Monitoring Wireless Devices

This chapter describes how to use WCS to monitor your wireless LANs. It contains these sections:

- Monitoring Rogue Access Points, page 6-2
- Finding Clients, page 6-5
- Finding Coverage Holes, page 6-6
- Pinging a Network Device from a Controller, page 6-7
- Viewing Controller Status and Configurations, page 6-7
- Viewing WCS Statistics Reports, page 6-9
- Viewing Mesh Tree, page 6-11
- Running a Link Test, page 6-12
- Retrieving the Unique Device Identifier on Controllers and Access Points, page 6-14
Monitoring Rogue Access Points

Because unauthorized rogue access points are inexpensive and readily available, employees sometimes plug them into existing LANs and build ad hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. Even more alarming, wireless users frequently publish unsecure access point locations, increasing the odds of having the enterprise security breached.

Rather than having a person with a scanner manually detect rogue access points, the Cisco Wireless LAN Solution automatically collects information on rogue access points detected by its managed access points (by MAC and IP address) and allows the system operator to locate, tag, and contain them. It can also be used to discourage rogue access point clients by sending them deauthenticate and disassociate messages from one to four access points.

Rogue Access Point Location, Tagging, and Containment

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take appropriate action:

- Locate rogue access points
- Receive new rogue access point notifications, eliminating hallway scans
- Monitor unknown rogue access points until they are eliminated or acknowledged
- Determine the closest authorized access point, making directed scans faster and more effective
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
  - Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or wireless LAN security
  - Accept rogue access points when they do not compromise the LAN or wireless LAN security
  - Tag rogue access points as unknown until they are eliminated or acknowledged
  - Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Detecting and Locating Rogue Access Points

When the access points on your wireless LAN are powered up and associated with controllers, WCS immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies WCS, which creates a rogue access point alarm.

When WCS receives a rogue access point message from a controller, an alarm dashboard appears in the lower left corner of all WCS user interface pages. The alarm dashboard in Figure 6-1 shows 93 rogue access point alarms.
Follow these steps to detect and locate rogue access points.

**Step 1**
Click the **Rogues** indicator to display the Rogue AP Alarms page. This page lists the severity of the alarms, the rogue access point MAC addresses, the rogue access point types, the date and time when the rogue access points were first detected, and their SSIDs.

**Step 2**
Click any **Rogue MAC Address** link to display the associated Alarms > Rogue - AP MAC Address page. This page shows detailed information about the rogue access point alarm.

**Step 3**
To modify the alarm, choose one of these commands from the Select a command drop-down menu and click **GO**.
- **Assign to me**—Assigns the selected alarm to the current user.
- **Unassign**—Unassigns the selected alarm.
- **Delete**—Deletes the selected alarm.
- **Clear**—Clears the selected alarm.
- **Event History**—Enables you to view events for rogue alarms.
- **Detecting APs** (with radio band, location, SSID, channel number, WEP state, short or long preamble, RSSI, and SNR)—Enables you to view the access points that are currently detecting the rogue access point.
- **Rogue Clients**—Enables you to view the clients associated with this rogue access point.
- **Set State to ‘Unknown - Alert’**—Tags the rogue access point as the lowest threat, continues to monitor the rogue access point, and turns off containment.
- **Set State to ‘Known - Internal’**—Tags the rogue access point as internal, adds it to the known rogue access points list, and turns off containment.
- **Set State to ‘Known - External’**—Tags the rogue access point as external, adds it to the known rogue access points list, and turns off containment.
- **1 AP Containment through 4 AP Containment**—When you select level 1 containment, one access point in the vicinity of the rogue unit sends deauthenticate and disassociate messages to the client devices that are associated to the rogue unit. When you select level 2 containment, two access points in the vicinity of the rogue unit send deauthenticate and disassociate messages to the rogue’s clients and so on up to level 4.

**Step 4**
From the Select a command drop-down menu, choose **Map (High Resolution)** and click **GO** to display the current calculated rogue access point location on the Maps > Building Name > Floor Name page.

