CHAPTER 6

Monitoring Wireless Devices

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

- Rogue Access Point Location, Tagging, and Containment, page 6-1
- Configuring ACS View Server Credentials, page 6-2
- Receiving Radio Measurements, page 6-2
- Monitoring Mesh Networks Using Maps, page 6-3
- Mesh Statistics for an Access Point, page 6-15
- Viewing the Mesh Network Hierarchy, page 6-19
- Monitoring Channel Width, page 6-23
- Viewing Clients Identified as WGBs, page 6-28
- Retrieving the Unique Device Identifier on Controllers and Access Points, page 6-29
- Coverage Hole, page 6-32
- Viewing DHCP Statistics, page 6-34
- Guest User Monitoring, page 6-36
- RRM Dashboard, page 6-36

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.

Configuring ACS View Server Credentials

In order to facilitate communication between WCS and the ACS View Server and to access the ACS View Server tab, you must add a view server with credentials. Follow these steps to configure the ACS View Server Credentials.

Note WCS only supports ACS View Server 5.1 or above.

Step 1 Choose **Configure > ACS View Server**.

Step 2 Enter the port number of the ACS View Server you are adding. (Some ACS View Servers do not allow you to change the port on which HTTPS runs.)

Step 3 Enter the password that was established on the ACS View Server. Confirm the password.

Step 4 Specify the number of retries that will be attempted.

Step 5 Click **Submit**.

Receiving Radio Measurements

On the client page, 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 Client User Name column.

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

Note Only associated Cisco Compatible Extension clients using version 2.0 or greater have this option.

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.

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.

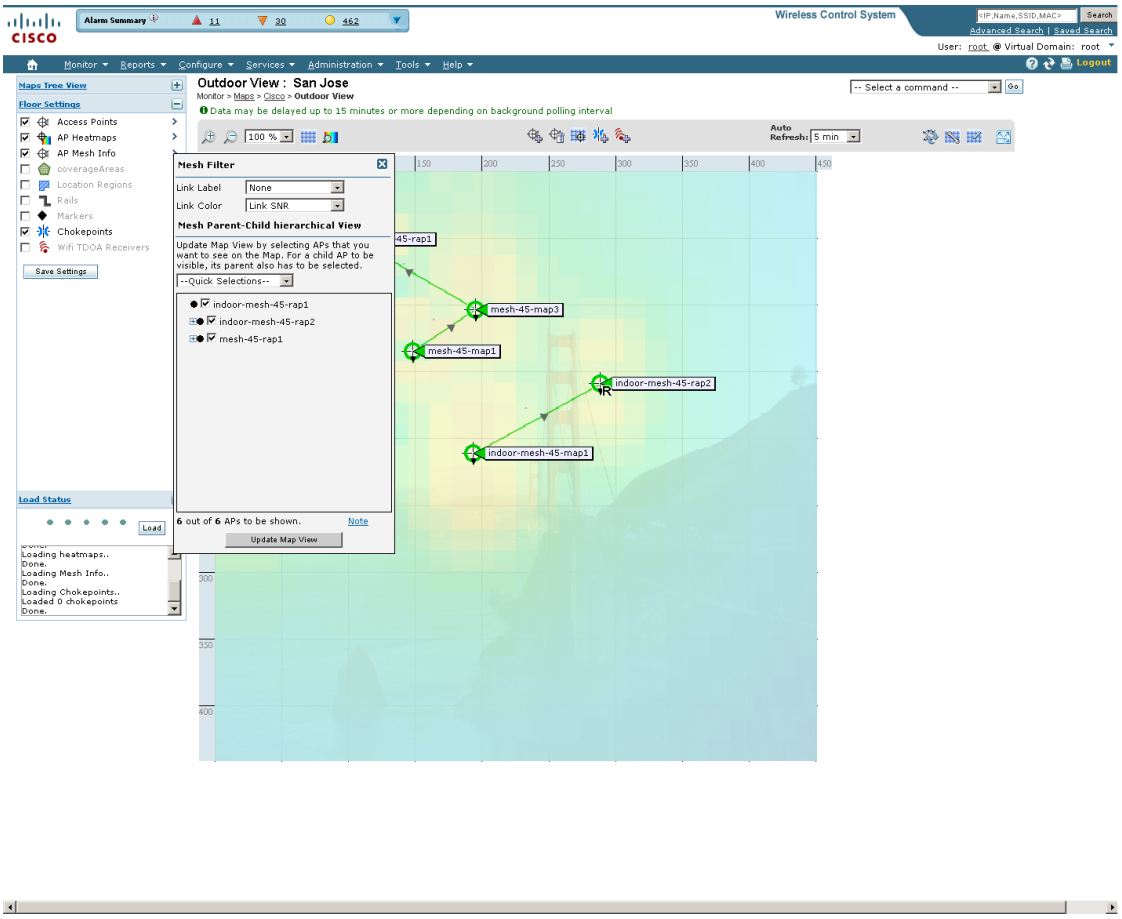
To view details on a specific mesh link between two mesh access points or a mesh access point and a root access point, do the following:

Step 1 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 Click the arrow to the right of AP Mesh Info in the left sidebar menu (see Figure 6-1). A Mesh Filter dialog box appears.

Figure 6-1 Mesh Filter Page



Step 4 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 6-1 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.

The following Bridging Link information displays:

Table 6-1 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.

Step 5 Click either **Link Test**, **Child to Parent or Link Test**, **Parent to Child**. After the link test is complete, a results page appears.

Note A link test runs for 30 seconds.

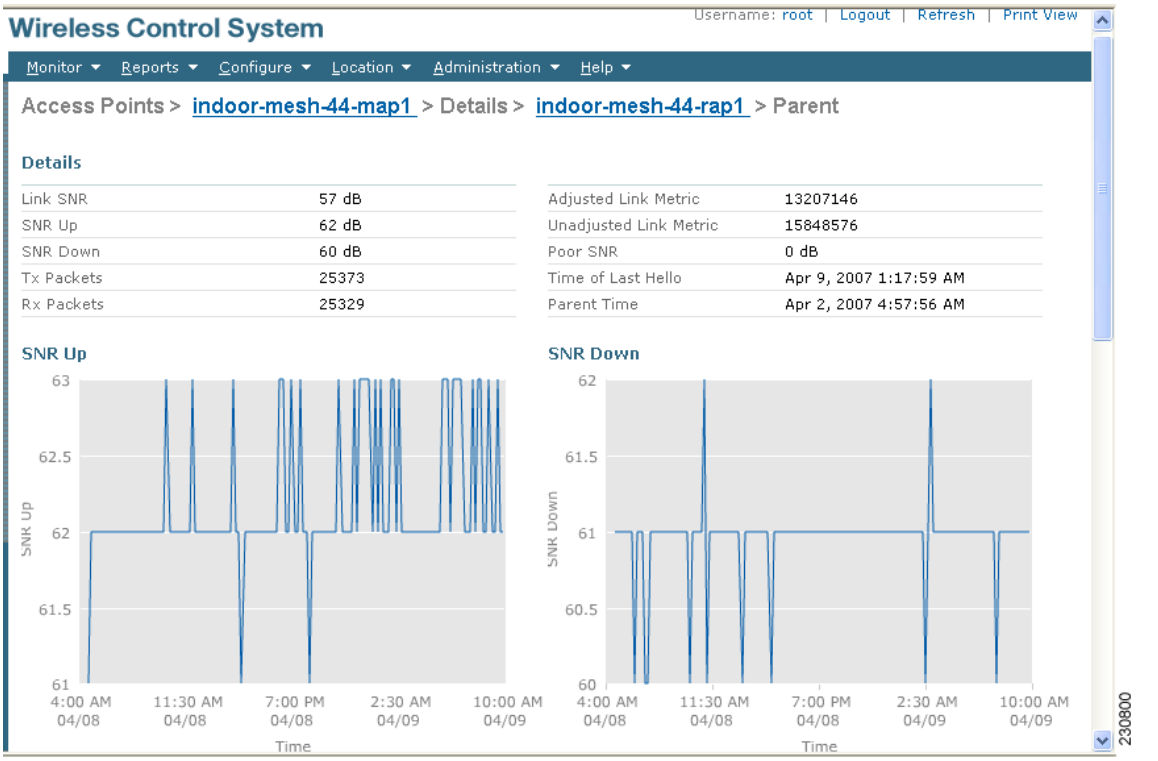
Note You cannot run link tests for both links (child-to-parent and parent-to-child) at the same time.

Step 6 To view a graphical representation of SNR statistics over a period of time, click the arrow on the link. A page with multiple SNR graphs appears (see Figure 6-2).

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 6-2 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 16-26.

