CHAPTER 9

Configuring Access Points

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

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 menu, choose **Enable**.

To then configure an access point's priority, refer to "Configuring Access Points" section on page 9-16.

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 WCS 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 WCS 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. Refer to the "Configuring Access Point Templates" section on page 12-111 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.

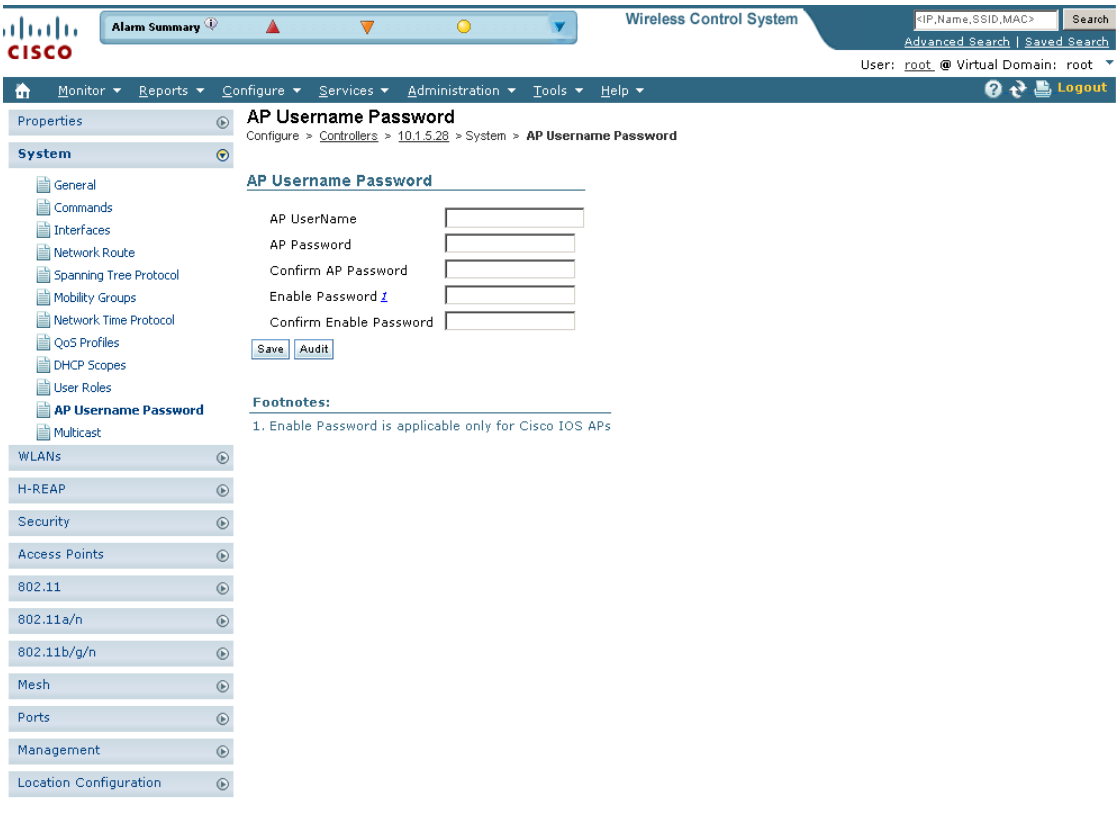
Follow these steps to establish a global username and password.

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 window appears (see Figure 9-1).

Figure 9-1 AP Username Password Window



Step 4 In the AP Username field, enter the username that is to be inherited by all access points that join the controller.

Step 5 In the AP Password field, enter the password that is to be inherited by all access points that join the controller. Re-enter in the Confirm AP Password field.

Step 6 For Cisco autonomous access points, you must also enter and confirm an enable password. In the AP Enable Password field, enter the enable password that is to be inherited by all access points that join the controller. Re-enter in the Confirm Enable Password field.

Step 7 Click **Save**.

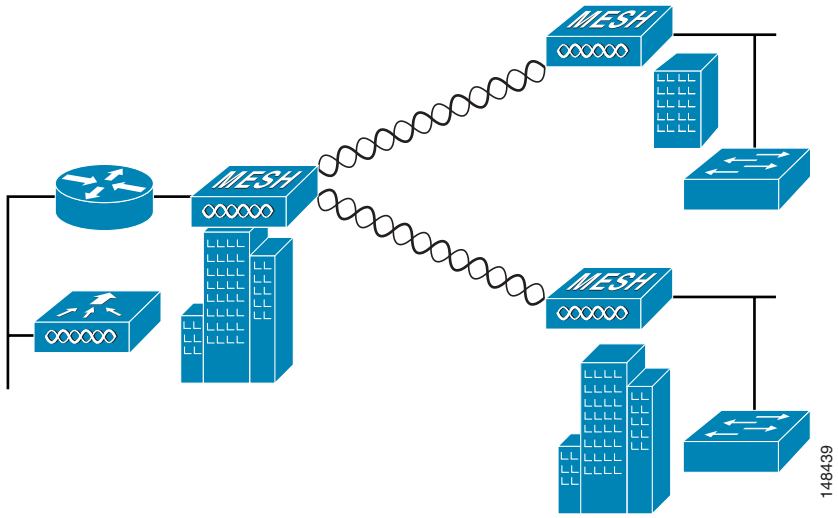
Configuring Ethernet Bridging and Ethernet VLAN Tagging

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 9-2).

