



Monitoring Wireless Devices

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

- Monitoring Rogue Access Points, Adhocs, and Clients, page 6-1
- Rogue Access Point Location, Tagging, and Containment, page 6-16
- Monitoring Clients, page 6-19
- WLAN Client Troubleshooting, page 6-20
- Enabling Automatic Client Troubleshooting, page 6-35
- Finding Clients, page 6-35
- Receiving Radio Measurements, page 6-39
- Monitoring Mesh Networks Using Maps, page 6-40
- Mesh Statistics for an Access Point, page 6-51
- Viewing the Mesh Network Hierarchy, page 6-56
- Monitoring Channel Width, page 6-59
- Viewing Clients Identified as WGBs, page 6-62
- Running a Link Test, page 6-63
- Retrieving the Unique Device Identifier on Controllers and Access Points, page 6-64
- Coverage Hole, page 6-68
- Viewing DHCP Statistics, page 6-70
- RRM Dashboard, page 6-71

Monitoring Rogue Access Points, Adhocs, and Clients

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.

Interpreting Security Summary Window

You can see a summary of existing events and the security state of the network by choosing **Monitor > Security**. The Security Summary window appears (see Figure 6-1).

Figure 6-1 Security Summary Window

ababa	Wireless Control	Syster	n		Virtual Domain: root			• Username: •	oot Logout Refresh Print View	
CISCO	🖨 Monitor = Br	sports •	configure •	• Mgbilty •	Administration · Icols ·	Help =				
	Security Summary									
	Security									
ique APs	Index : 26.08 Top Se	curity Iss	es View	All Devices						
ue Adhocs	MPP Clie	ant Protecti	on set to Op	stional for						
we Clients	Interfac	e set to ma	nagement	for WLAN. (21)						
nned Clients	- 50 No WLA settable WPA+W	N Key Mani when Auth PA2). (17)	gement me entication P	ethods set(Only fethod is						
	No WLA	N Encryptic	n Methods :	set. (13)						
	None as	WLAN Aut	nentication I	Method. (13)						
	Rogue APs and Adhoc R	Last	24	Total	Adhar Danuar	Last	24	Total		
rm Summary ⁰	No Malicious Rogue APs fo	und	nours	Acuve	No Adhoc Rogues found	nour	nours	Active		
cious AD 0 0 0 erage Hole 0 0 0	Unclassified Rogue APs	Last Hour	24 Hours	Total Active	Friendly Rogue APs	Last Hour	24 Hours	Total Active		
trollers 12 1	Alert	97	489	482	Internal	0	0	2		
Access Points 2 0 2 Location 0 0 4 Math Links 0 0 0 WCS 0 0 0	Threats And Attacks	Last Hour	24 Hours	Total Active	AP Threats/Attacks	Last Hour	24 Hours	Total Active		
	No Attacks Detected				Fake AP Attack	0	0	2		
	NFP Attacks	Last Hour	24 Hours	Total Active	Client Security Events	Last Hour	24 Hour	Total Active		
	No MFP Attacks found				No Client Security Events f	ound				
					Cisco Wired IPS Events	Las	z4 r Hou	Total Active		
					No Cisco Wired IPS Events	found				

The Security Summary window provides information in the following sections:

- Security Index
- Top Security Issues
- Malicious Rogue Access Points
- Adhocs Rogues
- Unclassified Rogue Access Points
- Friendly Rogue Access Points
- Attacks Detected
- Access Point Threats or Attacks
- MFP Attacks
- Client Security Events
- Cisco Wired IPS Events

Security Index

The Security Index gives an indication of the security of the WCS managed network, and it is calculated as part of daily background tasks. It is calculated by assigning weight to the various security configurations and displaying it in visual form. The combined weighting can vary from 0 to 100 where 0 signifies the least secured and 100 is the maximum secured. The weighting comes from the lowest scoring controller and the lowest scoring Location Server/Mobility Service Engine related security configurations that are maintained within WCS itself. The Security Index of the WCS managed network is calculated as the lowest scoring controller plus the lowest scoring Location Service/Mobility Service Engine.

The security thermometer color range is represented as follows:

- Above 80 Green
- Below 80 but greater than 60 Yellow
- Below 60 Red



Guest WLANs are excluded from the WLANs. A WLAN which has web authentication or web passthrough enabled is identified as a guest WLAN.

The security index of the latest release is the benchmark for the required security configurations. For example, if AES encryption was not present in an earlier version of code, the index is reduced by the number associated with the AES encryption security configuration. Likewise, if new security configurations are introduced, the weighting would be altered.



The configurations stored in WCS may not be up-to-date with the ones in the controllers unless the Refresh from Controller command is run from WCS. You can run Security Index calculations from the Configuration Sync task to get the latest configuration data from all the controllers. Refer to the "Configuration Sync" section on page 16-4 for steps on enabling the security index.

Top Security Issues

The View All and Devices links sort relevant columns and show a report of security issues occurring across all controllers. If you click **View All**, the Security Index Detailed Report appears (see Figure 6-2). It displays all security issues found across all controllers, location servers, and mobility service engines. It details problems found in a particular security configuration retrieved from the device. If a particular issue has been acknowledged (just as you would an alarm), it will be ignored the next time the Configuration Sync task runs (provided Security Index Calculation is enabled).

Note

In some cases, when an ACK happens and is ignored in the next iteration, the final security index score may change. There could be multiple reasons for this change:

- The acknowledged issue on the controller is not directly affecting the security index score.

- The acknowledged issue on a WLAN is not directly affecting the security index score. Only the lowest scoring WLAN of the lowest scoring controller affects the security index score, so an issue on any other WLAN would not make the score higher.

- Some cases, like SSH and Telnet being enabled on a controller, are both flagged as issues. However, a Telnet issue has a higher precedence than an SSH issue. For instance, if SSH is acknowledged on a controller with the lowest score, no changes would occur for the security index.

L

The following three different view can be viewed:

- Show Unacknowledged which shows only unacknowledged security issues (the default value). When **View All** is clicked, this view is shown.
- Show Acknowledged shows acknowledged security issues.
- Show All shows all security issues (acknowledged or unacknowledged).

Figure 6-2 Security Index Detailed Report

abab	Wireless C	ontrol	System	Virtual Domain: root	Username: root Logout Refresh Print View	*
CISCO	💼 Mon	itor = <u>B</u> e	ports ▼ <u>C</u> or	figure • Mgbility • Administration • Iools • Help •		
	Security Ind	ex Detail	ed Report		Entries 1 - 50 of 110 He = 1 2 2 > He	60
	C IP	Device	Device	Device Security Issue	Security Solution	Acknowledges
Regue Adhocs	20.20.10.30	Maz_30	Controller	Controller Maz_30 has the Protection Type set to None.	Controller Maz_30 needs to be configured with Protection Type set to MFP.	No
Roque Clients	20.20.10.30	Maz_30	Controller	Controller Maz_30 has no enabled IDS Sensor configured.	Controller Maz_30 needs to be configured with at least one enabled IDS Sensor.	No
Shunned Clients	20.20.10.30	Maz_30	Controller	Controller Maz_30 has SNMP V1 or V2 with default Community.	Controller Maz_30 needs to be configured with SNMP V3 with Auth and Privacy Types and without default user.	No
	20.20.10.30	Maz_30	Controller	Controller Maz_30 has Teinet enabled.	Controller Maz_30 needs to be configured with Telnet disabled.	No
	20.20.10.5	Maz5	Controller	WLAN Id 2 on controller Maz5 has None as the Authentication Method.	WLAN Id 2 on controller Mas5 needs to be configured with WPA+WPA2 as the Authentication Method.	No
	20.20.10.5	Maz5	Controller	WLAN Id 2 on controller Ma25 has none of the Encryption Methods set.	WLAN Id 2 on controller Maz5 needs to be configured with WPA+WPA2 as the Authentication Method with only AES as the Encryption Method.	No
	0 20.20.10.5	Maz5	Controller	WLAN Id 2 on controller Ma25 has none of the Key Management methods set(Only settable when Authentication Method is WPA+WPA2).	WLAN Id 2 on controller Ma25 needs to be configured with at least one Key Management methods like CCKM enabled(Only settable when Authentication Method is WPA+WPA2).	No
	20.20.10.5	Maz5	Controller	WLAN Id 2 on controller Ma25 has MIP Client Protection set to Optional.	WLAN Id 2 on controller MazS needs to be configured with MFP Client Protection set to Required.	No
	20.20.10.5	Maz5	Controller	WLAN Id 2 on controller Ma25 has Interface set to management.	WLAN Id 2 on controller Maz5 needs to be configured with Interface set to neither management or one which is vlan.	No
	20.20.10.5	Maz5	Controller	WLAN Id 1 on controller Ma25 has MFP Client Protection set to Optional.	WLAN Id 1 on controller Ma25 needs to be configured with MFP Client Protection set to Required.	No
	20.20.10.5	Mez5	Controller	WLAN Id 1 on controller Ma25 has Interface set to management.	WLAN Id 1 on controller Maz5 needs to be configured with Interface set to neither management or one which is vlan.	No
	20.20.10.5	Maz5	Controller	WLAN Id 10 on controller Ma25 has MFP Client Protection set to Optional.	WLAN Id 10 on controller MazS needs to be configured with MFP Client Protection set to Required.	No
	20.20.10.5	Maz5	Controller	WLAN Id 10 on controller Ma25 has Interface set to management.	WLAN Id 10 on controller MarS needs to be configured with Interface set to neither management or one which is vlan.	No
Alarm Summary 9	20.20.10.5	Mez5	Controller	WLAN Id 3 on controller Ma25 has MIP Client Protection set to Optional.	WLAN Id 3 on controller Maz5 needs to be configured with MFP Client Protection set to Required.	No
Malicious AP	20.20.10.5	Maz5	Controller	WLAN Id 3 on controller Maz5 has Interface set to management.	WLAN Id 3 on controller Ma25 needs to be configured with Interface set to neither management or one which is vlan.	No
Security 50 g	20.20.10.5	Mez5	Controller	Controller MazS has the Protection Type set to None.	Controller MazS needs to be configured with Protection Type set to MFP.	No
Controllers 12 1	20.20.10.5	Maz5	Controller	Controller MazS has no enabled IDS Sensor configured.	Controller MazS needs to be configured with at least one enabled IDS Sensor.	No
Access Points 2 0 5 Location 0 0 5	□ 20.20.10.5	Maz5	Controller	Controller MazS has SNMP V1 or V2 with default Community.	Controller MarS needs to be configured with SNMP V3 with Auth and Privacy Types and without default user.	No
Wesh Links 0 0 0	20.20.10.5	Mez5	Controller	WLAN Id 5 on controller Ma25 has None as the Authentication Method.	WLAN Id 5 on controller Ma25 needs to be configured with WPA+WPA2 as the Authentication Method.	No

If you click **Devices** from the Security Summary window (Figure 6-1), the Security Index Controller Report appears (see Figure 6-3). This screen shows the security violation report as a summary for each controller. By row, each controller shows the number of security issues that occurred on that controller and provides a link to all security issues.



The security score of the lowest scoring controller is not the same as the security index for WCS. Some score comes from the lowest scoring Location or Mobility Server Engine, and the lowest scoring controller score shown is calibrated to out of 100.

abab	Wireless Control	System	ual Domain: roat	Username: rost Logout Refresh Print View	
CISCO	👌 Monitor = Beports = Configure = Mgbility =		≜dministration + Icols + Help +		
	Security Index Contro	oller Report			

Roque APs	IP Address	Device Name	Security Score	Security Issues Count	
Reason Lillions	20.20.10.5	Maz5	27.18	25	
Kogue Konocs	20.20.11.2	Mazil	30.76	22	
Rogue Clients	20.20.10.205	Maz2112	31.34	42	
Shunned Clients					
Malidous AP 0 0 Coverage Hole 0 0 Controllers 12 0 Controllers 12 0 Locess Points 2 0 Locess Points 0 0	0 0 5 5 5				

Figure 6-3 Security Index Controller Report

If you click the number in the Security Issues Count column, the Security Index Detailed Report appears (see Figure 6-2).

Table 6-1 lists top security issues, provides a description of why the issue occurs, and defines what action should be taken as a solution. Table 6-2 lists top security issues for location and mobility servers, provides a description of why the issue occurs, and defines what action should be taken as a solution.