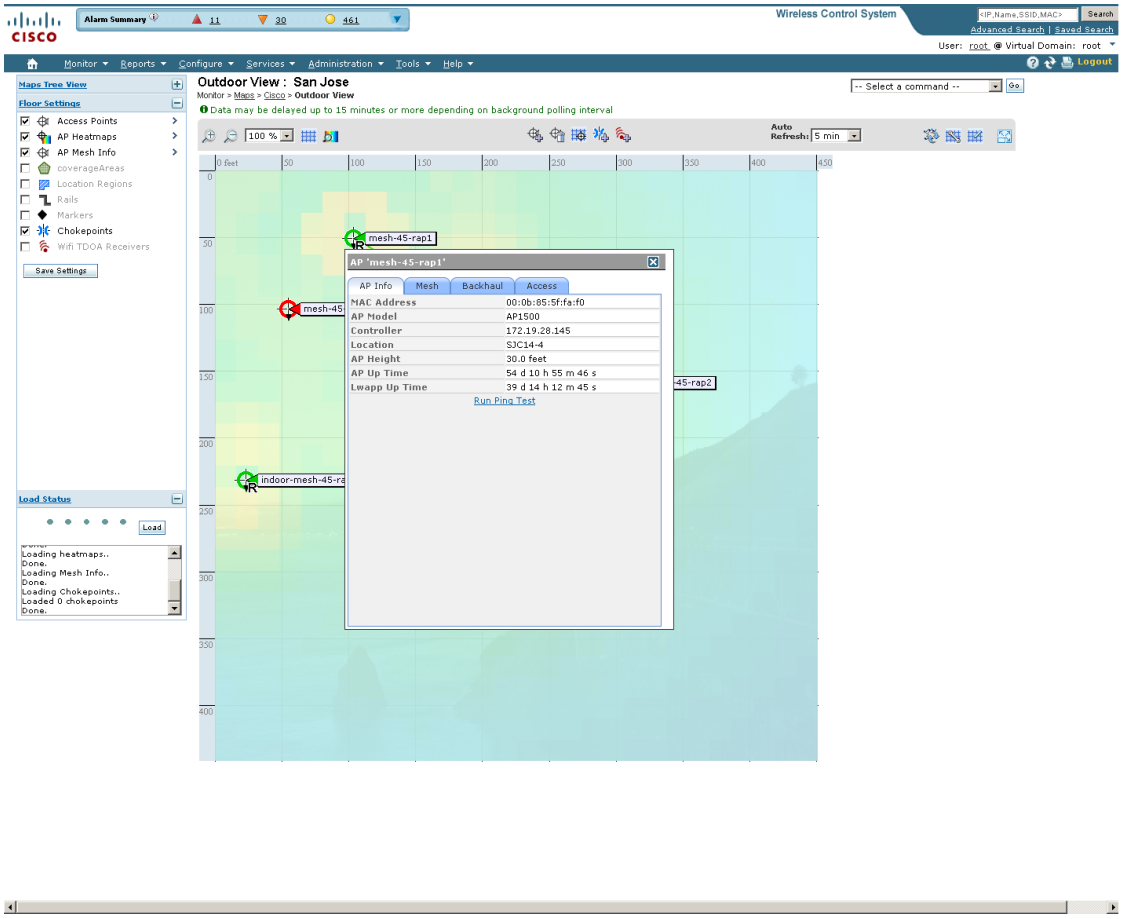
To view summary and detailed configuration information for a mesh access point from a mesh network map, do the following:

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 dialog box page with configuration information for the selected access point appears (see Figure 6-3).

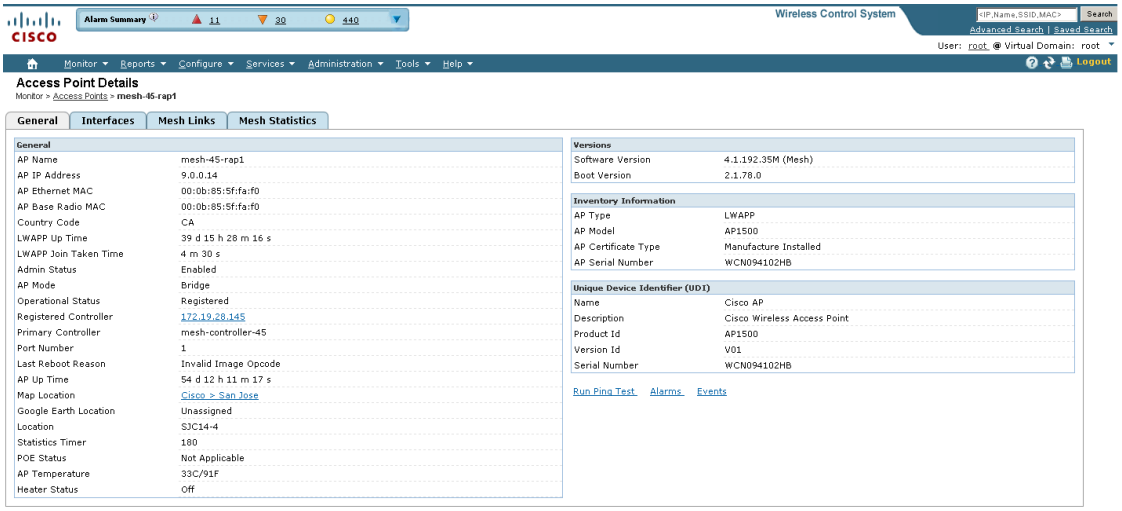
Figure 6-3 Mesh AP Summary Dialog Box



Step 4 To view detailed configuration information for an access point, double-click the access point appearing on the map. The configuration details for the access point appears (see Figure 6-4).

Note For more details on the View Mesh Neighbors link in the access point dialog box (see Figure 6-3), see the "Monitoring Mesh Access Point Neighbors Using Maps" section on page 6-8. 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 6-4 Mesh AP Detail Page



251691

Step 5 In the Access Point configuration page, 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 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 page.

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 6-15.

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:

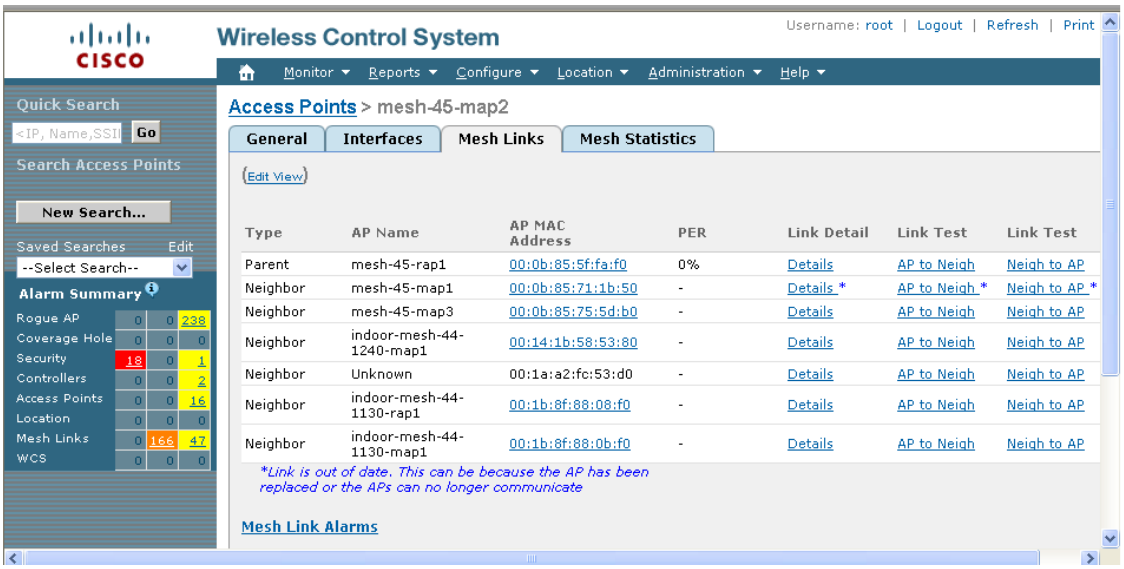
Step 1 Choose **Monitor > Maps**.

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.

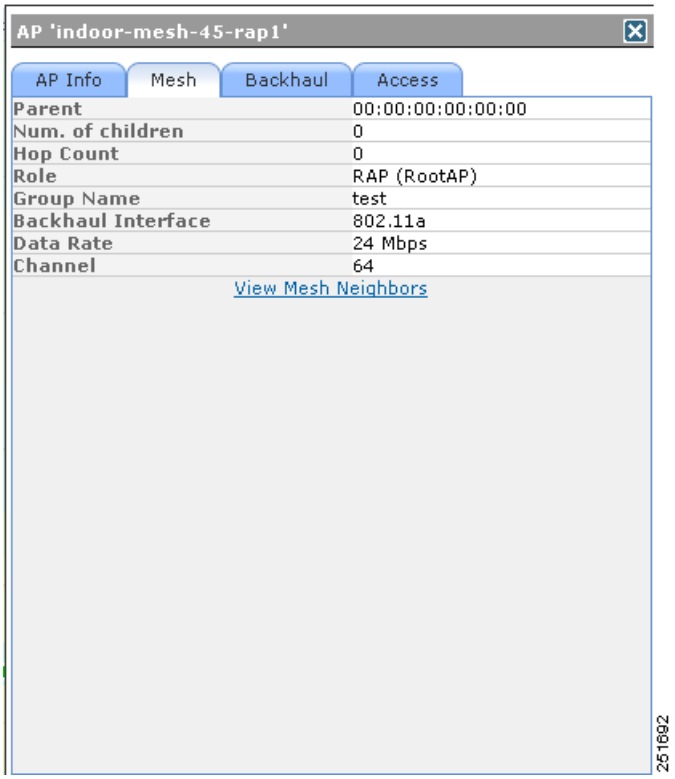
Step 4 Click the **Mesh Links** tab (see Figure 6-5).

