CHAPTER 6

Monitoring Wireless Devices

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

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.
- Trusted Missing—Number of trusted missing rogues.
- 802.11a/n—Number of rogue access points broadcasting on 802.11a/n.
- 802.11b/g/n—Number of rogue access points broadcasting on 802.11b/n and/or 802.11g/n.
- On Network—Number of rogue access points on the same subnet as the detecting port.
- Off Network—Number of rogue access points NOT on the same subnet as the detecting port.

Step 3 Under **Most Recent Rogue Adhocs**, click a MAC Address of a specific rogue adhoc to view its associated alarm details. You can also click **Rogue Adhocs** from the left sidebar menu to view all current rogue adhoc alarms and see their severity, rogue MAC address, vendor, radio type, strongest access point RSSI, owner, date and time, state, SSID, map location, and acknowledgement status.

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

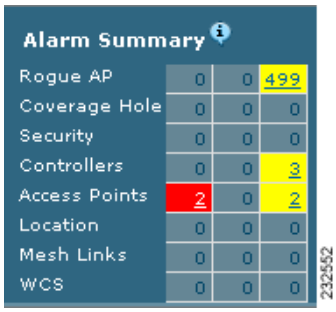
- Monitor unknown rogue access points until they are eliminated or acknowledged
- Determine the closest authorized access point, making directed scans faster and more effective
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. 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 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.

Figure 6-1 Alarm Monitor for Rogue Access Points



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.

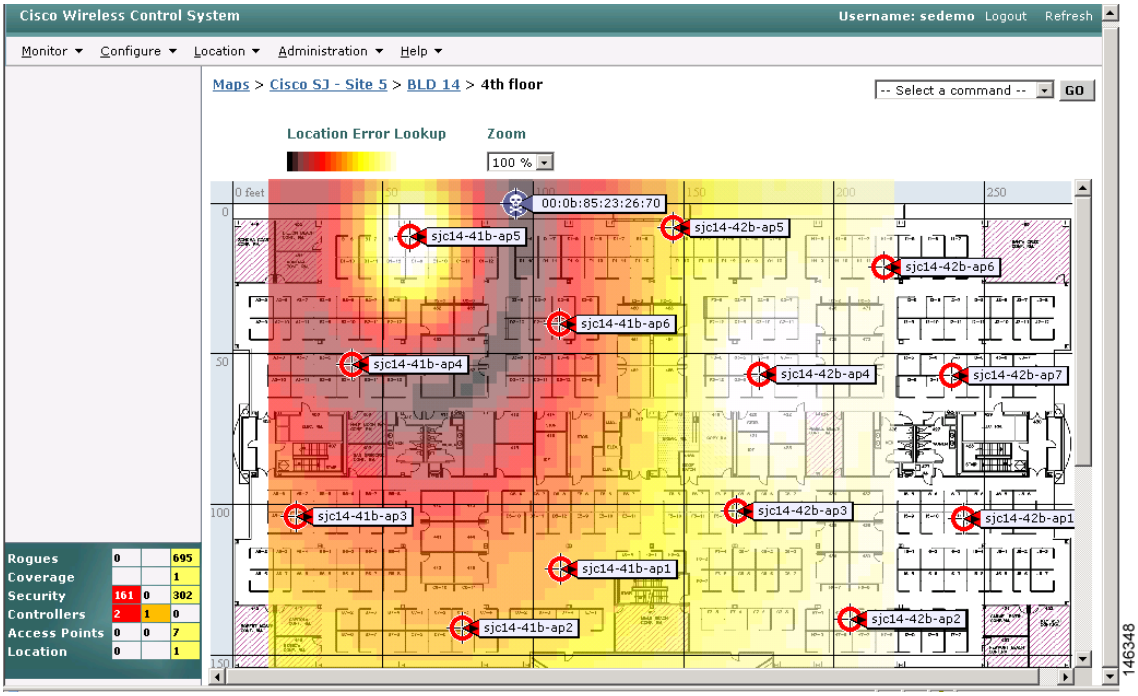
  Set State to 'Known - Internal'—Tags the rogue access point as internal, adds it to the known rogue access points list, and turns off containment.

  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.

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.

Monitoring Clients

This section provides access to the controller clients summary details. The information assists in identifying, diagnosing, and resolving client issues. To monitor clients, choose Monitor > Clients. The Client Summaries window appears.

The Client Summaries window contains the following portions:

Most Recent Client Notification

- Client—IP address, MAC address, or user-defined name of client.

- Event Type—Reason for client notification. For example, disassociated, WEP decrypt error, or authentication failure.
- Date/Time—Date and time of client notification.

Manually Disabled Clients

Choose **Monitor > Clients** and then click **Manually Disabled Clients** to access this page.

This page enables you to view manually disabled client template information.

- MAC Address—Client MAC address.
- Description—Optional user-defined description.

Top 5 APs

The Top 5 APs section includes the following:

- AP Name—This is the name assigned to the access point. Click an item in the list to see the details of that access point.
- Map Location —The name of the map where the client is located.
- a/n Clients—The number of 802.11a clients currently associated with the controller.
- b/g/n Clients—The number of 802.11b clients and 802.11g clients currently associated with the controller.
- Total Client—Total number of clients currently associated with the controller.

Clients Detected by Location Servers

Displays clients detected by location servers within the last 15 minutes.

- Server Name—User-defined location server name.
- Server Address—IP address of location server.
- Total Clients—Total number of clients currently associated with the location server.

Client Count

A graphic shows the associated clients during a given time frame.

Client Troubleshooting

In the Client Troubleshooting portion, enter the IP address, MAC address, or user-defined client name and click **Troubleshoot** to continue to the client details.

WLAN Client Troubleshooting

The client reporting protocol is used by the client and the access point to exchange client information. Client reports are collected automatically when the client associates. Follow these steps to run diagnostic tests and reports and to view available logs:

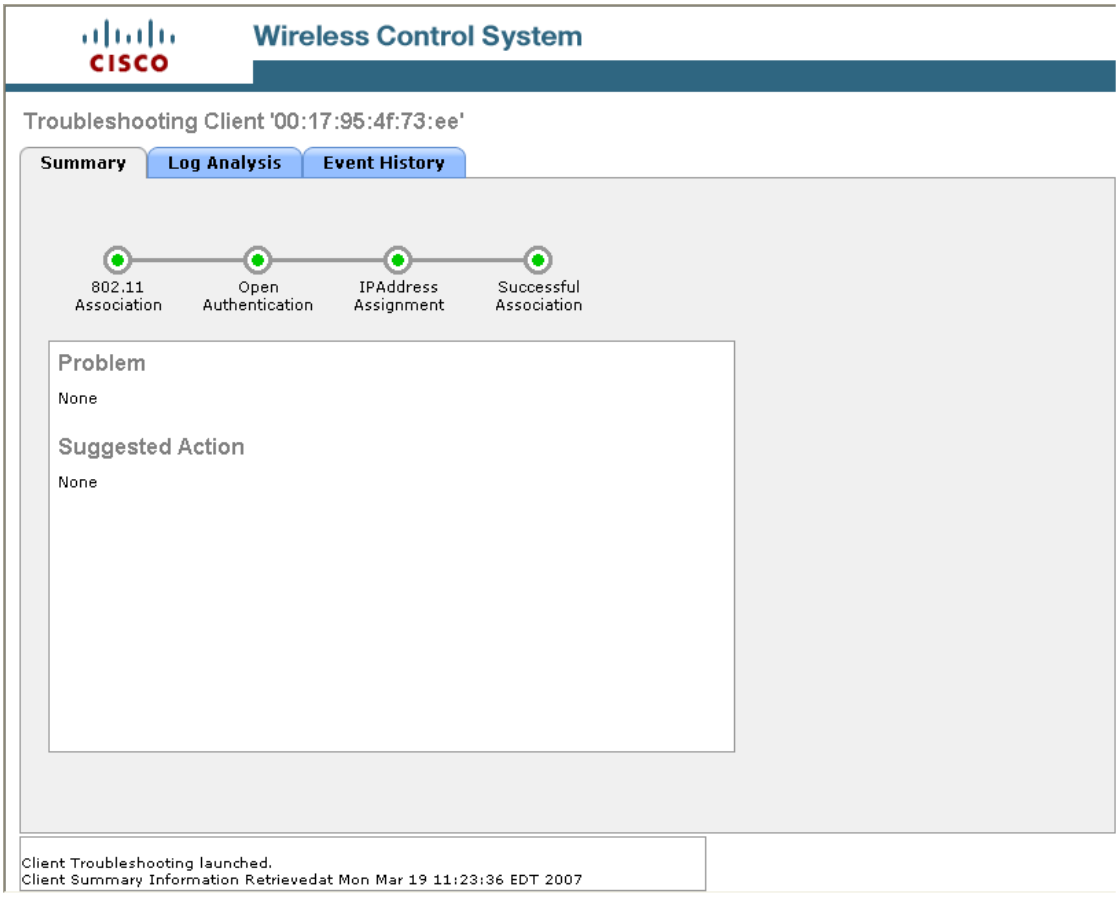
Step 1 Choose **Monitor > Clients**.

Step 2 (optional) In the Quick Search area, type the MAC address of the client in question.

Note To get the current status of the client, you must instead click **New Search** and choose the **Search on Controller Now** option. This option more accurately reflects the 802.11 state of the client because a quick search only periodically updates the database information.

Step 3 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).The number of tabs that appear depends on whether the client is a Cisco Compatible Extensions version 5 client or not. The Cisco Compatible Extensions Version 5 clients contain additional tabs like Test Analysis, Messaging, Event Log, and so on. 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.

Note Some Cisco Compatible Extension features do not function properly if you use a web browser other than Internet Explorer 6.0 on a Windows workstation.

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

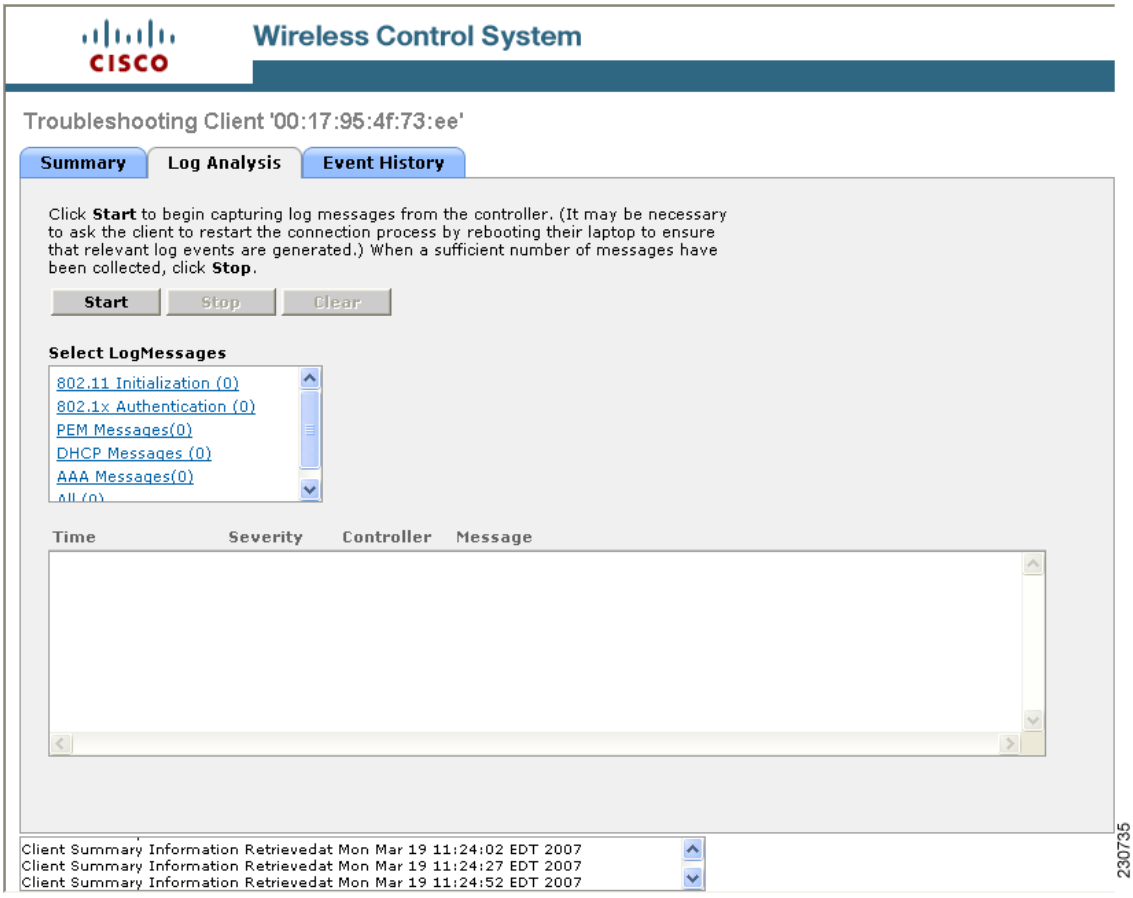
Step 5 To begin capturing log messages about the client from the controller, click **Start**. To stop log message capture, click **Stop**. To clear all log messages, click **Clear**.

