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
- WLAN Client Troubleshooting, page 6-5
- Finding Clients, page 6-16
- Receiving Radio Measurements, page 6-19
- Finding Coverage Holes, page 6-20
- Pinging a Network Device from a Controller, page 6-20
- Viewing Controller Status and Configurations, page 6-21
- Monitoring Mesh Networks Using Maps, page 6-22
- Monitoring Mesh Health, page 6-28
- Mesh Security Statistics for an Access Point, page 6-30
- Viewing the Mesh Network Hierarchy, page 6-32
- Running a Link Test, page 6-36
- Retrieving the Unique Device Identifier on Controllers and Access Points, page 6-38
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 Unified Wireless Network 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 AP Details

This section provides information on rogue access points.

**Step 1** Choose Monitor > Security to navigate to the Security Summary page.

**Step 2** The following values are displayed:

- **Alert**—Number of rogues in alert state. Rogue access point radios appear as “Alert” when first scanned by the controller, or as “Pending” when operating system identification is underway.
- **Contained**—Number of contained rogues.
- **Threat**—Number of threat rogues.
- **Contained Pending**—Number of contained rogues pending.
- **Known Contained**—Number of known contained rogues.
- **Trusted Missing**—Number of trusted missing rogues.
- **Removed**—Number of removed rogues.
- **Known**—Number of known rogues.
- **Acknowledged**—Number of acknowledged rogues.
- **802.11a**—Number of rogue access points broadcasting on 802.11a.
- **802.11b**—Number of rogue access points broadcasting on 802.11b and/or 802.11g.
- **On Network**—Number of rogue access point on the same subnet as the detecting port.
- **Off Network**—Number of rogue access point NOT on the same subnet as the detecting port.
- **Adhoc**—Number of adhoc rogues.

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
Monitoring 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 monitor appears in the lower left corner of all WCS user interface pages. The alarm monitor 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 at its most likely location. In the case of an underdeployed network for location with only one access point and an omni antenna, the most likely location is somewhere on a ring around the access point, but the center of likelihood is at the 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.
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.

**WLAN Client Troubleshooting**

Follow these steps to run diagnostic tests and reports and to view available logs:

**Step 1** Choose Monitor > Clients.
Step 2  To troubleshoot a client, enter the MAC address of the client in the Client field and click **Troubleshoot**. The troubleshooting client options appear (see Figure 6-3). If the MAC address is unknown, enter search criteria of the client (such as user name, floor, and so on) in the Quick Search of the left-hand menu.

*Figure 6-3  Troubleshooting Client Tab*

The summary page displays a brief description of the problem and recommends a course of action to resolve the issue.

Step 3  To view log messages logged against the client, click the **Log Analysis** tab (see Figure 6-4).

Step 4  To begin capturing log messages about the client from the controller, click **Start**. To stop log message capture, click **Stop**. To clear all log messages, click **Clear**.

**Note**  Log messages are captured for ten minutes and then stopped automatically. A user must click **Start** to continue.

Step 5  To select which log messages to display, click one of the links under Select Log Messages (the number between parentheses indicates the number of messages). The messages appear in the box. It includes the following information:
- A status message
- The controller time
- A severity level of info or error (errors are displayed in red)
- The controller to which the client is connected

**Figure 6-4  Log Analysis Tab**

**Step 6** To display a summary of the client’s events history, click the **Event History** tab (see Figure 6-5). This page displays client and access point events that occurred within the last 24 hours.
Step 7  Close the Troubleshooting Client window. The General tab displays the client details and properties of the access point with which the client is associated (see Figure 6-6). Table 6-1, Table 6-2, and Table 6-3 describe the fields displayed on this General tab.
### Figure 6-6  Client Details Window

![Client Details Window](image)

### Table 6-1  General Tab / Client Properties

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client User Name</td>
<td>The username the client used for authentication.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>The IP address of the client.</td>
</tr>
<tr>
<td>Client MAC Address</td>
<td>The MAC address of the client.</td>
</tr>
<tr>
<td>Client Vendor</td>
<td>The client’s vendor information.</td>
</tr>
<tr>
<td>Controller</td>
<td>The IP address of the controller to which the client is registered. Clicking the controller’s IP address displays information about the controller.</td>
</tr>
<tr>
<td>Port</td>
<td>The port on the controller to which the client is connected.</td>
</tr>
</tbody>
</table>
### Table 6-1  General Tab / Client Properties