Figure 6-5 Access Points > Mesh Links Page



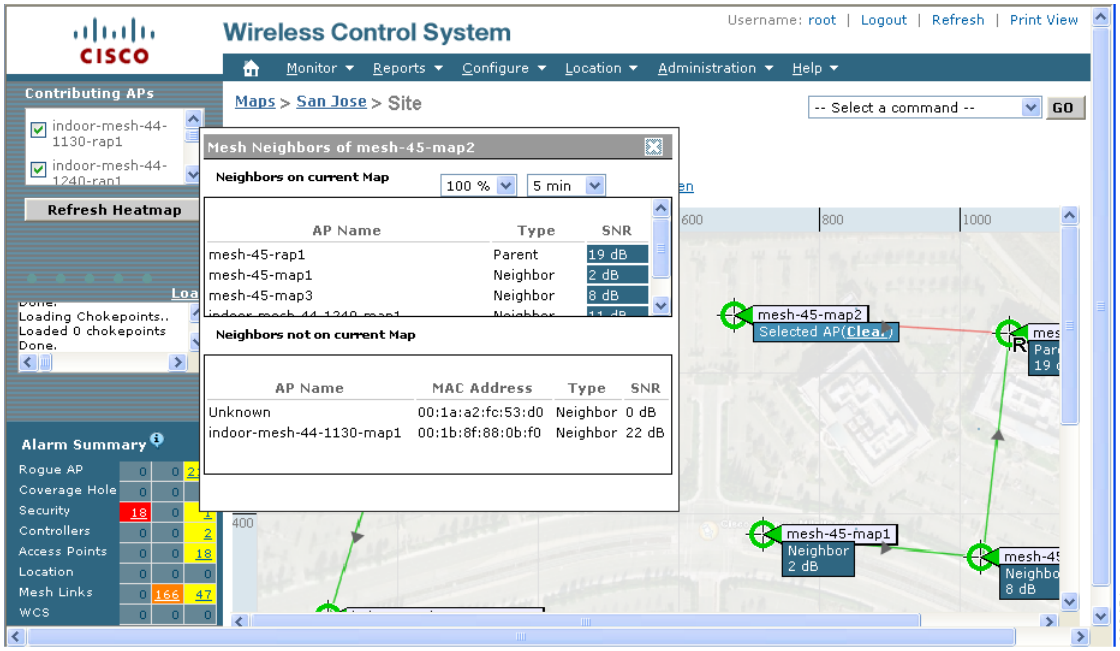
Note You can also view mesh link details for neighbors of a selected access point by clicking on the **View Mesh Neighbors** link from the Mesh tab of the access point configuration summary page, which displays when you mouse over an access point on a map (see Figure 6-6).

Figure 6-6 Access Point Configuration Summary Dialog Box



Note Signal-to-noise (SNR) appears on the View Mesh Neighbors page (see Figure 6-7).

Figure 6-7 View Mesh Neighbors Dialog Box



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 lists at the top of the mesh neighbors page 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 access 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 page for mesh access points.

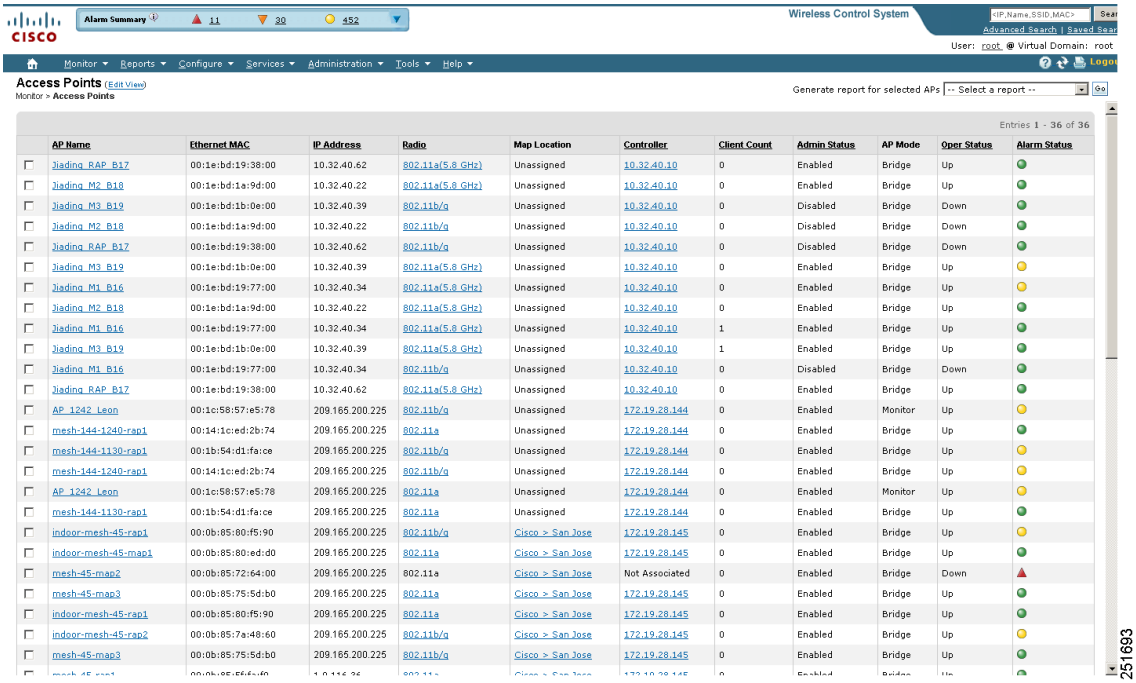
To view the mesh health details for a specific mesh access point, follow these steps.

Step 1 Choose **Monitor > Access Points**. A listing of radios belonging to access points appears (see Figure 6-8).

Note The radio status (not an access point status) is displayed when you choose Monitor > Access Points. The given status is updated frequently from traps and wireless status polling and takes several minutes to reflect actual radio status. The overall status of an access point can be found by viewing the access point on a map.

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 Type, AP Mode, Radio Type, and 802.11n Support.

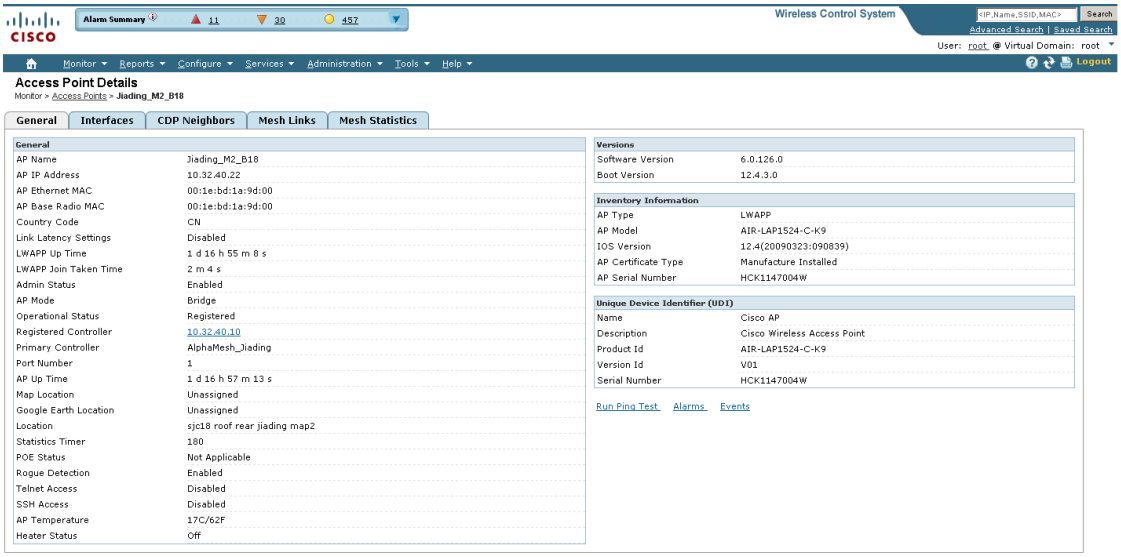
Figure 6-8 Monitor > Access Points



Step 2 Click the AP Name link to display details for that mesh access point. The General tab for that mesh access point appears (see Figure 6-9).

Note You can also access the General tab for a mesh access point from a Cisco WCS map page. To display the page, double-click the mesh access point label. A tabbed page appears and displays the General tab for the selected access point.

Figure 6-9 AP Name > General Properties Tab



251694

To add, remove, or reorder columns in the table, click the Edit View link In the Monitor > Access Points page. Table 6-2 displays optional access point parameters available from the Edit View page.

Table 6-2 Monitor Access Points Additional Search Results Parameters

Column	Options
AP Model	Indicates the model of the access point.
AP Type	Indicates the type of access point (unified or autonomous).
Antenna Azim. Angle	Indicates the horizontal angle of the antenna.
Antenna Diversity	Indicates if antenna diversity is enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports in order to choose the preferred antenna.
Antenna Elev. Angle	Indicates the elevation angle of the antenna.
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.
Antenna Mode	Indicates the antenna mode such as omni, directional, or non-applicable.
Antenna Name	Indicates the antenna name or type.
Antenna Type	Indicates whether the antenna is internal or external.

