packets received from the mesh network to the wired network.
- Configuration to support VLAN tagging on the 802.11a backhaul Ethernet interface is not required within the mesh network.
  - This includes the RAP uplink Ethernet port. The required configuration happens automatically using a registration mechanism.
  - Any configuration changes to an 802.11a Ethernet link acting as a backhaul are ignored, and a warning results. When the Ethernet link no longer functions as a backhaul, the modified configuration is applied.
- You cannot configure VLANs on port-02-cable modem port of a 152x access point. Configure VLANs on ports 0 (PoE-in), 1 (PoE-out), and 3 (fiber).
- If bridging between two MAPs, enter the distance (mesh range) between the two access points that are bridging. (Not applicable to applications in which you are forwarding traffic connected to the MAP to the RAP, access mode.)
- Each sector supports up to 16 VLANs; therefore, the cumulative number of VLANs supported by a RAP's children (MAPs) cannot exceed 16.
- Ethernet ports on access points function as *normal*, *access,* or *trunk* ports in an Ethernet tagging deployment.
  - Normal mode–In this mode, the Ethernet interface is VLAN-transparent by default and does not accept or send any tagged packets. Tagged frames from clients are dropped. Untagged frames are forwarded to the native VLAN on the RAP trunk port.
  - Access mode–In this mode only untagged packets are accepted. You must tag all packets with a user-configured VLAN called access-VLAN. For this mode to take effect, the global VLAN mode should be non-VLAN transparent.

    Use this option for applications in which information is collected from devices connected to the MAP such as cameras or PCs and then forwarded to the RAP. The RAP then applies tags and forwards traffic to a switch on the wired network.
  - Trunk mode—This mode requires the user to configure a native VLAN and an allowed VLAN list (no defaults). In this mode, both tagged and untagged packets are accepted. You can accept untagged packets and tag them with the user-specified native VLAN. You can accept tagged packets if they are tagged with a VLAN in the allowed VLAN list. For this mode to take effect, the global VLAN mode should be non-VLAN transparent.

    Use this option for bridging applications such as forwarding traffic between two MAPs resident on separate buildings within a campus.

- The switch port connected to the RAP must be a trunk.
  - The trunk port on the switch and the RAP trunk port must match.
- A configured VLAN on a MAP Ethernet port cannot function as a Management VLAN.
- The RAP must always connect to the native VLAN (ID 1) on a switch.
  - The RAP's primary Ethernet interface is by default the native VLAN of 1.

Enabling Ethernet Bridging and VLAN Tagging

To enable Ethernet Bridging and VLAN tagging on a RAP or MAP, follow these steps:

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

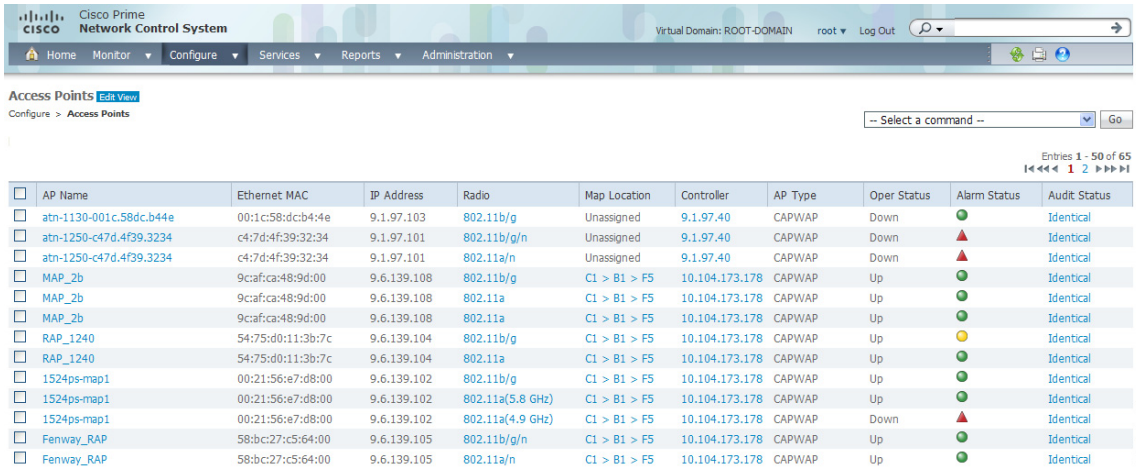
Step 2 Click the name of the mesh access point for which you want to enable Ethernet bridging. A configuration page for the access point appears.

Step 3 In the Bridging Information section, choose the appropriate backhaul rate from the Data Rate drop-down list. The default value is 24 Mbps for the 802.11a backhaul interface.

Step 4 In the Bridging Information section, choose **Enable** from the Ethernet Bridging drop-down list.

Step 5 Click the appropriate Ethernet interface link (such as FastEthernet or gigabitEthernet1). (See Figure 9-18.)

Figure 9-18 Configure > Access Points > AP Name Page



Step 6 Within the Ethernet interface page, perform one of the following:

Note The configuration options vary for each of the VLAN modes (normal, access, and trunk).

a. If you are configuring a MAP and RAP normal ports and chose FastEthernet0, choose **Normal** from the VLAN Mode drop-down list.

In this mode, the Ethernet interface is VLAN-transparent by default and does not accept or send any tagged packets. Tagged frames from clients are dropped. Untagged frames are forwarded to the native VLAN on the RAP trunk port.

b. If you are configuring a MAP access port and chose **gigabitEthernet1** (port 1-PoE out),

1. Choose **Access** from the VLAN Mode drop-down list.
2. Enter a VLAN ID. The VLAN ID can be any value between 1 and 4095.
3. Click **Save**.

Note VLAN ID 1 is not reserved as the default VLAN.

Note A maximum of 16 VLANs in total are supported across all of a RAP's subordinate MAPs.

c. If you are configuring a RAP or MAP trunk port and chose **gigabitEthernet0** (or **FastEthernet0**) (port 0-PoE in),

1. Choose **trunk** from the VLAN Mode drop-down list.
2. Enter a native VLAN ID for *incoming* traffic. The native VLAN ID can be any value between 1 and 4095. Do not assign any value assigned to a user-VLAN (access).
3. Enter a trunk VLAN ID for *outgoing* traffic, and click **Add**.

   The added trunk appears in the summary column of allowed VLAN IDs.

   If forwarding *untagged* packets, do not change the default trunk VLAN ID value of zero (such as MAP-to-MAP bridging, campus environment).

   If forwarding *tagged* packets, enter a VLAN ID (1 to 4095) that is not already assigned (such as RAP to switch on wired network).

Note To remove a VLAN from the list, click **Delete**.

4. Click **Save**.

Note At least one mesh access point must be set to RootAP in the mesh network.

Autonomous to Lightweight Migration Support

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

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

You may also choose to convert autonomous access points to lightweight. Once an access point is converted to lightweight, the previous status or configuration of the access point is not retained.

From NCS, the following functions are available when managing autonomous access points:

- Adding Autonomous Access Points to NCS, page 9-159
- Viewing Autonomous Access Points in NCS, page 9-163
- Adding and viewing autonomous access points from the Monitor > Maps page (see the "Monitoring Maps" section on page 6-1 for more information)
- Monitoring associated alarms
- Performing an autonomous access point background task
  - Checks the status of autonomous access points managed by NCS.
  - Generates a critical alarm when an unreachable autonomous access point is detected.
- Running reports on autonomous access points
  - See Reports > Inventory Reports and Reports > Client Reports > Client Count for more information
- Supporting Autonomous Access Points in Work Group Bridge (WGB) mode, page 9-164
- Migrating a Autonomous Access Point to a Lightweight Access Point, page 11-138

Adding Autonomous Access Points to NCS

From NCS, the following methods are available for adding autonomous access points:

- Adding Autonomous Access Points by Device Information, page 9-159 (IP addresses and credentials).
- Adding Autonomous Access Points by CSV File, page 9-160.
- Removing Autonomous Access Points, page 9-162

Adding Autonomous Access Points by Device Information

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

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

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

Step 2 From the Select a command drop-down list, 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 autonomous access points.

Step 6 Enter the SNMP Parameters parameters:

- Version—Choose from v1, v2, or v3.
- Retries—Indicates the number of controller discovery attempts.
- Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The valid range is 2 to 90 seconds. The default is 10 seconds.
- Community—Public or Private.

Step 7 Enter the Telnet/SSH Parameters:

Note Default values are used if the Telnet/SSH parameters are left blank.

- Protocol—Select the protocol you want to use (either Telenet or SSH).
- User Name—Enter the user name. (Default username is admin.)

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

- Password/Confirm Password—Enter and confirm the password. (Default password is admin.)
- Enable Password/Confirm Password—Enter and confirm an enable password.
- Telnet Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The default is 60 seconds.

Note Cisco autonomous access points are shipped from the factory with *Cisco* as the default enable password. This password allows users to log into the non-privileged mode and execute show and debug commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the access point's console port.

Step 8 Click **Add**.

Note After the AP is added and it's inventory collection is completed, it will appear in Access Point list page (Configure > Access Points). If it is not found in the Access Points list, choose Configure > Unknown Device page to check the status. For details, see the "Configuring Unknown Devices" section on page 9-199.

Note Autonomous access points are not counted towards the total device count for your license.

Adding Autonomous Access Points by CSV File

Autonomous access points can be added to NCS 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 list, 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.

The sample CSV files for V2 devices are as follows:

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name,
snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password,
snmp_retries, snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v2,public,,,,,3,4
209.165.201.0,255.255.255.0,v2,public,,,,,3,4,Cisco,Cisco,2,10
```

Note The SNMP, telnet, or SSH credentials are mandatory.

The sample CSV files for V3 devices are as follows:

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type,
snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4
209.165.201.0,255.255.255.224,v3,default1,HMAC-MD5,default1,DES,default1,3,4,Cisco,Cisco,2
,10
```

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- telnet_username
- telnet_password
- enable_password
- telnet_retries
- telnet_timeout

Step 6 Click **OK**.

Bulk Update of Autonomous Access Points

You can update multiple autonomous access points credentials by importing a CSV file.

To update autonomous access point(s) information in a bulk, follow these steps:

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

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

Step 3 From the Select a command drop-down list, choose **Bulk Update APs**. The Bulk Update Autonomous Access Points page appears.

Step 4 Click **Choose File** to select a CSV file, and then find the location of the CSV file you want to import.

Step 5 Click **Update and Sync**.

Sample CSV File for the Bulk Update of Autonomous Access Points

The sample CSV files for V2 devices are as follows:

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name,
snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password,
snmp_retries, snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v2,public,,,,,3,4
209.165.201.0,255.255.255.0,v2,public,,,,,3,4,Cisco,Cisco,2,10
```

Note The SNMP, telnet, or SSH credentials are mandatory.

The sample CSV files for V3 devices are as follows:

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type,
snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4
209.165.201.0,255.255.255.224,v3,default1,HMAC-MD5,default1,DES,default1,3,4,Cisco,Cisco,2
,10
```

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- telnet_username
- telnet_password
- enable_password
- telnet_retries
- telnet_timeout

Removing Autonomous Access Points

To remove an autonomous access point from NCS, follow these steps:

Step 1 Select the check boxes of the access points you want to remove.

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

Viewing Autonomous Access Points in NCS

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 the following:

- 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.

Downloading Images to Autonomous Access Points (TFTP)

Lightweight access point images are bundled with controller images and managed by the controller. Autonomous access point images must be handled by a NMS system such as WLSE, CiscoWorks, or NCS.

To download images to autonomous access points (using TFTP), follow these steps:

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

Step 2 Select the check box of the autonomous access point to which you want to download an image. The AP Type column displays whether the access point is autonomous or lightweight.

Step 3 From the Select a command drop-down list, choose **Download Autonomous AP Image (TFTP)**. The Download images to Autonomous APs page appears.

Step 4 Specify the following parameters:

- File is located on—Choose **Local machine** or **TFTP server**.
- Server Name—Select the Default Server or add a New server using the Server Name drop-down list.
- IP address—Specify the TFTP server IP address. This is automatically populated if the default server is selected.
- NCS Server Files In—Specify where the NCS server files are located. This is automatically populated if the default server is selected.
- Server File Name—Specify the Server File Name.

Step 5 Click **Download**.

Tip Some TFTP servers may not support files larger than 32 MB

Downloading Images to Autonomous Access Points (FTP)

To download images to autonomous access points (using FTP), follow these steps:

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

Step 2 Select the check box of the autonomous access point to which you want to download an image. The AP Type column displays whether the access point is autonomous or lightweight.

Step 3 From the Select a command drop-down list, choose **Download Autonomous AP Image (FTP)**. The Download images to Autonomous APs page appears.

Step 4 Enter the FTP credentials including username and password.

Step 5 Specify the following parameters:

- File is located on—Choose **Local machine** or **FTP server**.
- Server Name—Select the Default Server or add a New server using the Server Name drop-down list.
- IP address—Specify the FTP server IP address. This is automatically populated if the default server is selected.
- NCS Server Files In—Specify where the NCS server files are located. This is automatically populated if the default server is selected.
- Server File Name—Specify the Server File Name.

Step 6 Click **Download**.

Supporting Autonomous Access Points in Work Group Bridge (WGB) mode

Workgroup Bridge (WGB) mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The WGB and its wired clients are listed as client in NCS if the AP mode is set to Bridge, and the access point is bridge capable.

To view a list of all NCS clients that are WGBs, choose **Monitor > Clients**. From the Show drop-down list, choose **WGB Clients**, and click **Go**. The Clients (detected as WGBs) page appears. Click a User to view detailed information regarding a specific WGB and its wired clients.