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11 State</td>
<td>The client’s state:</td>
</tr>
<tr>
<td></td>
<td>- Idle— Normal operation; no rejections of client association requests</td>
</tr>
<tr>
<td></td>
<td>- AAA Pending— Completing an AAA transaction</td>
</tr>
<tr>
<td></td>
<td>- Authenticated— 802.11 association completed</td>
</tr>
<tr>
<td></td>
<td>- Associated— 802.11 association completed</td>
</tr>
<tr>
<td></td>
<td>- Power Save— Client in power save mode</td>
</tr>
<tr>
<td></td>
<td>- Disassociated— Disassociation completed</td>
</tr>
<tr>
<td></td>
<td>- To Be Deleted—To be deleted after disassociation</td>
</tr>
<tr>
<td></td>
<td>- Probing—Client not associated or authorized yet</td>
</tr>
<tr>
<td></td>
<td>- Blacklisted—Automatically disabled by the system due to perceived security threats</td>
</tr>
<tr>
<td>Interface</td>
<td>The name of the interface to which the client is connected.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The client has successfully joined an access point for the given SSID. VLAN ID is the reverse lookup of the interface used by the WLAN on the controller side.</td>
</tr>
<tr>
<td>802.11 State</td>
<td>The client’s state:</td>
</tr>
<tr>
<td></td>
<td>- Idle— Normal operation; no rejections of client association requests</td>
</tr>
<tr>
<td></td>
<td>- AAA Pending— Completing an AAA transaction</td>
</tr>
<tr>
<td></td>
<td>- Authenticated— 802.11 association completed</td>
</tr>
<tr>
<td></td>
<td>- Associated— 802.11 association completed</td>
</tr>
<tr>
<td></td>
<td>- Power Save— Client in power save mode</td>
</tr>
<tr>
<td></td>
<td>- Disassociated— Disassociation completed</td>
</tr>
<tr>
<td></td>
<td>- To Be Deleted—To be deleted after disassociation</td>
</tr>
<tr>
<td></td>
<td>- Probing—Client not associated or authorized yet</td>
</tr>
<tr>
<td></td>
<td>- Blacklisted—Automatically disabled by the system due to perceived security threats</td>
</tr>
<tr>
<td>Mobility Role</td>
<td>Associated or Unassociated.</td>
</tr>
<tr>
<td>Policy Manager State</td>
<td>Internal state of the client’s WLAN. Client is working properly when the state is RUN.</td>
</tr>
<tr>
<td>Anchor Address</td>
<td>N/A when the client is Local (has not roamed from its original subnet). Anchor IP Address (the IP Address of the original controller) when the client is Foreign (has roamed to another controller on a different subnet). Foreign IP Address (the IP Address of the original controller) when the client is Anchor (has roamed back to another controller on a different subnet).</td>
</tr>
<tr>
<td>Mirror Mode</td>
<td>Disable or enable.</td>
</tr>
<tr>
<td>CCX</td>
<td>Indicates if CCX is supported</td>
</tr>
</tbody>
</table>
Table 6-1  General Tab / Client Properties

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E2E</td>
<td>Indicates if E2E is supported.</td>
</tr>
<tr>
<td>WGB Status</td>
<td>Indicates the workgroup bridge status as regular client, WGB client, or WGB. If a client is a regular client, the WGB MAC address is not shown. If a client is a workgroup bridge, the state is WGB, and the MAC address is shown. A WGB is a mode that can be configured on an autonomous IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging.</td>
</tr>
</tbody>
</table>