Table 6-2 Monitor Access Points Additional Search Results Parameters (continued)

Column	Options
Audit Status	Indicates one of the following audit statuses: • Mismatch—Config differences were found between WCS and controller during the last audit. • Identical—No config differences were found during the last audit. • Not Available—Audit status is unavailable.
Base Radio MAC	Indicates the radio's MAC address.
Bridge Group Name	Indicates the name of the bridge group used to group the access points, if applicable.
CDP Neighbors	Indicates all directly connected Cisco devices.
Channel Control	Indicates whether the channel control is automatic or custom.
Channel Number	Indicates the channel on which the Cisco radio is broadcasting.
Controller Port	Indicates the number of controller ports.
Google Earth Location	Indicates whether a Google Earth location is assigned.
Location	The physical location of the access point.
Node Hops	Indicates the number of hops between access point.
OfficeExtend AP	Specifies if OfficeExtend AP is enabled or disabled. If it is disabled, the access point is remotely deployed, which increases the security risk.
POE Status	Indicates the Power-over-Ethernet status of the access point. The possible values include: • Low—The access point draws low power from the Ethernet. • Lower than 15.4 volts—The access point draws lower than 15.4 volts from the Ethernet. • Lower than 16.8 volts—The access point draws lower than 16.8 volts from the Ethernet. • Normal—The power is high enough for the operation of the access point. • Not Applicable—The power source is not from the Ethernet.
Primary Controller	Indicates the name of the primary controller for this access point.
Reg. Domain Supported	Indicates whether or not the regulatory domain is supported.
Serial Number	Indicates the access point's serial number.
Slot	Indicates the slot number.
Tx Power Control	Indicates whether the transmission power control is automatic or custom.
Tx Power Level	Indicates the transmission power level.
Up Time	Indicates how long the access point has been up in days, hours, minutes, and seconds.

Table 6-2 Monitor Access Points Additional Search Results Parameters (continued)

Column	Options
WLAN Override Names	Indicates the WLAN override profile names.
WLAN Override	Indicates whether WLAN Override is enabled or disabled. Each access point is limited to sixteen WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.

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 Choose **Monitor > Access Points**. A listing of radios belonging to access points appears (see Figure 6-8).

Note The radio status (not an access point status) is displayed when you choose Monitor > Access Points. The given status is updated frequently from traps and wireless status polling and takes several minutes to reflect actual radio status. The overall status of an access point can be found by viewing the access point on a map.

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.

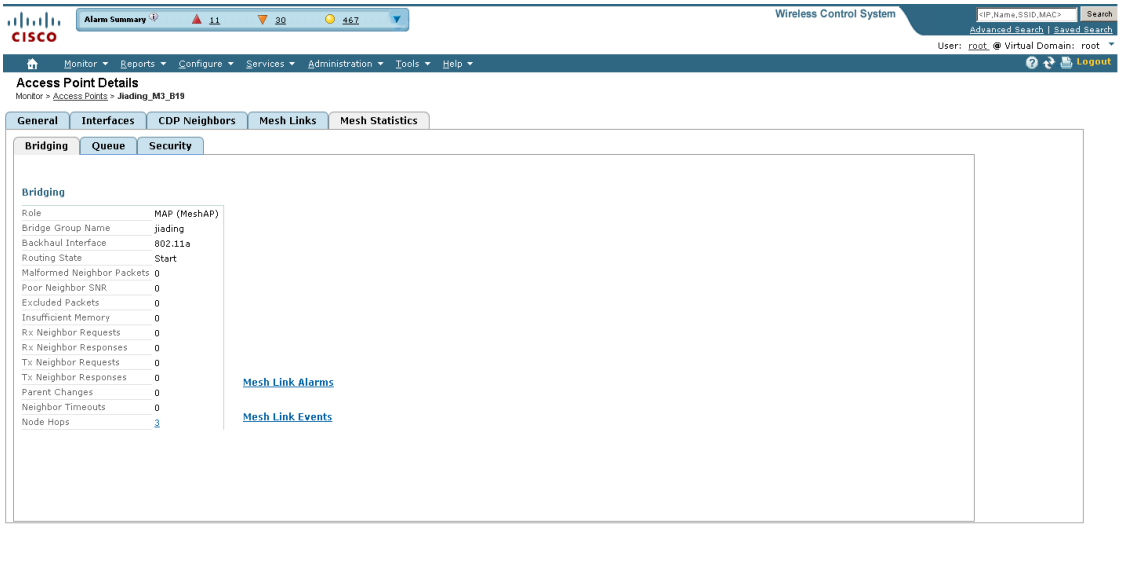
A tabbed page appears and displays the General Properties page for the selected access point.

Step 3 Click the **Mesh Statistics** tab (see Figure 6-10). A three-tabbed Mesh Statistics page 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 page for a mesh access point from a Cisco WCS map. To display the page, double-click the mesh access point label.

Figure 6-10 Monitor > Access Points > AP Name > Mesh Statistics



Summaries of the Bridging, Queue and Security Statistics and their definitions are provided in Table 6-3, Table 6-4 and Table 6-5 respectively.

Table 6-3 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	The name of the bridge group to which the MAP or RAP is a member. Assigning membership in a bridge group name is recommended. If one is not assigned, a MAP is by default assigned to a default bridge group name.
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.

Table 6-3 Bridging Mesh Statistics (continued)

Parameter	Description
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 6-4 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.

Table 6-4 Queue Mesh Statistics (continued)

Parameter	Description
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 6-5 Security Mesh Statistics

Parameter	Description
Packets Transmitted	Summarizes the total number of packets transmitted during security negotiations by the selected mesh access point.
Packets Received	Summarizes the total number of packets received during security negotiations by the selected mesh access point.
Association Request Failures	Summarizes the total number of association request failures 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.
Association Request Success	Summaries the total number of successful association requests 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 Timeouts	Summarizes the total number of authentication request timeouts 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.
Reassociation Request Failures	Summarizes the total number of failed 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.

Table 6-5 Security Mesh Statistics (continued)

Parameter	Description
Reassociation Request Success	Summarizes the total number of successful reassociation requests 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 Timeouts	Summarizes the total number of reauthentication request timeouts that occurred 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.
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.
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.
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.
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.

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 Choose **Monitor > Maps**.

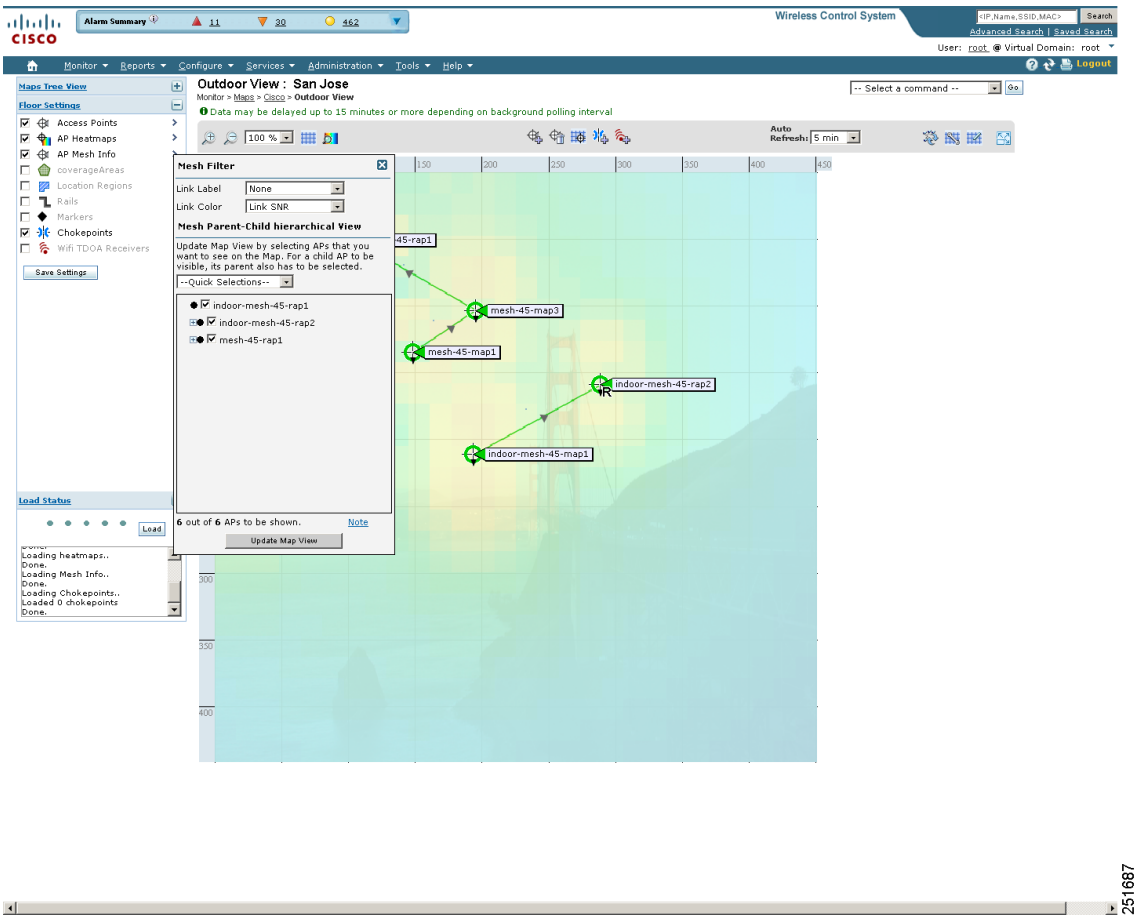
Step 2 Select the map you want to display.