Note You do not need to configure VLAN tagging to use Ethernet bridging for point-to-point and point-to-multipoint bridging deployments.

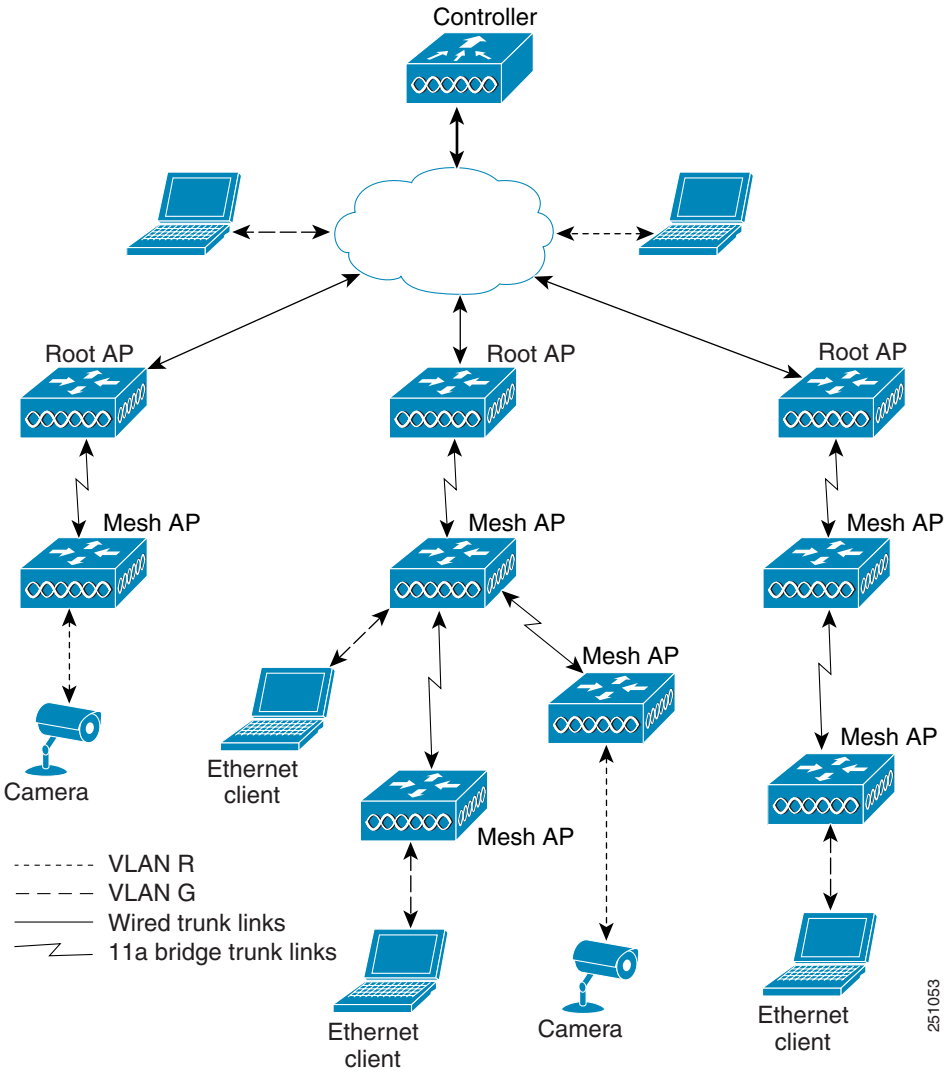
Figure 9-2 Point-to-Multipoint Bridging



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 9-3).

Figure 9-3 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). Refer to "Configuring Ethernet Bridging and Ethernet VLAN Tagging" section on page 9-3.
  - VLAN transparent is enabled by default. To set as non-VLAN transparent, you must uncheck the VLAN transparent option in the Global Mesh Parameters window.
- 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

Follow these steps to enable Ethernet Bridging and VLAN tagging on a RAP or MAP.