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

Step 6 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

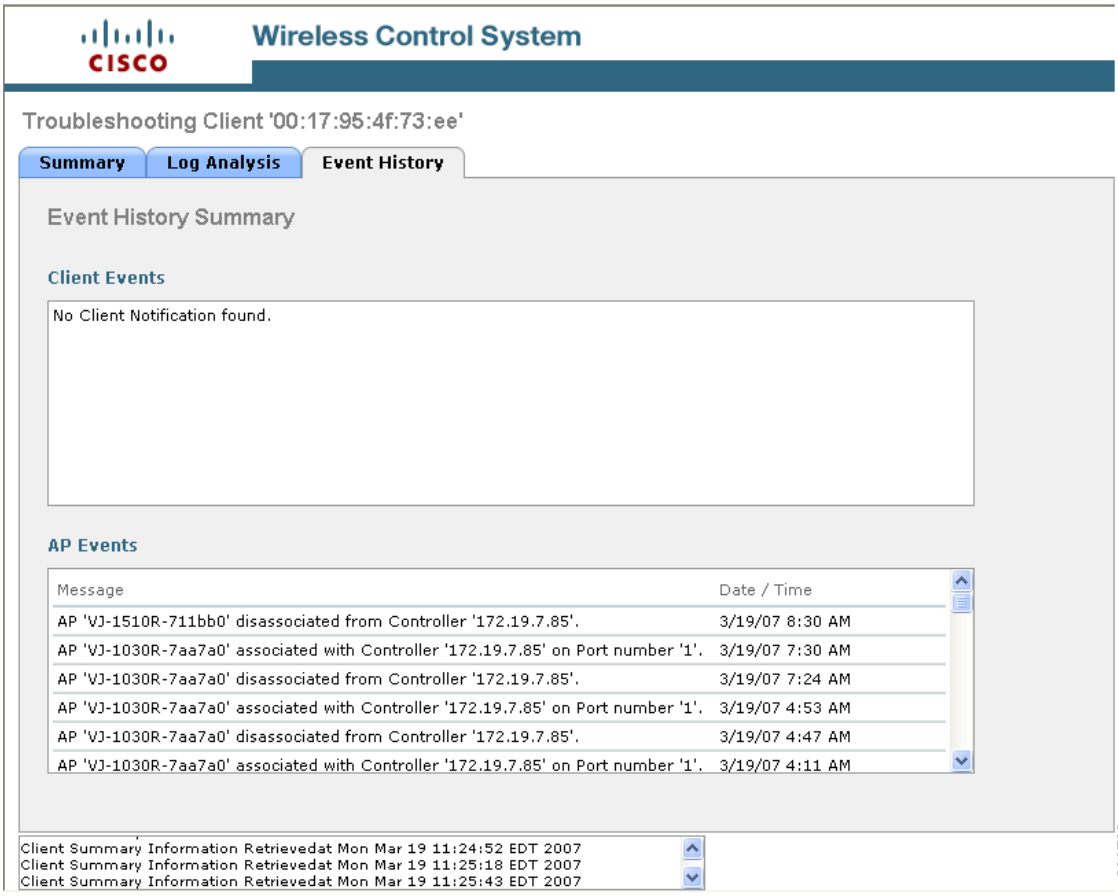
Figure 6-4 Log Analysis Tab



Step 7 To display a summary of the client's events history, click the **Event History** tab (see Figure 6-5).

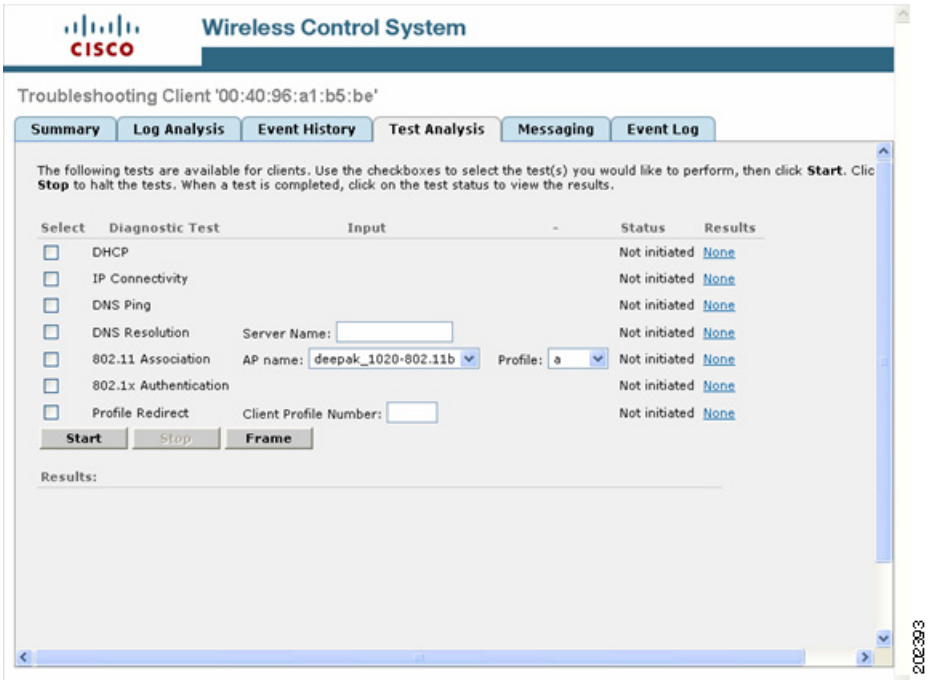
This page displays client and access point events that occurred within the last 24 hours.

Figure 6-5 Event History Tab



Step 8 (Optional) If Cisco Compatible Extension Version 5 clients are available, a Test Analysis tab as shown in Figure 6-6 appears.

Figure 6-6 Test Analysis Tab

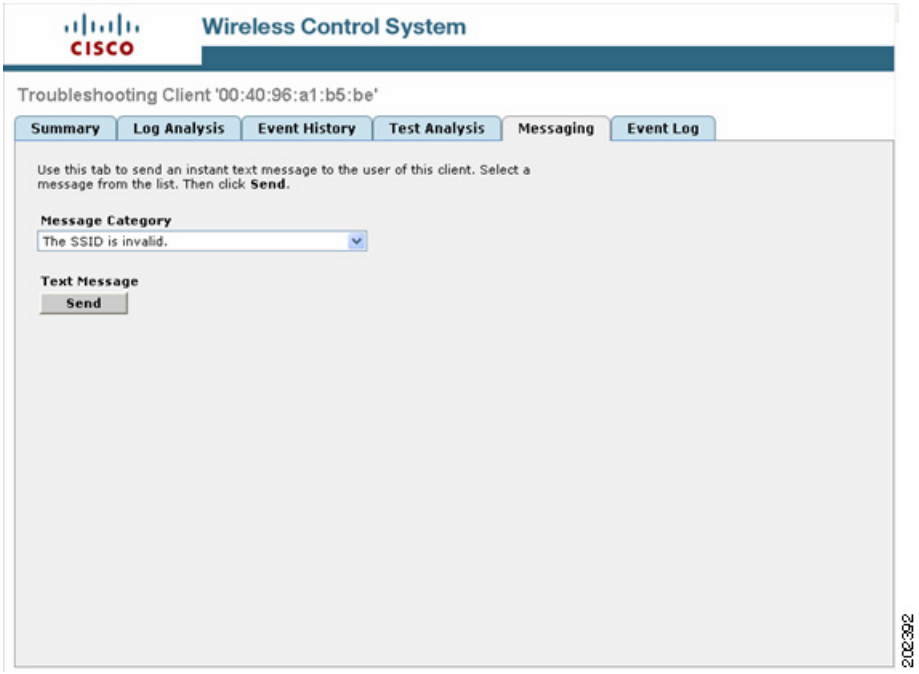


Step 9 The Test Analysis tab allows you to run a variety of diagnostic tests on the clent. Click the check box for the applicable diagnostic test, enter any input information (if applicable), and click **Start**. The following diagnostic tests are available:

- DHCP—Executes a complete DHCP Discover/Offer/Request/ACK exchange to determine that the DHCP is operating properly between the controller and the client.
- IP Connectivity—Causes the client to execute a ping test of the default gateway obtained in the DHCP test to determine that IP connectivity exists onthe local subnet.
- DNS Ping—Causes the client to execute a ping test of the DNS server obtained in the DHCP test to determine that IP connectivity exists to the DNS server.
- DNS Resolution—Causes the DNS client to attempt to resolve a network name known to be resolvable to determine that name resolution is functioning correctly.
- 802.11 Association—Directs an association to be completed with a specific access point to determine that the client is able to associate properly with a designated WLAN.
- 802.1X Authentication—Directs an association and 802.1X authentication to be completed with a specific access point to determine that the client is able to properly complete an 802.1x authentication with a designated WLAN.
- Profile Redirect—At any time, the diagnostic system may direct the client to activate one of the client's configured WLAN profiles and to continue operation under that profile.

Step 10 (Optional) If Cisco Compatible Extension Version 5 clients are available, a Messaging tab as shown in Figure 6-7 appears. Use this tab to send an instant text message to the user of this client. From the Message Category drop-down menu, choose a message and click **Send**.

Figure 6-7 Messaging Tab



Step 11 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 6-8). Table 6-1, Table 6-2, and Table 6-3 describe the fields displayed on this General tab.