Step 3 Select the **AP Mesh Info** check box in the left sidebar menu 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 4 Click the **AP Mesh Info** arrow to display the mesh parent-child hierarchy (see Figure 6-11).

Figure 6-11 Mesh Parent-Child hierarchical View



Step 5 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 6-11, the access point, *indoor-mesh-45-rap2*, has only one child, *indoor-mesh-44-map2*.

Step 6 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 6-6 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 6-6 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 page, 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 list. 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 list 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 6-7 defines the different link colors.

Table 6-7 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 6-12). 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 list.

b. Select the appropriate option from the menu. A description of the options is provided in Table 6-8.

Table 6-8 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.

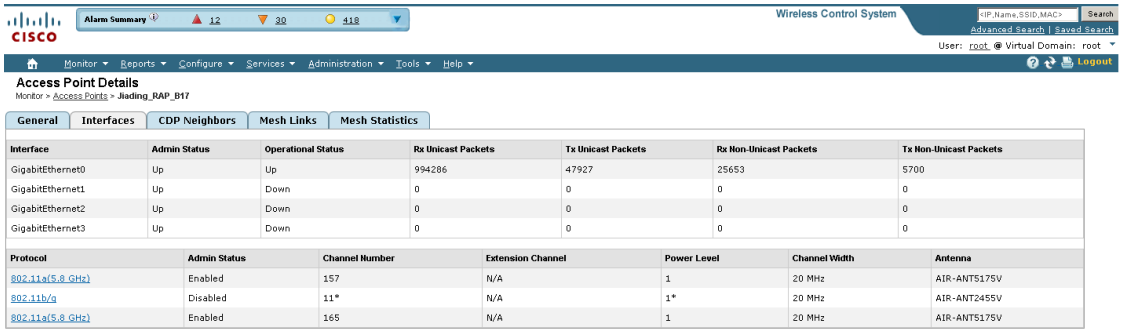
c. Click **Update Map View** to refresh the screen and redisplay the map view with the selected options.

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

Note You can also select or unselect 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.

Note If you want to have the MAC address appear with the client logo in the Monitor > Maps page, follow these steps:
a) Go to the Maps Tree View.
b) Click the > beside Clients.
c) Click to unselect the Small Icons check box.

Figure 6-12 Mesh Filter and Hope Count Configuration Page



251697

Monitoring Channel Width

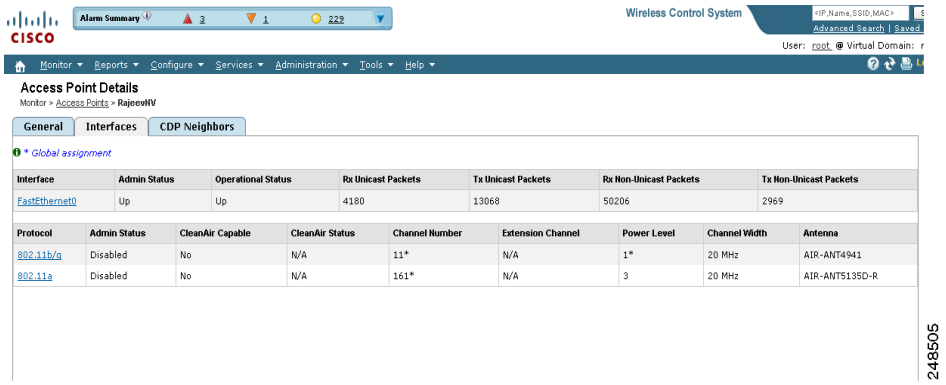
Follow these steps to view the channel width.

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

Note The radio status (not an access point status) is displayed when you choose Monitor > Access Points. The given status is updated frequently from traps and wireless status polling and takes several minutes to reflect actual radio status. The overall status of an access point can be found by viewing the access point on a map. Click an access point in the AP Name column.

Step 2 Click the **Interfaces** tab. The interfaces tab is shown in Figure 6-13.

Figure 6-13 Interfaces Tab



248505

Table 6-9 Interfaces Tab Parameters

Parameter	Description
Interface	
Admin Status	Indicates whether the Ethernet interface is enabled.
Operational Status	Indicates whether the Ethernet interface is operational.
Rx Unicast Packets	Indicates the number of unicast packets received.
Tx Unicast Packets	Indicates the number of unicast packets sent.
Rx Non-Unicast Packets	Indicates the number of non-unicast packets received.
Tx Non-Unicast Packets	Indicates the number of non-unicast packets sent.
Radio Interfaces	
Protocol	802.11a or 802.11b/g.
Admin Status	Indicates whether the access point is enabled or disabled.
Channel Number	Indicates the channel on which the Cisco Radio is broadcasting.
Extension Channel	Indicates the secondary channel on which the Cisco radio is broadcasting.
Power Level	Access Point transmit power level: 1 = Maximum power allowed per Country Code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.
Channel Width	Indicates the channel width for this radio interface. See "Configuring 40-MHz Channel Bonding" section on page 10-41 for more information on configuring channel bandwidth. **Note** Minimum (default) setting is 20 MHz. Maximum setting is the maximum channel width supported by this radio.
Antenna	Identifies the type of antenna.

Step 3 Click an interface name to view its properties (see Figure 6-14).

Figure 6-14 Interface Properties

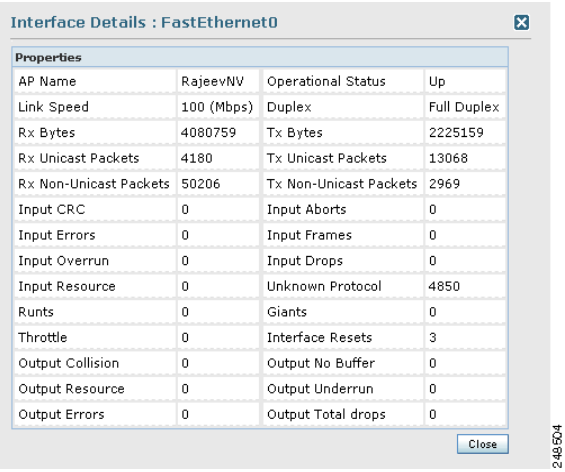


Table 6-10 Interface Properties

Parameters	Description
AP Name	Name of the Access Point.
Link speed	Indicates the speed of the interface in Mbps.
RX Bytes	Indicates the total number of bytes in the error-free packets received on the interface.
RX Unicast Packets	Indicates the total number of unicast packets received on the interface.
RX Non-Unicast Packets	Indicates the total number of non-unicast or mulitcast packets received on the interface.
Input CRC	Indicates the total number of CRC error in packets received on the interface.
Input Errors	Indicates the sum of all errors in the packets while receiving on the interface.
Input Overrun	Indicates the number of times the receiver hardware was incapable of handing received data to a hardware buffer because the input rate exceeded the capability of a receiver to handle the data.
Input Resource	Indicates the total number of resource errors in packets received on the interface.
Runts	Indicates the number of packets that are discarded because they are smaller than the minimum packet size of the medium.
Throttle	Indicates the total number of times the interface advised a sending NIC that it was overwhelmed by packets being sent and to slow the pace of delivery.
Output Collision	Indicates the total number of packet retransmitted due to an Ethernet collision.
Output Resource	Indicates the total number of resource errors in packets transmitted on the interface.

Table 6-10 Interface Properties (continued)

Parameters	Description
Output Errors	Indicates the sum of all errors that prevented the final transmission of packets out of the interface.
Operational Status	Indicates the operational state of the physical Ethernet interface on the AP.
Duplex	Indicates the duplex mode of an interface.
TX Bytes	Indicates the total number of bytes in the error-free packets transmitted on the interface.
TX Unicast Packets	Indicates the total number of unicast packets transmitted on the interface.
TX Non-Unicast Packets	Indicates the total number of non-unicast or mulitcast packets transmitted on the interface.
Input Aborts	Indicates the total number of packet aborted while receiving on the interface.
Input Frames	Indicates the total number of packet received incorrectly having a CRC error and a non-integer number of octets on the interface.
Input Drops	Indicates the total number of packets dropped while receiving on the interface because the queue was full.
Unknown Protocol	Indicates the total number of packet discarded on the interface due to an unknown protocol.
Giants	Indicates the number of packets that are discarded because they exceed the medium's maximum packet size.
Interface Resets	Indicates the number of times that an interface has been completely reset.
Output No Buffer	Indicates the total number of packets discarded because there was no buffer space.
Output Underrun	Indicates the number of times the transmitter has been running faster than the router can handle.
Output Total Drops	Indicates the total number of packets dropped while transmitting from the interface because the queue was full.

Viewing Google Earth Maps

Follow these steps to view Google Earth maps. See Chapter 21, "Google Earth Maps," for further information.

Step 1 Log in to WCS.

Step 2 Choose **Monitor > Google Earth Maps**. The Google Earth Maps page displays all folders and the number of access points included within each folder.

Step 3 Click **Launch** for the map you want to view. Google Earth opens in a separate page and displays the location and its access points.