Controller Security Issue	Why is this an issue?	What is the solution?
Static WEP configured as the authentication method for a WLAN.	Weak authentication method for a WLAN which can be broken by using tools available online if WLAN packets are sniffed.	Use the most secured authentication method — WPA+WPA2.
CKIP configured as the authentication method for a WLAN.	Weak authentication method for a WLAN.	Use the most secured authentication method — WPA+WPA2.
An authentication method as <i>None</i> for a WLAN.	No authentication method is a clear security risk for a WLAN.	Use the most secured authentication method — WPA+WPA2.
CKIP WEP 10/104 bits (with MMH or Key Permutation or both) as one of the encryption methods for a WLAN.	A weak encryption method for a WLAN.	Use the most secured encryption method —AES. AES is only available when WPA+WPA2 is the authentication method.
WEP 40/104/128 bits as one of the encryption methods (802.1X or WEP Authentication Method) for a WLAN.	A weak encryption method for a WLAN.	Use the most secured encryption method —AES. AES is only available when WPA+WPA2 is the authentication method.

Controller Security Issue	Why is this an issue?	What is the solution?
One of the encryption methods for a WLAN is TKIP.	A weak encryption method for a WLAN.	Use the most secured encryption method —AES. AES is only available when WPA+WPA2 is the authentication method.
None of the encryption methods for a WLAN are set.	A clear security risk exists for a WLAN when no encryption method is set.	Use the most secured encyrption method —AES. AES is only available when WPA+WPA2 is the authentication method.
None of the key management methods are set for a WLAN. You can set these methods only when the authentication method is WPA+WPA2.	A key management method enhances the security of keys. Without one, WLAN is less secure.	At least one key management method (such as CCKM enabled) must be enabled to improve the security of the WLAN. This method can be set only when the authentication method is WPA+WPA2.
MFP Client Protection is set to <i>optional</i> for a WLAN.	With the MFP Client Protection set to <i>optional</i> , authenticated clients may not be shielded from spoofed frames.	To shield authenticated clients from spoofed frames, set MFP Client Protection to <i>required</i> for a WLAN.
MFP Client Protection is set to <i>disabled</i> for a WLAN.	With the MFP Client Protection set to <i>disabled</i> , authenticated clients may not be shielded from spoofed frames.	To shield authenticated clients from spoofed frames, set MFP Client Protection to <i>required</i> for a WLAN.
The interface is mapped to <i>management</i> for a WLAN.	As recommended from SAFE, user traffic should be separated from management traffic.	The WLAN needs its interface mapped to a non-managment interface.
Client Exlusion is disabled for a WLAN.	With Client Exlusion policies disabled, an attacker is free to continuously try for access into the WLAN network.	The WLAN needs to have Client Exclusion policy enabled to prevent a single or a set of clients (rogues) from gaining access to the WLAN network.
The Protection Type is set to AP Authentication.	When AP Authentication is set, an access point checks beacon/probe-response frames in neighboring access points to see if they contain an authenticated information element (IE) that matches that of RF groups. Some level of security is introduced, but all management frames are not covered or open to alteration by rogue access points.	The Protection Type set to Management Frame Protection is the most secured option. It includes message integrity check (MIC) into all management frames sent by an access point, and if the management frames are altered, they can be detected by other access points.

Controller Security Issue	Why is this an issue?	What is the solution?
Protection Type is set to <i>none</i> .	No security for 802.11 management messages is passed between the access points and clients.	Protection Type set to Management Frame Protection is the most secured option. It includes message integrity check (MIC) into all management frames sent by an access point, and if the management frames are altered, they can be detected by other access points.
Rogue detection exists only on DCA channels.	Rogue detection done on only a subset of countries or channels is less secure than rogue detection done on all countries or channels.	Rogue detection should be turned on for all countries and channels to improve the chances of discovering rogue access points no matter where they are transmitting.
Detection and reporting of adhoc networks is turned off for rogue policies.	With detection and reporting of adhoc networks turned off, adhoc rogues go undetected.	Adhoc rogues need to be detected; therefore, detection and reporting of adhoc networks needs to be turned on for rogue policies.
The check for all Standard and Custom Signatures is disabled.	If the check for all Standard and Custom Signatures is disabled, various types of attacks from incoming 802.11 packets may go undetected.	The check for all Standard and Custom Signatures needs to be turned on to identify various types of attacks in incoming 802.11 packets.
The Excessive 802.11 Association Failures Client Exclusion Policy is disabled.	Excessive failed association attempts may consume system resources and launch potential denial-of-service attacks to the infrastructure.	Enable Excessive 802.11 Association Failures Client Exclusion Policy to prevent denial-of-service attacks on the infrastructure.
The Excessive 802.11 Authentication Failures Client Exclusion Policy is disabled.	Excessive failed authentication attempts can consume system resources and launch potential denial-of-sevice attacks to the infrastructure.	Enable Excessive 802.11 Authentication Failures Client Exclusion Policy to prevent denial-of-service attacks on the infrastructure.
The Excessive 802.1X Authentication Failures Client Exclusion Policy is disabled.	The excessive 802.1X failed authentication attempts can consume system resources and launch potential denial-of-service attacks to the infrastructure.	Enable the Excessive 802.1X Authentication Failures Client Exclusion Policy to prevent denial-of-service attacks to the infrastructure.
The Excessive 802.11 Web Authentication Failures Client Exclusion Policy is disabled.	If excessive 802.11 web is disabled, web authentication attempts consume system resources and launch potential denial-of-service attacks to the infrastructure.	Enable excessive 802.11 web authentication failures client exclusion policy to prevent denial-of-service attacks to the infrastructure.

Table 6-1 (continued)Top Security Issues

Controller Security Issue	Why is this an issue?	What is the solution?
IP Theft or Reuse Client Exclusion Policy is disabled.	If IP Theft or Reuse Client Exclusion Policy is disabled, an attacker masquerading as another client would not be disallowed.	Enable IP Theft or Reuse Client Exclusion Policy to prevent an attacker from getting into the network as another client.
No enabled IDS sensor is configured.	If no enabled IDS sensor is configured, IP level attacks are not detected.	Configure Enabled IDS Sensors to detect IP level attacks.
SNMP V1 or V2 with a default community is configured.	If SNMP V1 or V2 with default community is configured, the network is open to easy attacks because default communities are well known.	Enable SNMP V3 with Auth and Privacy type and no default user. This is the most secure SNMP connection.
SNMP V1 or V2 with a non-default community is configured.	SNMP V1 or V2 with a non-default community is slightly more secure than a default community but still less secure than SNMP V3.	Enable SNMP V3 with Auth and Privacy type and no default user. This is the most secure SNMP connection.
SNMP V3 with a default user is configured.	Using a default user makes SNMP V3 connections less secure.	Enable SNMP V3 with Auth and Privacy type and no default user. This is the most secure SNMP connection.
SNMP V3 with either Auth or Privacy Type set to <i>None</i> .	SNMP V3 with either Auth or Privacy Type set to none reduces the security of an SNMP V3 connection.	Enable SNMP V3 with Auth and Privacy types and no default user. This is the most secure SNMP connection.
HTTP is enabled (Web Mode is enabled but Secure Web Mode is disabled).	HTTP is less secure than HTTPS.	Enable HTTPS.
Telnet is enabled.	If Telnet is enabled, the controller has the risk of attack.	Disable Telnet to reduce the risk of attack.
SSH is enabled and timeout is set to zero.	If SSH is enabled and timeout is zero, the controller runs the risk of attack.	If SSH is enabled, the timeout must be set to zero to reduce the risk of attack.

Table 6-1 (continued) Top Security Issues

Location Server/Mobility Server Engine Security Issue	Why is this an issue?	What is the solution?
HTTP is enabled.	HTTP is less secure than HTTPS.	Enable HTTPS.
A default password is configured for a location user.	If a default password is configured, the Location Server/Mobility Server Engine is more susceptible to connections from outside the network.	Configure the Location Server/Mobility Server Engine user with a non-default password.

Table 6-2	Top Security Issues for Location and Mobility Servers
-----------	---

Malicious Rogue Access Points

This section provides information on rogue access points that are classified as *Malicious*. Table 6-3 describes the various parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a window with further information appears.

<u>Note</u>

Malicious access points are detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

Parameter	Description	
Alert	Indicates the number of rogues in an alert state.	
	Note An access point is moved to Alert if it is not on the neighbor list or part of the user-configured Friendly AP list.	
Contained	Indicates the number of contained rogues.	
Threat	Indicates the number of threat rogues.	
Contained Pending	Indicates the number of contained rogues pending.	
	Note Contained Pending indicates that the containment action is delayed due to unavailable resources.	

Table 6-3Malicious Rogue AP Details

Adhocs Rogues

This section provides information on rogue adhocs. This section provides information on rogue adhocs. Table 6-4 describes the various parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a window with further information appears.

Parameter	Description
Alert	Indicates the number of rogue adhocs in an alert state.
	Note An access point is moved to Alert if it is not on the neighbor list or part of the user-configured Friendly AP list.
Contained	Indicates the number of contained rogues.
Threat	Indicates the number of threat rogues.
Contained Pending	Indicates the number of contained rogues pending.
	Note Contained pending indicates that the containment action is delayed due to unavailable resources.

	Table 6-4	Rogue	Adhocs
--	-----------	-------	--------

Unclassified Rogue Access Points

This section provides information on rogue access points that are not classified. Table 6-5 describes the various parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a window with further information appears.



An unclassified rogue access point refers to a rogue access point that is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

Table 6-5	Unclassified	Rogue
-----------	--------------	-------

Parameter	Description
Alert	Number of unclassified rogues in alert state. Rogue access point radios appear as <i>Alert</i> when first scanned by the controller or as <i>Pending</i> when operating system identification is underway.
Contained	Number of contained unclassified rogues.
Contained Pending	Number of contained unclassified rogues pending.

Friendly Rogue Access Points

This section provides information on rogue access points that are classified as *friendly*. Table 6-6 describes the various parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a window with further information appears.



Friendly rogue access points are known, acknowledged, or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

Parameter	Description				
Alert	Indicates the number of rogues in an alert state.				
	Note An access point is moved to Alert if it is not on the neighbor list or part of the user-configured Friendly AP list.				
Internal	Indicates the number of internal access points.				
	Note Internal indicates that the detected access point is inside the network and has been manually configured as Friendly - Internal.				
External	Indicates the number of external access points.				
	Note External indicates that the detected access point is outside of the network and has been manually configured as Friendly - External.				

Table 6-6	Friendly Rogue AP Details
-----------	---------------------------

Attacks Detected

Attacks reflect network patterns that indicate a possible virus or hacker attack. When an attack occurs, the attack table is updated immediately. The table displays the number of attacks during the last one hour, last 24 hours, and the total active. You can use this information to assess the security state or security threats to the network.

If you click an underlined number in any of the time period categories, a window with further information appears.

Access Point Threats or Attacks

Table 6-7 describes the AP Threats or Attacks parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a window with further information appears.

Table 6-7 AP Threats/Attacks

Parameter	Description
Fake Attacks	Number of fake attacks
AP Missing	Number of missing access points
AP Impersonation	Number of access point impersonations
AP Invalid SSID	Number of invalid access point SSIDs
AP Invalid Preamble	Number of invalid access point preambles
AP Invalid Encryption	Number of invalid access point encryption
AP Invalid Radio Policy	Number of invalid access point radio policies
Denial of Service (NAV related)	Number of Denial of Service (NAV related) request
AP Detected Duplicate IP	Number of detected duplicate access point IPs

MFP Attacks

A value is provided for Infrastructure and client MFP attacks in the last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a window with further information appears.

Client Security Events

For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a window with further information appears.

Cisco Wired IPS Events

A value is provided for last hour, last 24 hours, and all. If you click an underlined number in any of the time period categories, a window with further information appears.