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

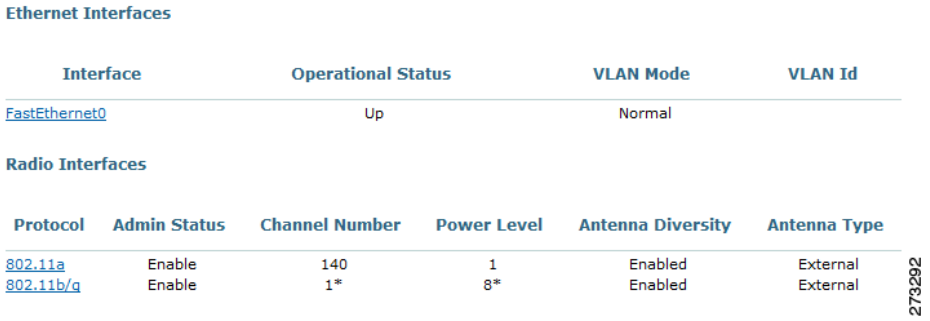
Step 2 Click the name of the mesh access point for which you want to enable Ethernet bridging. A configuration window for the access point appears.

Step 3 In the Bridging Information section, choose the appropriate backhaul rate from the Data Rate drop-down menu. 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 menu.

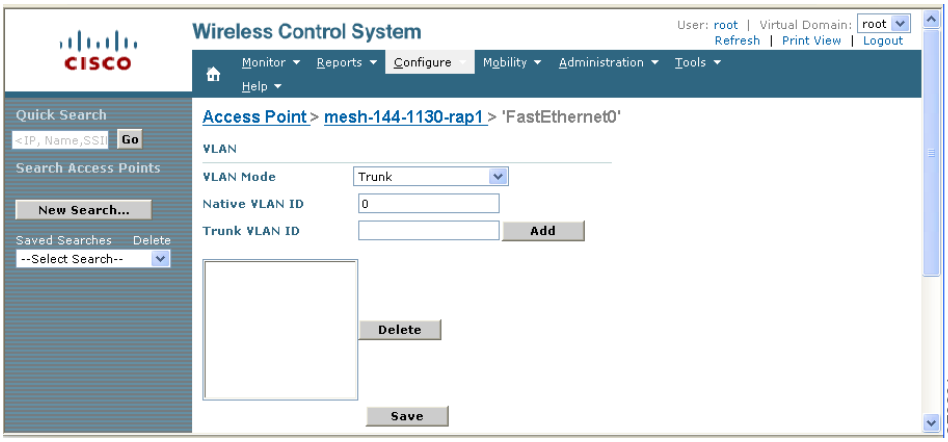
Step 5 Click the appropriate Ethernet interface link (such as FastEthernet or gigabitEthernet1) (see Figure 9-4).

Figure 9-4 Configure > Access Points > AP Name Window



Step 6 Within the Ethernet interface window, perform one of the following (see Figure 9-5):

Figure 9-5 Access Point > Ethernet Interface Window



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 menu.

   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 menu.
   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 menu.
   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 (WCS) 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 1250 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 WCS, the following functions are available when managing autonomous access points:

- Adding Autonomous access points
- Configuring autonomous access points
- Viewing current autonomous access points from the Monitor > Access Points page (see Monitoring Access Points for more information)
- Adding and viewing autonomous access points from the Monitor > Maps page (see Maps for more information)
- Monitoring associated alarms
- Performing an autonomous access point background task
  - Checks the status of autonomous access points managed by WCS.
  - 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
- Migrating autonomous access points to lightweight access points

Adding Autonomous Access Points to WCS

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

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

Adding Autonomous Access Points by Device Information

Autonomous access points can be added to WCS 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 menu, choose **Add Autonomous APs**.

Step 3 Click **Go**.

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

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

Step 6 Click the **Verify Telnet/SSH Credentials** check box if you want this controller to verify Telnet/SSH credentials. You may want to leave this unchecked (or disabled) because of the substantial time it takes for discovery of the devices.

Step 7 Enter the SNMP parameters including version number, number of retries, and timeout in seconds.

Step 8 Enter Telnet credentials for migration (optional).

Note The Telnet credentials are required to convert the access points from autonomous to unified and for access point CLI templates.

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

Step 9 Click **OK**.

Adding Autonomous Access Points by CSV File

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

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

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

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

Step 3 Click **Go**.

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

Step 5 Enter or browse to the applicable CSV file.

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
1.1.1.1,255.255.255.0,v2,public,,,,,,3,4
2.2.2.2,255.255.255.0,v2,public,,,,,,3,4,Cisco,Cisco,2,10

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
10.77.159.185,255.255.255.128,v3,default,HMAC-MD5,default,None,,3,4
10.77.159.203,255.255.255.128,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**.

To remove an autonomous access point from WCS:

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 WCS

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

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

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

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

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

Downloading Images to Autonomous Access Points

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 WCS. Follow these steps to download images to autonomous access points.