Table 6-2  General Tab / RF Properties (read only)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Name</td>
<td>The name of the access point to which the client is associated. Clicking the link displays information about the access point.</td>
</tr>
<tr>
<td>AP Type</td>
<td>The type of the access point.</td>
</tr>
<tr>
<td>AP Base Radio MAC</td>
<td>The MAC address of the access point’s base radio.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol used by the radio (802.11a or 802.11b/g).</td>
</tr>
<tr>
<td>AP Mode</td>
<td>The access point mode.</td>
</tr>
<tr>
<td>Profile Name</td>
<td>The profile name of the WLAN that the client is associated to or is trying to associate to.</td>
</tr>
<tr>
<td>SSID</td>
<td>The SSID assigned to this WLAN. The access points broadcast the SSID on this WLAN. Different WLANs can use the same SSID as long as the Layer 2 security is different.</td>
</tr>
<tr>
<td>Security Policy</td>
<td>The WLAN security policy that is used.</td>
</tr>
<tr>
<td>Association Id</td>
<td>Client’s access point association identification number.</td>
</tr>
</tbody>
</table>
Table 6-2  General Tab / RF Properties (read only)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason Code</td>
<td>The client reason code may be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Normal (0) — Normal operation.</td>
</tr>
<tr>
<td></td>
<td>• Unspecified reason (1) — Client associated but no longer authorized.</td>
</tr>
<tr>
<td></td>
<td>• PreviousAuthNotValid(2) — Client associated but not authorized.</td>
</tr>
<tr>
<td></td>
<td>• DeauthenticationLeaving (3) — The access point went offline, deauthenticating the client.</td>
</tr>
<tr>
<td></td>
<td>• DisassociationDueToInactivity (4) — Client session timeout exceeded.</td>
</tr>
<tr>
<td></td>
<td>• DisassociationAPBusy(5) — The access point is busy, performing load balancing, for example.</td>
</tr>
<tr>
<td></td>
<td>• Class2FrameFromNonAuthStation (6) — Client attempted to transfer data before it was authenticated.</td>
</tr>
<tr>
<td></td>
<td>• Class2FrameFromNonAssStation (7) — Client attempted to transfer data before it was associated.</td>
</tr>
<tr>
<td></td>
<td>• DisassociationStnHasLeft (8) — Controller moved the client to another access point using non-aggressive load balancing.</td>
</tr>
<tr>
<td></td>
<td>• StaReqAssociationWithoutAuth (9) — Client not authorized yet, still attempting to associate with a Cisco WLAN Solution.</td>
</tr>
<tr>
<td></td>
<td>• Missing Reason Code (99) — Client momentarily in an unknown state.</td>
</tr>
</tbody>
</table>

802.11 Authentication Which 802.11 authentication algorithm is in force.

Table 6-3  General Tab / Security

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated</td>
<td>Indicates whether the client has been authenticated.</td>
</tr>
<tr>
<td>Policy Type</td>
<td>The type of security policy used by the client.</td>
</tr>
<tr>
<td>Encryption Cypher</td>
<td>Encryption settings.</td>
</tr>
<tr>
<td>EAP Type</td>
<td>Type of Extensible Authentication Protocol (EAP) used.</td>
</tr>
</tbody>
</table>

Step 8  To obtain additional troubleshooting information and perform additional diagnostics tests, choose a command from the drop-down menu and click GO.

a. To test the link between the client and the access point to which it is associated, choose Link Test from the drop-down menu and click GO.

b. To disable XYZ, choose Disable from the drop-down menu and click GO.

c. To remove XYZ, choose Remove from the drop-down menu and click GO.
d. To enable the Mirror mode, choose **Enable Mirror Mode** from the drop-down menu and click **GO**.

e. To display a high-resolution map of the client’s recent location, choose **Recent Map (High Resolution)** from the drop-down menu and click **GO**.

f. To display a high-resolution map of the client’s present location, choose **Present Map (High Resolution)** from the drop-down menu and click **GO**.

g. To display a graph showing a history of the client-to-access point associations, choose **AP Association History Graph** from the drop-down menu and click **GO**.

h. To display a table showing a history of the client-to-access-point associations, choose **AP Association History Table** from the drop-down menu and click **GO**.

i. To display information about the reasons for client roaming, choose **Roam Reason** from the drop-down menu and click **GO**.

j. To display details of access points that can hear the client, including at which signal strength/SNR, choose **Detecting APs** from the drop-down menu and click **GO**.

k. To display the history of the client location based on RF fingerprinting, choose **Location History** from the drop-down menu and click **GO**.

l. To display client voice matrix, choose **Voice Metrics** from the drop-down menu and click **GO**.

**Step 9**

To display client statistics, click the **Statistics** tab (see Figure 6-7).

This page displays four graphs:

- **Client RSSI History (dBm)**— History of RSSI as detected by the access point to which the client is associated
- **Client SNR History**— History of SNR as detected by the access point to which the client is associated
- **Bytes Sent and Received (Kbps)**— The bytes sent and received by the client from the access point to which it is associated
- **Packets Sent and Received (per sec.)**— The packets sent and received by the client from the access point to which it is associated

**Table 6-4** describes the fields displayed on this Statistics tab.
Figure 6-7  Statistics Tab

Table 6-4  Statistics Tab / Client Statistics

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSSI</td>
<td>Receive signal strength indicator of the client RF session.</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal to noise ratio of the client RF session.</td>
</tr>
<tr>
<td>Bytes Sent and Received</td>
<td>Total number of bytes sent to the client and received by the controller from the client.</td>
</tr>
<tr>
<td>Packets Sent and Received</td>
<td>Total number of packets sent to the client and received by the controller from the client.</td>
</tr>
</tbody>
</table>
To display the client’s location information, click the **Location** tab (see **Figure 6-8**). Table 6-5 describes the fields display on this Location tab.