Monitoring Rogue Access Point

If you choose **Rogue APs** from the left sidebar menu (of the **Monitor > Security** page), the Rogue AP Alarms window appears (see Figure 6-4). This window allows you to view alarm details and messages regarding any anomalies with the controllers and access points.

ababa	Wi	reless	Control Syst	tem									Username:	doc Logout Refresh	Print View
CISCO		ئ 1	onitor • <u>R</u> eports	• <u>C</u> onfigu	re 🕶 🛛	Location •	Administra	ation 🕶	Help 🕶						
Quick Search	R	ogue AP	Alarms (<u>edt New</u>)					Entrie M	es 1 - 50 of 9 4 1 2 3 4 1	211 2 6 7 8 2	10 F M		Select	a command	• 60
Search Alarms		Severity	Roque MAC Address	¥endor	Radio Type	Strongest AP RSSI	No. of Roque Clients	owner	Date/Time	State	5510	Map Location A	cknowledged		
Alarm Summary ^O		Minor	00:16:90:90:f0:1e	Cisco	a	-79	0		4/8/08 2:17:49 PM	Alert	aire_wpaalpha	N	Þ		
Select Search		Minor	00:1a:e3:75:cf:1e	Cisco	8	-90	0		4/8/08 2:17:47 PM	Alert		N	Þ		
Security 79 0 18 Controllers 20 12 0		Minor	00:15:c7:fd:aa:6f	Cisco	a	-71	0		4/8/08 2:17:47 PM	Alert		N	0		
Access Points 104 0 25 Location 0 0 10		Minor	00:16:9c:90:f0:1c	Cisco	8	-80	0		4/8/08 2:17:39 PM	Alert		N	Þ		
Mesh Links 0 0 0		Minor	00:12:44:b5:de:c0	Cisco	a	-90	0		4/8/08 2:16:25 PM	Alert	Klingon2	N	•		
	П	Minor	00:16:9c:90:f0:1f	Cisco	•	-79	0		4/8/08 2:16:25 PM	Alert	aire_chinook	N	•		
		Minor	00:17:df:a9:o4:fb	Cisco	a	-87	0		4/8/08 2:13:25 PM	Alert	Spellbound	N	•		
	С	Minor	00:16:90:90:fd:3e	Cisco	•	-86	0		4/8/08 2:13:25 PM	Alert	aire_wpaalpha	N	•		
		Minor	00:16:9c:4b:8e:9d	Cisco	a	-85	0		4/8/08 2:13:25 PM	Alert		N	Þ		
	С	Minor	00:16:9c:4b:8e:9e	Cisco	a	-85	0		4/8/08 2:13:25 PM	Alert		N	•		
		Clear	00:16:9c:4b:8e:9b	Cisco	8	-85	0		4/8/08 2:11:31 PM	Removed		N	Þ		
	П	Minor	00:16:90:49:0f:10	Cisco	a	-87	0		4/8/08 2:11:31 PM	Alert	alpha	N	•		
		Minor	00:16:9c:4b:c5:8c	Cisco	8	-86	0		4/8/08 2:10:35 PM	Alert	guestnet	N	Þ		
	П	Minor	00:16:90:90:fd:3f	Cisco	a	-86	0		4/8/08 2:10:25 PM	Alert		N	Þ		
	С	Minor	00:11:92:9c:73:e0	Cisco	8	-84	0		4/8/08 2:10:25 PM	Alert	wnac_134wds	N	Þ		
	П	Minor	00:16:90:90:fd:3d	Cisco	a	-86	0		4/8/08 2:10:25 PM	Alert		N	6		
	С	Minor	00:12:d9:01:5e:b0	Cisco		-89	0		4/8/08 2:10:25 PM	Alert		N	p		
	С	Minor	00:16:90:90:ef:3d	Cisco	a	-91	0		4/8/08 2:10:25 PM	Alert		N	6		
	С	Clear	00:16:9c:b8:00:9e	Cisco	a	-87	0		4/8/08 2:08:41 PM	Removed		N	p		
	C	Minor	00:16:9c:4b:8e:9f	Cisco	a	-85	0		4/8/08 2:07:25 PM	Alert	blizzard	N	b		
	С	Minor	00:16:9c:b8:1e:fe	Cisco	a	-83	0		4/8/08 2:05:39 PM	Alert		N	Þ		
	П	Minor	00:16:9c:4b:c5:8e	Cisco	8	-86	0		4/8/08 2:04:25 PM	Alert		N	Þ		
	П	Minor	00:16:90:49:0f:1f	Cisco	a	-86	0		4/8/08 2:02:31 PM	Alert	aire_chinook	N	•		
	П	Minor	00:16:9c:49:0f:1d	Cisco	8	-90	0		4/8/08 1:56:31 PM	Alert	aire_SATCHMO	N	Þ		
	П	Minor	00:17:df:9e:9d:d1	Cisco	a	-84	0		4/8/08 1:55:35 PM	Alert	aire_wpaalpha	N	•		
	C	Minor	00:17:df:a2:45:60	Cisco	8	-87	0		4/8/08 1:55:25 PM	Alert	srk-lbf02	N	Þ		
	П	Minor	00:17:df:a9:o4:f8	Cisco	a	-88	0		4/8/08 1:52:25 PM	Alert	TearsInTheRain	N	0		
	С	Minor	00:17:df:a9:o4:f9	Cisco	a, b/g	-87	0		4/8/08 1:52:25 PM	Alert	ThunderSeven	N	Þ		
	С	Minor	00:17:df:a9:bc:ea	Cisco	a	-85	0		4/8/08 1:52:25 PM	Alert	SomebodysOutThere	N	6		
	C	Minor	00:17:df:a9:bc:e9	Cisco	a, b/g	-77	0		4/8/08 1:52:25 PM	Alert	ThunderSeven	N	p		
	С	Minor	00:1e:4a:e5:04:cb	Unknown	a, b/g	-90	0		4/8/08 1:49:35 PM	Alert	aire_wpapsk	N	6		
	С	Minor	00:17:df:a9:bc:e8	Cisco	a	-77	0		4/8/08 1:49:35 PM	Alert	TearsInTheRain	N	Þ		
	D	Minor	00:16:9c:4b:c5:8f	Cisco	a	-85	0		4/8/08 1:49:25 PM	Alert	blizzard	N	Þ		
	С	Minor	00:13:5f:0e:cd:30	Cisco	a	-83	0		4/8/08 1:49:25 PM	Alert	wpaalpha	N	•		
	П	Clear	00:1e:4a:e5:04:ce	Unknown	a, b/g	-89	0		4/8/08 1:47:49 PM	Removed	aire_leap	N	6		
	П	Minor	00:16:90:4b:c5:8b	Cisco	a	-83	0		4/8/08 1:46:35 PM	Alert		N	•		
	С	Minor	00:16:9c:90:fd:3c	Cisco		-86	0		4/8/08 1:46:25 PM	Alert		N	Þ		
	П	Minor	00:16:90:4b:8e:90	Cisco	a	-87	0		4/8/08 1:46:25 PM	Alert	guestnet	N	Þ		
	C	Minor	00:16:9c:4b:bf:be	Cisco		-80	0		4/8/08 1:46:25 PM	Alert		N	•		
	П	Minor	00:12:44:55:67:60	Cisco	a	-85	0		4/8/08 1:43:25 PM	Alert	philips	N			
	С	Minor	00:17:df:a9:o4:fa	Cisco		-87	0		4/8/08 1:43:25 PM	Alert	SomebodysOutThere	N	•		
		Minor	00:17:df:a9:o4:fc	Cisco	a	-88	0		4/8/08 1:43:25 PM	Alert	FightTheGoodFight	N	•		
	С	Minor	00:17:df:a9:bc:eb	Cisco	•	-85	0		4/8/08 1:43:25 PM	Alert	Spellbound	N	•		
		Minor	00:16:9c:b8:1e:ff	Cisco	a	-83	0		4/8/08 1:43:25 PM	Alert	blizzard	N	b		
		Minor	00:17:df:a9:o4:fe	Cisco	a	-88	0		4/8/08 1:40:25 PM	Alert	MagicPower	N	•		
		Minor	00:16:9c:b8:1e:fd	Cisco	a	-83	0		4/8/08 1:40:25 PM	Alert		N	b		
	П	Minor	00:16:90:b8:1e:fg	Cisco	a	-85	0		4/8/08 1:40:25 PM	Alert	guestnet	N	Þ		
		Minor	00:16:9c:48:d9:7c	Cisco		-84	0		4/8/08 1:40:25 PM	Alert		N	Þ		
		Minor	00:1e:4a:e5:04:c8	Unknown	a, b/g	-90	0		4/8/08 1:34:35 PM	Alert	aire_wpa2aes	N	Þ		
		Minor	00:16:9c:4b:c5:8d	Cisco		-84	0		4/8/08 1:34:25 PM	Alert		N	•		

Figure 6-4	Rogue AP Alarms
0	0

Monitoring Rogue Adhoc

If you choose **Rogue Adhocs** from the left sidebar menu (of the **Monitor > Security** page), the Rogue Adhoc Alarms window appears (see Figure 6-5). On this window you can view details of rogue adhoc alarms.

Figure 6-5 Rogue Adhoc Alarms Window



Monitoring Rogue Clients

If you choose **Rogue Clients** from the left sidebar menu (of the **Monitor > Security** page), the Rogue Clients window appears (see Figure 6-6). You can select search criteria in the left sidebar menu and then details about the rogue clients that are found is displayed.

ahaha	Wireless Co	ontrol System			Username: ro	ot Logout	Refresh	Print View
CISCO	🟠 Monitor 🗸	<u>R</u> eports v <u>C</u> onfigure v	Location 🔻	Administration 🔻	<u>T</u> ools ▼ <u>H</u> elp ▼			
Quick Search	Rogue Client	s						
<ip, go<="" name,ssii="" th=""><th>Please select crite</th><th>eria to search Rogue Clients</th><th>and then click</th><th>on the Search.</th><th></th><th></th><th></th><th></th></ip,>	Please select crite	eria to search Rogue Clients	and then click	on the Search.				
RogueClients								
Search for clients by All Rogue Clients								
Search In Location Servers								
Last detected within 15 Minutes								
Search								
Alarm Summary 🍳								
Malicious AP 0 0 280								
Security 4 2 2								
Controllers <u>6</u> <u>4</u> <u>8</u>								
Access Points 150 0 22 Location 0 0 0								
Mesh Links 0 0 0								

Figure 6-6 Rogue Clients Window

Monitoring Shunned Clients

When a Cisco IPS sensor on the wired network detects a suspicious or threatening client, it alerts the controller to shun this client. If the client to be shunned is currently associated to an access point and controller in a mobility group:

- 1. The shun entry is distributed to all controllers within the same mobility group.
- 2. The anchor controller adds this client to the dynamic exclusion list.
- 3. The foreign controller removes the client.

The next time the client tries to connect to a controller, the anchor controller rejects the handcuff and informs the foreign controller that the client is being excluded.

Choose **Monitor > Security** from the left sidebar menu and select **Shunned Clients** to access this window (see Figure 6-7).

											_
ahaha	Wireless	Control Sy	stem			Us	ername: roo	t Logout	Refresh	Print View	
CISCO	📅 Monit	tor v <u>R</u> eports v	<u>C</u> onfigure ▼	Location 🔻	Administration 🔻	<u>T</u> ools -	<u>H</u> elp ▼				
ShunnedClients Search for clients by All Shunned Clients I Search	Shunned Please select	Clients t criteria to search	Shunned Client	ts and then cli	ck on the Search.						
4											
Alarm Summary 0 200 Malicious AP 0 0 0 Coverage Hole 0 0 0 Security 4 2 2 Access Points 130 0 2 Location 0 0 0 Mash Links 0 1 0											200066

Figure 6-7 Shunned Clients Window

The Shunned Client window displays the client IP address, sensor IP address, and the controller for each shunned client.

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 6-8 shows 199 rogue access point alarms.

Alarm Summary 🌻							
Malicious AP	0	0	0				
Coverage Hole	0	0	0				
Security	0	0	0				
Controllers	0	0	0				
Access Points	0	0	0				
Location	4	0	0				
Mesh Links	0	0	0				
WCS	0	0	0				

Figure 6-8 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 6-9 shows a map that indicates that location of a rogue unit.



Figure 6-9 Map Indicating Location of Rogue Unit

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 (see Figure 6-10).



Figure 6-10 Clients Summary

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

Client—Enter the IP address, MAC address, or user-defined client name and click **Troubleshoot** to continue to the client details.

Diagnostic Notification Received—Indicates the number of diagnostic notifications received. Click the number to view the list of the diagnostic events.

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.