If you are using WCS Location, WCS compares RSSI signal strength from two or more access points to find the most probable location of the rogue access point and places a small skull-and-crossbones indicator in that location.
For an under-deployed locations-based network (only one access point and an omni antenna), the most likely location of the rogue access point is somewhere in the area around the non-rogue access point. If you are using WCS Base, WCS relies on RSSI signal strength from the rogue access point and places a small skull-and-crossbones indicator next to the access point receiving the strongest RSSI signal from the rogue unit. Figure 6-2 shows a map that indicates that location of a rogue unit.

Figure 6-2 Map Indicating Location of Rogue Unit

Acknowledging Rogue Access Points

Follow these steps to acknowledge rogue access points.

Step 1 Navigate to the Rogue AP Alarms page.
Step 2 Check the check box of the rogue access point to be acknowledged.
Step 3 From the Select a command drop-down menu, choose Set State to ‘Known - Internal’ or Set State to ‘Known - External’. In either case, WCS removes the rogue access point entry from the Rogue AP Alarms page.
Finding Clients

Follow these steps to use WCS to find clients on your wireless LAN.

**Step 1** Click Monitor > Devices > Clients to navigate to the Clients Summary page.

**Step 2** In the sidebar, choose All Clients in the Search For Clients By drop-down menu and click Search to display the Clients page.

*Note* You can search for clients under WCS Controllers or Location Servers.

**Step 3** Click the username of the client that you want to locate. WCS displays the corresponding Clients Client Name page.

**Step 4** To find the client, choose one of these options from the Select a command drop-down menu and click GO:

- **Recent Map (High Resolution)** — Finds the client without disassociating it.
- **Present Map (High Resolution)** — Disassociates the client and then finds it after reassociation.

When you choose this method, WCS displays a warning message and asks you to confirm that you want to continue.

If you are using WCS Location, WCS compares the RSSI signal strength from two or more access points to find the most probable location of the client and places a small laptop icon at its most likely location. If you are using WCS Base, WCS relies on the RSSI signal strength from the client and places a small laptop icon next to the access point that receives the strongest RSSI signal from the client. Figure 6-3 shows a heat map that includes a client location.
Finding Coverage Holes

Coverage holes are areas where clients cannot receive a signal from the wireless network. The Cisco Wireless LAN Solution radio resource management (RRM) identifies these coverage hole areas and reports them to WCS, enabling the IT manager to fill holes based on user demand. Follow these steps to find coverage holes on your wireless LAN.

Step 1 Click the Coverage indicator on the bottom left of the WCS user interface page (or click Monitor > Alarms and search for Coverage under Alarm Category) to display the Coverage Hole Alarms page.

Step 2 Click Monitor > Maps and search for access points by name (this search tool is case sensitive). WCS displays the Maps > Search Results page, which lists the floor or outdoor area where the access point is located.

Step 3 Click the floor or outdoor area link to display the related Maps > Building Name > Floor Name page.

Step 4 Look for areas of low signal strength near the access point that reported the coverage hole. These areas are the most likely locations of coverage holes. If there does not appear to be any areas of weak signal strength, make sure that the floor plan map is accurate.
Pinging a Network Device from a Controller

Follow these steps to ping network devices from a controller.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Click <strong>Configure &gt; Controllers</strong> to navigate to the All Controllers page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the desired IP address to display the <strong>IP Address &gt; Controller Properties</strong> page.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the sidebar, choose <strong>System &gt; Commands</strong> to display the <strong>IP Address &gt; Controller Commands</strong> page.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose <strong>Ping From Controller</strong> from the Administrative Commands drop-down menu and click <strong>GO</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Enter an IP Address (x.x.x.x) to Ping window, enter the IP address of the network device that you want the controller to ping and click <strong>OK</strong>. WCS displays the Ping Results window, which shows the packets that have been sent and received. Click <strong>Restart</strong> to ping the network device again or click <strong>Close</strong> to stop pinging the network device and exit the Ping Results window.</td>
</tr>
</tbody>
</table>

Viewing Controller Status and Configurations

After you add controllers and access points to the WCS database, you can view the status of the Cisco Wireless LAN Solution. To view the system status, click **Monitor > Network Summary** to display the Network Summary page (see Figure 6-4).
### Figure 6-4  Network Summary Page