### Table 6-5  Location Tab

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Location</td>
<td>Describes the location of the client in the map based on RF fingerprinting.</td>
</tr>
<tr>
<td>Asset Information</td>
<td>Describes the asset file destination and name.</td>
</tr>
<tr>
<td>Location Notifications</td>
<td>Displays the number of location notifications logged against the client.</td>
</tr>
<tr>
<td>Absence</td>
<td>The location server generates absence events when the monitored assets go missing. In other words, the location server cannot see the asset in the WLAN for the specified time.</td>
</tr>
</tbody>
</table>
Finding Clients

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

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

**Step 2** The sidebar area enables you to select a new configuration panel under the menu area that you have selected. You can make only one choice. The selector area options vary based on the menu that you select.

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

**Step 3** In the sidebar, click New Search. The Search Clients window appears (see Figure 6-9).
You can configure the following parameters in the Search clients window:

- **Search By**
- **Clients Detected By** — Choose WCS for clients stored in WCS that were detected through polling of the controllers from WCS. Choose Location Servers for clients stored on the location server that were detected by the location server through controller polling.
- **Last detected within** — A time increment from 5 minutes to 24 hours.
- **Client States** — Specify if you want to view clients only in a specific state such as idle, authenticated, associated, probing, or excluded.
- **Include Disassociated** — To include clients that are no longer on the network but for which WCS has historical records.
- **Restrict By Protocol** — To restrict the search by protocol. Then from the drop-down menu choose 802.11a, 802.11b, and 802.11g.
- **Restrict by SSID** — To restrict the search by SSID. Then enter the SSID in the text field.
- **CCX Compatible** — To search for CCX compatible clients.
- **E2E Compatible** — To search for E2E compatible clients.
- **Save Search** — To save the search in the Saved Searches drop-down menu.
- **Items per page** — The number of found items to display on the search results page.

**Step 4** Choose **All Clients** in the Search By drop-down menu and click **GO**. The related search results window appears. The search results are listed.

---

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

**Step 5** Click the username of the client that you want to locate. WCS displays the corresponding Clients **Client Name** page.

**Step 6** 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.
Finding Clients

- **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 6-10 shows a heat map that includes a client location.

**Figure 6-10  Map with Client Location**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes received</td>
<td>Total number of bytes received by the controller from the client.</td>
</tr>
<tr>
<td>Bytes sent</td>
<td>Total number of bytes sent to the client from the controller.</td>
</tr>
<tr>
<td>Packets received</td>
<td>Total number of packets received by the controller from the client.</td>
</tr>
<tr>
<td>Packets sent</td>
<td>Total number of packets sent to the client from the controller.</td>
</tr>
</tbody>
</table>
To generate a roam reason report, click **Roam Reason**. This reporting does not require any configuration.

To generate a voice TSM report, click **Voice Metrics**.

To generate a troubleshooting report, click **Troubleshoot**. You can choose a summary tab, a log analysis tab, or an event history tab.

### Receiving Radio Measurements

On the client window, you can receive radio measurements only if the client is CCX v2 (or higher) and is in the associated state (with a valid IP address). If the client is busy when asked to do the measurement, it determines whether to honor the measurement or not. If it declines to make the measurement, it shows no data from the client.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy errors</td>
<td>Number of policy errors for the client.</td>
</tr>
<tr>
<td>RSSI</td>
<td>Receive signal strength indicator of the client RF session.</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal-to-noise ratio of the client RF session.</td>
</tr>
<tr>
<td>Client RSSI History (dBm)</td>
<td>History of RSSI as detected by the access point with which the client is associated.</td>
</tr>
<tr>
<td>Client SNR History</td>
<td>History of SNR as detected by the access point with which the client is associated.</td>
</tr>
<tr>
<td>Bytes Sent and Received (Kbps)</td>
<td>Bytes sent and received with the associated access point.</td>
</tr>
<tr>
<td>Packets Sent and Received (per second)</td>
<td>Packets sent and received with the associated access point.</td>
</tr>
</tbody>
</table>

---

**Step 8** To generate a roam reason report, click **Roam Reason**. This reporting does not require any configuration.

**Step 9** To generate a voice TSM report, click **Voice Metrics**.

**Step 10** To generate a troubleshooting report, click **Troubleshoot**. You can choose a summary tab, a log analysis tab, or an event history tab.