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 6-11). 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.

ubleshoo	ting Client '00:	19:d2:69:aa:44	l.		
mmary (Log Analysis	Event History	ACS View Server		 _
			0		
802.11 Association	802.1X Authentication	IPAddress Assignment	Successful Association		
roblem					
one					
Suggeste	d Action				
lone					

Figure 6-11 Troubleshooting Client Tab

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



te 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 6-12).
- **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

CISC	• W	reless Control System	
oubleshoo	ting Client '0):17:95:4f:73:ee'	
Summary	Log Analysis	Event History	
Click Start to to ask the clic that relevant been collecte Start	begin capturing ant to restart the log events are g d, click Stop .	og messages from the controller. (It may be necessary connection process by rebooting their laptop to ensure nerated.) When a sufficient number of messages have	
	- orop	1000	
802.11 Initia 802.1x Auth PEM Messag DHCP Messag AAA Messag AII (n)	lization (0) entication (0) es(0) ges (0) es(0)		
Time	Sever	y Controller Message	<u> </u>
2			
			21
	-f-un-stine Detri	undet Men Mey 19 11/24/02 EDT 2007	

Figure 6-12 Log Analysis Tab

Step 7 To display a summary of the client's events history, click the Event History tab (see Figure 6-13). This page displays client and access point events that occurred within the last 24 hours.

cisco				
publeshootir	g Client '00):17:95:4f:73:ee'		
ummary L	og Analysis	Event History		
Event Histor	/ Summarv			
	,			
Client Events				
No Client Notific	ation found.]
AP Events				
AP Events Message			Date / Time	
AP Events Message AP 'VJ-1510R-7	11bb0' disasso	ciated from Controller '172.19.7.85'.	Date / Time 3/19/07 8:30 AM	
AP Events Message AP 'VJ-1510R-7 AP 'VJ-1030R-7	.1bb0' disasso aa7a0' associat	ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'.	Date / Time 3/19/07 8:30 AM 3/19/07 7:30 AM	
AP Events Message AP 'VJ-1510R-7 AP 'VJ-1030R-7 AP 'VJ-1030R-7	.1bb0' disasso aa7a0' associat aa7a0' disasso	ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'. ciated from Controller '172.19.7.85'.	Date / Time 3/19/07 8:30 AM 3/19/07 7:30 AM 3/19/07 7:24 AM	
AP Events Message AP 'VJ-1510R-7 AP 'VJ-1030R-7 AP 'VJ-1030R-7 AP 'VJ-1030R-7	.1bb0' disasso aa7a0' associat aa7a0' disasso aa7a0' disasso aa7a0' associat	ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'. ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'.	Date / Time 3/19/07 8:30 AM 3/19/07 7:30 AM 3/19/07 7:24 AM 3/19/07 4:53 AM	
AP Events Message AP 'VJ-1510R-7 AP 'VJ-1030R-7 AP 'VJ-1030R-7 AP 'VJ-1030R-7	.1bb0' disasso aa7a0' associat aa7a0' disasso aa7a0' disasso aa7a0' associat aa7a0' disasso	ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'. ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'. ciated from Controller '172.19.7.85'.	Date / Time 3/19/07 8:30 AM 3/19/07 7:30 AM 3/19/07 7:24 AM 3/19/07 4:53 AM 3/19/07 4:47 AM	
AP Events Message AP 'VJ-1510R-7 AP 'VJ-1030R-7 AP 'VJ-1030R-7 AP 'VJ-1030R-7 AP 'VJ-1030R-7	.1bb0' disasso aa7a0' associat aa7a0' disasso aa7a0' associat aa7a0' disasso aa7a0' disasso	ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'. ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'. ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'.	Date / Time 3/19/07 8:30 AM 3/19/07 7:30 AM 3/19/07 7:24 AM 3/19/07 4:53 AM 3/19/07 4:47 AM 3/19/07 4:11 AM	
AP Events Message AP 'VJ-1510R-7 AP 'VJ-1030R-7 AP 'VJ-1030R-7 AP 'VJ-1030R-7	.1bb0' disasso aa7a0' associat aa7a0' disasso aa7a0' associat aa7a0' associat	ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'. ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'. ciated from Controller '172.19.7.85' on Port number '1'.	Date / Time 3/19/07 8:30 AM 3/19/07 7:30 AM 3/19/07 7:24 AM 3/19/07 4:53 AM 3/19/07 4:47 AM 3/19/07 4:11 AM	
AP Events Message AP 'VJ-1510R-7 AP 'VJ-1030R-7 AP 'VJ-1030R-7 AP 'VJ-1030R-7	.1bb0' disasso aa7a0' associat aa7a0' disasso aa7a0' associat aa7a0' disasso aa7a0' associat	ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'. ciated from Controller '172.19.7.85'. ted with Controller '172.19.7.85' on Port number '1'. ciated from Controller '172.19.7.85' on Port number '1'.	Date / Time 3/19/07 8:30 AM 3/19/07 7:30 AM 3/19/07 7:24 AM 3/19/07 4:53 AM 3/19/07 4:47 AM 3/19/07 4:11 AM	

Figure 6-13 Event History Tab

Step 8 If you click the ACS View Server tab, you can inteface with the Cisco Access Control (ACS) System View Server (see Figure 6-14). You must have View Server credentials established before you can access this tab. (The tab will show the server list as empty if no view servers are configured.) Refer to the "Configuring ACS View Server Credentials" section on page 6-34 for steps on establishing credentials.

This server provides WCS with aggregated client status information from multiple ACS servers. The client status information allows you to further troubleshoot client issues and determine if they are related to authentication or authorization. Enter the date and time ranges to retrieve the historical authentication and authorization information and click **Submit**. The results of the query are displayed in the Authentication Records portion of the window and is used as a filter for the userid logged into the client.

🗿 https://172.19.32.19 - Monitor Client - Microsoft Internet Explorer	- 🗆 🗙
Wireless Control System	×
Troubleshooting Client '00:19:d2:69:aa:44' Summary Log Analysis Event History ACS View Server © Last 5 Minutes © Between	
🛃 Loaded 👘 📋 👘 🔂 Internet	///

Figure 6-14 ACS View Server Window

Step 9 (Optional) If Cisco Compatible Extension Version 5 clients are available, a Test Analysis tab as shown in Figure 6-15 appears.

ouble	shooting Client '00	0:40:96:a1:b5:be				
umma	ry Log Analysis	Event History	Test Analysis	Messaging	Event Log	
The foll Stop to	lowing tests are availabl a halt the tests. When a	e for clients. Use the c test is completed, click	heckboxes to sele on the test status	ct the test(s) you w to view the results	ould like to pe	rform, then click Start . Clic
Select	t Diagnostic Test	Inp	ut		Status	Results
	DHCP				Not initiated	None
	IP Connectivity				Not initiated	None
	DNS Ping				Not initiated	None
	DNS Resolution	Server Name:			Not initiated	None
	802.11 Association	AP name: deepak_1	020-802.11b 💌	Profile: a 💌	Not initiated	None
	802.1x Authentication				Not initiated	None
	Profile Redirect	Client Profile Number	r:		Not initiated	None
St. Result	art Stop	Frame				

Figure 6-15 Test Analysis Tab

- Step 10 The Test Analysis tab allows you to run a variety of diagnostic tests on the client. 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 on the 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.
 - 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.



To run the profile diagnostic test, the client must be on the diagnostic channel. This test uses the profile number as an input. To indicate a wildcard redirect, enter 0. With this redirect, the client is asked to disassociate from the diagnostic channel and to associate with any profile. You can also enter a valid profile ID. Because the client is on the diagnostic channel when the test is run, only one profile is returned in the profile list. You should use this profile ID in the profile redirect test (when wildcard redirecting is not desired). Step 11 (Optional) If Cisco Compatible Extension Version 5 clients are available, a Messaging tab as shown in Figure 6-16 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 6-16 Messaging Tab

cisc	0 W	vireless Contro	ol System			
Troublesho	oting Client	'00:40:96:a1:b5:b	e'			
Summary	Log Analysi	is Event History	Test Analysis	Messaging	Event Log	
Use this tab message fro Message C The SSID is Text Messa Send	to send an insta m the list. Then ategory s invalid. age	nt text message to the u click Send .	iser of this client. Sel	ect a		

Step 12 Close the Troubleshooting Client window. The **General** tab displays the client details and properties of the access point with which the client is associated. Table 6-8, Table 6-9, and Table 6-10 describe the fields displayed on this General tab.

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 clie registered. Clicking the controller's IP address di information about the controller.			
Port	The port on the controller to which the client is connected.		

 Table 6-8
 General Tab / Client Properties

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	Local, Anchor, Foreign, Export Anchor, Export Foreign.
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.

Table 6-8	General Tab /	Client Properties	(continued)
		•	

Parameter	Description	
Cisco Compatible Extension	Indicates the Cisco Compatible Extension version, if client supports it	
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 6-8 General Tab / Client Properties (continued)

Table 6-9 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.
АР Туре	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 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.

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 6-9 General Tab / RF Properties (read only) (continued)

Table 6-10 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 Cipher	Encryption settings.
EAP Type Type of Extensible Authentication Protocol (EAP) use	

- **Step 13** 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**.
- I. To display client voice matrix, choose Voice Metrics from the drop-down menu and click GO.
- **Step 14** To display client statistics, click the **Statistics** tab (see Figure 6-17).

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 (Kb/s)— 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 6-11 describes the fields displayed on this Statistics tab.

cisco k search ch clients ch clients c search c search	ahaha	Wireless Control System Virtual Domain: root Username: root Logout	Refresh Print View
k search ch clears a search b stammar • b stamar • b stamar • <th>cisco</th> <th>🚡 Monitor 🔹 Reports 👻 Configure 👻 Mability 💌 Administration 👻 Icols 👻 Help 💌</th> <th></th>	cisco	🚡 Monitor 🔹 Reports 👻 Configure 👻 Mability 💌 Administration 👻 Icols 👻 Help 💌	
Aum Still Central Statistill	k Search	Client 'unknown' - Cisco:a7:bd:81	Select a command 💌 🖸
I clarkt Sarch: Sarch: Sarch: Sarch: </td <td>ame,SSII Go</td> <td>General Statistics Location</td> <td></td>	ame,SSII Go	General Statistics Location	
Sarachov	h Clients	Client RSSI History (dBm) Client SNR History (dB)	
Searches tt Searches tt Searches Searches tt Searches Searche	Search	6h 1d 1w 2w 4w 3m 6m 1y Custom 6h 1d 1w 2w 4w 3m 6m 1y Custom	
Summary O summary O st Search	Searches <u>Ed</u> i		
Summary Original sector Rate	ct Search 💌		
Summery		a 25	
Summary 0 # 1 = 0 # 2 = 0 Bytes Sent and Received (kbps) Bottes Sent and Received (kbps) Bottes Sent and Received (kbps) bit 1 = 1 = 1 = 20 + 50 + 100 + 1100 + 1200 + 1300 + 100 +			
Summary 0 yr AP 0 <t< td=""><td></td><td>24</td><td></td></t<>		24	
Summary O summary O stram 2		a 6	
Summary 0 summary 1 summary 1 summary 2 summary 1 summary 2 summary 2 summary 1 summary 2			
i Summary u Sammary u Sam			
Summary O Bytes Sent and Received (kbps) Packets Sent and Received (per sec.) us AP 0 0 0 us AP 0 us AP 0 </td <td></td> <td></td> <td></td>			
Summary 0 (J AP 0 0 0 0 ge Holo 0 0 0 here 3 0 here 3 0 0 here 3 0 here		Bytes Sent and Received (Kbps) Packets Sent and Received (per sec.)	
Summary 0 gs Hole 0 0 gs Hole 0 0 mint 2 0		6h 1d 1w 2w 4w 3m 6m 1y Custom 6h 1d 1w 2w 4w 3m 6m 1y Custom	
9 Summary 9 ur 40 0 12 0 prove 2 0 0 0 12 0 prove 2 0 0 0 0 12 0 prove 2 0 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 100 1100 1200 1300 prove 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		50	
UT AP 0 6 20 0 FAC 0 0 0 V 6 0 0 V 6 0 0 V 7 0 0 0 Dott 12 0 100 1 Send Rate Baceive Rate	n Summary 🍳	16	
Que dout			
Imp 3 0 3 0 3 0			
A A	llers <u>5</u> 0	<u>8</u> 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	
URLS 0 0 00 1000 1100 1200 1300 00 1000 1100 1200 1300 0 000 1000 1	2011(S 17 0 20 0 0		
Send Rate Send Rate Send Rate	inks 0 0	8 8:00 9:00 10:00 11:00 12:00 13:00 8:00 9:00 10:00 11:00 12:00 13:00	
		Send Rate Receive Rate Send Rate Receive Rate	
		<	>

Figure 6-17 Statistics Tab

Table 6-11 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.
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 15 To display the client's location information, click the Location tab (see Figure 6-18). Table 6-12 describes the fields displayed on this Location tab.

			week Lessent Defreck Drivt View
ahaha	Wireless Control System	Username:	root Logout Refresh Print View
CISCO	Monitor ▼ Reports ▼ Configure ▼ Location ▼ Administratio	n ▼ <u>H</u> elp ▼	
Quick Search	Client 'unknown' - Cisco:4f:73:ee		Select a command V GO
<ip, mac="" name="" or=""> Go</ip,>	General Statistics Location		
Search Clients			
	Client Location	Asset Info	
New Search	No Location Information. Client is not detected by any Location	No Information. Client is no	t detected by any Location
Saved Searches <u>Edit</u>	Server.	Server.	
		Location Notifications	
		Absence	<u>0</u>
		Containment	<u>0</u>
		Distance	<u>0</u>
		All	<u>0</u>
Alarm Summary 획			
Rogue AP 0 2			
Coverage Hole 137			
Security 8 0 2 Controllers 5 3 0			
Access Points 30950 63			
Mesh Links 0 0 0			
Location 1 0 18			134
			230

Figure 6-18 Location Tab

Table 6-12Location 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.that		
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.		
Containment	The location server generates containment events when an asset is moved inside or outside of a designated area.		
	PTipYou 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 16 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 6-13 describes the parameters on the Manufacturer Information portion of the Cisco Compatible Extension (version 5) Info tab.