Note To use this feature, you must have Google Earth installed on your computer and configured to auto-launch when data is sent from the server. You can download Google Earth from Google's website.

To view details for a Google Earth Map folder, follow these steps:

Step 1 In the Google Earth Map page, click the folder name to open the details page for this folder. The Google Earth Details page provide the access point names and MAC or IP addresses.

Note To delete an access point, select the applicable check box, and click **Delete**.
To delete the entire folder, select the check box next to Folder Name, and click **Delete**. Deleting a folder also deletes all subfolders and access points inside the folder.

Step 2 Click **Cancel** to close the details page.

Google Earth Settings

Access point related settings can be defined from the Google Earth Settings page. To configure access point settings for the Google Earth Maps feature, follow these steps:

Step 1 Choose **Monitor > Google Earth Maps**.

Step 2 Configure the following parameters:

- Refresh Settings—Choose the **Refresh from Network** check box to enable this on-demand refresh. This option is applied only once and then disabled.

Caution Because this refresh occurs directly from the network, the length of time it takes to collect data depends on the number of access points.

- Layers—Layer filters for access points, access point heat maps, and access point mesh information can be selected and saved. Select the check box to activate the applicable layer, and click the **>** to open the filter page.

  Note These settings apply when Google Earth sends the request for the next refresh.

  - Access Points—From the Display drop-down list, select to display channels, Tx power level, coverage holes, MAC addresses, names, controller IP, utilization, profiles, or clients.

    Note If the access point layer is not checked, no data is returned and an error message is returned to Google Earth as a Placemark without an icon.

- AP Heatmap—From the Protocol drop-down list, choose **802.11a/n**, **802.11b/g/n**, **802.11a/n & 802.11b/g/n**, or **None**. Choose the cutoff from the RSSI Cutoff drop-down list (- 60 to - 90 dBm).

Note If both 802.11a/n and 802.11b/g/n protocols are chosen, the heat maps are generated for both and overlaid on top of each other. The order cannot be defined. To prevent this overlay, you must turn off individual overlay in Google Earth or change it in the Google Earth Settings on WCS.

- AP Mesh Info—Choose **Link SNR**, **Packet Error Rate**, or **none** from the Link Label drop-down list. Choose **Link SNR** or **Packet Error Rate** from the Link Color drop-down list.

Note When the AP Mesh Info check box is chosen, Mesh Links are also automatically shown.

Step 3 Click **Save** to confirm these changes or **Cancel** to close the page without saving the changes.

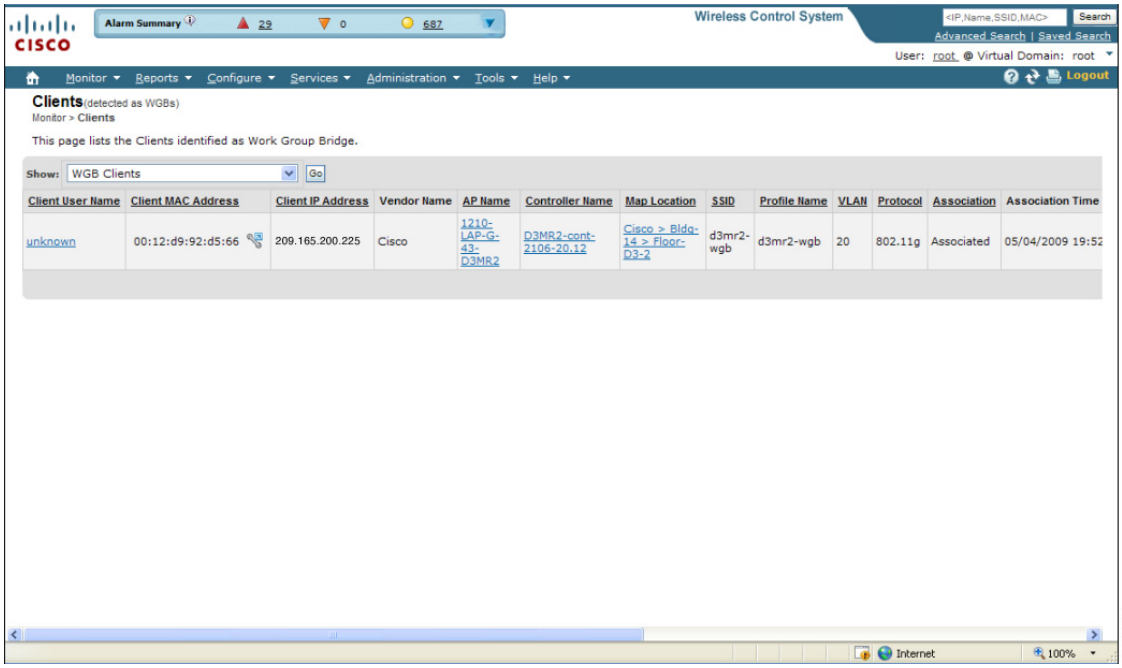
Viewing Clients Identified as WGBs

If an access point is bridge capable, and the AP mode was set to Bridge, you can view clients identified as WGBs. WGB clients bridge wireless to wired. Any Cisco 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. To see a list of all clients identified as a workgroup bridges, follow these steps:

Step 1 Choose **Monitor > Clients**.

Step 2 At the Show drop-down list, choose **WGB Clients**. The Clients (detected as WGBs) page appears (see Figure 6-15).

Figure 6-15 Monitor > WGBs



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:

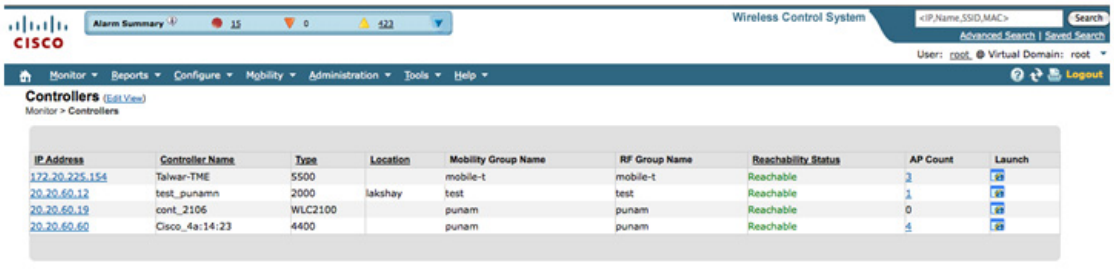
- The orderable product identifier (PID)
- The version of the product identifier (VID)
- The serial number (SN)
- The entity name
- The product description

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.

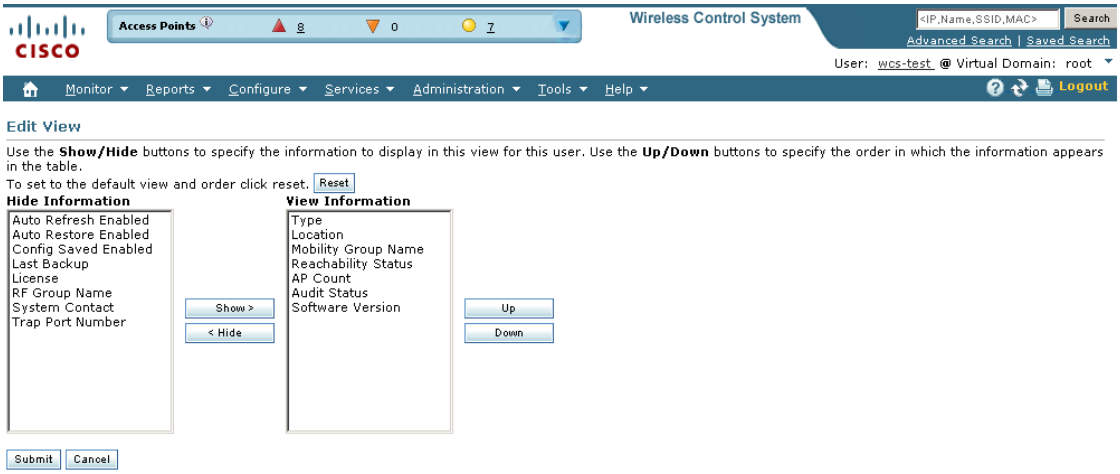
Step 1 Click **Monitor > Controllers**. The Monitor > Controllers page displays (see Figure 6-16).

Figure 6-16 Monitor > Controllers Page



Step 2 (Optional) If you want to change how the controller search results are displayed, click **Edit View**. The Edit View page appears (see Figure 6-17). In the left-hand page, highlight the areas you want to view and click **Show** to move them to the right-hand page. You can then highlight the areas in the right-hand menu and click **Up** or **Down** to rearrange the order.

Figure 6-17 Edit View Page



Step 3 Click the IP address of the controller (seen in Figure 6-16) whose UDI information you want to retrieve. Data elements of the controller UDI display. These elements are described in Table 6-11 and Table 6-12:

Table 6-11 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.

Table 6-11 Controllers Summary (continued)

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.
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.
Emergency Image Version	
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.
Gig Ethernet/Fiber Card	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 6-12 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.

Table 6-11 Controllers Summary (continued)

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 6-12 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

Coverage Hole

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 the WCS, enabling the IT manager to fill holes based on user demand.