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

Configuring Access Point Details

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

- Ethernet MAC
- IP Address
- Radio
- Map Location

- AP Type
- Controller
- Operation Status
- Alarm Status
- Audit Status

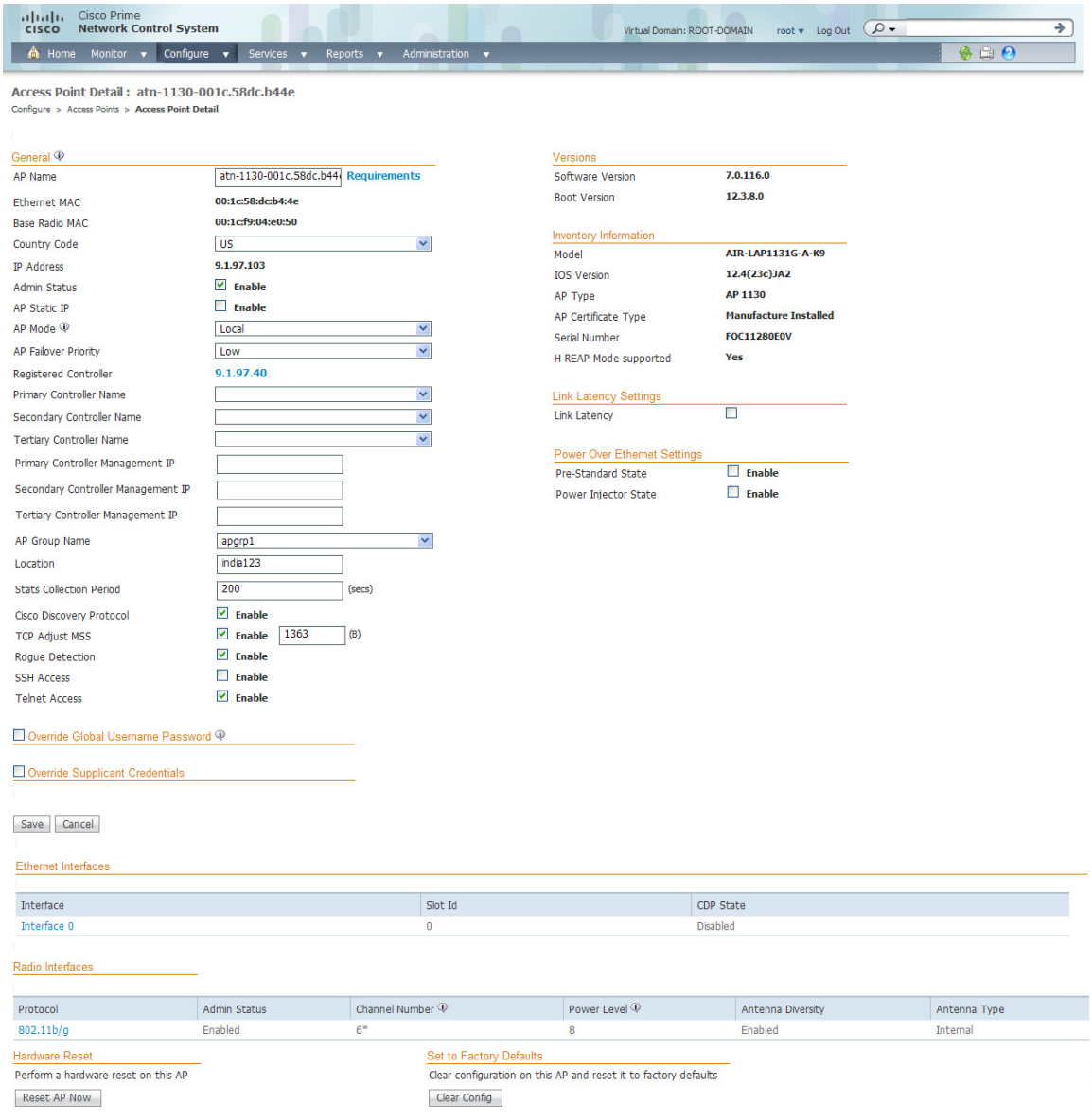
Note If you hover your mouse cursor over the Audit Status value, the time of the last audit is displayed.

Note You cannot configure the Cisco 600 Series Access Points from the this page. It can be configured from the AP Configuration Templates page only. For details on configuring AP Configuration Templates, see "Configuring AP Configuration Templates" section on page 11-127.

Step 1 Click the link under AP Name to see detailed information about that access point name. The Access Point Detail page appears (see Figure 9-19).

Figure 9-19 Detailed Access Point Information

.



Note The operating system software automatically detects and adds an access point to the Cisco NCS database as it associates with existing controllers in the Cisco NCS database.

Note Access point parameters may vary depending on the access point type.

Some of the parameters on the page are automatically populated.

- The General portion displays the Ethernet MAC, the Base Radio MAC, IP Address, and status.
- The Versions portion of the page displays the software and boot version.

- The Inventory Information portion displays the model, AP type, AP certificate type, serial number, and REAP mode support.
- The Ethernet Interfaces portion provides information such as interface name, slot ID, admin status, and CDP state.
- 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.

To set the configurable parameters, follow these steps:

Note Changing access point parameters causes the access point to be temporarily disabled and this may cause some clients to lose connectivity.

Step 2 Enter the name assigned to the access point.

Step 3 Use the drop-down list 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, see this location:

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

Step 4 If you want to enable the access point for administrative purposes, select the **Enable** check box.

Step 5 If you click **Enable** 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 6 Choose the role of the access point from the AP Mode drop-down list. No reboot is required after the mode is changed *except* when monitor mode is selected. You are notified of the reboot when you click **Save**. 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.

- H-REAP—Choose **HREAP** from the AP Mode drop-down list to enable Hybrid REAP for up to six access points. The H-REAP access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

Note To configure Local or HREAP access points for Cisco Adaptive wIPS feature, choose Local or HREAP, and select the **Enhanced wIPS Engine Enabled** check box.

- 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.

Note You can expand the monitor mode for tags to include location calculation by enabling the tracking optimized monitor mode (TOMM) feature. When TOMM is enabled, you can specify which four channels within the 2.4 GHz band (802.11b/g radio) of an access point to use to monitor tags. This allows you to focus channel scans on only those channels for which tags are traditionally found (such as channels 1, 6, and 11) in your network. To enable TOMM, you must also make additional edits on the 802.11b/g radio of the access point. See the "Configuring Access Point Radios for Tracking Optimized Monitor Mode" section on page 9-184 for configuration details.

Note You cannot enable both TOMM and wIPS at the same time. TOMM can be enabled only when wIPS is disabled.

Note To configure access points for Cisco Adaptive wIPS feature, choose **Monitor** and select the **Enhanced wIPS Engine Enabled** check box, and select **wIPS** from the Monitor Mode Optimization drop-down list.

- 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—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 www.wildpackets.com.
- Bridge—Bridge mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The bridge and its wired clients are listed as client in NCS if the AP mode is set to Bridge, and the access point is bridge capable.
- SE-Connect—This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.

Note This option is displayed only if the access point is CleanAir-capable.

Note Changing the AP mode reboots the access point.

Step 7 Disable any access point radios.

Step 8 From the AP Failover Priority drop-down list, choose Low, Medium, High, or Critical to indicate the access point's failover priority. The default priority is low. See the "Setting AP Failover Priority" section on page 9-152 for more information.

Step 9 In the Primary, Secondary, and Tertiary Controller fields, you can define the order in which controllers are accessed.

Step 10 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.

Note An access point group name to 31 characters for WLC versions earlier than 4.2.132.0 and 5.0.159.0.

Step 11 Enter a description of the physical location where the access point was placed.

Step 12 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 13 Choose **Enable** 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 14 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, causing those receiving access points which were configured to detect MFP frames to 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 15 Select 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 16 Select the check box to enable rogue detection. See the "Rogue Access Point Location, Tagging, and Containment" section on page 3-13 for more information on rogue detection.

Note Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see the *Cisco Wireless LAN Controller Configuration Guide*.

Step 17 Select the **Encryption** check box to enable encryption.

Note Enabling or disabling encryption functionality causes the access point to reboot, which then causes clients to lose connectivity.

Note DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security, but disabled by default for all other access points.

Note Cisco 5500 controllers can be loaded with one of the two types of images, AS_5500_LDPE_x_x_x_x.aes or AS_5500_x_x_x_x.aes. For the 5500 controller loaded with former image, you need to have DTLS License to show encryption.

Note For WiSM2 and 2500 controllers, it is mandatory to have DTLS license to show encryption.

Step 18 If rogue detection is enabled, 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.

Step 19 Select the **SSH Access** check box to enable SSH access.

Step 20 Select the **Telnet Access** check box to enable Telnet access.

Note An OfficeExtend access point may be connected directly to the WAN which could allow external access if the default password is used by the access point. Therefore, Telnet and SSH access are disabled automatically for OfficeExtend access points.

Step 21 If you want to override credentials for this access point, select the **Override Global Username Password** check box. You can then enter a new supplicant AP username, AP password, and Enable password that you want to assign for this access point.

Note On the System > AP Username Password page, you can set global credentials for all access points to inherit as they join a controller. These established credentials appear in the lower right of the AP Parameters tab page.

The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

Step 22 Select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. See the "Configuring Link Latency Settings for Access Points" section on page 9-203 for more information on link latency.

Step 23 You can now manipulate power injector settings through NCS without having to go directly to the controllers. In the Power Over Ethernet Settings section, select the check box to enable pre-standard or power injector state.

Pre-standard is chosen if the access point is powered by a high power Cisco switch; otherwise, it is disabled. If power injector state is selected, power injector options appear. The possible values are installed or override. If you choose override, you can either enter a MAC address or leave it empty so that it is supplied by WLC.

Note To determine which source of power is running NCS, go to **Monitor > Access Points**, click **Edit View**, and then choose and move POE Status to the View Information box. After you click **Submit**, the POE status appears in the last column. If the device is powered by an injector, the POE status appears as Not Applicable.

Step 24 Select the **Enable** check box to enable the following H-REAP configurations:

Note H-REAP settings cannot be changed when the access point is enabled.

- OfficeExtend AP—The default is Enabled.

  Note Unselecting the check box simply disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point, but it does put the access point at risk since it becomes remotely deployed. If you want to clear the access point's configuration and return it to factory default settings, click **Clear Config** at the bottom of the access point details page. If you want to clear only the access point's personal SSID, click Reset Personal SSID at the bottom of the access point details page.

When you select Enabled for the OfficeExtend AP, a warning message provides the following information:

- Configuration changes that automatically occur. Encryption and Link Latency are enabled. Rogue Detection, SSH Access, and Telnet Access are disabled.
- A reminder to configure at least one primary, secondary, and tertiary controller (including name and IP address).

Note Typically, an access point first looks for the primary controller to join. After that, the controller tries the secondary and then the tertiary controller. If none of these controllers are configured, the access point switches to a default discovery mode in an attempt to join whatever controller it may find.

An OfficeExtend access point searches only for a primary, secondary, or tertiary controller to join. It does not look any further for a configured controller. Because of this, it is important that you configure at least one primary, secondary, or tertiary controller name and IP address.

  - A warning the enabling encryption causes the access point to reboot and causes clients to lose connectivity.

- Least Latency Controller Join—When enabled, the access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.

Note The access point only performs this search once when it initially joins the controller. It does not recalculate the primary, secondary, and tertiary controllers' latency measurements once joined to see if the measurements have changed.

- Enable VLAN—When selected, enter the Native VLAN identifier.

  When Enable VLAN is selected, NCS displays locally switched VLANs.

Step 25 Select the role of the mesh access point from the Role drop-down list. 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 26 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 appears 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 27 Select the data rate for the backhaul interface from the drop-down list. 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 28 Choose **Enable** from the Ethernet Bridging drop-down list to enable Ethernet bridging for the mesh access point.

Step 29 Click **Save** to save the configuration.

Step 30 Re-enable the access point radios.

Step 31 If you need to reset this access point, click **Reset AP Now**.

Step 32 Click **Reset Personal SSID** to reset the OfficeExtend access point personal SSID to the factory default.

Step 33 If you need to clear the access point configuration and reset all values to the factory default, click **Clear Config**.

Configuring an Ethernet Interface

Note The 152x mesh access points are configured on any one of these four ports: port 0-PoE in, port 1-PoE out, Port 2 - cable, and port 3- fiber. Other APs (such as 1130,1140,1240,1250) are configured on Port 2 - cable.

To configure an Ethernet interface, follow these steps:

Step 1 Choose Configure > Access Points.

Step 2 Click the link under AP Name to see detailed information about that access point name. The Access Point Detail page appears.

Note The Access Point Details page displays the list of Ethernet interfaces.

Step 3 Click the link under Interface to see detailed information about that interface. The Ethernet Interface page appears.

This page displays the following parameters:

- AP Name—The name of the access point.
- Slot Id—Indicates the slot number.
- Admin Status—Indicates the administration state of the access point.
- CDP State—Select the CDP State check box to enable the CDP state.

Step 4 Click **Save**.

Importing AP Configuration

To import a current access point configuration file, follow these steps:

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

Step 2 From the **Select a command** drop-down list, choose **Import AP Config**.

A pop-up aleart box appears stating All Unified AP(s) are imported from CSV file only. Unified AP(s) from Excel and XML file are not imported.

Step 3 Click **OK** to close the pop-up alert box.

Step 4 Click **Go**.

Step 5 Enter the CSV file path in the text box or use the Browse button to navigate to the CSV file on your computer.

The first row of the CSV file is used to describe the columns included. The AP Ethernet Mac Address column is mandatory. The parameters on the page will be used for columns not defined in the CSV file.

Sample File Header:

ethernetMac,apName,location,primaryController,secondaryController,tertiaryController

00:1c:58:74:8c:22, ap-1, sjc-14-a, controller-4404-1, controller-4404-2, controller-4404-3

- ethernetMac—Access point ethernet MacAddress
- apName—Access point name
- location—Access point location
- primaryController—Primary Controller
- secondaryController—Secondary Controller
- tertiaryController—Tertiary Controller

The CSV file can contain following fields:

- AP Ethernet MacAddress—Mandatory
- AP Name—Optional
- Location—Optional
- Primary Controller—Optional
- Secondary Controller—Optional
- Tertiary Controller—Optional

Note Optional fields can remain empty. The AP Config Import ignores empty optional field values. However, if primaryMwar and secondaryMwar entries are empty then a unified access point update is not complete.