Figure 6-8 Client Details Window

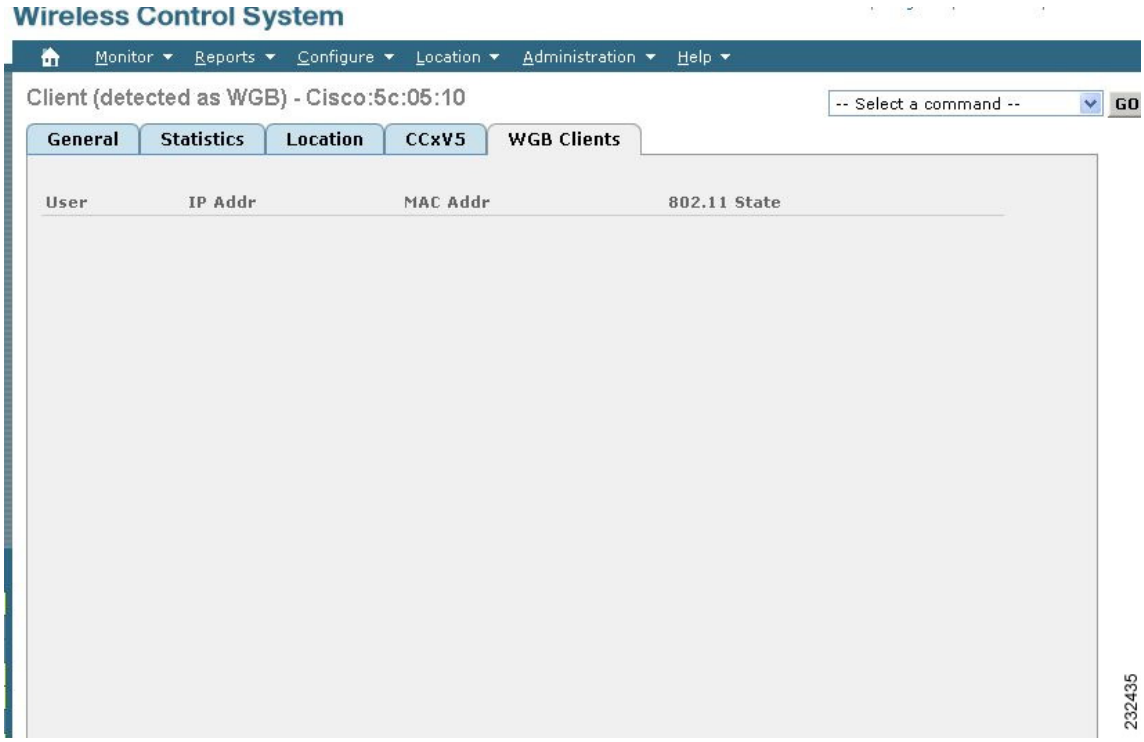


Table 6-1 General Tab / Client Properties

Parameter	Description
Client User Name	The username the client used for authentication.
Client IP Address	The IP address of the client.
Client MAC Address	The MAC address of the client.
Client Vendor	The client's vendor information.
Controller	The IP address of the controller to which the client is registered. Clicking the controller's IP address displays information about the controller.
Port	The port on the controller to which the client is connected.

Table 6-1 General Tab / Client Properties (continued)

Parameter	Description
802.11 State	802.11 state may be one of the following: • Idle (0)— normal operation: no rejections of client association requests • AAA Pending (1)— completing an AAA transaction • Authenticated (2)— 802.11 authentication completed • Associated (3)— 802.11 association completed • Power Save (4)— client in power save mode • Disassociated (5)— 802.11 disassociation completed • To Be Deleted (6)— to be deleted after disassociation • Probing (7)— client not associated or authorized yet
Interface	The name of the interface to which the client is connected.
VLAN ID	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.
802.11 State	The client's state: • Idle— Normal operation; no rejections of client association requests • AAA Pending— Completing an AAA transaction • Authenticated— 802.11 association completed • Associated— 802.11 association completed • Power Save— Client in power save mode • Disassociated— Disassociation completed • To Be Deleted—To be deleted after disassociated • Probing—Client not associated or authorized yet • Blacklisted—Automatically disabled by the system due to perceived security threats
Mobility Role	Associated or Unassociated.
Policy Manager State	Internal state of the client's WLAN. Client is working properly when the state is RUN.
Anchor Address	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).
Mirror Mode	Disable or enable.
Cisco Compatible Extension	Indicates if Cisco Compatible Extensions are supported

Table 6-1 General Tab / Client Properties (continued)

Parameter	Description
E2E	Indicates if E2E is supported.
WGB Status	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.

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

Parameter	Description
AP Name	The name of the access point to which the client is associated. Clicking the link displays information about the access point.
AP Type	The type of access point.
AP Base Radio MAC	The MAC address of the access point's base radio.
Protocol	The protocol used by the radio (802.11a/n or 802.11b/g/n).
AP Mode	The access point mode.
Profile Name	The profile name of the WLAN that the client is associated to or is trying to associate to.
SSID	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.
Security Policy	The WLAN security policy that is used.
Association Id	Client's access point association identification number.

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

Parameter	Description
Reason Code	The client reason code may be one of the following: • Normal (0) — Normal operation. • Unspecified reason (1) — Client associated but no longer authorized. • PreviousAuthNotValid(2) — Client associated but not authorized. • DeauthenticationLeaving (3) — The access point went offline, deauthenticating the client. • DisassociationDueToInactivity (4) — Client session timeout exceeded. • DisassociationAPBusy(5) — The access point is busy, performing load balancing, for example. • Class2FrameFromNonAuthStation (6) —Client attempted to transfer data before it was authenticated. • Class2FrameFromNonAssStation (7) — Client attempted to transfer data before it was associated. • DisassociationStnHasLeft (8) — Controller moved the client to another access point using non-aggressive load balancing. • StaReqAssociationWithoutAuth (9) — Client not authorized yet, still attempting to associate with a Cisco WLAN Solution. • Missing Reason Code (99) — Client momentarily in an unknown state.
802.11 Authentication	Which 802.11 authentication algorithm is in force.

Table 6-3 General Tab / Security

Parameter	Description
Authenticated	Indicates whether the client has been authenticated.
Policy Type	The type of security policy used by the client.
Encryption Cypher	Encryption settings.
EAP Type	Type of Extensible Authentication Protocol (EAP) used.

Step 12 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 13 To display client statistics, click the **Statistics** tab (see Figure 6-9).

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 6-9 Statistics Tab

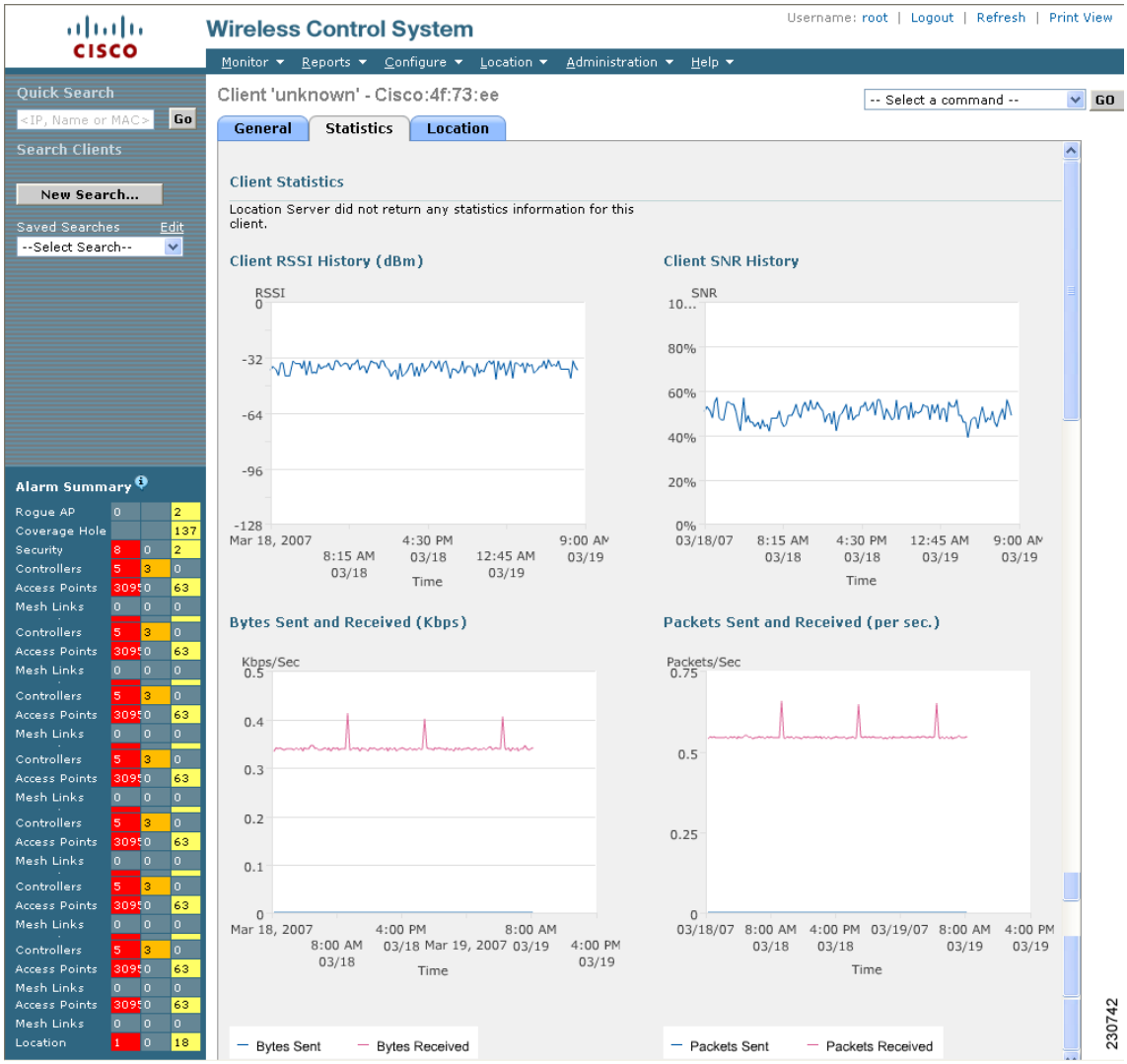


Table 6-4 Statistics Tab / Client Statistics

Parameter	Description
RSSI	Receive signal strength indicator of the client RF session.
SNR	Signal to noise ratio of the client RF session.
Bytes Sent and Received	Total number of bytes sent to the client and received by the controller from the client.
Packets Sent and Received	Total number of packets sent to the client and received by the controller from the client.

Table 6-4 Statistics Tab / Client Statistics (continued)

Parameter	Description
Client RSSI History (dBm)	History of RSSI as detected by the access point with which the client is associated.
Client SNR History	History of SNR as detected by the access point with which the client is associated.

Step 14 To display the client's location information, click the **Location** tab (see Figure 6-10). Table 6-5 describes the fields displayed on this Location tab.