WCS is informed about the reliability-detected coverage holes by the controllers. WCS alerts the user about these coverage holes. For more information on finding coverage holes, refer to Cisco Context-Aware Services documentation at this location:

http://www.cisco.com/en/US/docs/wireless/mse/3350/5.2/CAS/configuration/guide/msecg_ch7_CAS.html

Coverage holes are displayed as alarms. Pre-coverage holes are displayed as events.

Monitoring Pre-Coverage Holes

While coverage holes are displayed as alarms, pre-coverage holes are displayed as events.

Follow these steps to view pre-coverage hole events.

Step 1 Choose **Monitor > Events** to display all current events.

Step 2 To view pre-coverage hole events only, click the **Advanced Search** link in the upper right.

Step 3 In the New Search page, change the Search Category drop-down to **Events**.

Step 4 From the Event Category drop-down list, choose **Pre Coverage Hole**, and click **Go**.

The Pre-Coverage Hole Events page provides the information described in the following table:

Table 6-13 Pre-Coverage Hole Parameters

Parameter	Description
Severity	Pre-coverage hole events are always considered informational (Info).
Client MAC Address	MAC address of the client affected by the pre-coverage hole.
AP MAC Address	MAC address of the applicable access point.
AP Name	The name of the applicable access point.
Radio Type	The radio type (802.11b/g or 802.11a) of the applicable access point.
Power Level	Access point transmit power level: 1 = Maximum power allowed per country code setting, 2 = 50% power, 3 = 25% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.
Client Type	Client type can be any of the following: laptop(0) pc(1) pda(2) dot11mobilephone(3) dualmodephone(4) wgb(5) scanner(6) tabletpc(7) printer(8) projector(9) videoconfsystem(10) camera(11) gamingsystem(12) dot11deskphone(13) cashregister(14) radiotag(15) rfidsensor(16) server(17)
WLAN Coverage Hole Status	Determines if the current coverage hole state is enabled or disabled.
WLAN	The name for this WLAN.
Date/Time	The date and time the event occurred. Click the title to toggle between ascending and descending order.

Step 5 Choose a Client MAC Address to view pre-coverage hole details

- General—Provides the following information:

  - Client MAC Address
  - AP MAC Address
  - AP Name
  - Radio Type
  - Power Level
  - Client Type
  - Category
  - Created
  - Generated By
  - Device AP Address
  - Severity
- Neighbor AP's—Indicates the MAC addresses of nearby access points, their RSSI values, and their radio types.
- Message—Describes what device reported the pre-coverage hole and on which controller it was detected.
- Help—Provides additional information, if available, for handling the event.

Viewing DHCP Statistics

WCS provides DHCP server statistics for version 5.0.6.0 controllers or later. These statistics include information on the packets sent and received, DHCP server response information, and last request timestamp.

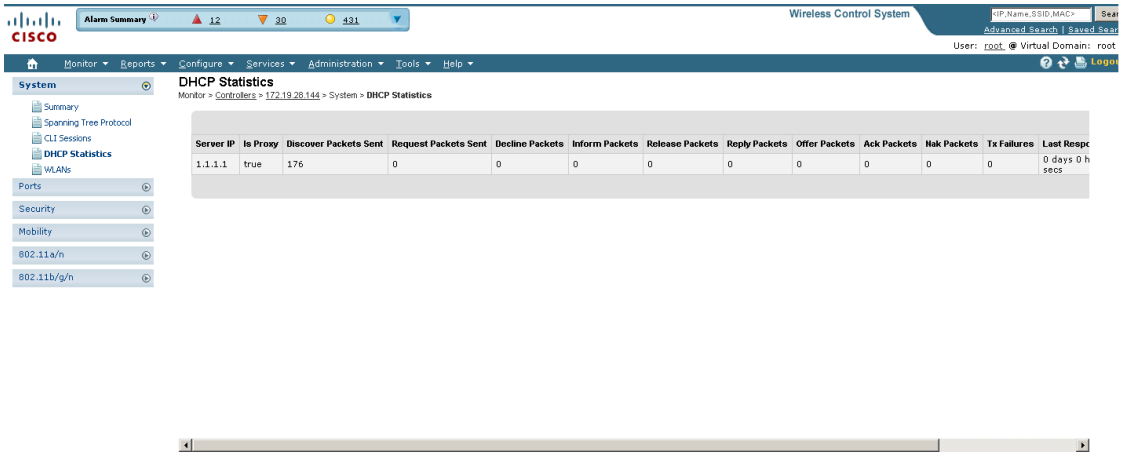
Follow these steps to view DHCP statistics.

Step 1 Choose **Monitor > Controllers**.

Step 2 Click one of the IP addresses in the IP Address column.

Step 3 From the left sidebar menu, choose **System > DHCP Statistics**. The DHCP Statistics page appears (see Figure 6-18).

Figure 6-18 DHCP Statistics Page



251700

The DHCP Statistics screen provides the following information:

Table 6-14 DHCP Statistics

Parameter	Description
Server IP	Identifies the IP address of the server.
Is Proxy	Identifies whether or not this server is proxy.
Discover Packets Sent	Identifies the total number of packets sent with the intent to locate available servers.
Request Packets Sent	Identifies the total number of packets sent from the client requesting parameters from the server or confirming the correctness of an address.
Decline Packets	Identifies the number of packets indicating that the network address is already in use.
Inform Packets	Identifies the number of client requests to the DHCP server for local configuration parameters because the client already has an externally configured network address.
Release Packets	Identifies the number of packets that release the network address and cancel the remaining lease.
Reply Packets	Identifies the number of reply packets.
Offer Packets	Identifies the number of packets that respond to the discover packets with an offer of configuration parameters.
Ack Packets	Identifies the number of packets that acknowledge successful transmission.
Nak Packets	Identifies the number of packets that indicate that the transmission occurred with errors.
Tx Failures	Identifies the number of transfer failures that occurred.

Table 6-14 DHCP Statistics

Parameter	Description
Last Response Received	Provides a timestamp of the last response received.
Last Request Sent	Provides a timestamp of the last request sent.

Guest User Monitoring

WCS provides monitoring and reporting capabilities in regards to guest user accounts. See the "Guest Reports" section on page 17-62 for a description of the reporting capabilities. The guest user components on the WCS home page provide a summary of guest users' deployment and network use. Guest users can also be monitored from the Monitor Controllers > Guest Users page.

The Monitor > Controllers > Guest Users page provides a list of all guest user accounts currently present on the controller. Follow these steps to monitor guest users.

Step 1 Choose **Monitor > Controllers** to access this page.

Step 2 Choose the IP address of the applicable controller.

Step 3 Click **Guest Users** located under Security on the left sidebar menu. The Guest User(s) page appears.

The following information displays for guest users currently present on the controller:

- Guest Username
- Profile—Indicates the profile to which the guest user is connected.
- Lifetime—Indicates the length of time that the guest user's account is active. Length of time displays in days, hours, and minutes or as Never Expires.
- Start Time—Indicates when the guest user's account was activated.
- Remaining Lifetime—Indicates the remaining time for the guest user's account.
- Role—Indicates the designated user role.
- First Logged in at—Indicates the date and time of the user's first login.
- Number of logins—Indicates the total number of logins for this guest user.
- Description—User-defined description of the guest user account for identification purposes.

RRM Dashboard

RRM automatically detects and configures new controllers and lightweight access points as they are added to the network. It then automatically adjusts associated and nearby lightweight access points to optimize coverage and capacity.

Lightweight access points can simultaneously scan all valid 802.11a/b/g channels for the country of operation as well as for channels available in other locations. The access points go "off-channel" for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

Note In the presences of voice traffic (in the last 100 ms), the access points defer off-channel measurements and do not change channels.

Each access point spends only 0.2 percent of its time off-channel. This activity is distributed across all access points so that adjacent access points are not scanning at the same time, which could adversely affect wireless LAN performance. In this way, administrators gain the perspective of every access point, thereby increasing network visibility.

Prior to WCS software release 5.1, WCS would receive traps whenever a change in the transmit power of the access point or channel occurred. These trap events or similar events such as RF regrouping were logged into WCS events as informational and were maintained by the event dispatcher. The reason for the transmit power or channel changes (such as signals from neighboring access points, interference, noise, load balancing, and so on) were not evident. You could not view these events and statistics to then perform troubleshooting practices.

A snapshot of the Radio Resource Management (RRM) statistics (delivered in 5.1) helps identify trouble spots and provides possible reasons for channel or power level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on grouping the events together (access point performance, configuration mismatch between controllers in the same RF group, coverage holes that were detected by access points based on threshold, coverage holes that were detected by controllers, ratios of access points operating at maximum power, and so on).

Note The RRM dashboard information is only available for lightweight access points.

Channel Change Notifications

Two adjacent access points on the same channel can cause either signal contention or signal collision. In the case of a collision, data is simply not received by the access point. This functionality can become a problem, for example, when someone reading e-mail in a cafe affects the performance of the access point in a neighboring business. Even though these are completely separate networks, someone sending traffic to the cafe on channel 1 can disrupt communication in an enterprise using the same channel. Controllers address this problem by dynamically allocating access point channel assignments to avoid conflict and to increase capacity and performance. Channels are “reused” to avoid wasting scarce RF resources. In other words, channel 1 is allocated to a difference access point far from the cafe, which is more effective than not using channel 1 altogether.