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

• Automated Troubleshooting Report—Displays the automated troubleshooting file.



You must click **Export** to save the .zip file. The file contains three logs: automated troubleshoot report, frame log, and watch list log.

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 $4 \ge 0.5 = 2$ dBm of gain.

Table 6-13 Manufacturer Information

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.

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 6-14 describes the parameters displayed in the Cisco Compatibility Extensions (version 5) Capability Information portion of the tab.

<u>Note</u>

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

Table 6-14 Client Statistics

Parameter	Description
Bytes Sent and Received (Kb/s)	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 17 To display the client's workgroup bridge information, click the WGB Clients tab. Table 6-15 describes the fields that display on this WGB tab.

Table 6-15	WGB Clients Ta	ab

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		

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.

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.

Enabling Automatic Client Troubleshooting

The Settings > Client page allows you to enable automatic client troubleshooting on a diagnostic channel. This feature is only available for Cisco Compatible Extension clients version 5.

Follow these steps to enable automatic client troubleshooting.

- Step 1 Choose Administration > Settings.
- **Step 2** From the left sidebar menu, choose **Client**.
- **Step 3** Choose the Automatically troubleshoot client on diagnostic channel check box.



If the check box is selected, WCS processes the diagnostic association trap. If it is not selected, WCS raises the trap, but automated troubleshooting is not initiated.

Step 4 Click Save.

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 6-19).

Search Clients		×
Search By	All Clients	•
Clients Detected By	WCS	•
Client States	All States	•
Restrict By Radio Band		
Restrict By Protocol		
Search on Controllers Now		
SSID		
Profile		
CCX Compatible		
E2E Compatible		
NAC State		
Include Disassociated		
Save Search		
Items per page	50	•
Go		

Figure 6-19	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.
- Client States Specify if you want to view clients only in a specific state such as idle, authenticated, associated, probing, or excluded.
- Restrict by Radio Band—To see the clients on a particular band, click the check box and choose 2.4GHz (802.11b/g or 802.11n) or 5 GHz (802.11a or 802.11n) from the drop-down menu.
- Restrict by Protocol—To restrict the search by protocol, choose 802.11a/n, 802.11b/n, and 802.11g/n from the drop-down menu.
- Search on Controllers Now—To search controllers rather than just the WCS database, click the check box. This search provides polling results in real time and delayed by 15 minutes, but it may take awhile to perform.
- SSID To restrict the search by SSID, choose an SSID from the drop-down menu.
- Profile—To restrict the search by the profile that the client is using, click the check box and choose the profile name from the drop-down menu.
- CCX Compatible To search for Cisco Compatible Extension compatible clients.
- E2E Compatible To search for E2E compatible clients.
- NAC state—Click the check box and choose the client's network admission control state from the drop-down menu. The choices are invalid (the client is currently probing and not associated), quarantine (the client must go through posture analysis), and access (the client has completed posture analysis and is clean), and not applicable.
- Include Disassociated To include clients that are no longer on the network but for which WCS has historical records.
- 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.



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 6-20 shows a heat map that includes a client location.

L



Figure 6-20 Map with Client Location

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

tatistics
ļ

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.
Bytes Sent and Received (Kb/s)	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.

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 6-21). A Mesh Link window appears.

<u>Note</u>

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

Figure 6-21 Mesh Link Details Window

Virele	ess Control System		Username: root Logout Refresh Print View
<u>M</u> onitor	▼ <u>R</u> eports ▼ <u>C</u> onfigure ▼ Lo	cation 👻 Administration 👻 Help 👻	
<u>Maps</u> >	San Jose Campus > Buildings	S	Select a command 💙 GO
> Laye	Zoom R 100 % ¥ 5	efresh 5 min 💌 <u>Full Screen</u>	
00	Mesh Link: 'indoor-mesh-44	-map1' to 'indoor-mesh-44-rapX	
00	Information fetched on Link SNR Link Type SNR UP SNR Down PER Tx Parent Packets Rx Parent Packets Time of Last Hello Link Test Child to Parent	Apr 9, 2007 9:51:53 AM 57 dB (Excellent) Child to Parent 62 dB 61 dB 0% 25353 25353 Apr 9, 2007 1:11:59 AM Link Test Parent to Child	indoor-mesh-44-rap1
00	mesh-45-map1		door-mesh-44-map2
23			

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 6-22).



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.

Wireless C	ontrol System		Username: root Logout Refresh	Print View
<u>M</u> onitor 🔻 <u>R</u> ep	ports 👻 <u>C</u> onfigure 👻 <u>L</u> ocation 👻 <u>A</u> dmin	nistration 🔻 <u>H</u> elp 🔫		
<u>Maps</u> > <u>San Jo</u>	<u>se Campus</u> > Buildings		Select a command	✓ G0
	Link Test Results	×]	
> Layers	Control 00 % V 5 min V Source moor-mesn-44-map1	172.19.28.44 00:0b:85:80:ed:d0	ZA 16 35 18 1	~
•••	Packet Error Rate Packets Sent Packets Received Good Packets Received Duplicate Packets Received Big Packets Received COE Chert Packets Received	0% 2489 2491 2490 42 0	R indoor-mesh-44-rap1	
100	PHY ERR Packets Received CRC ERR Packets Received Average SNR (dB) Highest SNR (dB) Lowest SNR (dB) Average Noise Ratio (dB) Highest Noise Ratio (dB)	0 1 51 66 60 -99 -99 -99		
500	Lowest Noise Katio (dB) Average RSSI (dBm) Highest RSSI (dBm) - Lowest RSSI (dBm)	-99 -38 -33 -40	r-mesh-44-map1	
800				< C 💌
<				>

Figure 6-22 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 6-23).

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 6-23 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



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).

Γ



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 14-15.

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 6-24).



Figure 6-24 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 6-25).

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 6-45. 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.

ahaha	Wireless (Control S	System			Username: r	root Logout	Refresh F.
CISCO	📅 <u>M</u> onito	r ▼ <u>R</u> eports	▼ <u>C</u> onfigure ▼	Location 🔻 <u>A</u>	dministration 🔻	<u>H</u> elp 🔻		
Quick Search	Access Poi	nts > mesł	1 -45- map2					
<ip, go<="" name,ssii="" th=""><th>General</th><th>Interfaces</th><th>Mesh Links</th><th>Mesh Stat</th><th>istics</th><th></th><th></th><th></th></ip,>	General	Interfaces	Mesh Links	Mesh Stat	istics			
Search Access Points								
New Search	General			Versions				
New Search	AP Name	m	esh-45-map2	Software Ver	sion 4.1.175.32	M (Mesh)		
Saved Searches Edit	AP Ethernet I	4AC 00	:0b:85:72:64:00	Boot Version	2.1.78.0			
Select Search 💌	AP Base Rad	io MAC 00	:0b:85:72:64:00					
	Country Cod	e US	5	Inventory I	nformation			
	AP IP Addres	s 0,	0.0.0	АР Туре	LWAPP			
	AP Up Time	5	d 22 h 4 m 4 s	AP Model	LAP1510			
	LWAPP Up Tir	me 5	d 21 h 59 m 50 s	AP Certificate	e Type Manufactu	re Installed		
	LWAPP Join T	aken Time 4 i	m 6 s	AP Serial Nur	mber WCN1017	0001		
	Admin Status	En En	able					
	AP Mode	Br	idge	Unique Dev	rice Identifier(U	DI)		
	Operational S	Status Re	gistered	Name	Cisco AP			
Alarm Summary 획	Registered C	ontroller 20	9.165.200.250	Description	Cisco Wireless	Access Point		
Rogue AP 0 0 222	Primary Cont	roller m	esh-controller-45	Product Id	AIR-LAP1510-A	-K9		
Coverage Hole 0 0 0	Port Number	1		Version Id	V01			
Security <u>19</u> 0 <u>1</u>	Map Location	<u>Sa</u>	n Jose > Site	Serial Numbe	er WCN10170001			
Access Points 0 0 17	Statistics Tim	ier 18	0					
Location 0 0 0	AP Temperat	ure 35	C/95F	<u>Alarms</u>				
Mesh Links 0 <u>165 47</u>	Heater Statu:	s Of	f					
wcs o o				Events				
:								>

Figure 6-25 Mesh AP Detail Window

- **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.



te 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 6-51.

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 6-26).