#### Controllers

<table>
<thead>
<tr>
<th>Controller</th>
<th>Total</th>
<th>Unreachable</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td></td>
<td>6</td>
</tr>
</tbody>
</table>

#### Coverage Areas

<table>
<thead>
<tr>
<th>Name</th>
<th>Total APs</th>
<th>Total Radios</th>
<th>b/g Radios</th>
<th>QoS Radios</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Richfield Campus</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>--RECO1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>---Richfield Lower Level</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>---Nikita</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>---Test</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Richfield Test Lab</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>---WAB TIME Lab</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Campus #2</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>---New Floor</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>---New Floor #2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

#### Most Recent Coverage Holes

No Coverage Holes found

#### Clients

Associated Clients vs. Time

#### Total APs not yet assigned to Maps:

2

#### Most Recent Rogue APs

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>SSID</th>
<th>Type</th>
<th>State</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:81:1b:26:e6</td>
<td>winetest</td>
<td>AP</td>
<td>Alert</td>
<td>11/18/05 1:44 PM</td>
</tr>
<tr>
<td>00:0b:81:29:54:d1</td>
<td>Strange Magic</td>
<td>AP</td>
<td>Alert</td>
<td>11/18/05 1:42 PM</td>
</tr>
<tr>
<td>00:0b:81:23:46:78</td>
<td>Always</td>
<td>AP</td>
<td>Alert</td>
<td>11/18/05 1:40 PM</td>
</tr>
<tr>
<td>00:07:5e:14:02:b1</td>
<td>guantial</td>
<td>AP</td>
<td>Alert</td>
<td>11/18/05 1:39 PM</td>
</tr>
<tr>
<td>00:0b:81:28:8a:7e</td>
<td>Strange Magic</td>
<td>AP</td>
<td>Alert</td>
<td>11/18/05 1:13 PM</td>
</tr>
</tbody>
</table>

#### Top 5 APs

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Map Location</th>
<th>a Clients</th>
<th>b/g Clients</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-22:43:cd</td>
<td>Unassigned</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>00:0b:81:29:54:d0</td>
<td>Campus #2 &gt; New Floor</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>00:0b:81:23:46:78</td>
<td>Campus #2 &gt; New Floor</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>ap-04:73:ef</td>
<td>Campus #2 &gt; New Floor</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ap-14:35:20</td>
<td>Richfield Campus &gt; RECO1 &gt; Nikita</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Viewing WCS Statistics Reports

WCS periodically collects statistics such as client counts, radio utilization, transmit power and channel information, and profile status and organizes them into reports. To view these reports, click **Monitor > Reports**.

### 802.11 Counters Report

This report shows a graph based on the parameters you selected for the 802.11 counters.

**Step 1** Choose **Monitor > Reports**.

**Step 2** From the left sidebar menu, choose **802.11 Counters**.

**Step 3** Specify if you want the report listed by controller, floor area, or outdoor area.

**Step 4** Specify if you want the report to list all controllers or select specific IP addresses.

**Step 5** Specify if you want the report to list all access points or select specific MAC addresses.

**Step 6** Choose if you want the report to focus on 802.11a or 802.11b/g radios.

**Step 7** Specify if you want the report for the last hour, last 6 hours, last day, last 2 days, last 3 days, last 4 days, last 5 days, last 6 days, or last 7 days.

**Step 8** Click **Generate Report**.

### Voice Statistics Report

These steps describe how to set the parameters for the voice statistics report. This report shows graphs based on the parameters you selected about voice statistics.

**Step 1** Choose **Monitor > Reports**.

**Step 2** From the left sidebar menu, choose **Voice Statistics**.

**Step 3** Specify if you want the report listed by controller, floor area, or outdoor area.

**Step 4** Specify if you want the report to list all controllers or select specific IP addresses.

**Step 5** Specify if you want the report to list all access points or select specific MAC addresses.

**Step 6** Choose if you want the report to focus on 802.11a or 802.11b/g radios.

**Step 7** Specify if you want the report for the last hour, last 6 hours, last day, last 2 days, last 3 days, last 4 days, last 5 days, last 6 days, or last 7 days.