The controller’s dynamic channel assignment (DCA) capabilities are also useful in minimizing adjacent channel interference between access points. For example, two overlapping channels in the 802.11b/g band, such as 1 and 2, cannot both simultaneously use 11/54 Mb/s. By effectively reassigning channels, the controller keeps adjacent channels separated, thereby avoiding this problem.

Notifications are sent to the WCS RRM dashboard when a channel change occurs. Channel changes depend on the dynamic channel assignment (DCA) configuration where the mode can be set to auto or on demand. When the mode is *auto*, channel assignment is periodically updated for all lightweight access points which permit this operation. When the mode is set to *on demand*, channel assignments are updated based upon request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global default.

In WCS software releases prior to 5.1, only radios using 20-MHz channelization are supported by DCA. In WCS software release 5.1, DCA is extended to support 802.11n 40-MHz channels in the 5-GHz band. 40-MHz channels allow radios to achieve higher instantaneous data rates (potentially 2.25 times higher than 20-MHz channels.) In WCS software release 5.1, you can choose between DCA working at 20 or 40 MHz.

Note Radios using 40-MHz channels in the 2.4-GHz band are not supported by DCA.

When a channel change trap is received and a channel change had occurred earlier, the event is marked as Channel Revised; otherwise, the event is marked as Channel Changed. Each event for channel change can be caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur. For example, suppose a channel change is caused by signal, interference, or noise. When the reason code is received in the notification, the reason code is refactored across the reasons. If three reasons caused the event to occur, the reason code is refactored to 1/3 or 0.33 per reason. If ten channel change events are received with the same reason code, all of the three reasons are equally factored to determine the cause of the channel change.

Transmission Power Change Notifications

The controller dynamically controls access point transmit power based on real0time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the access points' transmit power according to how the access points are seen by their third strongest neighbor.

The transmit power control algorithm reduces or increases an access point's power. However, the coverage hole algorithm can only increase access point power, thereby filling a coverage hole. For example, if a failed access point is detected, the coverage hole algorithm can automatically increase power on surrounding access points to fill the gap created by the loss in coverage.

Notifications are sent to the WCS RRM dashboard when transmission power changes occur. Each event for transmit power changes is caused by multiple reasons. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur.

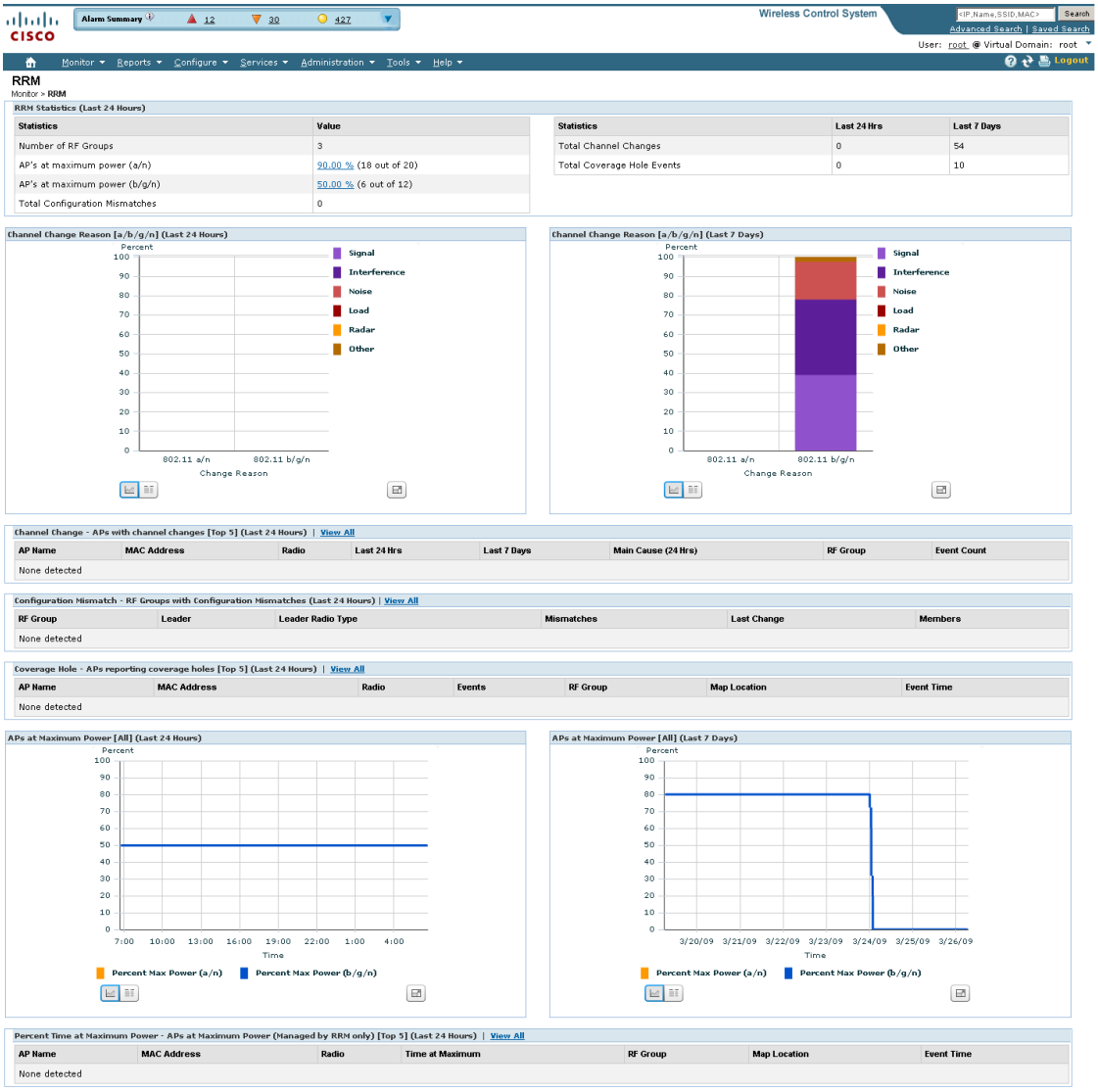
RF Grouping Notifications

When RRM is run on the controller, dynamic grouping is done, and a new group leader is chosen. Dynamic grouping has two modes: on and off. When the grouping is off, no dynamic grouping occurs, and each switch optimizes only its own lightweight access point parameters. When the grouping is on, switches form groups and elect leaders to perform better dynamic parameter optimization. With grouping on, configured intervals (in seconds) represent the period with which the grouping algorithm is run. (Grouping algorithms also run when the group contents change and automatic grouping is enabled.)

Viewing the RRM Dashboard

The RRM dashboard is accessed by choosing Monitor > RRM (see Figure 6-19).

Figure 6-19 RRM Statistics Dashboard



The dashboard is made up of the following parts:

- The RRM Statistics portion shows network-wide statistics
- The Channel Change Reason portion shows why channels changed for all 802.11a/b/g/n radios.
- The Channel Change shows all events complete with causes.
- The Configuration Mismatch portion shows comparisons between the leaders and members.
- The Coverage Hole portion rates how severe the coverage holes are and gives their location.
- The APs at Maximum Power
- The Percent Time at Maximum Power shows what percent of time the access points were at maximum power and gives the location of those access points.

The following statistics are displayed:

- Total Channel Changes—The sum total of channel changes across 802.11a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a screen with details for that access point only appears.
- Total Configuration Mismatches—The total number of configuration mismatches detected over a 24-hour.
- Total Coverage Hole Events—The total number of coverage hole events over a 24-hour and 7-day period.
- Number of RF Groups—The total number of RF groups currently managed by WCS.
- Configuration Mismatch—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- Percent of APs at MAX Power—The percentage of access points with 802.11a/n radios as a total percentage across all access points which are at maximum power. The maximum power levels are preset and are derived with reference to the present maximum power of the access point.

  Note Maximum power is shown in three areas of the RRM dashboard. This maximum power portion shows the current value and is poll driven.

- Channel Change Causes—A graphical bar chart for 802.11a/n radios. The chart is factored based on the reason for channel change. The chart is divided into two parts, each depicting the percentage of weighted reasons causing the event to occur over a 24-hour and 7-day period. Each event for channel change can be caused by multiple reasons, and the weight is equally divided across these reasons. The net reason code is factored and equated to one irrespective of the number of reasons for the event to occur.
- Channel Change APs—Each event for channel change includes the MAC address of the lightweight access point. For each reason code, you are given the most channel changes that occurred for the 802.11a/n access point based on the weighted reason for channel events. This count is split over a 24-hour and 7-day period.
- Coverage Hole Events APs—The top five access points filtered by IF Type 11 a/n which triggered a coverage hole event are displayed.
- Aggregated Percent Max Power APs—A graphical progressive chart of the total percentage of 802.11a/n lightweight access points which are operating at maximum power to accommodate coverage holes and events. The count is split over a 24-hour and 7-day period.

  Note This maximum power portion shows the values from the last 24 hours and is poll driven. The power is polled every 15 minutes or as configured for radio performance.

- Percent Time at Maximum Power—A list of the top five 802.11a/n lightweight access points which have been operating at maximum power.

  Note This maximum power portion shows the value from the last 24 hours and is only event driven.