Figure 6-26 Access Points > Mesh Links Panel

Cisco Monitor * Reports * Configure * Location * Administration * Help * Quick Search Access Points > mesh-45-map2 General Interfaces Mesh Links Mesh Statistics Search Access Points Type AP Name AP MAC Address PER Link Detail Link Test Link Test New Search- ·-Select Se	ahaha	Wireless (Control Syste	m		Username: ro	ot Logout R	efresh Print
Quick Search Search Access Points Access Points > mesh-45-map2 New Search Saved Searches Edit Yiew? Saved Searches Edit Yiew? New Search Type AP Name AP MAC Address PER Link Detail Link Test Link Test Neighbor mesh-45-rap1 00:0b:85:5f:faif0 0% Details AP to Neigh Neight to AP Neighbor mesh-45-rap1 00:0b:85:71:1b:50 Details AP to Neigh Neight to AP Neighbor mesh-45-map3 00:1b:85:75:1bi0 Details AP to Neigh Neight to AP Neighbor mesh-44-map1 00:1b:85:85:80 0 Details AP to Neigh Neight to AP Neighbor indoor-mesh-44- 00:1b:81:88:08:10 Details AP to Neigh Neight to AP Neighbor indoor-mesh-44- 00:1b:81:88:08:10 Details AP to Neigh Neight to AP Neighbor indoor-mesh-44- 00:1b:81:88:08:10 Details AP to Neigh Neight to AP Neighbor indoor-mesh-44- 00:1b:81:88:00:10 Details AP to Neigh Neight to AP Neighbor indoor-mesh-44- 00:1b:81:88:00:10 Details AP to Neigh Neig	CISCO	🚡 <u>M</u> onito	r ▼ <u>R</u> eports ▼ <u>C</u> or	figure 🔻 Location 👻 ,	Administration 🔻	<u>H</u> elp ▼		
c1P, Name;SSI 60 Search Access Points New Search Saved Searches Edit Select Search Alarm Summary ? Rogue AP Coverage Hole 0 Security 18 Outhoulers Access Points Neighbor Inderfaces Mesh Links 0 Security 18 Neighbor Neighbor Indoor-mesh-44- 00:11:82:75:53:d0 Details AP to Neigh Neighbor Indoor-mesh-44- 00:11:82:75:53:d0 Details AP to Neigh Neighbor	Quick Search	Access Poi	nts > mesh-45-ma	ap2				
Search Access Points Image: Cest View) Saved Searches Edit -Select Searches V Alarm Summary V Rogue AP 0000b185:5f1af10 0% Details AP to Neigh Neighbor Neighbor mesh-45-rap1 00:0b:85:7f1:1b:50 - Details AP to Neigh Neighbor Neighbor mesh-45-rap1 00:0b:85:7f1:1b:50 - Details AP to Neigh Neighbor Neighbor mesh-45-rap1 00:0b:85:7f1:1b:50 - Details AP to Neighb Neighbor Neighbor mesh-45-rap1 00:0b:85:7f1:1b:50 - Details AP to Neighb Neighbor Neighbor Neighbor Neighbor Neighbor Neighbor AP to Neigh Neighbor Neighbor Neighbor Neighbor Neighbor Neighbor AP to Neigh Neighbor <	<ip, go<="" name,ssii="" th=""><th>General</th><th>Interfaces Me</th><th>sh Links Mesh Sta</th><th>tistics</th><th></th><th></th><th></th></ip,>	General	Interfaces Me	sh Links Mesh Sta	tistics			
New Search Saved Searches Edit Select Searches Edit Select Searches Mar Alarm Summary ? Meighbor Neighbor mesh-45-map1 00:0b:85:75:15d:b0 - Details AP to Neigh Neighbor mesh-45-map1 00:0b:85:75:5d:b0 - Details AP to Neigh Neighbor mesh-45-map1 00:0b:85:75:5d:b0 - Details AP to Neigh Neighbor mesh-45-map1 00:1d:1b:58:73:80 - Details AP to Neigh Neighbor indoor-mesh-44- 1240-map1 00:14:1b:58:53:80 Neighbor Indoor-mesh-44- Neighbor ind	Search Access Points	(Edit View)						
Select Search Y Alarm Summary * Rogue AP 0 238 Coverage Hole 0 0 0 Security 18 0 1 Controllers 0 16 Neighbor 1130-rap1 Neighbor Neighbor AP to Neigh Neighbor AP Neighbor 1130-rap1 Neighbor 1130-rap1 Neighbor 1130-rap1 Neighbor 1130-rap1	New Search	Туре	AP Name	AP MAC Address	PER	Link Detail	Link Test	Link Test
Alarm Summary Image: Coverage Hole or controllers Neighbor mesh-45-map3 00:0b:85:71:1b:50 - Details AP to Neigh.* Neighbor Neighbor Coverage Hole or controllers 0 0 0 Neighbor mesh-45-map3 00:0b:85:75:5d:b0 - Details AP to Neigh.* Neighbor N	Select Search 🛛 👻	Parent	mesh-45-rap1	00:0b:85:5f:fa:f0	0%	<u>Details</u>	AP to Neigh	Neigh to AP
Rogue AP 0 228 Coverage Hole 0 0 0 00:0b:85:75:5d:b0 - Details AP to Neigh Neigh to AP Security 18 0 1 00:0b:85:75:5d:b0 - Details AP to Neigh Neigh to AP Security 18 0 1240-map1 00:14:1b:58:53:80 - Details AP to Neigh Neigh to AP Neighbor 1130-rap1 00:1b:8f:88:08:f0 - Details AP to Neigh Neigh to AP Neighbor indoor-mesh-44- 1130-rap1 00:1b:8f:88:08:f0 - Details AP to Neigh Neigh to AP Neighbor indoor-mesh-44- 1130-rap1 00:1b:8f:88:08:f0 - Details AP to Neigh Neigh to AP Neighbor indoor-mesh-44- 1130-map1 00:1b:8f:88:08:f0 - Details AP to Neigh Neigh to AP Neighbor indoor-mesh-44- 1130-map1 00:1b:8f:88:0b:f0 - Details AP to Neigh Neigh to AP Neighbor indoor-mesh-44- 1130-map1 00:1b:8f:88:0b:f0 - Details AP to Neigh Neigh to AP Wch Link	Alarm Summary 🌻	Neighbor	mesh-45-map1	00:0b:85:71:1b:50	-	Details_*	<u>AP to Neigh</u> *	Neigh to AP *
Coverage Hole 0 0 0 0 0 0 0 0 1240-map1 00:14:1b:58:53:80 - Details AP to Neigh Neighto AP Security 18 0 1 0 1240-map1 00:14:1b:58:53:80 - Details AP to Neight to AP Neighbor Indoor-mesh-44- 00:11a:a2:fc:53:d0 - Details AP to Neight Neight to AP Neighbor indoor-mesh-44- 00:11b:8f:88:08:f0 - Details AP to Neight Neight to AP Neighbor indoor-mesh-44- 00:11b:8f:88:08:f0 - Details AP to Neight Neight to AP Neighbor indoor-mesh-44- 00:11b:8f:88:08:f0 - Details AP to Neight Neight to AP Neighbor indoor-mesh-44- 00:11b:8f:88:08:f0 - Details AP to Neight Neight to AP Neighbor indoor-mesh-44- 00:11b:8f:88:08:f0 - Details AP to Neight Neight to AP Neighbor indoor-mesh-44- 00:11b:8f:88:08:f0 - Details AP to Neight Neight to AP *Link is out of date. This can be because the AP has been replaced or the APs can no longer communicate	Rogue AP 0 0 238	Neighbor	mesh-45-map3	00:0b:85:75:5d:b0	-	<u>Details</u>	AP to Neigh	Neigh to AP
Neighbor Unknown 00:1a:a2:fc:53:d0 Details AP to Neigh Neighbor Neighbor Access Points 0 <th>Coverage Hole 0 0 0</th> <th>Neighbor</th> <th>indoor-mesh-44- 1240-map1</th> <th><u>00:14:1b:58:53:80</u></th> <th>-</th> <th><u>Details</u></th> <th>AP to Neigh</th> <th>Neigh to AP</th>	Coverage Hole 0 0 0	Neighbor	indoor-mesh-44- 1240-map1	<u>00:14:1b:58:53:80</u>	-	<u>Details</u>	AP to Neigh	Neigh to AP
Access Points 0 1.6 Location 0 0 Mesh Links 0 166 0 0 0 WCS 0 0 Neighbor indoor-mesh-44- 1130-map1 00:1b:8f:88:0b:f0 - Details AP to Neighbor Neighbor *Link is out of date. This can be because the AP has been replaced or the APs can no longer communicate - Details AP to Neighbor Neighbor Mesh Link Alarms - - - Details AP to Neighbor Neighbor	Controllers 0 0 2	Neighbor	Unknown	00:1a:a2:fc:53:d0	-	<u>Details</u>	AP to Neigh	Neigh to AP
Mesh Links 0 166 47 Neighbor indoor-mesh-44- 1130-map1 00:1b:8f:88:0b:f0 - Details AP to Neigh Neighto AP *Link is out of date. This can be because the AP has been replaced or the APs can no longer communicate • Details AP to Neight Neighto AP Mesh Link Alarms • • • Details AP to Neight Nei	Access Points 0 0 <u>16</u> Location 0 0 0	Neighbor	indoor-mesh-44- 1130-rap1	00:1b:8f:88:08:f0	-	Details	AP to Neigh	Neigh to AP
*Link is out of date. This can be because the AP has been replaced or the APs can no longer communicate Mesh Link Alarms	Mesh Links 0 <u>166 47</u> WCS 0 0 0	Neighbor	indoor-mesh-44- 1130-map1	00:1b:8f:88:0b:f0	-	Details	AP to Neigh	Neigh to AP
		*Link is ou replaced o <u>Mesh Link i</u>	it of date. This can be i or the APs can no longe <mark>Marms</mark>	because the AP has been r communicate				



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 6-25).



Signal-to-noise (SNR) only appears on the View Mesh Neighbors panel (see Figure 6-26).



Figure 6-27 View Mesh Neighbors Panel

S, 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.

۵. 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 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 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 6-28).

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 6-28 Monitor > Access Points

ahaha	Wireless Co	ntrol Syst	em					Use	rname:	root Logo
CISCO	<u>M</u> onitor ▼ <u>R</u> epo	rts 🔻 <u>C</u> onfigur	re ▼ Location ▼ A	dministratio	n ▼ <u>H</u> elp ▼					
Quick Search <ip, mac="" name="" or=""> Go Search Access Points</ip,>	Access Points	s > Search Ro 56 N	esults (_{Edit View})		Ge	nerate report	for selec	ted APs	Sele	st a report
New Search	<u>AP Name</u>	IP Address	<u>Ethernet</u> <u>MAC</u>	<u>Radio</u>	Map Location	<u>Controller</u>	<u>Client</u> Count	<u>Admin</u> Status	AP Mode	<u>Oper</u> Status
Saved Searches Edit	noof17	10.32.34.174	00:0b:85:60:ba:80	<u>802.11a</u>	<u>Greggs Map</u> <u>> sdfs ></u> <u>sdfsa</u>	<u>10.32.32.12</u>	0	Enable	Local	Up
Alarm Summary 🎙	pole14-27	10.32.34.179	00:0b:85:70:4d:d0	802.11b/q	<u>Greggs Map</u> <u>> sdfs ></u> <u>sdfsa</u>	<u>10.32.32.12</u>	0	Enable	Local	Up
Rogue AP 0 940 Coverage Hole 0	roof12	10.32.34.141	00:0b:85:63:7e:60	<u>802.11b/q</u>	<u>Greggs Map</u> <u>> sdfs ></u> <u>sdfsa</u>	10.32.32.12	0	Disable	Local	Down
Security 5 0 0 Controllers 0 0 0 Access Points 39 0 31	pole12	10.32.34.251	00:0b:85:5c:b8:a0	<u>802.11a</u>	<u>Greggs Map</u> <u>> sdfs ></u> <u>sdfsa</u>	<u>10.32.32.12</u>	0	Enable	Local	Up
Mesh Links <mark>16 20 2</mark> Location 0 0 0	pole14-27	10.32.34.179	00:0b:85:70:4d:d0	<u>802.11a</u>	<u>Greggs Map</u> <u>> sdfs ></u> sdfsa	10.32.32.12	0	Enable	Local	Up

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 6-29).

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.

ahaha	Wireless Control System	Username: root Logout Refresh Pri	int View
CISCO	Monitor ▼ Reports ▼ Configure ▼ Location ▼	<u>A</u> dministration ▼ <u>H</u> elp ▼	
Quick Search <ip, mac="" name="" or=""> Go</ip,>	Access Points > pole14-27 General Mesh Links Mesh Statistics		
	General	Versions	
New Search	AP Name pole14-27	Software Version 4.1.140.1	
Saved Searches Edit	AP Ethernet MAC 00:0b:85:70:4d:d0	Boot Version 2.1.78.0	
Select Search 🛛 💙	AP Base Radio MAC 00:0b:85:70:4d:d0		
	Country Code US	Inventory Information	
	AP IP Address 10.32.34.179	AP Model LAP1510	
	Admin Status Enable	AP Certificate Type Manufacture Installed	
	AP Mode Bridge	AP Serial Number WCN1011000C	
	Operational Status Registered		
	Registered Controller 10.32.32.12	Unique Device Identifier(UDI)	
	Primary Controller Cisco_ff:7a:a3	Name Circo AB	
	Port Number 29	Description Cisco Wirelass Access Daint	
Alarm Summary 획	Map Location <u>Greggs Map > sdfs > sdfsa</u>	Description Cisco Wireless Access Point	
Roque AP 0 940	Statistics Timer 180	Version Id V01	
Coverage Hole 0	AP Temperature 9F/-12C	Serial Number WCN1011000C	
Security <mark>5</mark> 00	Heater Status Off	Scharwander WCMIDII000C	
Controllers 0 0 0 Access Points <mark>39 0 30</mark> Mesh Links 16 20 2	Run Ping Test	Alarms	
Location 0 0 0		Events	

Figure 6-29 AP Name > General Properties Page

To add, remove, or reorder columns in the table, click the Edit View link. Table 6-17 displays optional access point parameters available from the Edit View window.

Column	Options
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 $4 \ge 0.5 - 2$ 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 6-17 Monitor Access Points Additional Search Results Parameters

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.
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.
Node Hops	Indicates the number of hops between access point.
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.
Radio MAC	Indicates the radio's MAC address.
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.
WLAN Override Names	Indicates the WLAN override profile names.
WLAN Override	Indicates whether WLAN Override is enabled or disabled.

 Table 6-17
 Monitor Access Points Additional Search Results Parameters

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 6-30).

<u>Note</u>

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 6-30). A three-tabbed Mesh Statistics panel appears.



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.

<u>Note</u>

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.

ahaha	Wireless Control System Username: root Logout Refre	esh F 🔨
CISCO	Monitor ▼ Reports ▼ Configure ▼ Location ▼ Administration ▼ Help ▼	
Quick Search	Access Points > indoor-mesh-44-1240-rap1	
<ip, go<="" name,ssii="" th=""><th>General Interfaces CDP Neighbors Mesh Links Mesh Statistics</th><th></th></ip,>	General Interfaces CDP Neighbors Mesh Links Mesh Statistics	
Search Access Points	Bridging Queue Security	
New Search		
Saved Searches Edit	Bridging	
Select Search	Role RAP (RootAP)	=
	Bridge Group Name mesh-1240	
	Backhaul Interface 802.11a	
Alarm Summary 획	Routing State Maint	
Rogue AP 0 0 233	3 Malformed Neighbor Packets 0	
Coverage Hole 0 0 0	Poor Neighbor SNR O	
Security <u>19</u> 0 <u>1</u>	Excluded Packets 0	
Access Points 0 0 $\frac{2}{2}$	Insufficient Memory 0	
Location 0 0 0	Rx Neighbor Requests 3015	
Mesh Links 0 <u>78</u> 46	6 Rs Neighbor Responses 0	
wcs o o	Tx Neighbor Requests 0	
	Tx Neighbor Responses 3015 Mach Link Alarms	
	Parent Changes 1	
	Neighbor Timeouts 0	
	Node Hops <u>O</u> <u>Mesh Link Events</u>	

Figure 6-30 Monitor > Access Points > AP Name > Mesh Statistics

Summaries of the Bridging, Queue and Security Statistics and their definitions are provided in Table 6-18, Table 6-19 and Table 6-20 respectively.

Table 6-18 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.

Parameter	Description
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 6-18	Bridging Mesh Statistics (continued)
	Dhaging mean blatistics (continued)

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 6-19 Queue 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.
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.