Figure 6-10 Location Tab

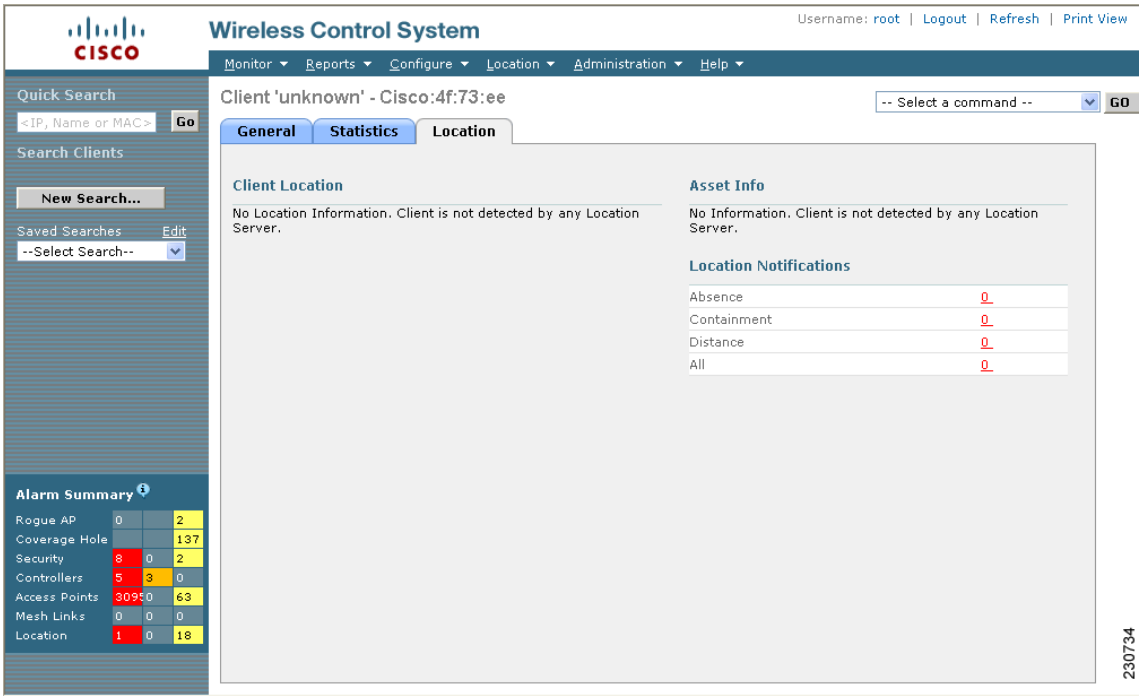


Table 6-5 Location Tab

Parameter	Description
Client Location	Describes the location of the client in the map based on RF fingerprinting.
Asset Information	Describes the asset file destination and name.
Location Notifications	Displays the number of location notifications logged against the client. Clicking a link displays the notifications.
Absence	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.

Table 6-5 Location Tab (continued)

Parameter	Description
Containment	The location server generates containment events when an asset is moved inside or outside of a designated area. **Tip** You define a containment area (campus, building, or floor) here. You can define a coverage area using the Map Editor.
Distance	The location server generates movement events when an asset is moved beyond a specified distance from a designated marker you define on a map.
All	The total of absence, containment, and distance notifications.

Step 15 Click the **Cisco Compatible Extension (version 5) Info** tab. Reports specific to compatible clients provide client details that enhance client diagnostics and troubleshooting. Table Table 6-6 describes the parameters on the Manufacturer Information portion of the Cisco Compatible Extension (version 5) Info tab.

Note The Cisco Compatible Extensions (version 5) manufacturing information displays for compatible clients only.

Table 6-6 Manufacturer Information

Parameter	Description
Organizationally Unique Identifier	The IEEE assigned organizational unique identifier, for example the first 3 bytes of the MAC address of the wireless network connected device.
ID	The manufacturer identifier of the wireless network adapter.
Model	Model of the wireless network adapter.
Serial Number	Serial number of the wireless network adapter.
Radio	Radio type of the client.
MAC Address	MAC address assigned to the client.
Antenna Type	Type of antenna connected to the wireless network adapter.
Antenna Gain	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.
Radio Receiver Sensitivity	
Provides the receiver sensitivity of the each wireless network adapter. It shows the minimum and maximum RSSI for each radio type as well as the data rate.	

Table 6-6 Manufacturer Information

Parameter	Description
CCXV5 Capability Information	
Lists the client status and service capability of the Cisco Compatible Extensions version 5 clients.	
Radio Channels	
Lists all channels used by each radio.	
Transmit Data Rates	
Lists all data rates used by each radio.	

Table 6-7 describes the parameters displayed in the Cisco Compatibility Extensions (version 5) Capability Information portion of the tab.

Note The Cisco Compatible Extensions (version 5) capability information displays for compatible extension clients only.

Table 6-7 Client Statistics

Parameter	Description
Bytes Sent and Received (Kbps)	Bytes sent and received with the associated access point.
Packets Sent and Received (per second)	Packets sent and received with the associated access point.

Step 16 To display the client's workgroup bridge information, click the **WGB Clients** tab. Table 6-8 describes the fields that display on this WGB tab.

Table 6-8 WGB Clients Tab

Parameter	Description
User	The user name assigned to the work group bridge.
IP Addr	The IP address of the workgroup bridge.
MAC Addr	The MAC address of the workgroup bridge.
802.11 State	Specifies whether the workgroup bridge is associated or not.

Finding Clients

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

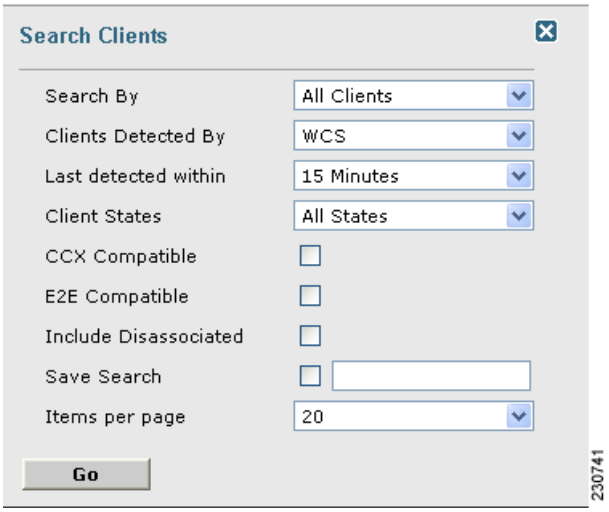
Step 1 Click **Monitor > Clients** to navigate to the Clients Summary page.

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 6-11).

Figure 6-11 Search Clients



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/n, 802.11b/n, and 802.11g/n.
- Restrict by SSID — To restrict the search by SSID. Then enter the SSID in the text field.
- Cisco Compatible Extensions — To search for Cisco Compatible Extension 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.

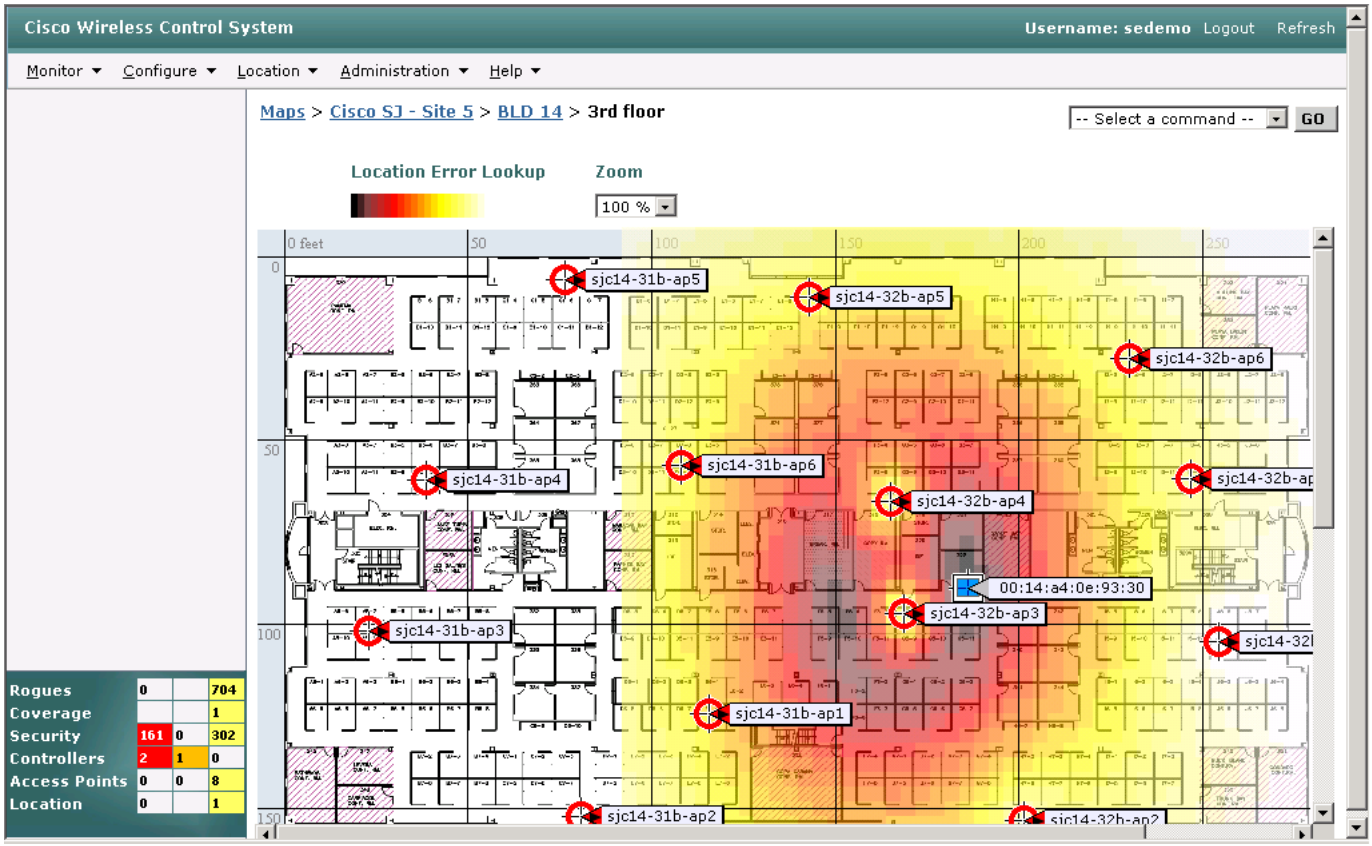
Note The Client RSSI History, Client SNR History, Bytes Sent and Received, and Packets Sent and Received reports are displayed. You can specify graph view or table view by clicking the appropriate icon. If it is a report where you can specify time period, enter both the start and end time or a specific time period.

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.
- **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 6-12 shows a heat map that includes a client location.

Figure 6-12 Map with Client Location



Step 7 To view statistics for the selected client, click the **Statistics** tab.

Table 6-9 Client Statistics

Parameter	Description
Bytes received	Total number of bytes received by the controller from the client.
Bytes sent	Total number of bytes sent to the client from the controller.
Packets received	Total number of packets received by the controller from the client.
Packets sent	Total number of packets sent to the client from the controller.
Policy errors	Number of policy errors for the client.
RSSI	Receive signal strength indicator of the client RF session.
SNR	Signal-to-noise ratio of the client RF session.
Client RSSI History (dBm)	History of RSSI as detected by the access point with which the client is associated.
Client SNR History	History of SNR as detected by the access point with which the client is associated.

Table 6-9 Client Statistics

Parameter	Description
Bytes Sent and Received (Kbps)	Bytes sent and received with the associated access point.
Packets Sent and Received (per second)	Packets sent and received with the associated access point.

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.

Step 11 A test analysis generates the following results:

- DHCP—Verifies that DHCP is operating correctly between the controller and the client.
- IP Connectivity—Determines that IP connectivity exists on the local subnet. The IP connectivity test causes the client to execute a ping test to the default gateway.
- DNS Ping—Verifies that IP connectivity exists to the DNS server by having the client perform a ping test to the DNS server.
- DNS Resolution—Verifies that name resolution is functioning correctly. To test, the client tests a network name known to be resolvable, such as www.cisco.com.
- 802.1X Association—Determines that the client is able to associate properly with a designated WLAN and with a specific access point.
- 802.1X Authentication—Determines that the client is able to complete an 802.1X authentication with a designated WLAN and with a specific access point.

Receiving Radio Measurements

On the client window, you can receive radio measurements only if the client is Cisco Compatible Extensions 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 the 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
- 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 is also communicated.

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 areas of weak signal strength are detected, 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.

Step 2 Click the desired IP address to display the *IP Address* > Controller Properties page.