Step 6 When the appropriate CSV file path appears in the Select CSV File text box, click **OK**.

Exporting AP Configuration

To export current access point configuration files, follow these steps:

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

Step 2 From the **Select a command** drop-down list, choose **Export AP Config**.

A pop-up alert box appears stating All Unified AP(s) are exported to CSV/EXCEL/XML file.

Step 3 Click **OK** to close the pop-up alert box.

Step 4 Click **Go** to view the current AP configurations including:

- apName
- ethernetMac
- location
- primaryController
- secondaryController
- tertiaryController

Step 5 Select the file option (CSV, Excel, XML) to export the access point configurations.

Step 6 In the File Download window, click **Save** to save the file.

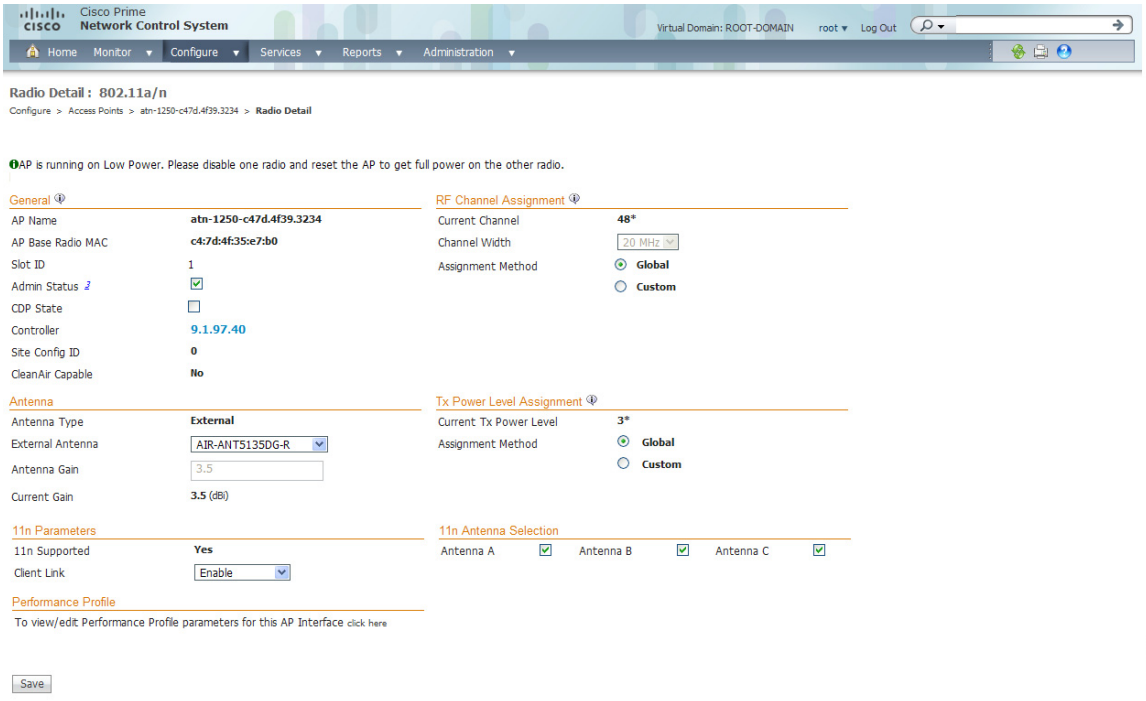
Configuring Access Points 802.11n Antenna

NCS provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

Note At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

If you choose **Configure > Access Points** and select an **802.11n** item from the Radio column, the following page appears (see Figure 9-20).

Figure 9-20 Access Point > 802.11a/n



The following 11n Parameters display and can be modified:

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

General

- AP Name—The operator-defined name of the access point.
- AP Base Radio MAC—MAC address of the access point's base radio.
- Admin Status—Select the box to enable the administration state of the access point.
- CDP State—Select the CDP State check box to enable CDP.
- Controller—IP address of the controller. Click the controller's IP address for more details.
- Site Config ID—Site identification number.
- CleanAir Capable—Displays if the access point is CleanAir capable.
- CleanAir—Select the check box to enable CleanAir.

Antenna

- Antenna Type—Indicates an external or internal antenna.
- Antenna Diversity—Select Right, Left, or Enabled.

  Note Antenna diversity refers to the Cisco Aironet access point feature where an access point samples the radio signal from two integrated antenna ports and choose the preferred antenna. This diversity option is designed to create robustness in areas with multi-path distortion.

  For external antenna, select one of the following:

  - Enabled—Use this setting to enable diversity on both the left and right connectors of the access point.
  - Left—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector.
  - Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector.

  For internal antennas, select one of the following:

  - Enabled—Use this setting to enable diversity on both Side A and Side B.
  - Side A—Use this setting to enable diversity on Side A (front antenna) only.
  - Side B—Use this setting to enable diversity on Side B (rear antenna) only.
- External Antenna—Select the external antenna or Other from the drop-down list.
- Antenna Gain—Enter the desired antenna gain in the text box.

  Note The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.

- Current Gain (dBm)—Indicates the current gain in dBm.

Table 9-4 lists the antenna names, gain, and descriptions.

Table 9-4 Antenna Names, Gain, and Descriptions

Antenna Name	Gain (dBi)	Description
AIR-ANT1000	0.00	AP 1000 Integrated antenna
CUSH-S5157WP	3.00	5.15-5.87 GHz diversity wideband panel antenna (side gain and back attenuation)
KODIAK-DIRECTIONAL	8.00	Integrated Kodiak directional antenna
KODIAK-OMNI	5.00	Kodiak omni antenna
AIR-ANT1728	5.20	Omni ceiling mount antenna
AIR-ANT1729	6.00	Patch wall mount antenna
AIR-ANT2012	6.50	Diversity patch wall mount antenna
AIR-ANT2410Y-R	10.00	Yagi master or wall mount antenna
AIR-ANT5959	2.00	Omni diversity ceiling mount antenna
AJAX-OMNI	5.00	Integrated Ajax omni antenna
AIR-ANT5135D-R	3.50	Omni dipole antenna
AIR-ANT5135DW-R	3.50	3.5-dBi white dipole antenna
AIR-ANT5135DG-R	3.50	3.5 dB5 gray non-articulating dipole antenna
AIR-ANT2422DW-R	2.20	2.2-dBi white dipole antenna
AIR-ANT2422DB-R	2.20	Omni dipole antenna
AIR-ANT2422DG-R	2.20	2.2 dBi gray non-articulating dipole antenna
AIR-ANT5145V-R	4.50	Omni diversity antenna
AIR-ANT5160V-R	6.00	Omni antenna
AIR-ANT3549	9.00	Patch wall mount antenna
AIR-ANT4941	2.20	Omni dipole antenna
AIR-ANT2506	0.00	Omni mass mount antenna
AIR-ANT3213	5.20	Omni diversity pillar antenna
CUSH-S24516DBP	3.00	Integrated 2.4/5 GHz hemispheric pattern
CUSH-S5153WBPX	6.00	Ceiling mount 6-dBi omni
AIR-ANT5170V-R	7.00	Wall mount diversity patch antenna
AIR-ANT5175V	7.50	Omni antenna for Wireless Bridge
AIR-ANT5195V-R	9.50	Wall mount patch antenna
AIR-ANT58G10SSA	9.50	Sector antenna for Wireless Bridge
AIR-ANT2455V	5.50	Omni antenna for Wireless Bridge
CUSH-S54717P	17.00	Patch array antenna for Wireless Bridge
CUSH-S49014WP	14.00	Patch array antenna for Wireless Bridge
CUSH-S2406BP	8.00	Omni antenna for Wireless Bridge
AIR-ANT1100	2.20	Default antenna for AP1100

Table 9-4 Antenna Names, Gain, and Descriptions (continued)

Antenna Name	Gain (dBi)	Description
BR1310	13.00	Integrated patch directional antenna
AIR-ANT2460	6.00	Patch wall mount antenna
AIR-ANT2465	6.50	Diversity patch wall mount antenna
AIR-ANT2485	9.00	Patch wall mount antenna
AIR-ANT2480V-N	8.00	2.4 GHz omni antenna for mesh
AIR-ANT5114P-N	14.00	5 GHz patch for mesh
AIR-ANT5117S-N	17.00	5 GHz sector for mesh
AIR-ANT2450V-N	5.00	2.4 GHz omni antenna
AIR-ANT5180V-N	8.00	5 GHz omni antenna
AIR-ANT2450S-R	5.50	2.4 GHz 135-degree sector antenna
AIR-ANT2451V-R	2.4 GHz—2.0 5 GHz—3.0	2.4 GHz and 5 GHz four-element dual band antenna. **Note** Two elements for the 2.4 GHz band and two elements for the 5 GHz band.
AIR-ANT2460NP-R	6.00	2.4 GHz MIMO (3-Element) Patch Antenna
AIR-ANT5160NP-R	6.00	5 GHz MIMO (3-Element) Patch Antenna
AIR-ANT2422SDW-R	2.20	2.4 GHz “Stubby” white monopole antenna
AIR-ANT5135SDW-R	3.50	5 GHz "Stubby" white monopole antenna
AIR-ANT2451NV-R	2.4 GHz—2.5 5 GHz—3.5	2.4 GHz and 5 GHz “6-pack” ceiling mount omni antenna
AIR-ANT2452V-R	5.2	2.4 GHz Diversity Wall Mount Omni-directional Antenna **Note** This is a replacement antenna to the existing AIR-ANT3213.
AIR-ANT24020V-R	2.0	External omni diversity ceiling mount antenna **Note** This is a replacement antenna to the existing antenna AIR-ANT5959.
AIR-ANT5140V-R	4.0	Omni antenna w/RP-TNC connectors(3)
AIR-ANT2430V-R	3.0	Omni antenna w/RP-TNC connectors(3)
AIR-ANT1949	2.4 GHz—13.5	External antenna
AIR-ANT2440NV-R	4.0	2.4 GHz MIMO Wall Mount Antenna
AIR-ANT5140NV-R	4.0	5 GHz MIMO Wall Mount Antenna
AIR-ANT2460P-R	6.0	Grayling Patch Antenna
AIR-ANT2485P-R	8.5	Grayling Patch Antenna
AIR-ANT2547V-N	2.4 GHz—4.0 5 GHz—7.0	2.4 GHz and 5 GHz dual band Omni-directional Antenna.
Internal-802.11	2	Internal AP802 Antenna

Table 9-4 Antenna Names, Gain, and Descriptions (continued)

Antenna Name	Gain (dBi)	Description
Internal-602i	2.4 GHz—4	Internal omni antenna
Internal-602i	5.0 GHz—4	Internal omni antenna

The following table lists the default values of some of the attributes of an access point when it is added to the NCS for the first time.

AP Type	Radio Type	Supported Antennas
AP 1200	802.11a	KODIAC-OMNI, KODIAK-DIRECTIONAL, AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R
	802.11b/g	AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1240	802.11a	AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R
	802.11b/g	AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1131	802.11a	AJAX-OMNI
	802.11b/g	AJAX-OMNI
AP 1100	802.11b/g (only b/g)	AIR-ANT1100
AP 1310	802.11a	AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R
	802.11b/g	BR1310, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1250	802.11a	AIR-ANT5135D-R, AIR-ANT5135SDW-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5160NP-R, AIR-ANT5170V-R, AIR-ANT5195V-R, AIR-ANT2451NV-R-5GHz
	802.11b/g	AIR-ANT2460, AIR-ANT2460NP-R, AIR-ANT2422SDW-R, AIR-ANT2451NV-R-2.4GHz, AIR-ANT2465, AIR-ANT2485, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1000	802.11a	AIR-ANT1000, AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R, CUSH-S5157WP, CUSH-S24516DBP

AP Type	Radio Type	Supported Antennas
	802.11b/g	AIR-ANT1000, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT5959, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, CUSH-S24516DBP, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1030	802.11a	AIR-ANT1000, AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R, CUSH-S5157WP, CUSH-S24516DBP
	802.11b/g	AIR-ANT1000, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT5959, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, CUSH-S24516DBP, AIR-ANT2452V-R, AIR-ANT24020V-R
AP 1500	802.11a	AIR-ANT5175V, AIR-ANT58G10SSA, CUSH-S54717P, CUSH-S49014WP
	802.11b/g	AIR-ANT2455V, CUSH-S2406BP
AP 1505	802.11a	AIR-ANT5175V, AIR-ANT58G10SSA, CUSH-S54717P, CUSH-S49014WP
	802.11b/g	AIR-ANT2455V, CUSH-S2406BP
AP 1260	802.11a	AIR-ANT5135DG-R, AIR-ANT5135D-R, AIR-ANT5135DB-R, AIR-ANT5135DW-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R, AIR-ANT5140V-R, AIR-ANT2451V-R, AIR-ANT2450S-R, AIR-ANT5135SDW-R, AIR-ANT2451NV-R-5GHz, AIR-ANT5160NP-R
	802.11b/g	AIR-ANT2422DG-R, AIR-ANT4941, AIR-ANT2422DB-R, AIR-ANT2422DW-R, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213, AIR-ANT2430V-R, AIR-ANT24120, AIR-ANT2414S-R, AIR-ANT1949, AIR-ANT2451V-R, AIR-ANT2450S-R, AIR-ANT2460NP-R, AIR-ANT2422SDW-R, AIR-ANT2451NV-R-2.4GHz, AIR-ANT24020V-R, AIR-ANT2452V-R
AP 1040	802.11a	Internal-1040-5.0 GHz
	802.11b/g	Internal-1040-2.4 GHz
AP 1140	802.11a	Internal-1140-5.0 GHz
	802.11b/g	Internal-1140-2.4 GHz
AP 1550	802.11a	AIR-ANT2547V-N-5.0GHz, Internal-1550-5.0 GHz
	802.11b/g	AIR-ANT2547V-N-2.4GHz,Internal-1550-2.4GHz
AP 3500e	802.11a	AIR-ANT5135DG-R,AIR-ANT5135D-R,AIR-ANT5135DB-R,AIR-ANT5135DW-R,AIR-ANT5145V-R,AIR-ANT5160V-R,AIR-ANT5170V-R,AIR-ANT5195V-R,AIR-ANT5140V-R,AIR-ANT2451V-R,AIR-ANT2450S-R,AIR-ANT5135SDW-R,AIR-ANT2451NV-R-5GHz,AIR-ANT5160NP-R