Table 6-20 Security Mesh Statistics

Parameter	Description
Reassociation Request Success	Summarizes the total number of successful reassociation requests between the selected mesh access point and its parent.
Reassociation Request Timeouts	Summarizes the total number of reassociation request timeouts between the selected mesh access point and its parent.
Reauthentication Request Failures	Summarizes the total number of failed reauthentication requests between the selected mesh access point and its parent.
Reauthentication Request Success	Summarizes the total number of successful reauthentication requests that occurred between the selected mesh access point and its parent.
Reauthentication Request Timeouts	Summarizes the total number of reauthentication request timeouts that occurred between the selected mesh access point and its parent.
Unknown Association Requests	Summarizes the total number of unknown association requests received by the parent mesh access point from its child. The unknown association requests often occur when a child is an unknown neighbor mesh access point.
Unknown Reassociation Request	Summarizes the total number of unknown reassociation requests received by the parent mesh access point from a child. This might happen when a child mesh access point is an unknown neighbor.
Unknown Reauthentication Request	Summarizes the total number of unknown reauthentication requests received by the parent mesh access point node from its child. This might occur when a child mesh access point is an unknown neighbor.

Table 6-20	Security Mesh	Statistics	(continued)

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 6-31).

ahaha	Wireless Control System	ne: root Logout Refresh Print View 🔮
CISCO	Monitor ▼ Reports ▼ Configure ▼ Location ▼ Administration ▼ Help ▼	
Contributing APs indoor-mesh-44- map2 □ indoor mesh 44	<u>Maps</u> > <u>San Jose Campus</u> > Buildings Zoom Refresh	Select a command 💟 GO
Refresh Heatmap	✓ Layers IOO % ✓ 5 min ✓ Full Screen ✓ Access Points → ✓ AP Heatmans	
Loading Mesh Info Done. Loading Chokepoints Loaded 0 chokepoints Done.	 ✓ AP Mesh Info ✓ Grid ✓ coverageAreas ✓ Markers ✓ Chokepoints 	indoor-mesh-44-rap1
Alarm Summary Rogue AP 0 520 Coverage Hole 0 0 Security 0 0 0 Controllers 0 0 0 Access Points 1 0 0 Location 0 0 0	Save Settings Image: Save Settings <t< th=""><th>indoor-mesh-44-map2</th></t<>	indoor-mesh-44-map2

Figure 6-31 Monitor > Maps > Selected Map

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

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 6-31, 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 6-21 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.

Note

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.

Table 6-21 Bridging Link Information

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.



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

Table 6-22 Definition for SNR and Packet Error Rate Link Cold

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%)



The Link label and color settings are reflected on the map immediately (see Figure 6-32). 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 6-23.

Table 6-23 Quick Selection Option

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.



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

<u>Note</u>

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 6-32 Mesh Filter and Hope Count Configuration Panel

Monitoring Channel Width

Follow these steps to view the channel width.

- Step 1 Choose Monitor > Access Points.
- **Step 2** Click an access point from the AP Name column.
- Step 3 Click the Interfaces tab. The Interfaces tab as shown in Figure 6-33 appears.

alulu	Wireless Contr	ol System	Virtu	al Domain: root	Username: root Lopout Refresh Print View	×
CISCO	🖨 Monitor •	Reports . Configure . Mg	ality - Adminis	tration · Tools · Help	,▼),	
Quick Search	Access Points > A	P4				
Search Access Points	Radio Interfaces					
Saved Searches Edit	Protocol Admin	Status Channel Number	Power Level	Channel Bandwidth	Antenna	
Select Search	602.11a Enable 602.11b/g Enable	161*	1*	NA NA	AIR-ANT5135D-R AIR-ANT4941	
Alarm Summary ^Q Malicious AP						
Coverage Hole 0 0 0 Security 2 0 4						
Controllers 11 2 1 Access Points 2 0 8						5
Location 0 0 4 Mesh Links 0 0 0						

Figure 6-33 Interfaces Tab

Step 4 The Interfaces tab displays the following parameters.

Table 6-24	Interfaces Ta	b Parameters
------------	---------------	--------------

Parameter	Description					
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.					
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 Bandwidth Indicates the channel width for this radio interface. See "Configuring 40-MHz Channel Bonding" section on pag 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 Name	Identifies the type of antenna.					

Viewing Google Earth Maps

Follow these steps to view Google Earth maps. Refer to Chapter 18, "Google Earth Maps," for further information.

Step 1 Log in to WCS.

- **Step 2** Choose **Monitor > Google Earth Maps**. The Google Earth Maps window 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 window 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 web site.

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

Step 1 From the Google Earth Map window, click the folder name to open the details window for this folder. The Google Earth Details window 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 window.

Google Earth Settings

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

- Step 1 Choose Monitor > Google Earth Maps.Step 2 From the Select a command drop-down menu, choose Settings.
- Step 3 Click GO.
- **Step 4** 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

n 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 window.



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

 Access Points—From the drop-down menu, 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 menu, 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 menu (- 60 to 90 dBm).



- te 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 menu. Choose Link SNR or Packet Error Rate from the Link Color drop-down menu.



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

Step 5 Click **Save** to confirm these changes or **Cancel** to close the window without saving the changes.

Viewing Clients Identified as WGBs

When you click Monitor > WGB, you get a list of all clients identified as a workgroup bridges (see Figure 6-34). 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 6-34 Monitor > WGBs

Clients(detected as WGBs) (Edit View)

This page lists the Clients identified as Work Group Bridge.

<u>User</u>	Vendor	IP Addr	MAC Addr	AP	Controller	Port	Loc Server	802.11 State	Profile Name	<u>SSID</u>	Authenticat
<none></none>	Cisco	10.32.33.139	00:17:94:5c:05:10	<u>SJC14-</u> <u>42A-</u> <u>AP-C2</u>	10.32.32.9	1	<unknown></unknown>	Associated	wgbme	wgbme	Yes
<none></none>	Cisco	10.32.33.110	00:19:30:f0:39:c6	<u>SJC14-</u> 42A- <u>AP-C2</u>	10.32.32.9	1	<unknown></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 6-36 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 6-35).



Figure 6-35 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**.

Cisco Wireless Control System Configuration Guide

Figure 6-36 shows a sample Cisco Compatible Extensions link test result and Figure 6-37 shows a sample ping test result.

User	Vendor	IP Addr 1	MAC Addr		AP	Controller	Port	802.11	State	SSID	Authen
<none></none>	Intel	0.0.0.0	00:0c:f1:1b:e	f:69	ap:14:08:50	10.76.109.113	1	Probing			No
<u><none></none></u>	Actiontec	0.0.0.0	00:20:e0:37:4	44:bd	ap:14:08:50	10.76.109.113	1	Probing			No
<u><none></none></u>	,	Link 1	Test from co	ntrol	ler 10 76 10	9 113 to Client	MAC	00.40.9	6'ad'6	7.45	
<none></none>		LIIIK				51115 to enem	5111415	0011012		1119	
<none></none>		Link Test	Statistics		Packe	ts Transmitte	d at d	ifferent	Data I	Rates	
<pre><none></none></pre>			Uplink	Downl	link	Data Rate (Mbps)	Upl	ink	Downlink
The second secon											
	Minimun	n RSSI(dBm)	-66	-6	6	1			()	0
rahul	Minimur Maximu	n RSSI(dBm) m RSSI(dBm)	-66 -64	-6 -6	6 0	1			()	0
<u>rahul</u>	Minimun Maximu Average	n RSSI(dBm) m RSSI(dBm) e RSSI(dBm)	-66 -64 -64	-6 -6 -6	6 0 2	1 2 5.5			(()))	0 0 0 0
<u>rahul</u>	Minimur Maximu Average Minimur	n RSSI(dBm) m RSSI(dBm) e RSSI(dBm) n SNR(dB)	-66 -64 -64 29	-6 -6 -6	6 0 2 1	1 2 5.5 6			((()))	0 0 0 0
<u>rahul</u> <none></none>	Minimun Maximu Average Minimun Maximu	n RSSI(dBm) m RSSI(dBm) e RSSI(dBm) n SNR(dB) m SNR(dB)	-66 -64 -64 29 31	-6 -6 -6 11	6 0 2 1 1	1 2 5.5 6 9))))	0 0 0 0 0
<u>rahul</u> <u><none></none></u>	Minimun Maximu Average Minimun Maximu Average	n RSSI(dBm) m RSSI(dBm) e RSSI(dBm) n SNR(dB) m SNR(dB) e SNR(dB)	-66 -64 -64 29 31 30	-6 -6 -6 11 11	6 0 2 1 1 1	1 2 5.5 6 9 11)))))	0 0 0 0 0
<u>rahul</u> <u><none></none></u> <u><none></none></u>	Minimun Maximu Average Minimun Maximu Average Packets	n RSSI(dBm) m RSSI(dBm) e RSSI(dBm) n SNR(dB) m SNR(dB) e SNR(dB) SNR(dB) Sent Count	-66 -64 -64 29 31 30 20	-6 -6 -6 11 11 11 21	6	1 2 5.5 6 9 11 12))))))	0 0 0 0 0 0
rahul <none> <none></none></none>	Minimun Maximu Average Minimun Maximu Average Packets Retries	n RSSI(dBm) m RSSI(dBm) e RSSI(dBm) n SNR(dB) m SNR(dB) e SNR(dB) Sent Count Packet Count	-66 -64 -64 29 31 30 20 1	6 6 11 11 11 20 1	6 0 2 1 1 1 0	1 2 5.5 6 9 11 12 18)))))))	0 0 0 0 0 0 0
<u>rahul</u> <none> <none></none></none>	Minimun Maximu Average Minimun Maximu Average Packets Retries Max. Re	n RSSI(dBm) m RSSI(dBm) e RSSI(dBm) n SNR(dB) m SNR(dB) e SNR(dB) Sent Count Packet Count try of One Pack	-66 -64 -64 29 31 30 20 1 xet 1	6 6 11 11 11 21 21 11 21	6 0 2 1 1 0	1 2 5.5 6 9 11 12 12 18 24))))))))	0 0 0 0 0 0 0 0 0
<u>rahul</u> <u><none></none></u> <u><none></none></u>	Minimun Maximu Average Minimun Maximu Average Packets Retries Max. Re Lost Pac	n RSSI(dBm) m RSSI(dBm) e RSSI(dBm) n SNR(dB) m SNR(dB) e SNR(dB) Sent Count Packet Count try of One Pack ket Count	-66 -64 -64 29 31 30 20 1 .et 1 0	6 6 11 11 11 20 11 11 21 11 11 0	6 0 2 1 1 0	1 2 5.5 6 9 11 12 18 24 24 36)))))))))	0 0 0 0 0 0 0 0 0 0 0 0 18
<u>rahul</u> <u><none≻< u=""> <u><none≻< u=""></none≻<></u></none≻<></u>	Minimun Average Minimun Average Packets Retries Max. Re Lost Pac	n RSSI(dBm) m RSSI(dBm) e RSSI(dBm) n SNR(dB) m SNR(dB) e SNR(dB) Sent Count Packet Count try of One Pack ket Count Global S	-66 -64 -69 31 30 20 1 :et 1 0 tatistics	6 6 11 11 11 2(1 1 1 1 0	6 0 2 1 1 0	1 2 5.5 6 9 11 12 18 24 36 36 48))))))))))))))))	0 0 0 0 0 0 0 0 0 0 0 18 2
<u>rahul</u> <none> <none></none></none>	Minimur Maximu Average Minimur Maximu Average Packets Retries Max. Re Lost Pac	n RSSI(dBm) m RSSI(dBm) e RSSI(dBm) n SNR(dB) m SNR(dB) e SNR(dB) Sent Count Packet Count try of One Pack ket Count Global S	-66 -64 -9 31 30 20 1 et 1 0 tatistics	6 6 11 11 11 20 1 1 1 1 0	6 0 2 1 1 0	1 2 5.5 6 9 9 11 12 18 24 36 48 54)))))))))))))))))))	0 0 0 0 0 0 0 0 0 18 2 0
<u>rahul</u> <u><none></none></u> <u><none></none></u>	Minimum Average Minimum Average Packets Retries Max. Ret Lost Pac	n RSSI(dBm) m RSSI(dBm) e RSSI(dBm) n SNR(dB) e SNR(dB) s SNR(dB) Sent Count Packet Count try of One Pack cket Count Global S ckets Lost	-66 -64 -64 29 31 30 20 1 :et 1 0 tatistics 0	6 6 -11 11 11 20 11 11 20 11 11 0	6 0 2 1 1 0 0	1 2 5.5 6 9 11 12 18 24 36 48 54)))))))))))))))))))	0 0 0 0 0 0 0 0 18 2 0 0

Figure 6-36 Cisco Compatible Extensions Link Test Result

Figure 6-37 Ping Test Result

Link T	est from Controller 10.76.109. MAC 00:0c:f1:1b:f4:60	121 to	Client
	Link Test Packets Sent	0	1
	Link Test Packets Received	20	
	Local Signal Strength(dBm)	202	
	Local Signal to Noise Ratio(dB)	31	

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 6-38).

ahaha	Wireles	s Contro	ol System	n			Username: root Logo	ut Refresh Print View
CISCO	<u>M</u> onitor 🔻	<u>R</u> eports 🔻	<u>C</u> onfigure 🔻	Location 🔻	<u>A</u> dministration	•		
Search Controllers	Controll	ers > Sear	ch Results					
New Search	(Edit View)							
Saved Searches Edit	IP Addre	<u>ss Cont</u>	roller Name	Туре		<u>Location</u>	Mobility Group Name	<u>Reachability Status</u>
Select Search 💌	172.19.35	. <u>26</u> CJ-44	402	4400			default	Reachable
	10.32.32.1	. <u>27</u> WCS 17 Cisco	-Beringer-Dev	4400 WiSM (:	Slot 0.Port 0)	IDF 2.2	akita	Reachable
Alarm Summary								
Rogues 0 143	2							
Coverage 0 Security 28 0 0								
Controllers 1 1 0								
Access Points 6 0 12 Mesh Links 0 0 0								738
Location 0 0 19								230

Figure 6-38 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 6-39). 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.