**Step 8** Click **Generate Report**. You can also go to **Monitor > Devices > Access Points**, select one or more access point, choose **Voice Statistics** from the Generate a report for selected AP drop-down menu and click **GO**.

The report displays the access point name and radio, the number of calls in progress, the number of roaming calls in progress, and the percentage of bandwidth in use.
Voice Metric Reports

Traffic stream metrics must be enabled on the 802.11b/g voice parameters controller(s) for this report to generate. Refer to the “Configuring an 802.11a Voice Template” section on page 9-36 for information on setting this parameter. This report displays the voice traffic stream metrics table.

**Step 1** From the left sidebar menu, choose **Monitor > Devices > Access Points**.

**Step 2** Click a check box to select an access point name that you want to run a report on.

**Step 3** From the Generate a report for selected AP drop-down menu, choose **Voice Metrics** and click **GO**.

This report displays the following values:

- **Time QoS**: Time that the statistics were gathered from the access point(s).
- **% PLR (Downlink)**: Percent of packet loss ratio on the downlink.
- **% PLR (Uplink)**: Percent of packet loss ratio on the uplink.
- **Avg Queuing Delay (ms) (Downlink)**: Average queuing delay in milliseconds for the downlink.
- **Avg Queuing Delay (ms) (Uplink)**: Average queuing delay in milliseconds for the uplink.
- **% Packets > 40 ms Queuing Delay**: Percentage of queuing delay packets greater than 40 ms.
- **% Packets > 20 ms Queuing Delay**: Percentage of queuing delay packets greater than 20 ms.
- **Roaming Delay**: Roaming delay in milliseconds.

Voice TSM Reports

This report shows what CCX clients are enabled on this access point. For traffic stream metrics template information, refer to the “Configuring QoS Templates” section on page 9-3.

**Step 1** From the left sidebar menu, choose **Monitor > Devices > Access Points**.

**Step 2** Click a check box to select an access point name that you want to run a report on.

**Step 3** From the Generate a report for selected AP drop-down menu, choose **Voice TSM Reports** and click **GO**.

This report displays the following values:

- **Average Queuing Delay (ms)**: Average queuing delay in milliseconds.
- **% Packet with less than 10 ms delay**: Percentage of packets with less than 10 milliseconds delay.
- **% Packet with more than 10 < 20 ms delay**: Percentage of packets with more than 10 milliseconds delay but less than 20 milliseconds delay.
- **% Packet with more than 20 < 40 ms delay**: Percentage of packets with more than 20 milliseconds delay but less than 40 milliseconds delay.
- **% Packet with more than 40 ms delay**: Percentage of packets with more than 40 milliseconds delay.
- **Packet Loss Ratio**: Ratio of lost packets.
- **Total Packet Count**: Number of total packets.
- **Roaming Count**: Number of packets exchanged for roaming negotiations in this 90 seconds metrics window.
Viewing Mesh Tree

A Mesh Tree View allows you to see the parent-child relationship with access points in an easily navigable tree view and to filter what access points display on the Map view, by selecting only access points of interest.

Click on the black box icon under View Filters to display the mesh tree view. This icon is available if mesh access points are present on the map.

The Mesh Tree View appears on the top of the map view and displays the following information:

- The icon next to each PAP access point represents the parent link status. A green icon represents a high SNR (above 25 dB), an amber icon represents an acceptable SNR (20-25 dB), and a red icon represents a low SNR (below 20 dB). Move your cursor over the icon in the mesh tree view to display the bridging link information.

- The link between the child and parent access point. When an access point is unselected, all of its descendents are grayed out and unselected.

You can modify the appearance of the map view by selecting an option from the Quick Selection drop-down list or by checking the applicable check boxes in the tree view. For a child access point to be visible, the parent access point to root access point must be selected.