AP Type	Radio Type	Supported Antennas
AP 3500e	802.11b/g	AIR-ANT2422DG-R,AIR-ANT4941,AIR-ANT2422DB-R,AIR-ANT2422DW-R,AIR-ANT2460,AIR-ANT2465,AIR-ANT2485,AIR-ANT1728,AIR-ANT2012,AIR-ANT1729,AIR-ANT2410Y-R,AIR-ANT5959,AIR-ANT3549,AIR-ANT2506,AIR-ANT3213,AIR-ANT2430V-R,AIR-ANT24120,AIR-ANT2414S-R,AIR-ANT1949,AIR-ANT2451V-R,AIR-ANT2450S-R,AIR-ANT2460NP-R,AIR-ANT2422SDW-R,AIR-ANT2451NV-R-2.4GHz,AIR-ANT24020V-R,AIR-ANT2452V-R
AP 3500i	802.11a	Internal-3500i-5 GHz
AP 3500i	802.11b/g	Internal-3500i-2.4 GHz
AP 3500p	802.11a	AIR-ANT5135DG-R, AIR-ANT5135D-R, AIR-ANT5135DW-R, AIR-ANT5140V-R, AIR-ANT5135SDW-R, AIR-ANT5160NP-R
AP 3500p	802.11b/g	AIR-ANT2422DG-R, AIR-ANT2422DB-R, AIR-ANT2422DW-R, AIR-ANT1728, AIR-ANT2410Y-R, AIR-ANT2506, AIR-ANT2430V-R, AIR-ANT1949, AIR-ANT2450S-R, AIR-ANT2460NP-R, AIR-ANT2451NV-R-2.4GHz, AIR-ANT2440NV-R, AIR-ANT2460P-R, AIR-ANT2485P-R
801GN	802.11a	Not Applicable
	802.11b/g	AIR-ANT4941, AIR-ANT2422DB-R
801AGN	802.11a	AIR-ANTM2050D-R
	802.11b/g	AIR-ANTM2050D-R
802GN	802.11a	Not Applicable
	802.11b/g	Internal-802.11
802AGN	802.11a	AIR-ANTM2050D-R
	802.11b/g	AIR-ANTM2050D-R

WLAN Override

The following 802.11a WLAN Override parameter appears:

- WLAN Override—Choose **Enable** or **Disable** from the drop-down list.

Note When you enable WLAN Override, operating system displays a table showing all current Cisco WLAN Solution WLANs. In the table, select WLANs to enable WLAN operation, and deselect WLANs to disallow WLAN operation for this 802.11a Cisco Radio.

Note WLAN override does not apply to access points that support the 512 WLAN feature.

Performance Profile

Click the URL to view or edit performance profile parameters for this access point interface.

- ClientLink—Enable or disable client link for the access point radios per interface. This feature is only supported for legacy (orthogonal frequency-division multiplexing) OFDM rates. The interface must support ClientLink, and OFDM rates must be enabled. Also, two or more antennas must be enabled for transmission, and all three antennas must be enabled for reception.

Note The maximum number of clients supported is 15. If the antenna configuration restricts operation to a single transmit antenna or OFDM rates are disabled, ClientLink cannot be used.

RF Channel Assignment

The following 802.11a RF Channel Assignment parameters appear:

- Current Channel—Channel number of the access point.
- Assignment Method—Select one of the following:
  - Global—Use this setting if your access point's channel is set globally by the controller.
  - Custom—Use this setting if your access point's channel is set locally. Select a channel from the drop-down list.

    For example, if you select 2(17 dBm) as the custom power, 2 corresponds to the Power Level and 17 is the Absolute Power (dBm).
- Channel width—Select the channel width from the drop-down list. The selections include 20, above 40, and below 40.

  RF Channel assignment supports 802.11n 40 MHz channel width in the 5-GHz band. 40-MHz channelization allows radios to achieve higher instantaneous data rates.

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

Tx Power Level Assignment

- Current Tx Power Level—Indicates the current transmit power level.
- Assignment Method—Select one of the following:
  - Global—Use this setting if your access point's power level is set globally by the controller.
  - Custom—Use this setting if your access point's power level is set locally. Choose a power level from the drop-down list.

11n Antenna Selection

NCS provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

Note At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

The following 11n Antenna Selection parameters appear:

- Transmit Antenna—Select the check box beside Antenna A or Antenna B to enable it.
- Receive Antenna—Select the check box beside Antenna A, B, or C to enable it.

11n Parameters

The following 11n parameter appears:

- 11n Supported—Indicates whether or not 802.11n radios are supported.

Configuring CDP

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

Note CDP is enabled on the bridge's Ethernet and radio ports by default.

Configuring CDP on Access Point

To configure CDP on Radio or Ethernet interfaces, follow these steps:

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

Step 2 Choose an access point associated with software release 5.0 or later.

Step 3 Click the slots of radio or an ethernet interfaces for which you want to enable CDP.

Step 4 Select the **CDP State** check box to enable CDP on the interface.

Step 5 Click **Save**.

Configuring Access Point Radios for Tracking Optimized Monitor Mode

To optimize monitoring and location calculation of tags, you can enable tracking optimized monitor mode (TOMM) on up to four channels within the 2.4-GHz band (802.11b/g radio) of an access point. This allows you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

After enabling Monitor Mode at the access point level, you must then enable TOMM and assign monitoring channels on the 802.11b/g radio of the access point.

Note For details on enabling Monitor Mode on an access point, see Step 6 in the "Configuring Access Point Details" section on page 9-164.

To set enable TOMM and assign monitoring channels on the access point radio, follow these steps:

Step 1 After enabling Monitor Mode at the access point level, choose **Configure > Access Points**.

Step 2 In the Access Points page, click the **802.11 b/g Radio** link for the appropriate access point.

Step 3 In the General portion, disable **Admin Status** by unselecting the check box. This disables the radio.

Step 4 Select the **TOMM** check box. This check box only appears for Monitor Mode APs. drop-down lists for each of the four configurable channels display.

Step 5 Select the four channels on which you want the access point to monitor tags.

Note You can configure fewer than four channels for monitoring. To eliminate a monitoring channel, select **None** from the channel drop-down list.

Step 6 Click **Save**. Channel selection is saved.

Step 7 In the Radio parameters page, re-enable the radio by selecting the **Admin Status** check box.

Step 8 Click **Save**. The access point is now configured as a TOMM access point.

The AP Mode displays as Monitor/TOMM on the Monitor > Access Points page.

Copying and Replacing Access Points

The Copy and Replace AP feature is useful if you need to remove an access point from the network and replace it with a new access point. All of the access point information, such as AP mode, name, and map location needs to be copied from the old access point to the new access point.

To access the **Copy and Replace AP** function, follow these steps:

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

Step 2 Select the check box for the applicable access point.

Step 3 From the Select a command drop-down list, choose **Copy and Replace AP**.

Step 4 Click **Go**.

The old access point needs to be removed from the network first. This access point then becomes unassociated to any controller.When you plug in the new access point, it is associated with the controller and NCS refreshes the information. At that point, select the old unassociated access point and choose to copy and replace the configuration to the new access point.

Note If a different access point type is used to replace an older access point, only the configuration parameters that apply will be copied.

- Check box
- MAC Address
- Name—Name of the access point.
- Controller IP Address—IP address of controller to which the access point is associated.
- Map Location—Map location of the access point.
- Copy Location information

Command Buttons

- Copy to AP

- Cancel

Removing Access Points

To remove access points that are not associated, follow these steps:

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

Step 2 From the Select a command drop-down list, choose **Remove APs**.

Step 3 Click **Go**.

Step 4 Click **OK** to confirm the removal.

Scheduling and Viewing Radio Status

Scheduling Radio Status

To schedule a radio status change (enable or disable), follow these steps:

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

Step 2 Select the check box for the applicable access point(s).

Step 3 From the Select a command drop-down list, choose **Schedule Radio Status**.

Step 4 Click **Go**.

Step 5 Choose **Enable** or **Disable** from the Admin Status drop-down list.

Step 6 Use the Hours and Minutes drop-down lists to determine the scheduled time.

Step 7 Click the calendar icon to select the scheduled date for the status change.

Step 8 If the scheduled task is recurring, choose **Daily** or **Weekly**, as applicable. If the scheduled task is a one-time event, choose **No Recurrence**.

Step 9 Choose **Save** to confirm the scheduled task.

Viewing Scheduled Tasks

To view currently scheduled radio status tasks, follow these steps:

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

Step 2 Select the check box for the applicable access point(s).

Step 3 From the Select a command drop-down list, choose **View Scheduled Radio Task(s)**.

Step 4 Click **Go**.

The Scheduled Task(s) information includes:

- Scheduled Task(s)—Choose the task to view its access points and access point radios.
- Scheduled Radio adminStatus—Indicates the status change (Enable or Disable).
- Schedule Time—Indicates the time the schedule task occurs.
- Execution status—Indicates whether or not the task is scheduled.
- Recurrence—Indicates Daily or Weekly if the scheduled task is recurring.
- Next Execution—Indicates the time and date of the next task occurrence.
- Last Execution—Indicates the time and date of the last task occurrence.
- Unschedule—Click **Unschedule** to cancel the scheduled task. Click **OK** to confirm the cancellation.

Viewing Audit Status (for Access Points)

An Audit Status column on the Configure > Access Points page 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.

To view the audit status, follow these steps:

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 list. 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.

Filtering Alarms for Maintenance Mode Access Points

The NCS uses critical alarms to track if the managed access points are down. The Controller sends three different alarms when:

- Access point is down
- Radio A of the access point is down

- Radio B/G of the access point is down

In Release 7.0.172.0 and later, these 3 alarms are clubbed into one alarm.

When an access point is under technical maintenance, the critical alarms need to be deprioritized. You can deprioritize the severity of an alarm of an access point using the **Configure > Access Points** page. When you move an access point to maintenance state, the alarm status for that access point appears in black color.

This section consists of the following topics:

- Placing an Access Point in Maintenance State, page 9-188
- Removing an Access Point from Maintenance State, page 9-188

Placing an Access Point in Maintenance State

To move an access point to the maintenance state, follow these steps:

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

The Access Points page appears.

Step 2 From the drop-down list available in the right side, choose **Place in Maintenance State** and click **Go**.

The access point is moved to maintenance state.

Once the access point is moved to maintenance state, the access point down alarms would be processed with lower severity instead of critical.

Removing an Access Point from Maintenance State

To remove an access point from the maintenance state, follow these steps:

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

The Access Points page appears.

From the drop-down list available in the right side, choose **Remove from Maintenance State** and click **Go**.

The access point is removed from the maintenance state.

Searching Access Points

Use the search options in the uppermost right corner of the page to create and save custom searches:

- New Search: Enter an IP address, name, SSID, or MAC, and click Search.
- Saved Searches: Click **Saved Search** to choose a category, a saved custom search, or choose other criteria for a search from the drop-down lists.
- Advanced Search: An advanced search allows you to search for a device based on a variety of categories and filters.

See the "Using the Search Feature" section on page 2-33 for further information.

After you click **Go**, the access point search results appear (see Table 9-5).

Table 9-5 Access Point Search Results

Parameter	Options
IP Address	IP address of the access point.
Ethernet MAC	MAC address of the access point.
AP Name	Name assigned to the access point. Click the access point name item to display details.
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.
AP Type	Access point radio frequency type.
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
Audit Status	The audit status of the access point.
Serial Number	The serial number of the access point.
AP Mode	Describes the role of the access point modes such as Local, H-REAP, Monitor, Rogue Detector, Sniffer, Bridge, or SE-Connect. (as described in Step 6 of Configuring Access Points).

Viewing Mesh Link Details

You can access mesh link details in several ways:

- Click the **Mesh** dashboard on the NCS home page
- Choose **Monitor** > **Access Points**, and click the **Mesh Links** tab and then click the **Details** link
- After you import a KML file from Google Earth, click the **AP Mesh** link

The current statistics are displayed at the top of the page followed by diagrams for certain statistics.

- SNR Graph—SNR Up and Down graphs are combined into one graph. Each set of data is represented by different colors.
- Link Metrics Graph—The Adjusted Link Metric and Unadjusted Link Metric is combined into one graph. Each set of data is represented by different colors.
- Packet Error Rate Graph—Displays the packet error rates in a graph.
- Link Events—The last five events for the link are displayed.

- Mesh Worst SNR Links—Displays the worst signal-to-noise ratio (SNR) links.
- AP Uptime—These statistics help determine if an access point is rebooting frequently.
- LWAPP Join Taken Time—These statistics determine how long it takes an access point to join.
- Location Links—Allows you to navigate to the NCS map or the Google Earth location.

Viewing or Editing Rogue Access Point Rules

You can view or edit current rogue access point rules on a single WLC. See the "Configuring a Rogue AP Rules Template" section on page 11-78 for more information.

To access the rogue access point rules, follow these steps:

Step 1 Choose **Configure > Controllers**.

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

Step 3 From the left sidebar menu, choose **Security > Rogue AP Rules**. The Rogue AP Rules displays the rogue access point rules, the rule types (malicious or friendly), and the rule sequence.

Step 4 Choose a **Rogue AP Rule** to view or edit its details.

Configuring Switches

You can add switches to the NCS database in order to view overall switch health and endpoint monitoring and to do switchport tracing. While this switch functionality appears under the Configuration menu in NCS, you are configuring the NCS system and not the switches. You cannot configure switch features using NCS.