Edit View Window

Figure 6-39

ahaha	Wireless Control System	/iew
CISCO	Monitor • Reports • Configure • Location • Administration • Help •	
	Edit View	
	Use the Show/Hide buttons to specify the information to display in this view for this user. Use the Up/Down buttons to specify the ord which the information appears in the table.	er in
	To set to the default view and order click reset. Reset	
	Primary Controller Radio Map Location Controllers Map Location Controllers AP Mode Oper Status Alarm Status Up Serial Number Down	
Alarm Summary	submit Cancel	
Rogues 0 Coverage 0 Security 30 0 Controllers 1 1 Access Points 6 0 Mesh Links 0 0		

Step 3 Click the IP address of the controller (seen in Figure 6-38) whose UDI information you want to

ep 3	Click the IP address of the controller (seen in Figure 6-38) whose UDI information you want to retrieve.
	Data elements of the controller UDI display. These elements are described in Table 6-25 and Table 6-26:

Parameter	Description				
General Portion					
IP Address	Local network IP address of the controller management interface.				
Name	User-defined name of the controller.				
Туре	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.				
Power Supply One	Indicates the presence or absence of a power supply and its operations state.				

Table 6-25Controllers Summary

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 PresentDisplays 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 6-26 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 6-25	Controllers Summary	(continued)
------------	---------------------	-------------

Table 6-26 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

I

Type of Controller	Maximum Number of Crypto Cards
Cisco 4100 Series	One
Cisco 4400 Series	Two

Table 6-26 Maximum Number of Crypto Cards That Can Be Installed on a Cisco Wireless LAN Controller Controller

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 the "Finding Coverage Holes" section on page 5-9.



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, choose **Pre-coverage Hole** from the Event Category drop-down menu on the left sidebar and click **Search**.

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

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: $1 = Maximum power allowed per country code setting, 2 = 50\% power, 3 = 25\% power, 4 = 6.25 to 12.5% power, and 5 = 0.195 to 6.25% power.$

 Table 6-27
 Pre-Coverage Hole Parameters

Parameter	Description
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)
Date/Time	The date and time the event occurred. Click the title to toggle between ascending and descending order.

 Table 6-27
 Pre-Coverage Hole Parameters (continued)

Step 3 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 window appears (see Figure 6-40).

Figure 6-40	DHCP Statistics Window	
-------------	------------------------	--



The DHCP Statistics screen provides the following information:

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

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.

WCS software release 5.1 introduces a snapshot of the Radio Resource Management (RRM) statistics. It helps to 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).



The RRM dashboard information is only available for LWAPP 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 Mbps. 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 LWAPP 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 channelization allows 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.



Radios using 40-MHz channelization 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 only reduces an access point's power. However, the coverage hole algorithm can 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 LWAPP 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 6-41).

cisco	🚡 Monitor 🕶 Reports 🕶 Co	onfigure 👻 M <u>o</u> bility 👻	Administration 🔻	Tools ▼ Help ▼	
	RRM				
	RRM Statistics (Last 24 Hours)				
n Summary 🌻	Statistics	¥alue		Statistics	Las
us AP 0 0 0	Number of RF Groups	4		Total Channel Changes	
	AP's at max. power (a/n)	<u>80.00 %</u> ((4 out of 5)	Total Coverage Holes	
Ilers <u>11</u> 0 <u>1</u>	AP's at max. power (b/g/n)	<u>100.00 %</u>	(6 out of 6)		
Points <u>1</u> 0 <u>6</u>	Total Configuration Mismatches	0			
h Links 0 0 0 5 0 0 0	Channel Change Reason (a/b/g/n)			Cha	nnel Change Reason
	(Last 24 Hours)				(Last 7 Days)
	105		Signal	105	
	90		Interference	90 -	
	76		Noise	75	
	60			60	
	45		Load	45	
			Radar	~	
	30		Other	30	
	16		- I	15	
	0			o	
	802.11 a/n	802.11 b/g/n		802.11 a/n	802.11 b/g/n
	Change Reaso	1h			hange Reason
				Es BI	
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches recorde	Radio n last 24 hours nups with Configurati der Mi ed in last 24 hours (ANC	Last 24 Hrs ion Mismatches (La ismatches D/OR) All Controllers r	st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha	ive formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches recorde Coverage Hole - APs reporting co	Radio n last 24 hours oups with Configurati der Mi ed in last 24 hours (ANC coverage holes [Top	Last 24 Hrs ion Mismatches (La ismatches D/OR) All Controllers r 5] (Last 24 Hours)	Last 7 bays Hain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha	ive formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches recorde Coverage Hole - APs reporting co	Radio n last 24 hours hups with Configurati der Mi ed in last 24 hours (ANC coverage holes [Top	Last 24 Hrs ion Mismatches (La ismatches 2/OR) All Controllers r 5] (Last 24 Hours)	st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha	ive formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches recorde Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2	Radio n last 24 hours oups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top s Radi 14 hours	Last 24 Hrs ion Mismatches (La ismatches 5//OR) All Controllers r 5] (Last 24 Hours) o Ev	Last 7 Days Hain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map	ive formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches recorde Coverage Hole - APS reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max	Radio n last 24 hours ups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top : s Radi 24 hours c Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches 2/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	Last 7 Gays Hain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pr	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches records Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max	Radio n last 24 hours ups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top - s Radi 14 hours R Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches 2/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Po	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches records Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max	Radio n last 24 hours ups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top : s Radi 24 hours c Power APs (Last 24	Last 24 Hrs ion Mismatches (La ismatches 2/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	Last 7 bays Hain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Po	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lear No Configuration Mismatches recorde Coverage Hole - APS reporting of AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max	Radio n last 24 hours ups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top - s Radi 24 hours x Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches D/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	Last 7 bays Hain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pd	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Leax No Configuration Mismatches records Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max	Radio n last 24 hours ups with Configurati der Ni ed in last 24 hours (ANC overage holes [Top s Radi 24 hours E Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches D/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	Last 7 bays Prain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pr	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Leac No Configuration Mismatches records Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 100 00 00 00 00 00 00 00 00 0	Radio n last 24 hours ups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top s Radi 14 hours 14 hours 15 Power APs (Last 24	Last 24 Hrs ion Mismatches (La ismatches //OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	Last 7 bays Hain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Po	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches records Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 100 00 00 00 00 00 00 00 00 0	Radio n last 24 hours ups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top s Radi 24 hours 24 hours 25 Power APs (Last 24	Last 24 Hrs ion Mismatches (La ismatches 5/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Po	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches recorde Coverage Hole - APs reporting of AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 100 00 00 00 00 00 00 00 00 0	Radio n last 24 hours ups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top s Radi Hours Rower APs (Last 24	Last 24 Hrs ion Mismatches (La ismatches 2/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	Last 7 bays Hain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pc 00	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lear No Configuration Mismatches recorder Coverage Hole - APS reporting of AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 100 00 00 00 00 00 00 00 00 0	Radio n last 24 hours ups with Configurati der Mi di n last 24 hours (ANC overage holes [Top - s Radi 24 hours x Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches D/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	Last 7 bays Hain Cau st 24 Hours) <u>Yiew All</u> Last Change nay be RF Leader and may not ha <u>Yiew All</u> ents RF Group Map Aggr. Pd 00 00 00 00 00 00 00 00 00 00 00 00 00	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lear No Configuration Mismatches recorder Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 100 100 100 100 100 100 100 10	Radio n last 24 hours ups with Configuration der Ni ed in last 24 hours (ANC overage holes [Top - s Radi 24 hours E Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches D/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	Last 7 bays Hain Cause st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pe	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches recorder Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 100 100 100 100 100 100 100 100 100 10	Radio n last 24 hours ups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top s Radi 14 hours 14 hours 15 Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches //OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	Last 7 bays Hain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pc 00	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches records Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 100	Radio n last 24 hours ups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top s Radi Hours Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches)/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pc 90	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lear No Configuration Mismatches recorder Coverage Hole - APS reporting of AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 100	Radio n last 24 hours ups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top - s Radi 24 hours x Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches D/OR) All Controllers r S] (Last 24 Hours) o Ev 4 Hours)	Last 7 bays Hain Cau st 24 Hours) <u>Yiew All</u> Last Change nay be RF Leader and may not ha <u>Yiew All</u> ents RF Group Map Aggr. Po 00 00 00 00 00 00 00 00 00 0	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Leas No Configuration Mismatches records Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 100 00 00 00 00 00 00 00 00 0	Radio n last 24 hours ups with Configuration der Ni ed in last 24 hours (ANC overage holes [Top - s Radi 24 hours Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches D/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours)	Last 7 bays Hain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pe 100 100 100 100 100 100 100 10	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lear No Configuration Mismatches recorder Coverage Hole - APs reporting of AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 100 10 10 10 10 10 10 10 10 1	Radio n last 24 hours ups with Configuration der Nil ed in last 24 hours (ANC overage holes [Top - s Radi Phours Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches 5/OR) All Controllers r 5] (Last 24 Hours) 0 Ev 4 Hours)	Last 7 bays Hain Cause st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pe	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches records Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 100	Radio n last 24 hours ups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top s Radi 14 hours Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches //OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours) 12.00 13.00 14.00	Last 7 bays Hain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pt 00 00 00 00 00 00 00 00 00 00 00 00 00	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lead No Configuration Mismatches records Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 00 00 00 00 00 00 00 00 00 0	Radio n last 24 hours ups with Configurati der Mi ed in last 24 hours (ANC overage holes [Top s Radi t4 hours c Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches)/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours) 12:00 13:00 14:00 r(b/g/n)	Last 7 bays Hain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pc 00 00 00 00 00 00 00 00 00 00 00 00 00	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Leav No Configuration Mismatches records Coverage Hole - APs reporting co AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 00 00 00 00 00 00 00 00 00 0	Radio n last 24 hours ups with Configuration der Mile din last 24 hours (ANC overage holes [Top is Radi 14 hours Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches)/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours) 12.00 13.00 14.00 r(b/g/n)	st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pr 10 10 10 10 10 10 10 10 10 10 10 10 10	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lean No Configuration Mismatches recorder Coverage Hole - APS reporting of AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 00 00 00 00 00 00 00 00 00 0	Radio n last 24 hours ups with Configurati der Ni ed in last 24 hours s Radi r Power APs (Last 2- Control of the second secon	Last 24 Hrs ion Mismatches (La ismatches D/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours) 12:00 13:00 14:00 r(b/g/n) E er [Top 5] (Last 24	Last 7 bays Frain Cau st 24 Hours) <u>Yiew All</u> Last Change may be RF Leader and may not ha <u>Yiew All</u> ents RF Group Map Aggr. Po 00 00 00 00 00 00 00 00 00 0	ve formed RF Groups
	AP Name MAC Address No RRM Channel changes recorded in Configuration Mismatch - RF Gro RF Group Lear No Configuration Mismatches records Coverage Hole - APs reporting of AP Name MAC Address No Coverage holes detected in last 2 Aggr. Percent Max 100	Radio n last 24 hours ups with Configuration der Mile din last 24 hours (ANC overage holes [Top - s Radi A hours Power APs (Last 2-	Last 24 Hrs ion Mismatches (La ismatches)/OR) All Controllers r 5] (Last 24 Hours) o Ev 4 Hours) 12:00 13:00 14:00 r(b/g/n) er [Top 5] (Last 24	Last 7 bays Hain Cau st 24 Hours) <u>View All</u> Last Change nay be RF Leader and may not ha <u>View All</u> ents RF Group Map Aggr. Pd 00 00 00 00 00 00 00 00 00 00 00 00 00	ve formed RF Groups

Figure 6-41 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 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.



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 LWAPP 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 LWAPP 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.





٠

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