Step 3 In the sidebar, choose **System > Commands** to display the *IP Address* > Controller Commands page.

Step 4 Choose **Ping From Controller** from the Administrative Commands drop-down menu and click **GO**.

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

WCS displays the Ping Results window, which shows the packets that have been sent and received. Click **Restart** to ping the network device again or click **Close** to stop pinging the network device and exit the Ping Results window.

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:

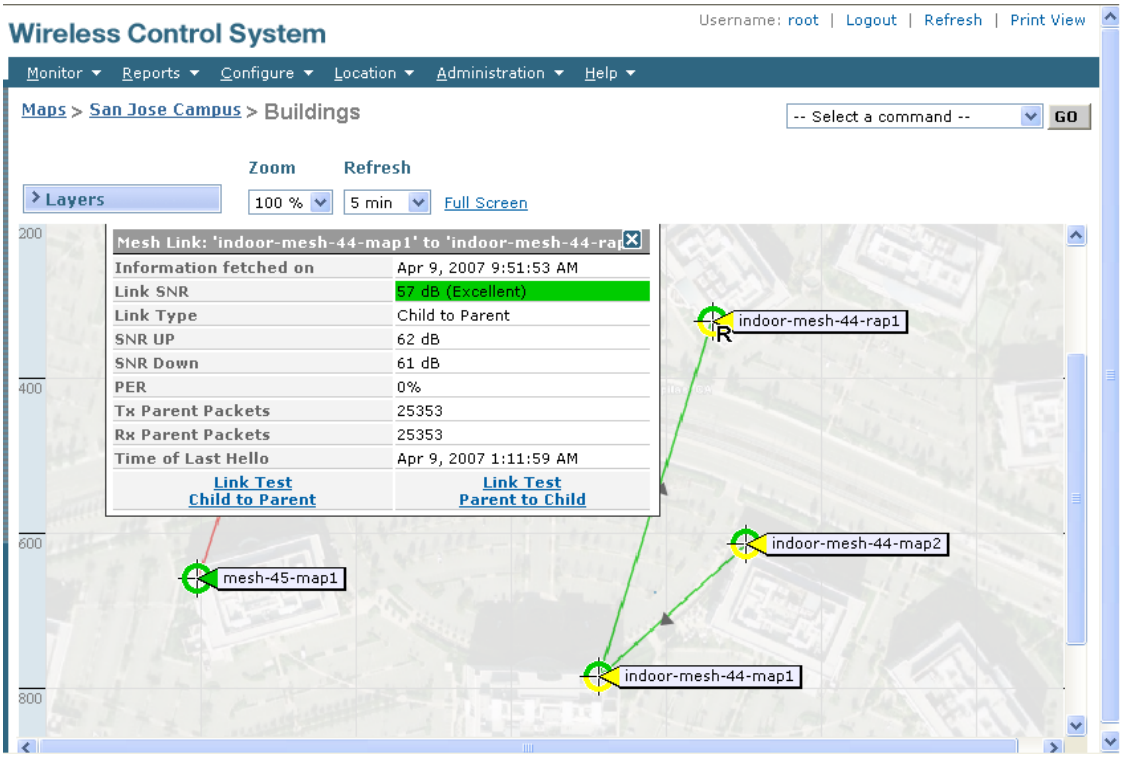
Step 1 In Cisco WCS, choose **Monitor > Maps**.

Step 2 Click 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 6-13). 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.

Figure 6-13 Mesh Link Details Window

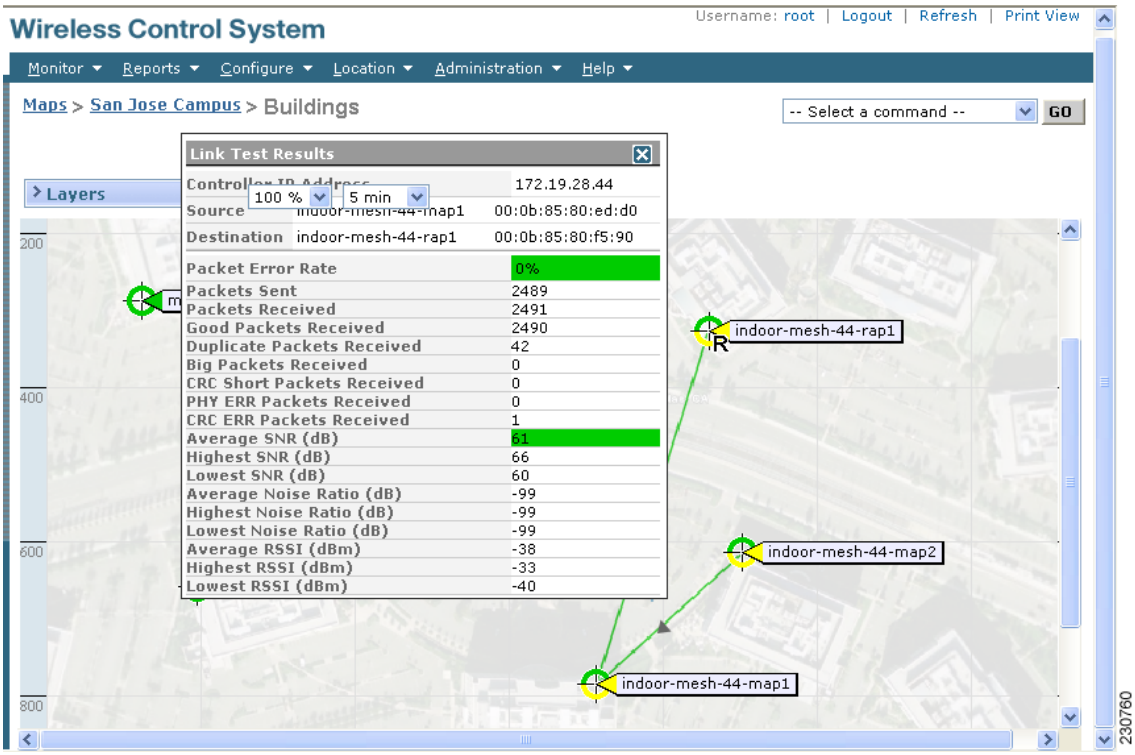


Step 4 Click either **Link Test**, **Child to Parent or Link Test**, or **Parent to Child**. After the link test is complete, a results page appears (see Figure 6-14).

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.

Figure 6-14 Link Test Results

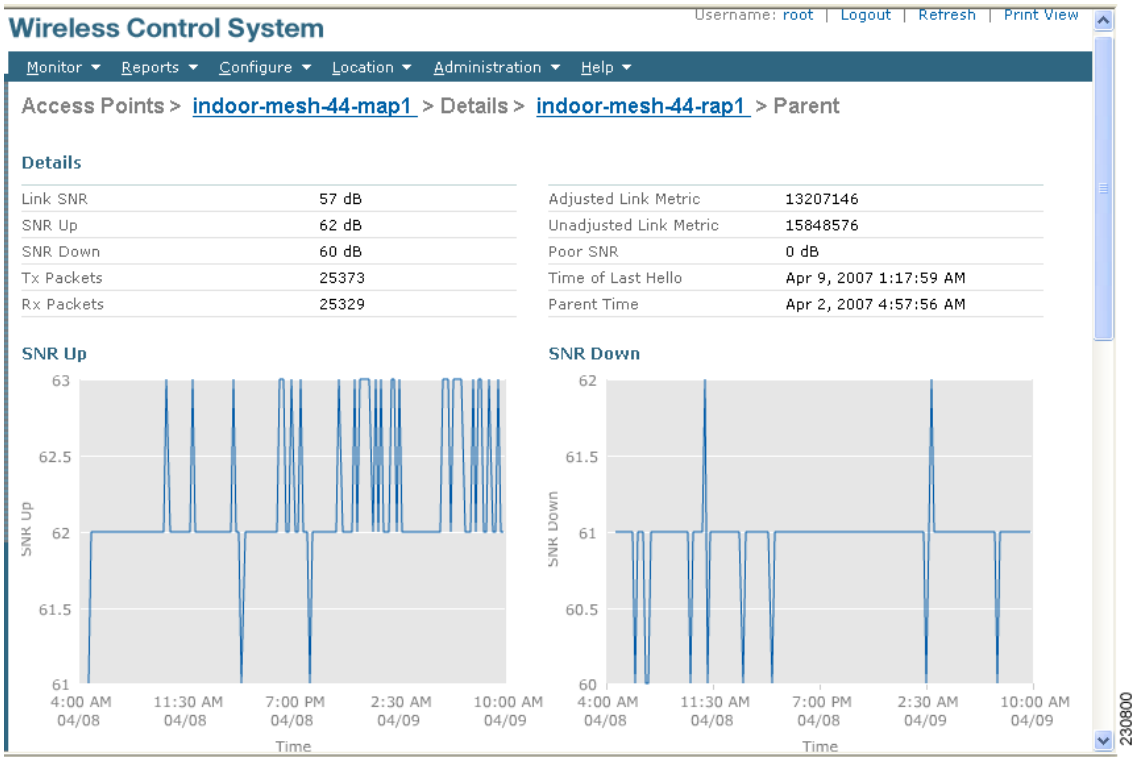


Step 5 To view a graphical representation of SNR statistics over a period of time, click the arrow on the link. A window with multiple SNR graphs appears (see Figure 6-15).

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.

Figure 6-15 Mesh SNR Graphs Page (Top)



Monitoring Mesh Access Points Using Maps

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

- Parent
- Number of children
- Hop count
- 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, controller IP address, location, height of access point, access point up time, and LWAPP up time).

Note You can also view detailed configuration 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 13-9.

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 the **Map Name** that corresponds to the outdoor area, campus, building, or floor location of the access point 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 6-16).

Figure 6-16 Mesh AP Summary Panel

Step 4 To view detailed configuration information for an access point, click the arrow portion of the mesh access point label. The configuration details for the access point appears (see Figure 6-17).

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 6-32. If the access point has an IP address, a Run Ping Test link is also visible at the bottom of the mesh access point panel.

Figure 6-17 Mesh AP Detail Window

Note The information on external batteries (such as charging level and remaining capacity) for mesh access points is not accurately reflected.

Step 5 At the Access Point configuration window, follow these steps to view configuration details for the mesh access point.

a. Choose the **General** tab to view the overall configuration of the mesh access point such as AP name, MAC address, AP and LWAPP Up time, associated controllers (registered and primary) operational status, and software version.

Note The software version for mesh access points is appended the letter *m* and the word *mesh* in parentheses.

b. Choose the **Interface** tab to view configuration details for the interfaces supported on the mesh access point. Interface options are radio and Ethernet.

c. Choose the **Mesh Links** tab to view parent and neighbors' details (name, MAC address, packet error rate, and link details) for the mesh access point. You can also initiate link tests from this panel.

d. Choose the **Mesh Statistics** tab to view details on the bridging, queue, and security statistics for the mesh access point. For more details on mesh statistics, refer to the "Mesh Statistics for an Access Point" section on page 6-35.