NCS allows you to:

- Add switches under **Configure > Switches** and specify CLI and SNMP credentials. See Adding Switches for more information.
- Monitor Switches under **Monitor > Switches**. See Monitoring Switches for more information.
- Run switch-related reports under the Reports menu. See

Note From the Configure > Switches page, you can also add a location-capable switch for tracking wired clients by mobility services engine and NCS.

- Configuring Switches, page 9-190
- Configuring Spectrum Experts, page 9-200

Note The following switches are supported: 3750, 3560, 3750E, 3560E, and 2960.

Related Topic

- Features Available by Switch Type
- Configuring Switch NMSP and Location

Features Available by Switch Type

When you add a switch to NCS, you specify how the switch is to be managed. Based on how you specify the switch is to be managed, NCS determines which features are available:

- Monitored switches—You can add switches (under **Configure > Switches**) and monitor switch operation (under **Monitor > Switches**). Each switch counts as a single device against the total device count for your license. If you have unused device counts available in your license engine, you can add a switch to NCS. If you have no remaining device counts available, you cannot add additional switches to NCS.
- Switch Port Tracing (SPT) only switches—Switches perform switch port tracing only. SPT-only switches appear under **Configure > Switches** and in inventory reports, but SPT-only switches do not appear under **Monitor > Switches** or on the dashboards. Licensing does not apply to SPT switches.

Viewing Switches

Select **Configure > Switches** to see a summary of all switches in the NCS database. The summary information includes the following:

- Management IP Address—IP address of the switch. Click the IP address of a switch to get more details. See Viewing Switch Details for more information.
- Device Name—Name of the switch.
- Device Type— Type of switch.
- Reachability Status—Indicates **Reachable** if the switch is reachable or **Unreachable** if the switch is unreachable.
- Inventory Collection Status—Status of the last inventory collection. The possible values are OK, Partial, Failed, NA (for SPT-only switches), or In Progress.
- Inventory Status Detail—Specifies the status of the latest inventory collection. If the inventory collection was not successful, lists the possible reasons for the failure.
- Last Inventory Collection Date—Displays the most recent date in which the inventory was collected.
- Creation Time— Date and time the switch was added to NCS.
- License Status—Indicates the license status of the switch, which can be **Full Support** or **SPT only**. See Features Available by Switch Type for more information.

Click any column heading to sort the information by that column. You can switch between ascending and descending sort order by clicking the column heading more than once.

Related Topic

- Viewing Switch Details

Viewing Switch Details

Select **Configure > Switches** to see a summary of all switches in the NCS database. Click an IP address under the Management IP Address column to see detailed information about that switch Table 9-6 describes the summary information that is displayed:

Table 9-6 Configure > Switches Summary Information

General Parameters	
IP Address	IP address of the switch.
Device Name	Name of the switch.
Last Inventory Collection Date	Date and time of the last inventory collection
Inventory Collection Status	Status of the last inventory collection. The possible values are OK, Partial, or Failed.
Software Version	Version of software running on the switch.
Location	Location of the switch.
Contact	Contact name for the switch.
Reachability Status	Indicates **Reachable** if the switch is reachable or **Unreachable** if the switch is unreachable.
SNMP Parameters	
Version	SNMP version number, which can be v1, v2c, or v3. **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. See Configuring SNMPv3 on Switches for more information.
Retries	Retries (in seconds) allowed before the process stops without success.
Timeout	SNMP timeout value (in seconds).
If you selected v3 in the Version pulldown menu, the following fields appear:	
Username	Username
Auth. Type	Authentication type with can be None, HMAC-SHA, or HMAC-HD5.
Auth. Password	Authentication password.
Privacy Type	Privacy type with can be None, CBC-DES, or CFB-AES-128.
Privacy Password	Privacy password.
Community	If you selected v1 or v2c, this field indicates the SNMP community string.
Telnet/SSH Parameters	
Protocol	Protocol used.
User Name	User name.
Password	Password.
Confirm Password	Confirm the password by entering it again.
Enable Password	Enable password.
Confirm Password	Confirm the password by entering it again.
Timeout	Timeout value (in seconds).

Modifying SNMP Parameters

To modify SNMP parameters for a switch, follow these steps:

Step 1 Select **Configure > Switches**, then click the IP address of the switch for which you want to change SNMP credentials.

Step 2 Modify the necessary SNMP Parameters fields, then click:

- **Reset** to restore the previously saved parameters.
- **Save** to save and apply the changes you made.
- **Cancel** to exit without saving your changes and return to the previous screen.

Modifying Telnet/SSH Parameters

To modify Telnet or SSH parameters for a switch, follow these steps:

Step 1 Select **Configure > Switches**, then click the IP address of the switch for which you want to change Telnet or SSH credentials.

Step 2 Modify the necessary Telnet/SSH Parameters fields, then click:

- **Reset** to restore the previously saved parameters.
- **Save** to save and apply the changes you made.
- **Cancel** to exit without saving your changes and return to the previous screen.

Adding Switches

When you add a switch to the NCS database, by default, NCS verifies the SNMP credentials of the switch. If the device credentials are not correct, you receive an SNMP failure message but the switch is added to the NCS database.

To add a switch to NCS, follow these steps:

Step 1 Choose **Configure > Switches**.

Step 2 From the Select a command drop-down list, choose **Add Switches**, then click **Go**.

Step 3 Complete the fields as described in Table 9-7:

Table 9-7 Adding a Switch

Field	Description
General Parameters	
Add Format Type	Select: • **Device Info** to manually enter comma-separated IP addresses of Ethernet switches. • **CSV File** to import a CSV file that contains IP addresses of multiple switches. Enter the CSV file path in the text box or use the Browse button to navigate to the CSV file on your computer. See Configuring SNMPv3 on Switches for more information.
IP Addresses	If you selected Device Info, enter comma-separated IP addresses of the Ethernet switches.

Table 9-7 Adding a Switch (continued)

Field	Description
License Level	Select: • **Full** • **SPT only** to specify Switch Port Tracing support only.
SNMP Parameters **Note** Enter SNMP parameters for the write access, if available. If you enter read-only access parameters, the switch is added but NCS is unable to modify the configuration.	
Version	Enter the SNMP version number, which can be v1, v2c, or v3. **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. See Configuring SNMPv3 on Switches for more information.
Retries	Enter the retries (in seconds) allowed before the process stops without success.
SNMP Timeout (in secs)	Enter the SNMP timeout value (in seconds).
If you selected v1 or v2c in the Version pulldown menu, the Community field appears:	
Community	Enter the SNMP community string.
If you selected v3 in the Version pulldown menu, the following fields appear:	
Username	Enter the username.
Auth. Type	Enter the authentication type with can be None, HMAC-SHA, or HMAC-HD5.
Auth. Password	Enter the authentication password.
Privacy Type	Enter the privacy type with can be None, CBC-DES, or CFB-AES-128.
Privacy Password	Enter the privacy password.
Telnet/SSH Parameters	
Protocol	Select the protocol.
User Name	Enter the user name.
Password	Enter the password.
Confirm Password	Confirm the password by entering it again.
Enable Password	Enter the enable password.
Confirm Password	Confirm the enable password by entering it again.
Timeout (in secs)	Enter the timeout value (in seconds).

Step 4 Click:

- **Add** to add the switch.
- **Cancel** to cancel the operation and return to the list of switches.

Configuring SNMPv3 on Switches

The following is an example for configuring SNMPv3 on the switch:

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

If the switch has VLANs, you must configure each VLAN, otherwise switch porting tracing will fail. The following is an example if the switch has VLANs 1 and 20.

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

Note When you create SNMP v3 view, make sure you include all of the OIDs.

Sample CSV File for Importing Switches

The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory. The following example shows a sample CSV file.

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name,
snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password,
snmp_retries,
snmp_timeout,protocol,telnet_username,telnet_password,enable_password,telnet_timeout
16.1.1.3,255.255.255.0,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
16.1.1.4,255.255.255.0,v2,public,,,,,3,10,ssh2,cisco,cisco,cisco,60
16.1.1.5,255.255.255.0,v2,public,,,,,3,10,,cisco,cisco,cisco,60
16.1.1.6,255.255.255.0,v2,public,,,,,3,10,telnet,cisco,cisco,cisco,60
3.3.3.3,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4
4.4.4.4,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4,telnet,cisco,cisco,
cisco,60
```

The CSV file can contain the following fields:

- ip_address—IP address
- network_mask—Network mask
- snmp_version—SNMP credentials version. Can be v1, v2, or v3.
- snmp_community—SNMP community (Mandatory for v2.)
- snmpv2_community—SNMP V2 community.
- snmpv3_user_name—SNMP V3 username (Mandatory for v3.)
- snmpv3_auth_type—SNMP V3 authorization type. Can be None or HMAC-MD5 or HMAC-SHA (Mandatory for v3.)
- snmpv3_auth_password—SNMP V3 authorization password (Mandatory for v3).
- snmpv3_privacy_type—SNMP V3 privacy type. Can be None or DES or CFB-AES-128 (Mandatory for v3.)
- snmpv3_privacy_password—SNMP V3 privacy password (Mandatory for v3.)
- snmp_retries—SNMP retries
- snmp_timeout—SNMP timeout
- protocol—telnet, ssh2
- telnet_username—for switches and APs, if configured (Mandatory if configured.)
- telnet_password—for switches and APs (mandatory)
- enable_password

- telnet_timeout

Configuring Switch NMSP and Location

Choose **NCS > Configure > Switches > *Switch IP Address* > NMSP & Location** to view the NMSP and Location information for switches.

Note NMSP is supported by:

- Cisco Catalyst 3000 and 4000 series switches
- IOS Release 12.50 and above

You can enable or disable NMSP status and configure switch and switch port location as described in the following sections:

- Enabling and Disabling NMSP for Switches
- Configuring a Switch Location
- Configuring a Switch Port Location

Enabling and Disabling NMSP for Switches

You can enable or disable NMSP for a switch by choosing **NCS > Configure > Switches > *Switch IP Address* > NMSP & Location > NMSP Status**.

Table 9-8 lists the options available in the NMSP Status Page.

Table 9-8 Parameters of the NMSP Status page

Parameter	Description
NMSP	Select or Unselect this option to enable or disable NMSP for the switch.
MSE IP Address	Displays the IP address of the MSE if the switch is associated to an MSE. To associate this switch to an MSE, click Go to Synchronize button. This takes to the Synchronization page. You can synchronize this switch with an MSE. Alternately, you could use **NCS > Services > Synchronize Services > Wired Switches** to synchronize switches to an MSE. For more information on Synchronization, see "Synchronizing Services" section on page 16-10.

Configuring a Switch Location

You can configure the location for a switch using the Switch Location option.

Step 1 Choose **NCS > Configure > Switches > *Switch IP Address* > NMSP & Location > Switch Location**.

Step 2 In the Map Location pane, select the following from the drop-down list boxes:

- Campus

- Building
- Floor

Step 3 Click **Import Civic** to import the civic information to the switch.

The fields in the Civic Location pane are populated after the civic information is imported.

Configuring a Switch Port Location

You can configure location for switch ports using the Switch Port Location option.

Step 1 Choose **NCS > Configure > Switches > *Switch IP Address* > NMSP & Location > Switch Port Location**.

Step 2 Select one or more ports on which you want to configure location.

Step 3 From the drop-down list, select Configure Location, then click **Go**.

The Switch Port Location Configuration page appears.

The Switch Ports pane lists the ports that you have selected to configure location.

Step 4 In the Map Location pane, select the following from the drop-down list boxes:

- Campus
- Building
- Floor

Step 5 Click **Import Civic** to import the civic information to the switch port.

The fields in the Civic Location pane are populated after the civic information is imported.

Removing Switches

When you remove a switch from the NCS database,

- Inventory information for that switch is removed from the database.
- Alarms for the switch remain in the database with a status of Clear. By default, cleared alarms are not displayed in the NCS interface.
- Saved reports remain in the database even if the switch on which the report was run is removed.

To remove a switch from NCS, follow these steps:

Step 1 Choose **Configure > Switches**.

Step 2 Select the check box(es) of the switch(es) you want to remove.

Step 3 From the Select a command drop-down list, choose **Remove Switches**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Related Topic

- Adding Switches

Refreshing Switch Configuration

By default, inventory information is collected every six hours. If you make configuration changes and want the changes displayed immediately instead of waiting for the next inventory collection, you can refresh the switch as shown in the following steps:

Step 1 Choose **Configure > Switches**.

Step 2 Select the check box(es) of the switch(es) whose configuration you want to refresh.

Step 3 From the Select a command drop-down list, choose **Refresh Config from Switch**.

Step 4 Click **Go**.

Enabling Traps and Syslogs on Switches for Wired Client Discovery

This section describes how to configure switches to send traps and syslogs to NCS to discover the clients as they connect/disconnect.

This section consists of the following topics:

MAC Notification for Traps (used for non-identity client discovery)

This IOS switch feature forwards SNMP traps from the switch to the NCS server for MAC notifications (for non-802.1x clients).

IOS configuration example:

```
snmp-server enable traps mac-notification change move threshold
snmp-server host<IP address of NCS server> version 2c <community-string> mac-notification
mac address-table notification change interval 5
mac address-table notification change history-size 10
mac address-table notification change


interface <interface>
 description non-identity clients
 switchport access vlan <VLAN ID>
 switchport mode access
 snmp trap mac-notification change added  <- interface level config for MAC Notification
  snmp trap mac-notification change removed <- interface level config for MAC Notification
```

Debug Commands

```
debug snmp packets
```

Show Commands

```
show mac address-table notification change
```

References

For more information about Configuring MAC Change Notification Traps, see http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/swadmin.html#wp1246821

Syslog Configuration

Note This feature is used for identity clients discovery.

The syslog configuration forwards syslog messages from a catalyst switch to NCS server.

IOS configuration Example:

```
archive
 log config
  notify syslog contenttype plaintext
logging facility auth
logging <IP address of NCS server>
```

For more information, see http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_50_se/configuration/guide/swlog.html

Configuring Unknown Devices

To configure the unknown devices, follow these steps:

Step 1 Choose **Configure > Unknown Devices**. The Unknown Devices page appears. The summary information includes the following:

- IP Address—IP address of the device.
- Device Type— Type of device.
- Reachability Status—Indicates Reachable if the device is reachable or Unreachable if the device is unreachable.
- Inventory Collection Status—Status of the last inventory collection. The possible values are OK, Partial, Failed, NA, or In Progress
- Inventory Status Detail—Specifies the status of the latest inventory collection. If the inventory collection was not successful, lists the possible reasons for the failure.
- Creation Time— Date and time the device was added to NCS.

Step 2 From the Unknown Devices page, you can perform the following functions:

- Remove Devices— To remove a device from the unknown devices table, select the device(s) and select **Remove Devices** from the Select a command drop-down list.

- Update Device Credentials—To update the device credentials of a device, select the device and select **Update Device Credentials** from the Select a command drop-down list. The Update Device Credentials page appears.
- Bulk Update Devices—To update the device credentials in a bulk, select **Bulk Update Devices** from the Select a command drop-down list. The Bulk Update Devices page appears.You can choose a CSV file.

Note The CSV file contains a list of devices to be updated, one device per line. Each line is a comma separated list of device attributes. The first line describes the attributes included. The IP address attribute is mandatory.

Configuring Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to NCS. This feature allows the NCS 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 NCS. The status appears as reachable or unreachable.

This section contains the following topics:

- Adding a Spectrum Expert, page 9-200
- Monitoring Spectrum Experts, page 9-201

Adding a Spectrum Expert

To add a Spectrum Expert, follow these steps:

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

Step 2 From the Select a command drop-down list, choose **Add Spectrum Expert**.

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

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 NCS.

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

Monitoring Spectrum Experts

You also have the option to monitor spectrum experts.

To monitor spectrum experts, follow these steps:

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.

Viewing 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 NCS. 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.

Viewing 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. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device.
- 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 NCS.

- Discover Time—Indicates when the interferer was discovered.
- Affected Channels—Identifies affected channels.
- Number of APs Affected—The number of access points managed by NCS 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 NCS.
  - 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.

Viewing 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:

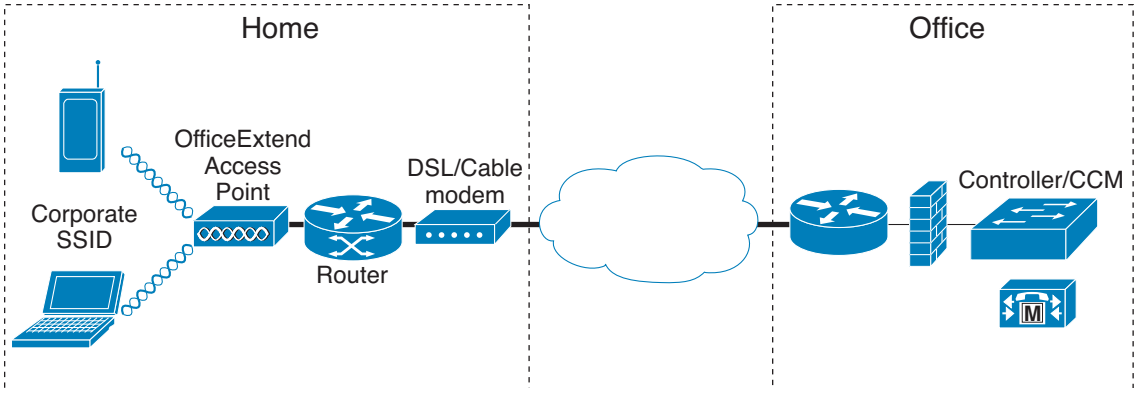
- Total Interferer Count—Given from the specific spectrum expert.
- Active Interferers Count Chart—Displays a pie chart that groups interferers by category.
- Active Interferer Count Per Channel—Displays the number of interferers grouped by category on different channels.
- AP List—Provides a list of 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. You can select specific RADIUS or LDAP servers to provide external authentication on the Security > AAA page.

OfficeExtend Access Point

An OfficeExtend access point provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. The teleworker's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Figure 9-21 illustrates a typical OfficeExtend access point setup.

Figure 9-21 Typical OfficeExtend Access Point Setup



Note OfficeExtend access points are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), thereby enabling an entire group of computers to be represented by a single IP address. In controller release 6.0, only one OfficeExtend access point can be deployed behind a single NAT device.

Currently, only Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 series controller with a WPlus license can be configured to operate as OfficeExtend access points.

Note Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.

Licensing for an OfficeExtend Access Point

Make sure that the WPlus license is installed on the 5500 series controller. After the license is installed, you can enable the OfficeExtend mode on an 1130 series or 1140 series access point.

Note The operating system software automatically detects and adds an access point to the Cisco NCS database as it associates with existing controllers in the Cisco NCS database.

Configuring Link Latency Settings for Access Points

You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to a controller but is especially useful for hybrid-REAP access points, for which the link could be a slow or unreliable WAN connection.

Note Link latency is supported for use only with hybrid-REAP access points in connected mode. Hybrid-REAP access points in standalone mode are not supported.

Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the access point to the controller and back. This time can vary due to network link speed and controller processing loads. The access point timestamps the outgoing echo requests to the controller and the echo requests received from the controller. The access point sends this delta time to the controller as the system round-trip time. The access point sends heartbeat packets to the controller at a default interval of 30 seconds.

Note Link latency calculates the CAPWAP response time between the access point and the controller. It does not measure network latency or ping responses.

The controller displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the controller is up or can be cleared and allowed to restart.

To configure link latency, follow these steps:

Step 1 In the Configure > Access Point details page, select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. The default value is unselected.

Step 2 Click **Save** to save your changes.

The link latency results appear below the Enable Link Latency check box:

- Current—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- Minimum—Since link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- Maximum—Since the link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

Step 3 To clear the current, minimum, and maximum link latency statistics on the controller for this access point, click **Reset Link Latency**. The updated statistics appear in the Minimum and Maximum fields.

Configuring Chokepoints

Chokepoints are low frequency transmitting devices. When a tag passes within range of placed chokepoint, the low-frequency field awakens the tag that in turn sends a message over the Cisco Unified Wireless Network including the chokepoint device ID. The transmitted message includes sensor information (such as temperature and pressure). A chokepoint location system provides room level accuracy (ranging from few inches to 2 feet depending on the vendor).

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be entered into the location database and plotted on a NCS map.

- Configure New Chokepoints, page 9-205
- Editing Current Chokepoints, page 9-207

Configure New Chokepoints

Adding a Chokepoint to NCS Database

To add a chokepoint to the NCS database, follow these steps:

Step 1 Choose **Configure > Chokepoints**.

Step 2 From the Select a command drop-down list, choose **Add Chokepoints**.

Step 3 Click **Go**.

Step 4 Enter the MAC address and name for the chokepoint.

Step 5 Select the check box to indicate that it is an Entry/Exit Chokepoint.

Step 6 Enter the coverage range for the chokepoint.

Note Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 7 Click **OK**.

Note After the chokepoint is added to the database, it can be placed on the appropriate NCS floor map.

Adding a Chokepoint to a NCS Map

To add the chokepoint to a map, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 In the Maps page, click the link that corresponds to the floor location of the chokepoint.

Step 3 From the Select a command drop-down list, choose **Add Chokepoints**.

Step 4 Click **Go**.

Note The Add Chokepoints summary page lists all recently-added chokepoints that are in the database but not yet mapped.

Step 5 Select the check box next to the chokepoint that you want to place on the map.

Step 6 Click **OK**.

A map appears with a chokepoint icon located in the top-left hand corner. You are now ready to place the chokepoint on the map.

Step 7 Left-click the chokepoint icon and drag and place it in the proper location.

Note The MAC address, name, and coverage range of the chokepoint appear in the selected chokepoints detail page when you click the chokepoint icon for placement.

Step 8 Click **Save**.

You are returned to the floor map and the added chokepoint appears on the map.

Note The newly created chokepoint icon may or may not appear on the map depending on the display settings for that floor.

Note The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

Note MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint display when you pass a mouse over its map icon

Step 9 If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.

Note Do not select the **Save Settings** check box unless you want to save this display criteria for all maps.

Note You must synchronize network design to the mobility services engine or location server to push chokepoint information.

Removing a Chokepoint from a NCS Map

To remove an chokepoint from the map, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 On the Maps page, choose the link that corresponds to the floor location of the chokepoint.

Step 3 From the Select a command drop-down list, choose **Remove Chokepoints**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Removing a Chokepoint from NCS

To remove an chokepoint from NCS, follow these steps:

Step 1 Choose **Configure > Chokepoints**.

Step 2 Select the check box of the chokepoint that you want to delete.

Step 3 From the Select a command drop-down list, choose **Remove Chokepoints**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Editing Current Chokepoints

To edit a current chokepoint in the NCS database and appropriate map, follow these steps:

Step 1 Choose **Configure > Chokepoints**. The Configure > Chokepoints page displays the following information for each current chokepoint: MAC address, chokepoint name, entry/exit chokepoint, range, static IP address, and map location for the chokepoint.

Step 2 Click the chokepoint you want to edit in the MAC Address column.

Step 3 Edit the following parameters, as necessary:

- Name
- Entry/Exit Chokepoint—Click to enable.
- Range—Coverage range for the chokepoint.

Note The chokepoint range is product-specific and is supplied by the chokepoint vendor.

- Static IP Address

Step 4 Click **Save**.

Configuring WiFi TDOA Receivers

Using WiFi TDOA Receivers to Enhance Tag Location Reporting

The Wi-Fi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset. TDOA receivers use the method of Time Difference of Arrival (TDOA) to calculate tag location. This method uses data from a minimum of three TDOA receivers to generate a tagged asset location.

Note

- If a TDOA receiver is not in use and the partner engine software is resident on the mobility service engine, then the location calculations for tags are generated using RSSI readings from access points.
- The Cisco Tag engine can calculate the tag location using the RSSI readings from access points.

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must:

1. Have a mobility services engine active in the network.

   See the "Adding a Mobility Services Engine" section on page 16-5 for details on adding a mobility services engine.

2. Add the TDOA receiver to the NCS database and map.

   See the "Adding Wi-Fi TDOA Receivers to Cisco NCS and Maps" section on page 9-208 for details on adding the TDOA receiver to NCS.

3. Activate or start the partner engine service on the MSE using NCS.
4. Synchronize NCS and mobility services engines.

   See the "Synchronizing Services" section on page 16-10 for details on synchronization.

5. Set up the TDOA receiver using the *AeroScout System Manager*.

Note See the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide* for configuration details at the following URL: http://support.aeroscout.com.

Adding Wi-Fi TDOA Receivers to Cisco NCS and Maps

After the Wi-Fi TDOA receiver is installed and configured by the *AeroScout System Manager* and the partner software is downloaded on the mobility services engine, you are ready to add the TDOA receiver to the mobility services engine database and position it on a NCS map.

After adding TDOA receivers to NCS maps, you continue to make configuration changes to the TDOA receivers using the *AeroScout System Manager* application rather than NCS.

Note For more details on configuration options, see the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide* at the following link: http://support.aeroscout.com.

To add a TDOA receiver to the NCS database and appropriate map, follow these steps:

Step 1 In NCS, click **Configure > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

Note To view or edit current WiFi TDOA receiver details, click the MAC Address link to open the details page.

Step 2 From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**.

Step 3 Click **Go**.

Step 4 Enter the MAC address, name and static IP address of the TDOA receiver.

Step 5 Click **OK** to save the TDOA receiver entry to the database.

Note After you add the TDOA receiver to the database, you can place the TDOA receiver on the appropriate NCS floor map. To do so, continue with Step 6.

Note A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Step 6 To add the TDOA receiver to a map, choose **Monitor > Maps**.

Step 7 In the Maps page, select the link that corresponds to the floor location of the TDOA receiver.

Step 8 From the Select a command drop-down list, choose **Add WiFi TDOA receivers**.

Step 9 Click **Go**.

Note The All WiFi TDOA Receivers summary page lists all recently-added TDOA receivers that are in the database but not yet mapped.

Step 10 Select the check box next to each TDOA receiver to add it to the map.

Step 11 Click **OK**. A map appears with a TDOA receiver icon located in the top-left hand corner. You are now ready to place the TDOA receiver on the map.

Step 12 Left-click the TDOA receiver icon and drag and place it in the proper location on the floor map.

Note The MAC address and name of the TDOA receiver appear in the left pane when you click the TDOA receiver icon for placement.

Step 13 Click **Save** when the icon is placed correctly on the map. The added TDOA receiver appears on the floor heat map.

Note The icon for the newly added TDOA receiver may or may not appear on the map depending on the display settings for that floor. If the icon did not appear, proceed with Step 14.

Step 14 If the TDOA receiver does not appear on the map, click **Layers** to collapse a selection menu of possible elements to display on the map.

Step 15 Select the **WiFi TDOA Receivers** check box. The TDOA receiver appears on the map.

Note When you place your cursor over a TDOA receiver on a map, configuration details display for that receiver.

Step 16 Click **X** to close the Layers page.

Note Do not choose **Save Settings** from the Layers menu unless you want to save this display criteria for all maps.

Step 17 You can now download the partner engine software to the mobility services engine.

Viewing or Editing Current Wi-Fi TDOA Receivers

To view a current TDOA receiver to the NCS database, follow these steps:

Step 1 In NCS, choose **Configure > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

Step 2 Click the MAC Address link to view the TDOA receiver details including MAC address, name, and static IP address.

Step 3 If you make any changes to the receiver name or IP address, click **Save** to confirm these changes.

Note A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Removing Wi-Fi TDOA Receivers from Cisco NCS and Maps

You can remove one or multiple WiFi TDOA receivers at a time. If you remove a TDOA receiver from a map it remains in the NCS database but is labeled as unassigned.

To delete a TDOA receiver from NCS, follow these steps:

Step 1 In NCS, choose **Configure > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

Step 2 Select the check box next to each TDOA receiver to be deleted.

Step 3 From the Select a command drop-down list, choose **Remove WiFi TDOA Receivers**.

Step 4 Click **Go**.

Step 5 To confirm TDOA receiver deletion, click **OK** in the dialog box.

In the **All WiFi TDOA Receivers** page, a message confirms the deletion. The deleted TDOA receiver is no longer listed in the page.

Configuring Scheduled Configuration Tasks

The Scheduled Configuration Tasks feature allows you to view, modify, and delete scheduled access point template and configuration group tasks. To access the Scheduled Configuration Tasks page, choose **Configure > Scheduled Configuration Tasks**.

This section contains the following topics:

AP Template Tasks