---

**Receiving Radio Measurements**

On the client window, you can receive radio measurements only if the client is CCX v2 (or higher) and is in the associated state (with a valid IP address). If the client is busy when asked to do the measurement, it determines whether to honor the measurement or not. If it declines to make the measurement, it shows no data from the client.

**Step 1** Choose Monitor > Clients.

**Step 2** Choose a client from the Clients column or enter a client in the Client Troubleshooting section on the bottom right and click **Troubleshoot**.

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

**Step 4** Click the check box to indicate if you want to specify beacon measurement, frame measurement, channel load, or noise histogram. The different measurements produce differing results:

- **Beacon Response**
  - Channel—the channel number for this measurement
  - BSSID—6-byte BSSID of the station that sent the beacon or probe response
  - PHY—Physical Medium Type (FH, DSS, OFDM, high rate DSS or ERP)
  - Received Signal Power—the strength of the beacon or probe response frame in dBm
  - Parent TSF—the lower 4 bytes of serving access point’s TSF value
  - Target TSF—the 8-byte TSF value contained in the beacon or probe response
  - Beacon Interval—the 2-byte beacon interval in the received beacon or probe response
  - Capability information—as present in the beacon or probe response

---
Finding Coverage Holes

Coverage holes are areas where clients cannot receive a signal from the wireless network. The Cisco Unified Wireless Network 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.

Step 1 Click Configure > Controllers to navigate to the All Controllers page.

- Frame Measurement
  - Channel— Channel number for this measurement
  - BSSID— BSSID contained in the MAC header of the data frames received
  - Number of frames— Number of frames received from the transmit address
  - Received Signal Power— The signal strength of 802.11 frames in dBm

- Channel Load
  - Channel— The channel number for this measurement
  - CCA busy fraction— The fractional duration over which CCA indicated the channel was busy during the measurement duration defined as ceiling (255 times the duration the CCA indicated channel was busy divided by measurement duration)

- Noise Histogram
  - Channel— The channel number for this measurement
  - RPI density in each of the eight power ranges

Step 5 Click Perform Measurement to initiate the measurement.

The measurements take about 5 msec to perform. A message from WCS indicates the progress. If the client chooses not to perform the measurement, that will also be communicated.
Viewing Controller Status and Configurations

After you add controllers and access points to the WCS database, you can view the status of the Cisco Unified Wireless Network Solution. To view the system status, click Monitor > Network Summary to display the Network Summary page (see Figure 6-11).
Monitoring Mesh Networks Using Maps

You can access and view details for the following elements from a mesh network map in Cisco WCS:

- Mesh Link Statistics
- Mesh Access Points
- Mesh Access Point Neighbors

Details on how this information is accessed and the information displayed for each of these items is detailed in the following sections.

Monitoring Mesh Link Statistics Using Maps

You can view the SNR for a specific mesh network link, view the number of packets transmitted and received on that link, and initiate a link test from the Monitor > Maps display.
To view details on a specific mesh link between two mesh access points or a mesh access point and a root access point, do the following:

**Step 1**
In Cisco WCS, choose **Monitor > Maps**.

**Step 2**
Click on the **Map Name** that corresponds to the outdoor area, campus, building, or floor you want to monitor.

**Step 3**
Move the cursor over the link arrow for the target link (see Figure 6-12). A Mesh Link window appears.

*Note*
The AP Mesh Info check box under the Layers drop-down menu must be checked for links to appear on the map.

**Step 4**
Click either **Link Test, Child to Parent** or **Link Test, Parent to Child**. After the link test is complete, a results page appears (see Figure 6-13).

*Note*
A link test runs for 30 seconds.

*Note*
You cannot run link tests for both links (child-to-parent and parent-to-child) at the same time.
Step 5
To view a graphical representation of SNR statistics over a period of time, click on the arrow on the link. A window with multiple SNR graphs appears (see Figure 6-14).

The following graphs are displayed for the link:

- **SNR Up**—Plots the RSSI values of the neighbor from the perspective of the access point.
- **SNR Down**—Plots the RSSI values that the neighbor reports to the access point.
- **Link SNR**—Plots a weighed and filtered measurement based on the SNR Up value.
- **The Adjusted Link Metric**—Plots the value used to determine the least cost path to the root access point. This value is the ease to get to the rooftop access point and accounts for the number of hops. The lower the ease value, the less likely the path is used.
- **The Unadjusted Link Metric**—Plots the least cost path to get to the root access point unadjusted by the number of hops. The higher the value for the unadjusted link, the better the path is.
Monitoring Mesh Access Points Using Maps

You can view the following information for a mesh access point from a mesh network map:

- Parent
- Number of children
- Role
- Group name
- Backhaul interface
- Data Rate
- Channel

**Note**

This information is in addition to the information shown for all access points (MAC address, access point model, location, and height of access point).