The following table describes the Mesh Parent-Child Hierarchical window parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select only Root APs</td>
<td>Choose this setting if you want the map view to display root access points only.</td>
</tr>
<tr>
<td>Select up to 1st hops</td>
<td>Choose this setting if you want the map view to display 1st hops only.</td>
</tr>
<tr>
<td>Select up to 2nd hops</td>
<td>Choose this setting if you want the map view to display 2nd hops only.</td>
</tr>
<tr>
<td>Select up to 3rd hops</td>
<td>Choose this setting if you want the map view to display 3rd hops only.</td>
</tr>
<tr>
<td>Select up to 4th hops</td>
<td>Choose this setting if you want the map view to display 4th hops only.</td>
</tr>
<tr>
<td>Select All</td>
<td>Select this setting if you want the map view to display all access points.</td>
</tr>
</tbody>
</table>

Click **Update Map View** to refresh the screen and redisplay the map view with the selected options.

**Note**

Map view information is retrieved from the WCS database and is updated every 15 minutes.

Move your cursor over the icon to display the bridging link information.

- Roaming Delay: Roaming delay in milliseconds
Running a Link Test

A link test uses a ping to test the link quality. The RF parameters of the ping reply packets received by the access point are polled by the controller to find the link quality. Because radio link quality can differ depending on the direction (client to access point versus access point to client), it is critical to have CCX linktest support so that link quality is tested in both directions. It polls the controller every so many seconds until the row status indicates success or failure. During the link test, the table is populated. If the link test fails, the controller reverts to a ping test.

You can access the link test in one of two ways. The first option is described below.

**Step 1** Choose Monitor > Devices > Clients.
**Step 2** From the left sidebar menu, choose All Clients in the Search for Clients By drop-down menu.
**Step 3** In the Client States drop-down menu, choose All States. The client list page appears.
**Step 4** Click the Link Test link in the last column. The link test begins. Figure 6-5 shows a sample link test result. The results show on the same page if the client is associated. Unsuccessful link tests show a failure message.

Another option for accessing the link test is as follows:

**Step 1** Choose Monitor > Devices > Clients.
**Step 2** Click the URL under the Total Clients column in the Clients Detected by Location Servers portion of the window.
**Step 3** Click a link in the User column to advance to the detail page.
**Step 4** From the Select a command drop-down menu, choose Link Test.

---

**Table 6-2 Bridging Link Information**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information fetched on</td>
<td>Date and time that information was compiled.</td>
</tr>
<tr>
<td>Link SNR</td>
<td>Link signal-to-noise ratio (SNR).</td>
</tr>
<tr>
<td>Link Type</td>
<td>Hierarchical link relationship.</td>
</tr>
<tr>
<td>SNR Up</td>
<td>Signal-to-noise radio for the uplink (dB).</td>
</tr>
<tr>
<td>SNR Down</td>
<td>Signal-to-noise radio for the downlink (dB).</td>
</tr>
<tr>
<td>Tx Parent Packets</td>
<td></td>
</tr>
<tr>
<td>Rx Parent Packets</td>
<td></td>
</tr>
<tr>
<td>Link State</td>
<td></td>
</tr>
<tr>
<td>Adjusted Link Metric</td>
<td></td>
</tr>
<tr>
<td>Parent Link Metric</td>
<td></td>
</tr>
<tr>
<td>Poor SNR</td>
<td></td>
</tr>
<tr>
<td>Time of Last Hello</td>
<td>Date and time of last hello.</td>
</tr>
</tbody>
</table>
Figure 6-5 shows a sample CCX link test result and Figure 6-6 shows a sample ping test result.

**Figure 6-5  CCX Link Test Result**

![CCX Link Test Result Table]

**Figure 6-6  Ping Test Result**

![Ping Test Result Table]
The unique device identifier (UDI) standard uniquely identifies products across all Cisco hardware product families, enabling customers to identify and track Cisco products throughout their business and network operations and to automate their asset management systems. The standard is consistent across all electronic, physical, and standard business communications. The UDI consists of five data elements:

- The orderable product identifier (PID)
- The version of the product identifier (VID)
- The serial number (SN)
- The entity name
- The product description

The UDI is burned into the EEPROM of controllers and lightweight access points at the factory and can be retrieved through the GUI.

Follow these steps to retrieve the UDI on controllers and access points.

Step 1  Click **Monitor > Devices > Controllers**.

Step 2  Click on the IP address of the controller whose UDI information you want to retrieve. Five data elements of the controller UDI display on this window.