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:

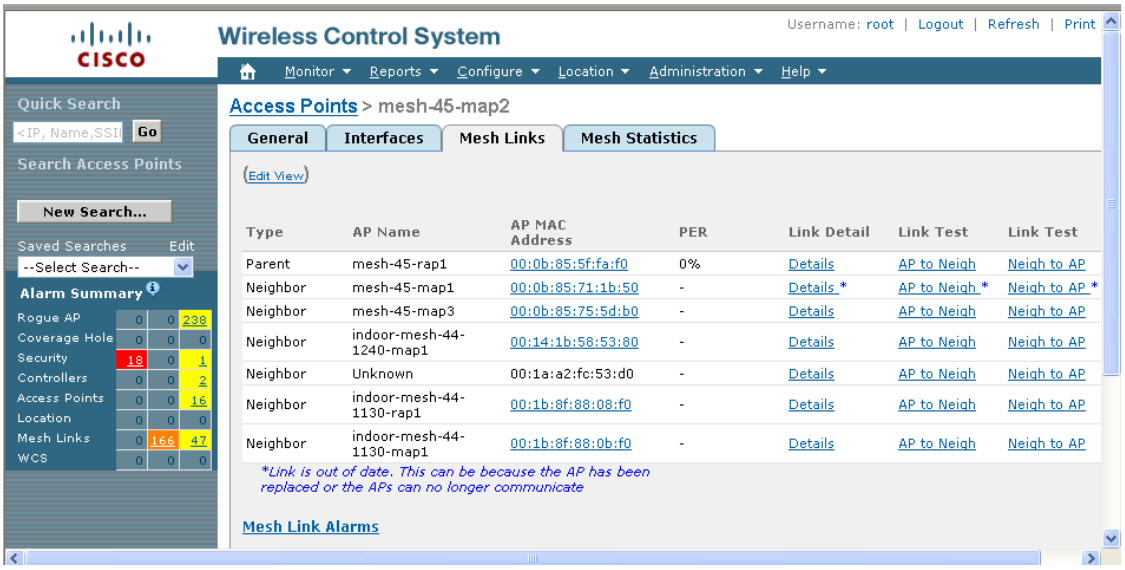
Step 1 In Cisco WCS, choose **Monitor > Maps**.

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

Step 3 To view detailed information on mesh links for a mesh access point, click the arrow portion of the access point label. The Access Points screen appears.

Step 4 Click the Mesh Links tab (see Figure 6-18).

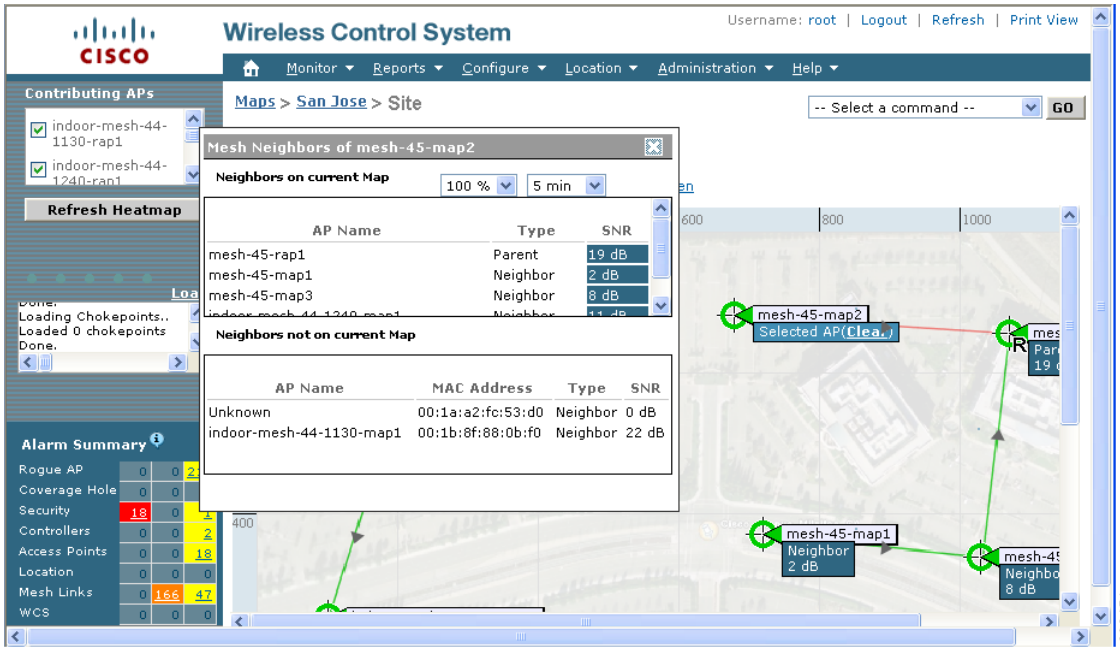
Figure 6-18 Access Points > Mesh Links Panel



Note You can also mesh link details for neighbors of a selected access point by clicking on the View Mesh Neighbors link on the access point configuration summary panel that displays when you mouse over an access point on a map (see Figure 6-17).

Note Signal-to-noise (SNR) only appears on the View Mesh Neighbors panel (see Figure 6-18).

Figure 6-19 View Mesh Neighbors Panel



Note In addition to listing the current and past neighbors in the panel that displays, labels are added to the mesh access points map icons to identify the selected access point, the neighbor access point, and the child access point. Select the **clear** link of the selected access point to remove the relationship labels from the map.

Note The drop-down menus at the top of the mesh neighbors window indicate the resolution of the map (100%) displayed and how often the information displayed is updated (5 mins). You can modify these default values.

Monitoring Mesh Health

Mesh Health monitors the overall health of Cisco Aironet 1500 and 1520 series outdoor access points as well as Cisco Aironet 1130 and 1240 series indoor access points when configured as mesh access points, except as noted. Tracking this environmental information is particularly critical for access points that are deployed outdoors. The following factors are monitored:

- Temperature: Displays the internal temperature of the access point in Fahrenheit and Celsius (Cisco Aironet 1510 and 1520 outdoor access points only).
- Heater status: Displays the heater as on or off (Cisco Aironet 1510 and 1520 outdoor access points only)
- AP Up time: Displays how long the access point has been active to receive and transmit.
- LWAPP Join Taken Time: Displays how long it took to establish the LWAPP connection (excluding Cisco Aironet 1505 acces points).

- LWAPP Up Time: Displays how long the LWAPP connection has been active (excluding Cisco Aironet 1505 access points).

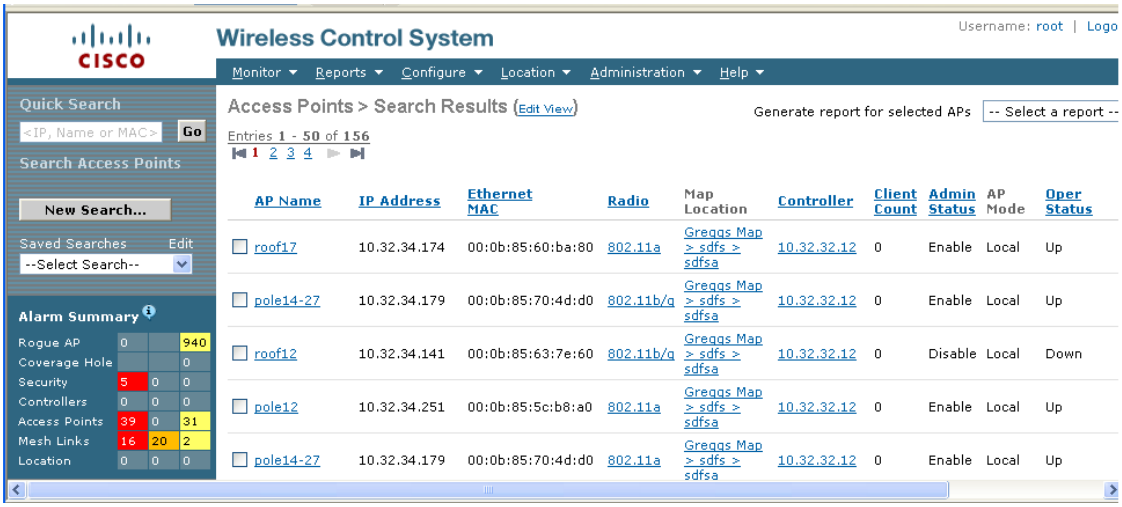
Mesh Health information is displayed in the General Properties panel for mesh access points.

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 6-20).

Note You can also use the New Search button to display the mesh 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 6-20 Monitor > Access Points



Step 2 Click the AP Name link to display details for that mesh access point. The General Properties panel for that mesh access point appears (see Figure 6-21).

Note You can also access the General properties panel for a mesh access point from a Cisco WCS map window. To display the panel, click the arrow portion of the mesh access point label. A tabbed panel appears and displays the General properties panel for the selected access point.

Figure 6-21 AP Name > General Properties Page

Mesh 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 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:

- Bridging
- Queue
- Security

To view the mesh 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 6-22).

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 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.

Step 3 Click the **Mesh Statistics** tab (see Figure 6-22). A three-tabbed Mesh Statistics panel appears.

Note The Mesh Statistics tab and its subordinate tabs (Bridging, Queue and Security) only appear for mesh access points. The Mesh Link Alarms and Mesh Link Events links are accessible from each of the three tabbed panels.

Note You can also access the Mesh Securities panel for a mesh access point from a Cisco WCS map. To display the panel, click the arrow portion of the mesh access point label.

Figure 6-22 Monitor > Access Points > AP Name > Mesh Statistics

Summaries of the Bridging, Queue and Security Statistics and their definitions are provided in Table 6-10, Table 6-11 and Table 6-12 respectively.

Table 6-10 Bridging Mesh Statistics

Parameter	Description
Role	The role of the mesh access point. Options are mesh access point (MAP) and root access point (RAP).
Bridge Group Name (BGN)	The name of the bridge group to which the MAP or RAP is a member. Assigning membership in a BGN is recommended. If one is not assigned, a MAP is by default assigned to a default BGN.
Backhaul Interface	The radio backhaul for the mesh access point.
Routing State	The state of parent selection. Values that display are seek, scan and maint. Maint displays when parent selection is complete.
Malformed Neighbor Packets	The number of malformed packets received from the neighbor. Examples of malformed packets include malicious floods of traffic such as malformed or short DNS packets and malformed DNS replies.
Poor Neighbor SNR	The number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.
Excluded Packets	The number of packets received from excluded neighbor mesh access points.
Insufficient Memory	The number of insufficient memory conditions.
RX Neighbor Requests	The number of broadcast and unicast requests received from the neighbor mesh access points.
RX Neighbor Responses	The number of responses received from the neighbor mesh access points .
TX Neighbor Requests	The number of unicast and broadcast requests sent to the neighbor mesh access points.
TX Neighbor Responses	The number of responses sent to the neighbor mesh access points.
Parent Changes	The number of times a mesh access point (child) moves to another parent.
Neighbor Timeouts	The number of neighbor timeouts.
Node Hops	The number of hops between the MAP and the RAP. Click the value link to display a sub-panel which enables you to configure details of what is reported, how often the node hop value is updated, and view a graphical representation of the report.

Table 6-11 Queue Mesh Statistics

Parameter	Description
Silver Queue	The average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Gold Queue	The average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Platinum Queue	The average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Bronze Queue	The average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Management Queue	The average and peak number of packets waiting in the management queue during the defined statistics time interval. Packets dropped and queue size is also summarized.

Table 6-12 Security Mesh Statistics

Parameter	Description
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.

Table 6-12 Security Mesh Statistics (continued)

Parameter	Description
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.

Table 6-12 Security Mesh Statistics (continued)

Parameter	Description
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.

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.