**Note**

You can also view detailed configuration details and access alarm and event information from the map. For detailed information on the Alarms and Events displayed, refer to the “Alarm and Event Dictionary” section on page 14-8.
To view summary and detailed configuration information for a mesh access point from a mesh network map, do the following:

**Step 1** In Cisco WCS, choose **Monitor > Maps**.

**Step 2** Click on the **Map Name** that corresponds to the outdoor area, campus, building, or floor location of the access point that you want to monitor.

**Step 3** To view summary configuration information for an access point, move the cursor over the access point that you want to monitor. A window with configuration information for the selected access point appears (see **Figure 6-15**).

**Step 4** To view detailed configuration information for an access point, click on the arrow portion of the mesh access point label. The configuration details for the access point appears (see **Figure 6-16**).

**Note** For more details on the View Mesh Neighbors link in the access point panel above, see the “Monitoring Mesh Access Point Neighbors Using Maps” section on page 6-27. If the access point has an IP address, a Run Ping Test link is also visible in the access point panel.
Monitoring Mesh Access Point Neighbors Using Maps

To view details on neighbors of a mesh access point from a mesh network map, do the following:

---

**Step 1**  
In Cisco WCS, choose **Monitor > Maps**.

**Step 2**  
Click on the **Map Name** that corresponds to the outdoor area, campus, building, or floor you want to monitor.

**Step 3**  
Move the cursor over the access point for which you want to display neighbor info. A window with configuration information for the selected access point appears.

**Step 4**  
Click on the View Mesh Neighbors link. A panel appears with summary information of the neighbors for the selected access point (see Figure 6-17).
Monitoring Mesh Health

Mesh Health monitors the temperature and heater status for Cisco Aironet 1510 access points. Tracking this environmental information is particularly critical for access points that are deployed outdoors.

- Temperature is displayed in Fahrenheit and Celsius.
- Heater status is displayed as on or off.

Mesh Health information is displayed in the General Properties page for access points.

To view the mesh health details for a specific mesh access point, follow these steps.

**Step 1** Choose **Monitor > Access Points**. A listing of access points appears (see **Figure 6-18**).
You can also use the New Search button to display the access point summary shown below. With the New Search option, you can further define the criteria of the access points that display. Search criteria include AP Name, IP address, MAC address, Controller IP or Name, Radio type, and Outdoor area.

**Figure 6-18 Monitor > Access Points**

![Wireless Control System](image)

### Step 2
Click on the AP Name link to display details for that access point. The General Properties summary for that access point appears (see Figure 6-19).

AP Temperature and Heater Status are displayed at the bottom of the General summary (left-side).
Mesh Security Statistics for an Access Point

Mesh Statistics are reported when a child mesh access point authenticates or associates with a parent mesh access point.

Security statistic entries are removed and no longer displayed when the child mesh access point disassociates from the controller.

The following mesh security statistics are displayed for mesh access points:

- **Association Request Failures**: Summarizes the total number of association request failures that occur between the selected mesh access point and its parent.
- **Association Request Success**: Summarizes the total number of successful association requests that occur between the selected mesh access point and its parent.
- **Association Request Timeouts**: Summarizes the total number of association request time outs that occur between the selected mesh access point and its parent.
- **Authentication Request Failures**: Summarizes the total number of failed authentication requests that occur between the selected mesh access point and its parent.
- **Authentication Request Success**: Summarizes the total number of successful authentication requests between the selected mesh access point and its parent mesh node.
- **Authentication Request Timeouts**: Summarizes the total number of authentication request timeouts that occur between the selected mesh access point and its parent.
Chapter 6  Monitoring Wireless Devices

Mesh Security Statistics for an Access Point

- **Invalid Association Request:** Summarizes the total number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This state might occur when the selected child is a valid neighbor but is not in a state that allows association.

- **Invalid Reassociation Request:** Summarizes the total number of invalid reassociation requests received by the parent mesh access point from a child. This might happen when a child is a valid neighbor but is not in a proper state for reassociation.