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

Step 2 Click 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 menu, choose **Download Autonomous AP Image**. The image download window appears.

To ensure that no more than ten access points are selected for download, a check is made. The image must be compatible with all of the selected access points. Scheduling an immediate task initiates the image download. It is periodically refreshed.

Work Group Bridge (WGB) Mode

Wireless Group Bridge (WGB) mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The WGB and its wired clients are listed as client in WCS if the AP mode is set to Bridge, and the access point is bridge capable.

To view a list of all WCS clients that are WGBs, choose **Monitor > Clients.** At the Show drop-down menu, choose **WGB Clients** and click **Go**. The Clients (detected as WGBs) window appears. Click a User to view detailed information regarding a specific WGB and its wired clients.

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

Autonomous Access Point to Lightweight Access Point Migration

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

Note Once an access point is converted to lightweight, the previous status or configuration of the access point is not retained.

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

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

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

- View Migration Analysis Summary—Lists the pass or fail status as required for an access point conversion. Only those access points with all criteria as pass are eligible for conversion.

Viewing the Migration Analysis Summary

Follow these steps to view the Migration Analysis Summary.

Note You can also view the migration analysis summary by choosing Tools > Migration Analysis.

Step 1 Choose **Configure > Autonomous AP Migration Templates**.

Step 2 Click **View Migration Analysis Summary** from the Select a command drop-down menu and click **Go**. The Migration Analysis Summary window appears.

The autonomous access points are eligible for migration only if all the criteria have a pass status. A red X designates ineligibility, and a green checkmark designates eligibility. These columns represent the following:

- Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- Software Version Criteria—Conversion is supported only from Cisco IOS 12.3(7)JA releases excluding 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, and 12.3(11)JA3.
- Role Criteria—A wired connection between the access point and controller is required in order to send the association request; therefore, the following autonomous access point roles are required:
  - root

  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only
- Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.

Upgrading Autonomous Access Points

You can choose to upgrade the autonomous access points manually or automatically. From the Migration Analysis window, you can select the access point with the software version listed as failed and choose Upgrade Firmware (Manual or Automatic) from the Select a command drop-down menu. This process upgrades the autonomous firmware image of the IOS access point to a supported version.

WCS uses a Telnet-based connection to upgrade the access point firmware. If you choose the automatic option, the internal TFTP server is used with the default images present in WCS. The default images as per device type are as follows:

- ap801-k9w7-tar.124-10b.JA3.tar
- c1100-k9w7-tar.123-7.JA5.tar
- c1130-k9w7-tar.123-7.JA5.tar
- c1200-k9w7-tar.123-7.JA5.tar
- c1240-k9w7-tar.12307.JA5.tar
- c1250-k9w7-tar.124-10b.JA3.tar
- c1310-k9w7-tar.123-7.JA5.tar

If you choose the manual option, an additional screen with TFTP server IP, file path, and file path name appears. The final window is the report page.

Changing Station Role to Root Mode

Because a wired connection between the access point and controller is required in order to send the association request, the autonomous access point must be assigned the appropriate role. If the role shows as ineligible, you can choose **Change Station Role to Root Mode** from the Select a command drop-down menu.

Running Migration Analysis

You can choose **Run Migration Analysis** from the Select a command drop-down menu of the Migration Analysis Summary window. The resulting migration analysis summary shows the current status of different criteria. Initially, migration analysis is run automatically when the access point is discovered.

Generating the Migration Analysis Report

You can choose **View Migration Analysis Report** from the Select a command drop-down menu of the Migration Analysis Summary window to generate a report. The report includes the following:

- Access point address
- Status

- Timestamp
- Access point logs

Disabling Access Points that are Ineligible

If an autonomous access point is labelled as ineligible for conversion, you can disable it.

Adding/Modifying a Migration Template

If you want to add a migration template, choose **Add Template** from the Select a command drop-down window of the Configure > Autonomous AP Migration Templates window.

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

Enter or modify the following migration parameters:

General

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

Upgrade Options

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

Controller Details

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

- Controller IP—Enter the IP address of the WLAN controller you are wanting to add to the newly migrated access point.
- AP Manager IP—Specify the controller the access point should join by entering the access point manager IP address.

  Note For SSC-enabled access points, this IP address must be the same as the controller IP field. For MIC-enabled access points, the IP addresses need not match.

- User Name—Enter a valid username for login of the WLAN controller.
- Password—Enter a valid password for this username used during WLAN controller login.

TFTP Details

When you installed and set up WCS, it provided its own TFTP and FTP server.

- TFTP Server IP—Enter the IP address of the WCS server.
- File Path—Enter the TFTP directory which was defined during WCS setup.
- File Name—Enter the CAPWAP conversion file defined in the TFTP directory during WCS setup (for example, c1240-rcvk9w8-tar.123-11JX1.tar).