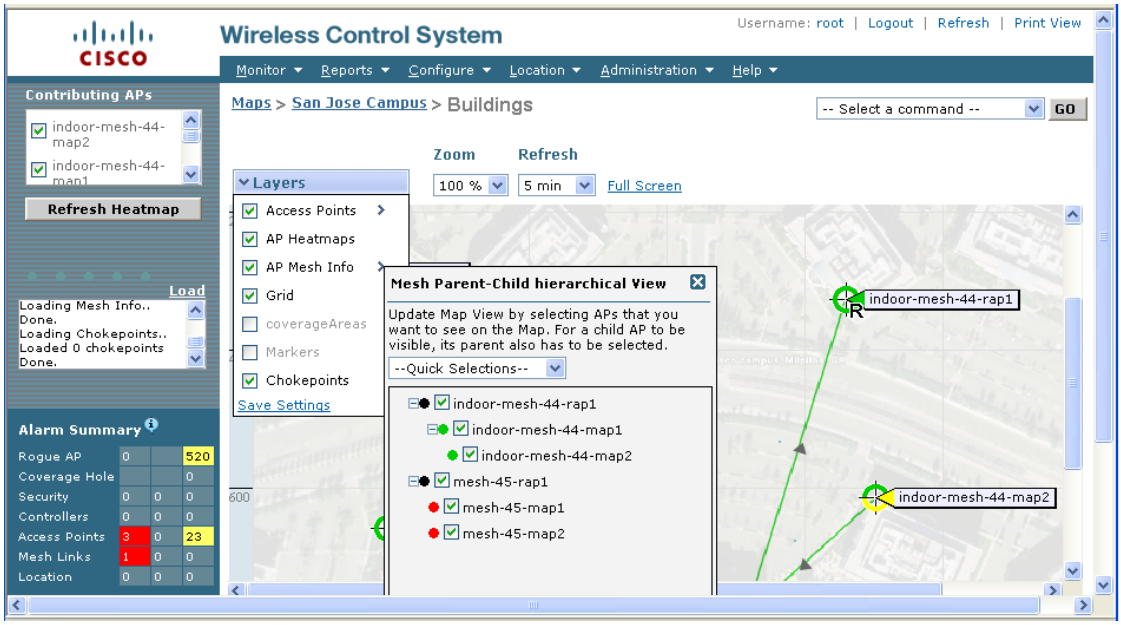
To view the mesh network hierarchy for a selected network, do the following:

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 6-23).

Figure 6-23 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 6-23, the access point, *indoor-mesh-45-rap2*, has only one child, *indoor-mesh-44-map2*.

Step 7 Move the cursor over the colored dot next to each mesh access point child to view details on the link between it and its parent. Table 6-13 summarizes the parameters that display.

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.

Table 6-13 Bridging Link Information

Parameter	Description
Information fetched on	Date and time that information was compiled.
Link SNR	Link signal-to-noise ratio (SNR).
Link Type	Hierarchical link relationship.
SNR Up	Signal-to-noise radio for the uplink (dB).
SNR Down	Signal-to-noise radio for the downlink (dB).
PER	The packet error rate for the link.
Tx Parent Packets	The TX packets to a node while acting as a parent.
Rx Parent Packets	The RX packets to a node while acting as a parent.
Time of Last Hello	Date and time of last hello.

Using Mesh Filters to Modify Map Display of Maps and Mesh Links

In the mesh hierarchical window, you can also define mesh filters to determine which mesh access points display on the map based on hop values as well as what labels display for mesh links.

Mesh access points are filtered by the number of hops between them and their root access point.

To use mesh filtering, follow these steps:

Step 1 To modify what label and color displays for a mesh link, follow these steps:

a. In the Mesh Parent-Child Hierarchical View, select an option from the Link Label drop-down menu. Options are None, Link SNR, and Packet Error Rate.

b. In the Mesh Parent-Child Hierarchical View, select an option from the Link Color drop-down menu to define which parameter (Link SNR or Packet Error Rate) determines the color of the mesh link on the map.

Note The color of the link provides a quick reference point of the SNR strength or Packet Error Rate.

Table 6-14 Definition for SNR and Packet Error Rate Link Color

Link Color	Link SNR	Packet Error Rate (PER)
Green	Represents a SNR above 25 dB (high value)	Represents a PER of one percent (1%) or lower
Amber	Represents a SNR between 20 and 25 dB (acceptable value)	Represents a PER that is less than ten percent (10%) and greater than one percent (1%)
Red	Represents a SNR below 20 dB (low value)	Represents a PER that is greater than ten percent (10%)

Note The Link label and color settings are reflected on the map immediately (see Figure 6-24). You can display both SNR and PER values simultaneously.

Step 2 To modify which mesh access points display based on the number of hops between them and their parents, do the following:

a. In the Mesh Parent-Child Hierarchical View, click the **Quick Selections** drop-down menu.

b. Select the appropriate option from the menu. A description of the options is provided in Table 6-15.

Table 6-15 Quick Selection Options

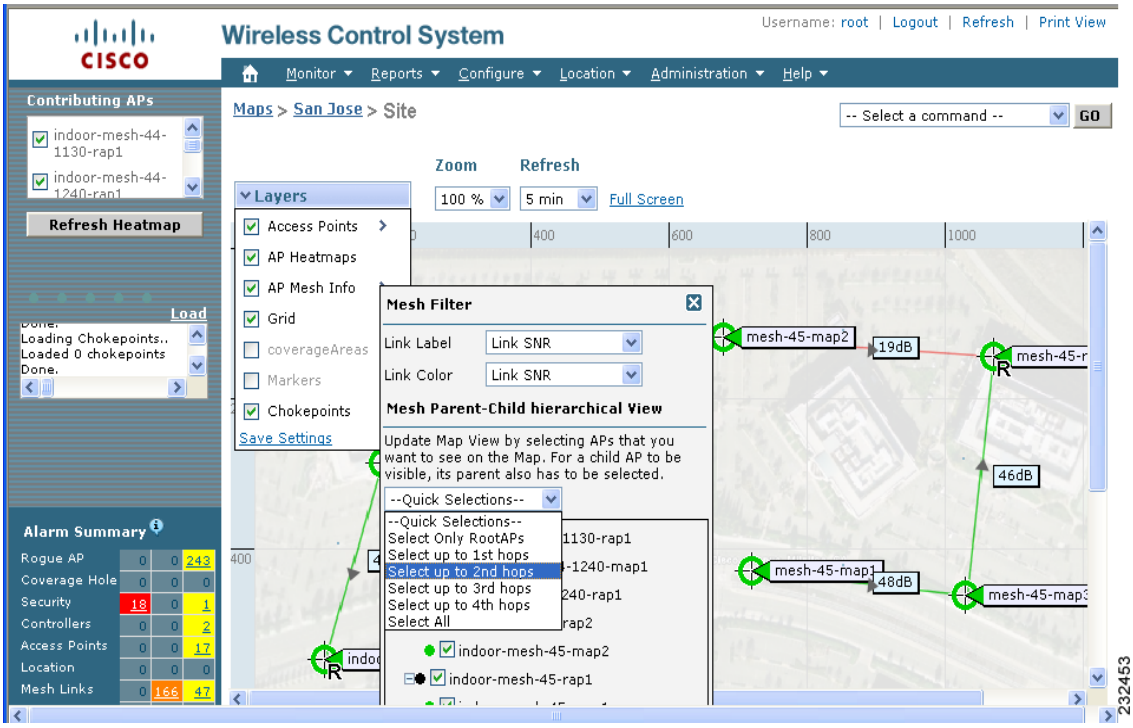
Parameter	Description
Select only Root APs	Choose this setting if you want the map view to display root access points only.
Select up to 1st hops	Choose this setting if you want the map view to display 1st hops only.
Select up to 2nd hops	Choose this setting if you want the map view to display 2nd hops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

c. 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.

Note You can also check or uncheck the check boxes of access points in the mesh hierarchical view to modify which mesh access points are displayed. For a child access point to be visible, the parent access point to root access point must be selected.

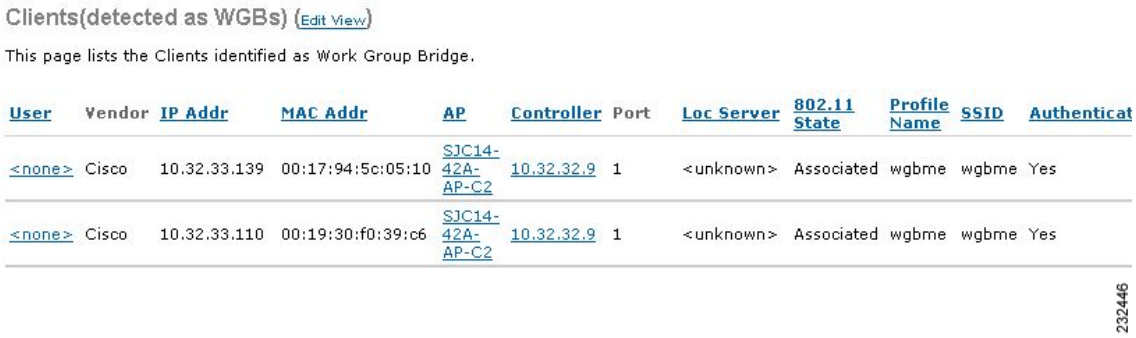
Figure 6-24 Mesh Filter and Hope Count Configuration Panel



Viewing Clients Identified as WGBs

When you click Monitor > WGB, you get a list of all clients identified as a workgroup bridges (see Figure 6-25). WGB clients bridge wireless to wired. Any IOS access point can take on the role of a WGB, acting as a wireless client with a wired client connected to it. The information about this WGB is propogated to the controller and appears as a client in both WCS and WLC.

Figure 6-25 Monitor > WGBs



Clients(detected as WGBs) (Edit View)

This page lists the Clients identified as Work Group Bridge.

User	Vendor	IP Addr	MAC Addr	AP	Controller	Port	Loc Server	802.11 State	Profile Name	SSID	Authenticat
<none>	Cisco	10.32.33.139	00:17:94:5c:05:10	SJC14-42A-AP-C2	10.32.32.9	1	<unknown>	Associated	wgbme	wgbme	Yes
<none>	Cisco	10.32.33.110	00:19:30:f0:39:c6	SJC14-42A-AP-C2	10.32.32.9	1	<unknown>	Associated	wgbme	wgbme	Yes

232446

Running a Link Test

A link test uses a ping from parent-to-child or 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 Cisco Compatible Extensions 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.

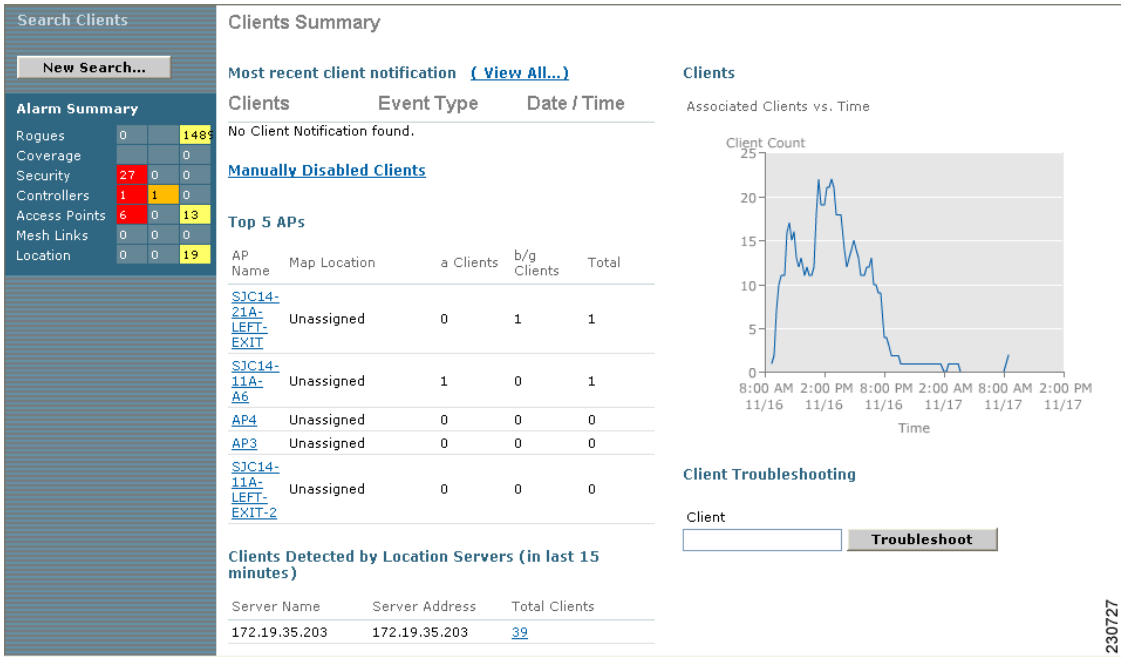
Step 3 In the Client States drop-down menu, choose **All States**. The client list page appears.