- **Invalid Reauthentication Request:** Summarizes the total number of invalid reauthentication requests received by the parent mesh access point from a child. This may happen when a child is a valid neighbor but is not in a proper state for reauthentication.

- **Packets Received:** Summarizes the total number of packets received during security negotiations by the selected mesh access point.

- **Packets Transmitted:** Summarizes the total number of packets transmitted during security negotiations by the selected mesh access point.

- **Reassociation Request Failures:** Summarizes the total number of failed reassociation requests between the selected mesh access point and its parent.

- **Reassociation Request Success:** Summarizes the total number of successful reassociation requests between the selected mesh access point and its parent.

- **Reassociation Request Timeouts:** Summarizes the total number of reassociation request timeouts between the selected mesh access point and its parent.

- **Reauthentication Request Failures:** Summarizes the total number of failed reauthentication requests between the selected mesh access point and its parent.

- **Reauthentication Request Success:** Summarizes the total number of successful reauthentication requests that occurred between the selected mesh access point and its parent.

- **Reauthentication Request Timeouts:** Summarizes the total number of reauthentication request timeouts that occurred between the selected mesh access point and its parent.

- **Unknown Association Requests:** Summarizes the total number of unknown association requests received by the parent mesh access point from its child. The unknown association requests often occur when a child is an unknown neighbor mesh access point.

- **Unknown Reassociation Request:** Summarizes the total number of unknown reassociation requests received by the parent mesh access point from a child. This might happen when a child mesh access point is an unknown neighbor.

- **Unknown Reauthentication Request:** Summarizes the total number of unknown reauthentication requests received by the parent mesh access point node from its child. This might occur when a child mesh access point is an unknown neighbor.

To view the mesh security statistics for a specific mesh access point, follow these steps:

**Step 1**  
In Cisco WCS, choose **Monitor > Access Points**. A listing of access points appears (see Figure 6-20).

**Note**  
You can also use the New Search button to display the access point summary. With the New Search option, you can further define the criteria of the access points that display. Search criteria include AP Name, IP address, MAC address, Controller IP or Name, Radio type, and Outdoor area.

**Step 2**  
Click on the **AP Name** link of the target mesh access point.

A tabbed panel appears and displays the General Properties page for the selected access point.
Viewing the Mesh Network Hierarchy

You can view the parent-child relationship of mesh access points within a mesh network in an easily navigable display. You can also filter which access points display on the Map view, by selecting only access points of interest.

To view the mesh network hierarchy for a selected network, do the following:

**Step 1** In Cisco WCS, choose Monitor > Maps.

**Step 2** Select the map you want to display.

**Step 3** Click the Layers arrow to expand that menu (see Figure 6-21).
Figure 6-21 Monitor > Maps > Selected Map

Step 4 Check the **AP Mesh Info** check box if it is not already checked.

*Note* The AP Mesh Info check box is only selectable if mesh access points are present on the map. It must be checked to view the mesh hierarchy.

Step 5 Click the **AP Mesh Info** arrow to display the mesh parent-child hierarchy.

Step 6 Click the **plus (+)** sign next to a mesh access point to display its children.

All subordinate mesh access points are displayed when a negative (-) sign displays next to the parent mesh access point entry. For example, in Figure 6-21, the access point, *indoor-mesh-44-map1*, has only one child, *indoor-mesh-44-map2*.

Step 7 Move the cursor over the colored dot next to each mesh access point to view its signal-to-noise ratio (SNR).

A window displays with the exact SNR for that mesh access point (see Figure 6-22).

The color of the dot also provides a quick reference point of the SNR strength:

- A green dot represents a high SNR (above 25 dB).
- An amber dot represents an acceptable SNR (20-25 dB).
- A red dot represents a low SNR (below 20 dB).
- A black dot indicates a root access point.
Using Filtering to Modify Map Display

In the mesh hierarchal window, you can also define filters to determine which mesh access points display on the map. Mesh access points are filtered by the number of hops between them and their root access point.

To modify the mesh access points that displays on the map, do the following:

Step 1 In the Mesh Parent-Child Hierarchal View, click on the Quick Selections drop-down menu (see Figure 6-23).

Step 2 Select the appropriate option from the menu. A description of the options is provided in Table 6-7.
Step 3  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.
Running a Link Test

A link test uses a ping from parent-to-child to child-to-parent 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 > 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 6-25 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 method for accessing the link test is as follows:

**Step 1** Choose Monitor > Clients. The Clients Summary window appears (see Figure 6-24).
Step 2  Click the URL under the Total Clients column of 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.