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

- **Select AP**s—Selecting this option provides a list of autonomous access points in WCS from which to choose the access points for conversion. Only those access points with migration eligibility as *pass* can be chosen for conversion.
- **Select File**—To provide CSV information for access points intended for conversion.

Configuring Access Points

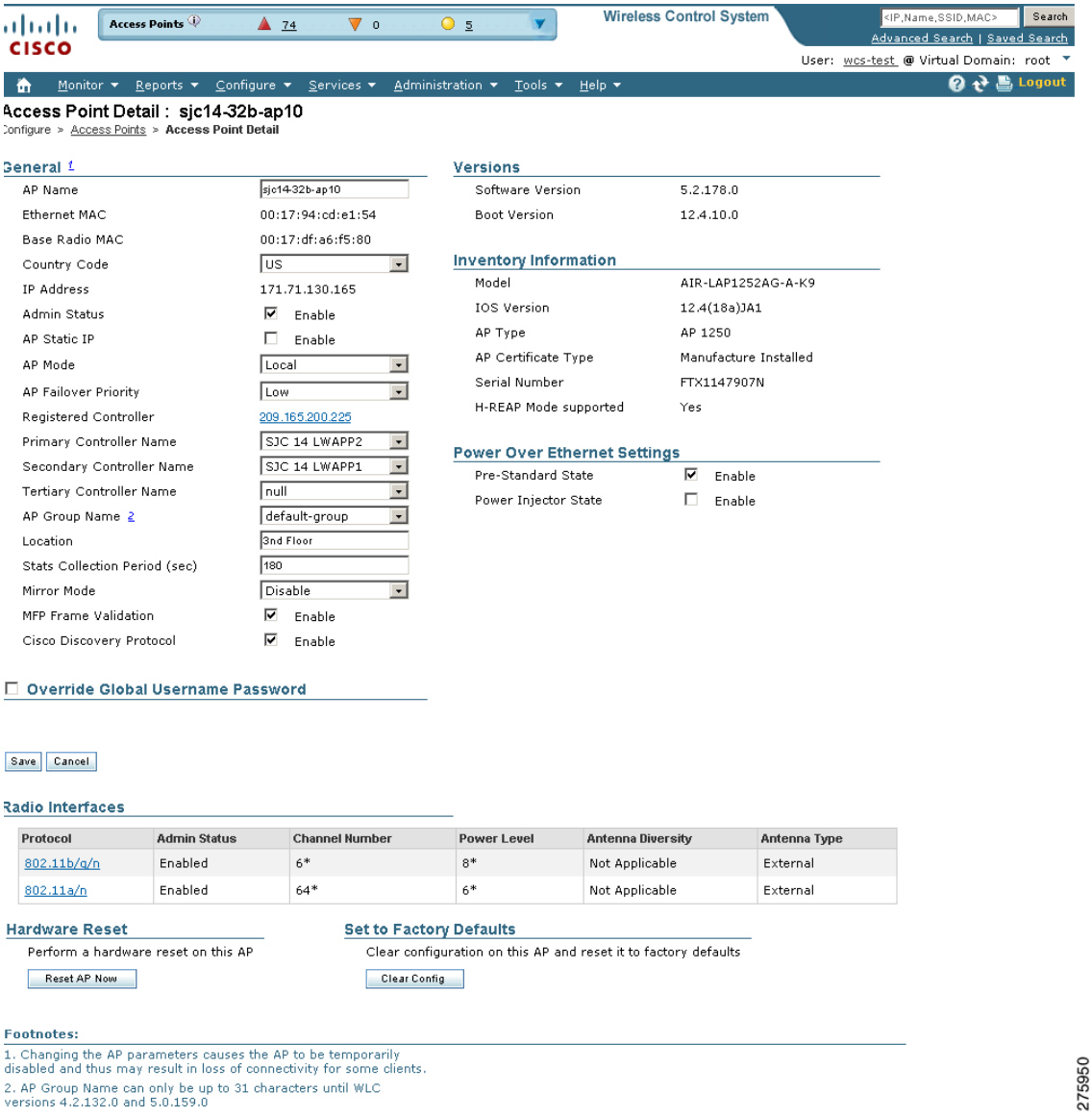
Choose **Configure > Access Points** to see a summary of all access points in the Cisco WCS database. The summary information includes the following:

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

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

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

Figure 9-6 Detailed Access Point Information



Note The operating system software automatically detects and adds an access point to the Cisco WCS database as it associates with existing controllers in the Cisco WCS database.

Note Access point parameters may vary depending on the access point type.

Some of the parameters on the window are automatically populated.