Step 4 Click the **Link Test** link in the last column. The link test begins. Figure 6-27 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 6-26).

Figure 6-26 Clients Summary



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 6-27 shows a sample Cisco Compatible Extensions link test result and Figure 6-28 shows a sample ping test result.

Figure 6-27 Cisco Compatible Extensions Link Test Result

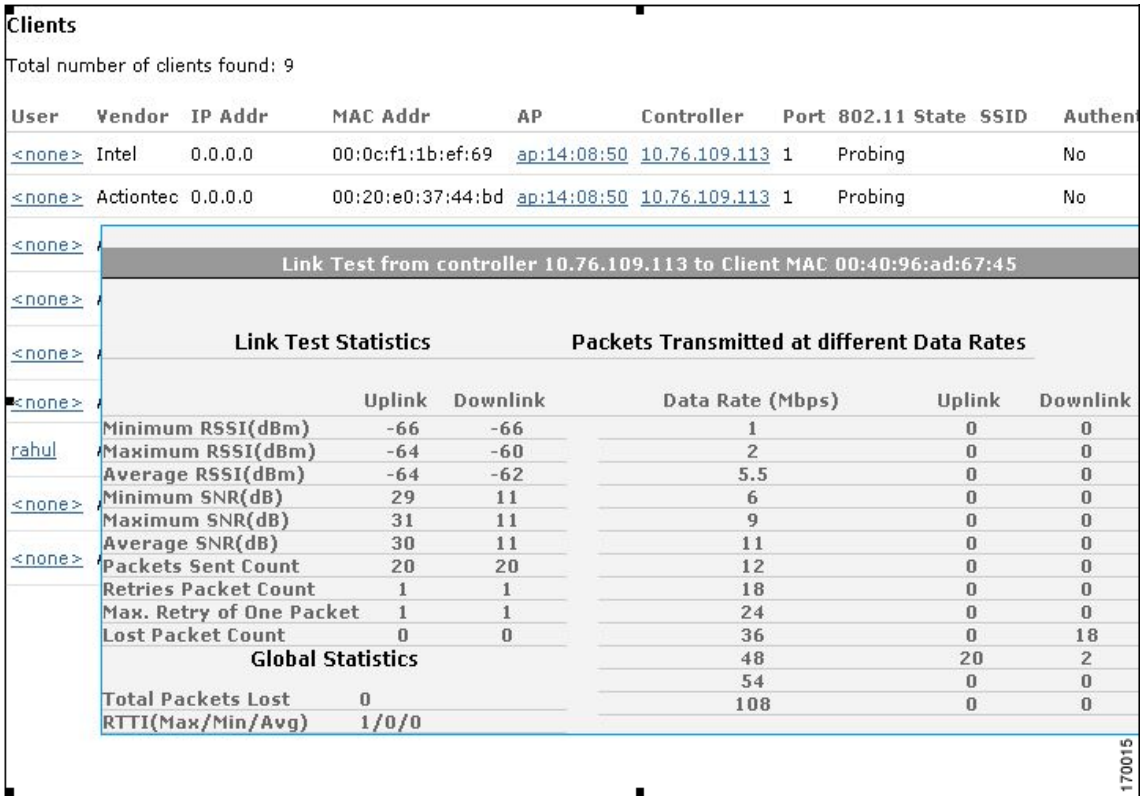
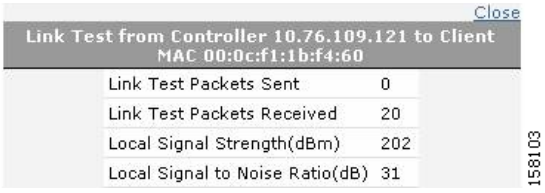


Figure 6-28 Ping Test Result



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)

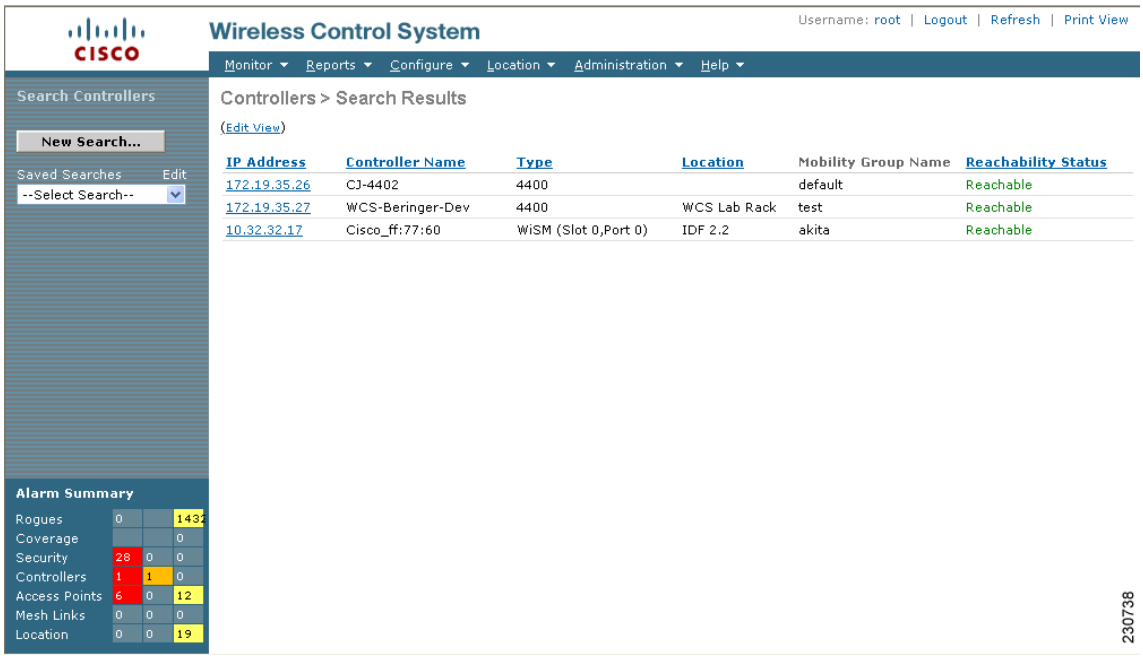
- The serial number (SN)
- The entity name
- The product description

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.

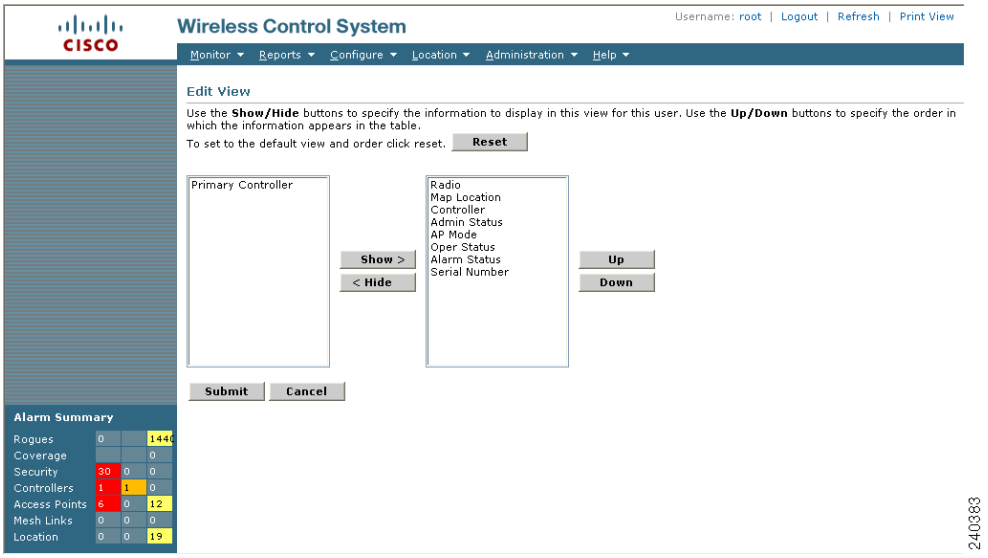
Step 1 Click **Monitor > Controllers**. The Controller > Search Results window displays (see Figure 6-29).

Figure 6-29 Controllers > Search Results



Step 2 (optional) If you want to change how the controller search results are displayed, click **Edit View**. The Edit View window appears (see Figure 6-30). 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.

Figure 6-30 Edit View Window



Step 3 Click the IP address of the controller (seen in Figure 6-29) whose UDI information you want to retrieve. Data elements of the controller UDI display on this window:

Table 6-16 Controllers Summary

Parameter	Description
General Portion	
IP Address	Local network IP address of the controller management interface.
Name	User-defined name of the controller.
Type	The type of controller. **Note** For WiSM, the slot and port numbers are also given.
UP Time	Time in days, hours, and minutes since the last reboot.
System Time	Time used by the controller.
Internal Temperature	The current internal temperature of the unit (in Centigrade).
Location	User-defined physical location of the controller.
Contact	The contact person for this controller, their textual identification, and ways to contact them. If no contact information is known, this is an empty string.
Total Client Count	Total number of clients currently associated with the controller.
Current LWAPP Transport Mode	Lightweight Access Point Protocol transport mode. Communications between controllers and access points. Selections are Layer 2 or Layer 3.

Table 6-16 Controllers Summary (continued)

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	
Software Version	The operating system release, version.dot.maintenance number of the code currently running on the controller.
Description	Description of the inventory item.
Model No.	Specifies the machine model as defined by the Vital Product Data.
Serial No.	Unique serial number for this controller.
Burned-in MAC Address	The burned-in MAC address for this controller.
Number of APs supported	The maximum number of access points supported by the controller.
GigE Card Present	Displays the presence or absence of the optional 1000BASE-T/1000BASE-SX GigE card.
Crypto Card One	Displays the presence or absence of an enhanced security module which enables IPSec security and provides enhanced processing power. See Table 6-17 for information on the maximum number of crypto cards that can be installed on a controller. **Note** By default, enhanced security module is not installed on a controller.
Crypto Card Two	Displays the presence or absence of a second enhanced security module.
GIGE Port(s) Status	
Port 1	Up or Down
Port 2	Up or Down
Unique Device Identifier (UDI)	
Name	Product type. Chassis for controller and Cisco AP for access points.
Description	Description of controller and may include number of access points.
Product Id	Orderable product identifier.
Version Id	Version of product identifier.
Serial Number	Unique product serial number.

Table 6-17 Maximum Number of Crypto Cards That Can Be Installed on a Cisco Wireless LAN Controller

Type of Controller	Maximum Number of Crypto Cards
Cisco 2000 Series	None
Cisco 4100 Series	One
Cisco 4400 Series	Two