Figure 6-25 shows a sample CCX link test result and Figure 6-26 shows a sample ping test result.
Retrieving the Unique Device Identifier on Controllers and Access Points

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 > Controllers. The Controller > Search Results window displays (see Figure 6-27).

**Figure 6-27  Controllers > Search Results**

You can optionally change how the controller search results are displayed by clicking Edit View. The Edit View window appears (see Figure 6-28). In the left-hand window, highlight the areas you want to view and click Show to move them to the right-hand window. You can then highlight the areas in the right-hand menu and click Up or Down to rearrange the order.

**Step 2**

Step 3
Click on the IP address of the controller (seen in Figure 6-27) whose UDI information you want to retrieve. Data elements of the controller UDI display on this window:

Table 6-9 Controllers Summary

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Portion</strong></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Local network IP address of the controller management interface.</td>
</tr>
<tr>
<td>Name</td>
<td>User-defined name of the controller.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of controller.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>For WiSM, the slot and port numbers are also given.</td>
</tr>
<tr>
<td>UP Time</td>
<td>Time in days, hours, and minutes since the last reboot.</td>
</tr>
<tr>
<td>System Time</td>
<td>Time used by the controller.</td>
</tr>
<tr>
<td>Internal Temperature</td>
<td>The current internal temperature of the unit (in Centigrade).</td>
</tr>
<tr>
<td>Location</td>
<td>User-defined physical location of the controller.</td>
</tr>
<tr>
<td>Contact</td>
<td>The contact person for this controller, their textual identification, and ways to contact them. If not contact information is known, this is an empty string.</td>
</tr>
<tr>
<td>Total Client Count</td>
<td>Total number of clients currently associated with the controller.</td>
</tr>
<tr>
<td>Current LWAPP Transport Mode</td>
<td>Lightweight Access Point Protocol transport mode.</td>
</tr>
<tr>
<td></td>
<td>Communications between controllers and access points.</td>
</tr>
<tr>
<td></td>
<td>Selections are Layer 2 or Layer 3.</td>
</tr>
</tbody>
</table>
### Retrieving the Unique Device Identifier on Controllers and Access Points

#### Power Supply One
Indicates the presence or absence of a power supply and its operations state.

#### Power Supply Two
Indicates the presence or absence of a power supply and its operation state.

### Inventory Portion

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Version</td>
<td>The operating system release, version.dot.maintenance number of the code currently running on the controller.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the inventory item.</td>
</tr>
<tr>
<td>Model No.</td>
<td>Specifies the machine model as defined by the Vital Product Data.</td>
</tr>
<tr>
<td>Serial No.</td>
<td>Unique serial number for this controller.</td>
</tr>
<tr>
<td>Burned-in MAC Address</td>
<td>The burned-in MAC address for this controller.</td>
</tr>
<tr>
<td>Number of APs supported</td>
<td>The maximum number of access points supported by the controller.</td>
</tr>
<tr>
<td>GigE Card Present</td>
<td>Displays the presence or absence of the optional 1000BASE-T/1000BASE-SX GigE card.</td>
</tr>
<tr>
<td>Crypto Card One</td>
<td>Displays the presence or absence of an enhanced security module which enables IPSec security and provides enhanced processing power. See Table 6-10 for information on the maximum number of crypto cards that can be installed on a controller.</td>
</tr>
<tr>
<td>Crypto Card Two</td>
<td>Displays the presence or absence of a second enhanced security module.</td>
</tr>
<tr>
<td>Port 1 Status</td>
<td>Up or Down</td>
</tr>
<tr>
<td>Port 2 Status</td>
<td>Up or Down</td>
</tr>
</tbody>
</table>

### Unique Device Identifier (UDI)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Product type. Chassis for controller and Cisco AP for access points.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of controller and may include number of access points.</td>
</tr>
<tr>
<td>Product Id</td>
<td>Orderable product identifier.</td>
</tr>
<tr>
<td>Version Id</td>
<td>Version of product identifier.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Unique product serial number.</td>
</tr>
</tbody>
</table>
## Table 6-10  Maximum Number of Crypto Cards that can be installed on a Cisco Wireless LAN Controller

<table>
<thead>
<tr>
<th>Type of Controller</th>
<th>Maximum Number of Crypto Cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 2000 Series</td>
<td>None</td>
</tr>
<tr>
<td>Cisco 4100 Series</td>
<td>One</td>
</tr>
<tr>
<td>Cisco 4400 Series</td>
<td>Two</td>
</tr>
</tbody>
</table>