- The General portion displays the Ethernet MAC, the Base Radio MAC, IP Address, and status.
- The Versions portion of the window 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 Radio Interfaces portion provides the current status of the 802.11a/n and 802.11b/g/n radios such as admin status, channel number, power level, antenna mode, antenna diversity, and antenna type.

Follow the steps below to set the configurable parameters.

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

- You can configure up to 20 countries per controller.
- Because only one auto-RF engine and one list of available channels exist, configuring multiple countries limits the channels available to auto-RF in the common channels. A common channel is one that is legal in each and every configured country.
- When you configure access points for multiple countries, the auto-RF channels are limited to the highest power level available in every configured country. A particular access point may be set to exceed these limitations (or you may manually set the levels in excess of these limitations), but auto-RF does not automatically choose a non-common channel or raise the power level beyond that available in all countries.

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

- 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. Refer to the "Configuring Access Point Radios for Tracking Optimized Monitor Mode" section on page 9-31 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, choose Monitor. Choose the **Enhanced wIPS Engine Enabled** check box and select **wIPS** from the Monitor Mode Optimization drop-down menu. If wIPS is disabled, you cannot use monitor mode optimization. Before you can enable an access point to be in wIPS mode, you must disable the access point radios. If you do not disable the access point radio, an error message displays. After you have enabled the access point for wIPS, re-enable the radios.

- 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 http://www.wildpackets.com/support/legacy/airopeek/overview.
- 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 WCS if the AP mode is set to Bridge, and the access point is bridge capable.

Step 7 Disable any access point radios.

Step 8 From the AP Failover Priority drop-down menu, choose Low, Medium, High, or Critical to indicate the access point's failover priority. The default priority is low. See "Setting AP Failover Priority" section on page 9-1 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 Click the **Cisco Discovery Protocol** check box if you want to enable it. CDP is a device discovery protocol that runs on all Cisco-manufactured equipment, such as routers, bridges, and communication servers. Each device sends periodic messages to a multicast address and listens to the messages that others send in order to learn about neighboring devices. When the device boots, it sends a CDP packet specifying whether the device is inline power enabled so that the requested power can be supplied.

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

Step 16 Check the check box to enable rogue detection. Refer to the "Rogue Access Point Location, Tagging, and Containment" section on page 16-18 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, refer to the *Cisco Wireless LAN Controller Configuration Guide*.

Step 17 Check 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. Encryption is available only if the access point is connected to a 5500 series controllers with a PLUS license.

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 Check the **SSH Access** check box to enable SSH access.

Step 20 Check 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, check 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 window.

The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

Step 22 Check the **Enable Link Latency** check box to enable link latency for this access point or uncheck it to prevent the access point from sending the round-trip time to the controller after every echo response is received. Refer to the "Configuring Link Latency Settings for Access Points" section on page 9-38 for more information on link latency.

Step 23 You can now manipulate power injector settings through WCS without having to go directly to the controllers. In the Power Over Ethernet Settings section, check 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 checked, 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 WCS, 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 Check 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 Clearing 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, WCS displays locally switched VLANs.

Step 25 Select the role of the mesh access point from the Role drop-down menu. The default setting is MAP.

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

Step 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 menu. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps.

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

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

Step 28 Choose **Enable** from the Ethernet Bridging drop-down menu 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**.

Downloading Images

From the Select a command drop-down menu in the Configure > Access Points window, you can select Download Autonomous AP Image. TFTP is used for the download. WCS verifies that no more than ten access points are selected for download. An appropriate warning also appears if another download is in progress. The image must be compatible with all of the selected access points prior to image download. The image download starts immediately and cannot be scheduled for a future time. An image download status screen is displayed and refreshed periodically.

Importing Access Point Configuration

From the Select a command drop-down menu in the Configure > Access Points window, you can download the startup configurations of access points that are saved in the WCS database using the Import AP Config command. Only the most recent configuration is maintained in the WCS database. You cannot download a single configuration to multiple access points with this feature. For multiple access points, you must instead use the Modify Access Point Configuration feature. You can click the Session Output icon to see the session playback of the IOS command.