The AP Template Tasks page allows you to view, modify, delete, enable, or disable current access point template tasks. To access the AP Template Tasks page and view current access point template tasks, choose **Configure > Scheduled Configuration Tasks**.

Modifying a Current AP Template Task

To modify a current access point template task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Select the template name of the applicable task.

Step 3 In the AP Radio/Template page, click the **Apply/Schedule** tab.

Step 4 Make any necessary changes to the current schedule or access point template, and click **Schedule**.

Viewing AP Status Report for the Scheduled Task

The AP Status Report for the scheduled task includes the following information:

- AP Name—Lists all of the access points included in the scheduled access point template task.
- Ethernet MAC—Indicates the Ethernet MAC addresses for the applicable access points.
- Controller—Indicates the associated controller for each of the applicable access points.
- Map—Displays the map location for the applicable access points.
- Status—Indicates whether the access point template has been successfully applied. Possible states include Not Initiated, Success, Failure, Partial Failure, and Not Reachable.

- Task Execution Time—Indicates the execution time of the scheduled task for the applicable access point.

To view the status report for the access points included in the scheduled task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Select the AP Status Report for the applicable task.

Enabling or Disabling a Current AP Template Task

To enable or disable a current access point template task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Select the check box of the scheduled task to be enabled or disabled.

Step 3 From the Select a command drop-down list, choose **Enable Schedule** or **Disable Schedule**, as applicable.

Step 4 Click **Go**.

Viewing AP Template Task History

To view previous scheduled task reports, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Select the check box of the applicable scheduled task.

Step 3 From the Select a command drop-down list, choose **View History**.

Step 4 Click **Go**.

Deleting a Current AP Template Task

To delete a scheduled access point template task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 Select the check box of the applicable scheduled task.

Step 3 From the Select a command drop-down list, choose **Delete Task(s)**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Configuring Config Groups

The Config Group Tasks page allows you to view, modify, delete, enable, or disable current configuration group tasks. To access the Config Group Tasks page and view current config group tasks, choose **Configure > Scheduled Configuration Tasks > ConfigGroup**.

Modifying a Current Config Group Task

To modify a current configuration group task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Select the group name of the applicable task.

Step 4 From the Config Groups page, click the **Apply/Schedule** tab.

Step 5 Make any necessary changes to the current schedule and click **Schedule**.

Viewing Controller Status Report for the Scheduled Task

The Controller Status Report for the scheduled task includes the following information:

- Group Name—Name of the config group.
- Schedule—Indicates whether the task is enabled, disabled, or expired.
- Last Run Time—Indicates the date and time of the most recent scheduled task.
- Next Scheduled Run—Indicates the date and time of the next scheduled task.
- Controller Status Report—Indicates the number of status reports for this config group. Click the number link to view the status reports.

To view the controller status report, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Select the Controller Status Report for the applicable task. The Controller Status Report provides the following information:

- Controller
- Status of task (such as Not Initiated, Success, Failure, Partial Failure, Partial Success, Not Reachable)
- Number of templates applied

- Number of templates failed
- Time and date of the task execution

Enabling or Disabling a Current Config Group Task

To enable or disable a current configuration group task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Select the check box of the scheduled task to be enabled or disabled.

Step 4 From the Select a command drop-down list, choose **Enable Schedule** or **Disable Schedule**, as applicable.

Step 5 Click **Go**.

Viewing Config Group Task History

To view previous scheduled task reports, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Select the check box of the applicable scheduled task.

Step 4 From the Select a command drop-down list, choose **View History**.

Step 5 Click **Go**.

Deleting a Current Config Group Task

To delete a scheduled configuration group task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **ConfigGroup**.

Step 3 Select the check box of the applicable scheduled task.

Step 4 From the Select a command drop-down list, choose **Delete Task(s)**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

Viewing WLAN Configuration Scheduled Task Results

Note There is no drop-down command list provided for WLAN Configuration.

To view and manage all scheduled WLAN tasks in NCS, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **WLAN Configuration** to open the WLAN Configuration Task List page.

Step 3 If scheduled configuration tasks are available, the WLAN Configuration Task List page contains the following parameters:

- Schedule Task Name—The user-defined name of the new scheduled task.
- Schedule—Indicates the status of the scheduled task.
- WLAN Status—Indicates the status of the WLAN.
- Controller IP Address—Indicates the IP address of the controller.
- Last Run Time—Indicates the date and time of the most recent scheduled task.
- Next Scheduled Run—Indicates the date and time of the next scheduled task.
- Recurrence—Indicates Daily or Weekly if the scheduled task is recurring.

Step 4 Select the Task Name link to open the WLAN Schedule Detail page. In this page, you can modify the date and time of the scheduled task. See the "Managing WLAN Status Schedules" section on page 9-75 for more information.

Step 5 Select the check box of the scheduled task and use the Select a command drop-down list located in the WLAN Configuration Task List page to enable, disable, or delete selected tasks.

- Enable Schedule—Enable the task if its schedule is disabled on the server.
- Disable Schedule—Disable the running scheduled task on the server. Once disabled, the task will not run at the scheduled time. You can re-enable the task at a later time.
- View History—View the execution results for individual WLAN tasks including reasons for any failures.
- Delete Task(s)—Delete the selected task from the NCS server.

Downloading Software Task

By using this feature you can schedule tasks for downloading software to controllers. The Download Software Tasks page allows you to add, delete, view, enable, or disable scheduled download software tasks. To access the Download Software Tasks page and view current download software tasks, choose **Configure > Scheduled Configuration Tasks > Download Software**.

- Deleting a Download Software Task, page 9-219
- Enabling or Disabling a Download Software Task, page 9-219

Adding a Download Software Task

To add a download software task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software** to open the Download Software Task List page.

Step 3 From the Select a command drop-down list, choose **Add Download Software Task**.

Step 4 Click **Go**. The New Download Software Task page appears.

Step 5 Configure the following information:

- General
  - Task Name—Enter a Scheduled Task Name to identify this scheduled software download task.
- Schedule Details
  - Download Type—Select the download type. Select the **Download software to controller** check box to schedule download software to controller or select the **Pre-download software APs** check box to schedule the pre-download software APs. If you select **Download software to controller**, specify the image details.

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

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

  - Reboot Type—Indicates whether the reboot type is manual, automatic, or scheduled.

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

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

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

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

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

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

- Image Details—Specify the TFTP or FTP Server Information:

  Note Complete these details if you selected the Download software to controller option under Schedule Details.

  TFTP—Specify the TFTP Server Information:

  - From the File is Located on drop-down list, choose **Local machine** or **TFTP server**.

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

  - Specify the IP address of the TFTP server. This is automatically populated if the default server is selected.
  - Specify the local file name or click **Browse** to navigate to the appropriate file.
  - If you selected TFTP server previously, specify the File Name.

  FTP—Specify the FTP Server Information:

  - FTP Credentials Information—Enter the FTP username, password, and port if you selected the FTP radio button.
  - From the File is Located on parameter, choose **Local machine** or **FTP server**.

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

  - Specify the IP address of the FTP server. This is automatically populated if the default server is selected.
  - Specify the local file name or click the **Browse** button to navigate to the appropriate file.
  - If you selected FTP server previously, specify the File Name.

Step 6 Click **Save**.

Modifying a Download Software Task

To modify a download software task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Select the Task Name link to open the Download Software Task page.

Step 4 Make any necessary changes.

Note Any changes in Download Type (Download/Pre-download) or Server Type (FTP/TFTP) for the task in 'Enabled' state will set the task to 'Disabled' state and all the existing controllers will be disassociated from the task.

Step 5 Click **Save**.

Selecting Controllers for the Download Software Task

This page lists all the supported controllers that can be selected for the scheduled image download/pre-download task.

To select a controller for scheduled image download, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Click the Controller to open the Download Software Task details page.

Step 4 In the Download Software Task details page, Click **Select Controller** to view the controller list.

Note The Select Controllers page can also be accessed from Configure > Scheduled Configuration Tasks > Download Software > click hyperlink in the Select Controller column for any download task which is in Enabled, Disabled or in Expired state.

Note If the pre-download option is chosen for the task, then the controllers with software version 7.0.x.x or later only will be listed.

Note Controllers with Reachability Status 'Unreachable' cannot be selected for Download Software Task.

Step 5 Make any necessary changes.

Step 6 Click **Save**.

Viewing Download Software Results

To view the Schedule Run Results report, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Select the **Task Name** check box.

Step 4 From the Select a command drop-down list, choose **Schedule Run Results**.

Step 5 Click **Go**. The Schedule Run Results page provides the information:

- IP Address—The IP address of the controller to which the software to be downloaded.
- Controller Name—Name of the controller.
- Scheduled Run Time—Scheduled time of the download process.
- Last Updated Time—Last update time of the schedule download status (or result).
- Transfer Status—Current download status of the image in controller. For example, Not Initiated, Wrong file Type, Writing the code into flash, Transfer Successful.
- Reboot Status—Reboot status of the controller. For example, NA (if the reboot type is "Manual"), Reboot failed, Reboot Successful.
- Details—Detailed status about the download and reboot process.

Deleting a Download Software Task

To delete a scheduled download software task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Select the check box of the applicable scheduled task.

Step 4 From the Select a command drop-down list, choose **Delete Download Software Task**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

Enabling or Disabling a Download Software Task

To enable or disable a download software task, follow these steps:

Step 1 Choose **Configure > Scheduled Configuration Tasks**.

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Select the check box of the scheduled task to be enabled or disabled.

Step 4 From the Select a command drop-down list, choose **Enable Schedule** or **Disable Schedule**, as applicable.

Step 5 Click **Go**.

Configuring wIPS Profiles

NCS provides several pre-defined profiles from which to choose. These profiles (based on customer types, building types, industry types, and so on) allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. You can use a profile 'as is' or customize it to better meet your needs.

Tip To learn more about Cisco Adaptive wIPS features and functionality, go to **Cisco.com** to watch a multimedia presentation. Here you will find learning modules for a variety of NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

Pre-defined profiles include:

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

The wIPS Profiles page provides access to the wIPS profile list and the SSID group list. To access the wIPS Profile page, choose **Configure > wIPS Profiles**.

The current wIPS profile list and the SSID group list can be accessed from the left sidebar menu.

The wIPS Profiles page defaults to the Profile List. The SSID Group List page is accessible from the left sidebar menu.

Note Adaptive wIPS does not support the NCS partitioning feature.

Profile List

The wIPS Profiles > Profile List page allows you to view, edit, apply, or delete current wIPS profiles and to add new profiles.

Tip To learn more about Cisco Adaptive wIPS features and functionality, go to **Cisco.com** to watch a multimedia presentation. Here you will also find learning modules for a variety of NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To access the wIPS profile list for NCS, choose **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List. If the Profile List is not currently displayed, choose **Profile List** from the wIPS Profiles left sidebar menu.

The Profile List provides the following information for each profile:

- Profile Name—Indicates the user-defined name for the current profile. Click the profile name to view or edit profile details.

Note When you hover your mouse over the profile name, the Profile ID and version display.

- MSE(s) Applied To—Indicates the number of mobility services engines (MSEs) to which this profile is applied. Click the MSE number to view profile assignment details.
- Controller(s) Applied To—Indicates the number of controllers to which this profile is applied. Click the controller number to view profile assignment details.

Access the following features from the Select a command drop-down list:

- Adding a Profile, page 9-221
- Deleting a Profile, page 9-224
- Applying a Current Profile, page 9-224

The profile editor allows you to create new or modify current profiles. See the "Profile Editor" section on page 9-222 for more information.

Adding a Profile

A new wIPS profile can be created using the default or a pre-configured profile.

Tip To learn more about Cisco Adaptive wIPS features and functionality, go to **Cisco.com** to watch a multimedia presentation. Here you will also find learning modules for a variety of NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To add a wIPS profile, follow these steps:

Step 1 Select **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.

Step 2 From the Select a command drop-down list, choose **Add Profile**.

Step 3 Click **Go**.

Step 4 Type a profile name in the Profile Name text box of the Profile Parameters page.

Step 5 Select the applicable pre-defined profile, or choose **Default** from the drop-down list. Pre-defined profiles include:

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen

- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

Step 6 Select one of the following:

- Save—Saves the profiles to the NCS database with no changes and no mobility services engine or controller assignments. The profile appears in the profile list. Click the profile name to access the "Profile Editor" section on page 9-222 to edit the profile at a later time.
- Save and Edit—Saves the profile and launches the "Profile Editor" section on page 9-222.
- Cancel—Closes the Profile Parameters page without creating a profile.

Profile Editor

Tip To learn more about Cisco Adaptive wIPS features and functionality, **Cisco.com** to watch a multimedia presentation. Here you will also find learning modules for a variety of NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

The profile editor allows you to configure profile details including the following:

- SSID groups—Add, edit, or delete SSID groups.
- Policy inclusion—Determine which policies are included in the profile.
- Policy level settings—Configure settings for each policy such as threshold, severity, notification type, and ACL/SSID groups.
- MSE/controller applications—Select the mobility services engine(s) or controller(s) to which you want to apply the profile.

To configure profile details, follow these steps:

Step 1 Access the profile editor. This can be done in two ways:

- When creating a new profile, click **Save and Edit** in the Profile Parameters page.
- Click the profile name from the Profile List page.

Step 2 From the SSID Groups page, you can edit and delete current groups or add a new group. For more information on adding, editing, or deleting SSID groups, see the "Configure > wIPS > SSID Group List" section on page 9-225 for more information.

Step 3 When SSID groups have been added or edited as needed, select one of the following:

- Save—Saves the changes made to the SSID groups.
- Cancel—Returns to the profile list with no changes made.
- Next—Proceeds to the Profile Configuration page.

Step 4 From the Profile Configuration page, you can determine which policies are included in the current profile. The check boxes in the policy tree (located in the left Select Policy pane) indicate which policies are enabled or disabled in the current profile. You can enable or disable an entire branch or an individual policy as needed by selecting the check box for the applicable branch or policy.

Note By default, all policies are selected.

Note For detailed information regarding each of the wIPS policies, see the "wIPS Policy Alarm Encyclopedia" section on page 19-1.

Step 5 In the Profile Configuration page, click an individual policy to display the policy description and to view or modify current policy rule settings.

The following options are available for each policy:

- Add—Click **Add** to access the Policy Rule Configuration page to create a new rule for this policy.
- Edit—Select the check box of the applicable rule, and click **Edit** to access the Policy Rule Configuration page to edit the settings for this rule.
- Delete—Select the check box of the rule you want to delete, and click **Delete**. Click **OK** to confirm the deletion.

  Note There must be at least one policy rule in place. You cannot delete a policy rule if it is the only one in the list.

- Move Up—Select the check box of the rule you want to move up in the list. Click **Move Up**.
- Move Down—Select the check box of the rule you want to move down in the list. Click **Move Down**.

The following settings can be configured at the policy level:

- Threshold (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. When the threshold is reached for a policy, an alarm is triggered.

  Note Since every policy must contain at least one threshold, default thresholds are defined for each based on standard wireless network issues.

  Note Threshold options vary based on the selected policy.

  Note Alarms from Cisco Adaptive wIPS DoS and security penetration attacks are classified as security alarms. A summary of these attacks is located in the Security Summary page. Choose **Monitor > Security** to access this page. The wIPS attacks are located in the Threats and Attacks section.

- Severity—Indicates the level of severity of the selected policy. Parameters include critical, major, info, and warning. The value of this parameter may vary depending on the wireless network.
- Notification—Indicates the type of notification associated with the threshold.

- ACL/SSID Group—Indicates the ACL or SSID Group(s) to which this threshold is be applied.

Note Only selected groups trigger the policy.

Step 6 When the profile configuration is complete, select one of the following:

- Save—Saves the changes made to the current profile.
- Cancel—Returns to the profile list with no changes made.
- Back—Returns to the SSID Groups page.
- Next—Proceeds to the MSE/Controller(s) page.

Step 7 In the Apply Profile page, select the check box(es) of the mobility services engine and controller(s) to which you want to apply the current profile.

Step 8 When the applicable mobility services engine(s) and controller(s) are selected, choose one of the following:

- Apply—Applies the current profile to the selected mobility services engine/controller(s).
- Cancel—Returns to the profile list with no changes made.

Note A created profile can also be applied directly from the profile list. From the Profile List page, select the check box of the profile you want to apply and click **Apply Profile** from the Select a command drop-down list. Click **Go** to access the Apply Profile page.

Deleting a Profile

To delete a wIPS profile, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.

Step 2 Select the check box of the wIPS profile(s) you want to delete.

Step 3 From the Select a command drop-down list, choose **Delete Profile**.

Step 4 Click **Go**.

Step 5 Click **OK** to confirm the deletion.

Note If the profile is already applied to a controller, it cannot be deleted.

Applying a Current Profile

Tip To learn more about Cisco Adaptive wIPS features and functionality, **Cisco.com** to watch a multimedia presentation. Here you will also find learning modules for a variety of NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To apply a wIPS profile, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.

Step 2 Select the check box of the wIPS profile(s) you want to apply.

Step 3 From the Select a command drop-down list, choose **Apply Profile**.

Step 4 Click **Go**.

Step 5 Select the mobility services engine(s) and controller(s) to which the profile will be applied.

Note If the new assignment is different than the current assignment, you are prompted to save the profile with a different name

Step 6 When the applicable mobility services engine(s) and controller(s) are selected, choose one of the following:

- Apply—Applies the current profile to the selected mobility services engine/controller(s).
- Cancel—Returns to the profile list with no changes made.

Configure > wIPS > SSID Group List

The SSID (Service Set IDentifier) is a token or key which identifies an 802.11 (Wi-Fi) network. You must know the SSID to join an 802.11 network. SSIDs can be associated with a wIPS profile as a group using the SSID group list feature.

An SSID group can be added to a profile by importing it from the Global SSID Group List page (Configure > wIPS Profiles > SSID Group List) or by adding one directly from the SSID Groups page located in the "Profile Editor" section on page 9-222.

- Global SSID Group List—A global SSID group can be set up separately and added to multiple profiles as needed.
- SSID Groups

Tip To learn more about Cisco Adaptive wIPS features and functionality, **Cisco.com** to watch a multimedia presentation. Here you will also find learning modules for a variety of NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

Global SSID Group List

The SSID Group List page allows you to add or configure global SSID groups that you may later import into an applicable wIPS profile.

Tip To learn more about Cisco Adaptive wIPS features and functionality, **Cisco.com** to watch a multimedia presentation. Here you will also find learning modules for a variety of NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To access the SSID Group List page, choose **Configure > wIPS Profiles**. From the left sidebar menu, choose **SSID Group List**. The SSID Group List page display current SSID groups and their associated SSIDs.

The following functions are available in this page:

- Adding a Group, page 9-226
- Editing a Group, page 9-226
- Deleting Group, page 9-227

Adding a Group

To add an SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **SSID Group List**.

Step 3 From the Select a command drop-down list, choose **Add Group**.

Step 4 Click **Go**.

Step 5 In the SSID configuration page, type an SSID group name in the available text box.

Step 6 Enter the SSIDs in the SSID List text box. Separate multiple SSIDs with a space.

Step 7 When finished, select one of the following:

- Save—Saves the SSID group and adds it to the SSID Group List.
- Cancel—Closes the SSID configuration page without saving the new SSID group.

Note To import the SSID groups to a profile, choose **Configure > wIPS Profile**. Click the profile name for the applicable profile to open the SSID Groups page. From the Select a command drop-down list, choose **Add Groups from Global List**. Select the check box(es) for the SSID group(s) you want to import and click **Save**.

Editing a Group

To edit a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **SSID Group List**.

Step 3 Select the check box of the SSID group that you want to edit.

Step 4 From the Select a command drop-down list, choose **Edit Group**.

Step 5 Click **Go**.

Step 6 In the SSID configuration page, make the necessary changes to the SSID group name or the SSID list.

Step 7 When finished, select one of the following:

- Save—Saves the current changes and closes the SSID configuration page.

- Cancel—Closes the SSID configuration page without saving the changes.

Deleting Group

To delete a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **SSID Group List**.

Step 3 Select the check box of the SSID group(s) that you want to delete.

Step 4 From the Select a command drop-down list, choose **Delete Group**.

Step 5 Click **Go**.

Step 6 Click **OK** to confirm the deletion.

SSID Groups

The SSID Groups page is the first page displayed when you access the "Profile Editor" section on page 9-222. This page displays SSID groups that are included for the current wIPS profile.

From this page, you can add, import, edit, or delete an SSID group for the current profile.

Tip To learn more about Cisco Adaptive wIPS features and functionality, **Cisco.com** to watch a multimedia presentation. Here you will also find learning modules for a variety of NCS topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

The following functions for the current profile are available in this page:

- Adding a Group, page 9-227
- Adding Groups from Your Global List, page 9-228
- Editing a Group, page 9-228
- Deleting Group, page 9-228

Adding a Group

To add an SSID Group to the current wIPS profile, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **Profile List**.

Step 3 Click the profile name of the applicable wIPS profile.

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

Step 5 Click **Go**.

Step 6 In the SSID configuration page, type an SSID group name in the available text box.

Step 7 Enter the SSIDs in the SSID List text box. Separate multiple SSIDs with a comma.

Step 8 When finished, select one of the following:

- Save—Saves the SSID group and adds it to the SSID Group List.
- Cancel—Closes the SSID configuration page without saving the new SSID group.

Adding Groups from Your Global List

SSID groups can also be added by importing them from your Global SSID Groups list. See the "Global SSID Group List" section on page 9-225 for more information on creating a global SSID groups list.

To import SSID groups into a profile, follow these steps:

Step 1 Select **Configure > wIPS Profile**.

Step 2 Click the profile name for the applicable profile to open the SSID Groups page.

Step 3 From the Select a command drop-down list, choose **Add Groups from Global List**.

Step 4 Select the check box(es) for the SSID group(s) you want to import.

Step 5 Click **Save**.

Editing a Group

To edit a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **Profile List**.

Step 3 Click the profile name of the applicable wIPS profile.

Step 4 Select the check box of the SSID group that you want to edit.

Step 5 From the Select a command drop-down list, choose **Edit Group**.

Step 6 Click **Go**.

Step 7 In the SSID configuration page, make the necessary changes to the SSID group name or the SSID list.

Step 8 When finished, select one of the following:

- Save—Saves the current changes and closes the SSID configuration page.
- Cancel—Closes the SSID configuration page without saving the changes.

Deleting Group

To delete a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.

Step 2 From the left sidebar menu, choose **Profile List**.

Step 3 Click the profile name of the applicable wIPS profile.

Step 4 Select the check box of the SSID group that you want to delete.

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

Step 6 Click **Go**.

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

Configuring ACS View Servers

To facilitate communication between NCS and the ACS View Server and to access the ACS View Server tab, you must add a view server with credentials.

Note NCS only supports ACS View Server 5.1 or above.

To configure the ACS View Server Credentials, follow these steps:

Step 1 Choose **Configure > ACS View Server**.

Step 2 Enter the port number of the ACS View Server you are adding. (Some ACS View Servers do not allow you to change the port on which HTTPS runs.)

Step 3 Enter the password that was established on the ACS View Server. Confirm the password.

Step 4 Specify the time in seconds after which the authentication request times out and a retransmission is attempted by the controller.

Step 5 Specify the number of retries that will be attempted.

Step 6 Click **Submit**.

Configuring ACS View Server Credentials

To facilitate communication between NCS and the ACS View Server and to access the ACS View Server tab, you must add a view server with credentials.

To configure the ACS View Server Credentials, follow these steps:

Note NCS only supports ACS View Server 5.1 or above.

Step 1 Choose **Configure > ACS View Server**.

Step 2 Enter the port number of the ACS View Server you are adding. (Some ACS View Servers do not allow you to change the port on which HTTPS runs.)

Step 3 Enter the password that was established on the ACS View Server. Confirm the password.

Step 4 Specify the number of retries that will be attempted.

Step 5 Click **Submit**.

Configuring TFTP Servers

Use the Configure > TFTP Servers page to add or delete TFTP servers from NCS.

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

This section contains the following topics:

Adding a TFTP Server

To add a TFTP server, follow these steps:

Step 1 Choose **Configure > TFTP Servers**.

Step 2 From the Select a command drop-down list, choose **Add TFTP Server**.

Step 3 Enter a TFTP server name. This is a user-defined name for the server.

Step 4 Enter the IP address of the TFTP server.

Step 5 Click **Save**.

Deleting TFTP Servers

To delete a TFTP server, select the check box for the applicable server, and choose **Delete TFTP Servers** from the Select a command drop-down list. Click **Go** and then click **OK** to confirm the deletion.

Interactive Graphs

This section contains the following topics:

Interactive Graphs Overview

Interactive graph features are based upon Adobe Flex technology that uses flash to render the graphs on the browser and provide interactivity to the user.

Minimum Requirements include:

- Windows—Flash Player version 9.0.115.0.

- Linux—Flash Player version 9.0.115.0.

Note If you do not have a flash player or your version is not recent enough, an error page prompts you with this information. Click the **Get Latest Flash Player** link to access Adobe website. From this site, you can download the latest version of the flash player. You only need to download the flash player once. Remember to restart the browser following the download.

NCS Interactive Graphs include line, area, pie, and stacked bar graphs.

Interactive Graph Features

Interactive graph features include the following:

- Two distinct types of graphs:
  - Time-based Graphs
  - Non-Time based
- Support for automatic refresh—The graphs refresh automatically within a predetermined interval of time.
- Two graph views:
  - Graph (Chart) view (default)
  - Table (Grid) view

Note Use the two toggle buttons located at the bottom left side of the graph page to switch between the two graph views. To view the button type, hover your mouse cursor over the applicable button for a tool tip identifying View in Chart or View in Grid. Click **View in Chart** to view the data in a graph. Click **View in Grid** to view the data in a table.

- Enlarged View—Click the button located at the bottom right side of the graph to enlarge the graph in a separate page. The Chart View and Grid View buttons are available in the new page to change the type of graph displayed.

Time-based Graphs

For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed. The time-frame options include the following:

- 6h—Denotes the last six hours of data from the current time. The data is gathered from the current database table.
- 1d—Denotes the last day (24 hours) of data from the current time. The data is gathered from the current database table.
- 1w—Denotes the last week (seven days) of data from the current time. The data is gathered from the hourly aggregated table.
- 2w—Denotes the last two weeks of data from the current time. The data is gathered from the hourly aggregated table.

- 4w—Denotes the last four weeks of data from the current time. The data is gathered from the hourly aggregated table.
- 3m—Denotes the last three months of data from the current time. The data is gathered from the daily aggregated table.
- 6m—Denotes the last six months of data from the current time. The data is gathered from the weekly aggregated table.
- 1y—Denotes the past year (12 months) of data from the current time. The data is gathered from the weekly aggregated table.
- Custom—User-selected time period. Both days and hours can be set for the start and end dates. The use of a current or hourly, daily, or weekly aggregated source for data depends upon the selected start date.

Note The data management settings for aggregated tables are located in "Configuring Administrative Settings" section on page 15-3 under the Administration menu. The default settings have a value of 31 days for Daily Aggregated Data and ten weeks for Weekly Aggregated Data.

For more information on Interactive Graphs, see the "Interactive Graphs" section on page 9-230.