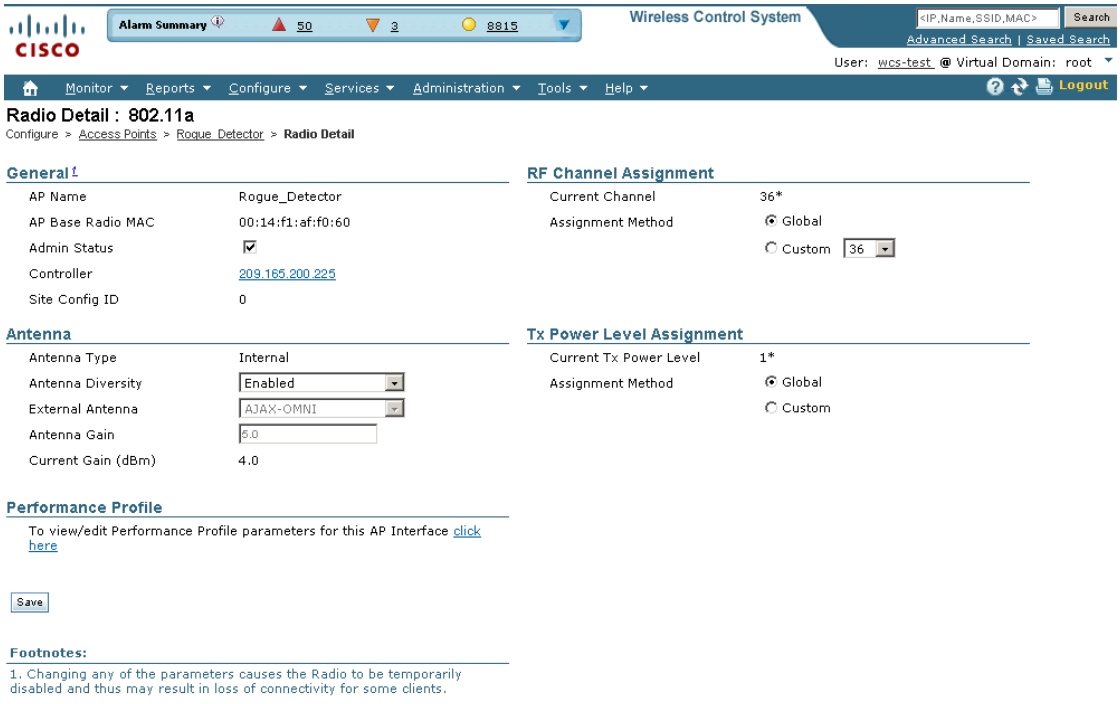
11n Antenna Selection

WCS 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 9-7).

Figure 9-7 Access Point > 802.11a/n



251726

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—Check the box to enable the administration state of the access point.
- Controller—IP address of the controller. Click the controller's IP address for more details.
- Site Config ID—Site identification number.

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 menu.
- 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 9-1 Antenna Names, Gain, and Descriptions

Antenna Name	Gain (dB)	Description
AIR-ANT1000	0.00	AP 1000 Integrated antenna
CUSH-S5157WP	3.00	5.15-5.87 GHz diversity wide-band 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		
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 2.4/5GHz 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
BR1310	13.00	Integrated patch directional antenna
AIR-ANT2460	6.00	Patch wall mount antenna

Table 9-1 Antenna Names, Gain, and Descriptions (continued)

Antenna Name	Gain (dB)	Description
AIR-ANT2465	6.50	Diversity patch wall mount antenna
AIR-ANT2485	9.00	Patch wall mount antenna
AIR-ANT2480V-N	8.00	2.4GHz omni antenna for mesh
AIR-ANT5114P-N	14.00	5GHz patch for mesh
AIR-ANT5117S-N	17.00	5GHz sector for mesh
AIR-ANT2450V-N	5.00	2.4GHz omni antenna
AIR-ANT5180V-N	8.00	5GHz omni antenna
AIR-ANT2450S-R	5.50	2.4GHz 135-degree sector antenna
AIR-ANT2451V-R	2.4GHz—2.0 5GHz—3.0	2.4GHz and 5GHz four-element dual band antenna. **Note** Two elements for the 2.4GHz band and two elements for the 5GHz band.

The following table lists the default values of some of the attributes of an access point when it is added to the WCS for the first time:

Table 9-2 Access Point Attributes

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
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
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

Table 9-2 Access Point Attributes (continued)

AP Type	Radio Type	Supported Antennas
AP 1250	802.11a	AIR-ANT5135D-R, AIR-ANT5145V-R, AIR-ANT5160V-R, AIR-ANT5170V-R, AIR-ANT5195V-R
	802.11b/g	AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT2410Y-R, AIR-ANT5959, AIR-ANT3549, AIR-ANT2506, AIR-ANT3213
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
	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
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
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

WLAN Override

The following 802.11a WLAN Override parameter appears:

- WLAN Override—Select Enable or Disable from the drop-down menu.

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 display:

- 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 menu. 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

WCS 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—Click the check box beside Antenna A or Antenna B to enable them.

- Receive Antenna—Click the check box beside Antenna A, B, or C to enable them.

11n Parameters

The following 11n parameters display:

- 11n Supported—Indicates whether or not 802.11n radios are supported.

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, refer to Step 6 in the "Configuring Access Points" section on page 9-16.

Follow the steps below to set enable TOMM and assign monitoring channels on the access point radio.

Step 1 After enabling Monitor Mode at the access point level, choose **Configure > Access Points**.

Step 2 At the Access Points window, choose the **802.11 b/g Radio** link for the appropriate access point.

Step 3 In the General portion, disable **Admin Status** by unchecking the check box. This disables the radio.

Step 4 Check the **TOMM** check box. This check box only appears for Monitor Mode APs. Drop-down menus 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 menu.

Step 6 Click **Save**. Channel selection is saved.

Step 7 At the Radio parameters window, re-enable the radio by checking 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** window.

Scheduling Radio Status

To schedule a radio status change (enable or disable), follow these steps:

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

Step 2 Choose the check box for the applicable access point(s).

Step 3 From the Select a command drop-down menu, choose **Schedule Radio Status**.

Step 4 Click **Go**.

Step 5 Choose **Enable** or **Disable** from the Admin Status drop-down menu.

Step 6 Use the **Hours** and **Minutes** drop-down menus 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 Choose the check box for the applicable access point(s).

Step 3 From the Select a command drop-down menu, 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 window shows an audit status for each of the access points. You can also view the audit report for the selected access points. The report shows the time of the audit, the IP address of the selected access point, and the synchronization status.

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

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

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

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

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

Searching Access Points

Use the search options in the right uppermost corner of the window 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 menus.
- **Advanced Search:** An advanced search allows you to search for a device based on a variety of categories and filters.

Refer to the "Using the Search Feature" section on page 2-28 for further information.

After you click **Go**, the access point search results appear:

Table 9-3 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.

Table 9-3 Access Point Search Results (continued)

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, or Bridge (as described in Step 6 of Configuring Access Points above).

Viewing Mesh Link Details

You can access mesh link details in several ways:

- Mesh Tab on the WCS Home page
- Monitor > Access Points and clicking the **Mesh Links** tab and then 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—
- Link Events—The last five events for the link are displayed.
- Mesh Worst 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 WCS 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. Follow these steps to access the rogue access point rules. Refer to the "Configuring a Rogue AP Rules Template" section on page 12-76 for more information.

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 Spectrum Experts

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

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

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

Adding a Spectrum Expert

To add a Spectrum Expert, follow these steps:

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

Step 2 Click **Add a Spectrum Expert** or choose **Add a Spectrum Expert** from the Select a command drop-down menu.

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

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

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

Monitoring Spectrum Experts

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

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

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

Spectrum Experts > Summary

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

Hostname—Displays the host name or IP address.

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

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

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

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

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

Interferers > Summary

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

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

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

Spectrum Experts Details

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

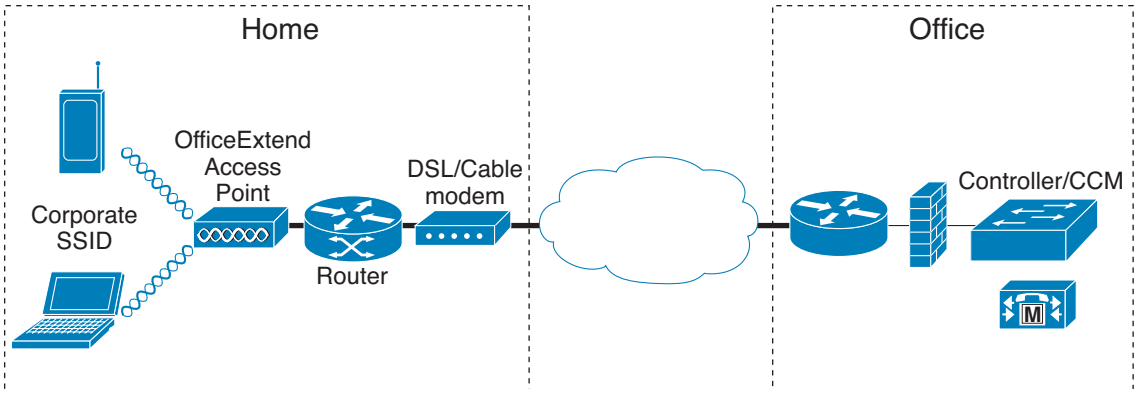
- Total Interferer Count—Given from the specific spectrum expert.
- Active Interferers Count Chart—Displays a pie chart that groups interferers by category.
- Active Interferer Count Per Channel—Displays the number of interferers grouped by category on different channels.
- AP List—Provides a list of access points detected by the spectrum expert. These access points are on channels that have active interferers detected.
- Affected Clients List—Provides a list of clients that are currently authenticated to an access point. You can select specific RADIUS or LDAP servers to provide external authentication on the **Security > AAA** panel.

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 9-8 illustrates a typical OfficeExtend access point setup.

Figure 9-8 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 WCS database as it associates with existing controllers in the Cisco WCS 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 From the Configure > Access Point details page, check the **Enable Link Latency** check box to enable link latency for this access point or uncheck 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 unchecked.

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.