Cisco Unified Wireless Control System

Introduction

The modern day Wi-Fi 802.11 wireless network has evolved to become an integral part of the overall enterprise infrastructure, and because such organizations are seeking similar capabilities from their wireless systems management as they have from their enterprise infrastructure management systems in the past. IT managers and other networking professionals expect capabilities in such tools, enabling them to ensure their mission-critical wireless network systems are reliable, available, and performing optimally. A robust and reliable centralized network management solution capable of uniformly managing geographically disparate WLANs is necessary to simplify operations and to reduce total cost of ownership.

This chapter describes the Cisco Wireless Control System (WCS) and addresses management considerations that you should consider when using it to design, deploy, and manage your enterprise wireless LAN. It is intended for the reader responsible for performing such tasks using Cisco Unified Wireless Network (UWN) technology.

The following sections discuss various areas of WLAN management including wireless LAN configuration and monitoring, RF management and system planning, intrusion monitoring, and location tracking as follows:

- Wireless Control System Overview—Describes network management in general, along with a brief overview of the Cisco Wireless Control System (WCS).
- Role of WCS Within the Unified Wireless Network Architecture—Describes the overall network architecture and illustrates management data flows.
- How WCS can be used to define and configure devices within your wireless network.
- Using WCS to Monitor Your Wireless Network—Discusses how to use WCS to monitor your network in daily operation. A detailed explanation of the relationship between traps, events, alarms, and notifications can be found in this section and should be valuable to anyone considering using WCS to alert management and other personnel.
- Using WCS to Locate Devices in Your Wireless Network—Examines how WCS can provide on-demand location of WLAN clients, asset tags, and rogues. The use of the Cisco Wireless Location Appliance is also discussed with references provided to comprehensive sources of information on Cisco Location-Based Services (LBS).
- Using WCS to Efficiently Deploy Your Wireless Network—Suggests aspects of WCS that you can use to assist you with efficient deployment of a multi-site wireless network.

- Traffic Considerations When Using WCS in Large Networks—Discusses the traffic generated by polling and other sources within WCS. Those users planning very large, multi-server implementations over remote networks should consider the information in this section when making planning and design decisions.
- Administering WCS—Examines WCS scheduled tasks, users, and database administration.

Wireless Control System Overview

The Cisco Wireless Control System (WCS) is a component of the Cisco Unified Wireless Network (UWN) that provides a powerful network management solution allowing the design, control, and monitoring of enterprise wireless networks from a centralized location. The benefit of this is simplified operations and reduced total cost of ownership because network administrators now have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and general WLAN systems management. WCS enhances the management and control capabilities already present in the Cisco UWM via the WLAN controller web user interface and command line interface (CLI).

WCS makes it possible for the point of control in an enterprise WLAN to move from individual controllers to a network of controllers. WCS provides graphical views of multiple controller hardware formats and offers a comparable level of configuration, performance monitoring, accounting, security, and fault management to that offered at the controller level.

WCS functionality can be grouped into the following areas:

- Network monitoring and troubleshooting

  Cisco WCS provides tools that enables the visualization of wireless networks as well as the monitoring of ongoing WLAN performance. Cisco WCS also provides a portal into the real-time RF management capabilities provided by Cisco wireless LAN controllers including automated channel assignments and access point transmit power settings. Quick visibility into coverage holes, device status alarms, and key usage statistics is provided for easy WLAN monitoring and troubleshooting.

- Indoor location tracking

  Cisco WCS provides you with the ability to efficiently track wireless devices, including Wi-Fi enabled laptops, PDAs, and voice handsets as well as mobile assets equipped with Wi-Fi 802.11 active RFID tags. The base version of WCS can determine with which access point a wireless device is associated and provides a general idea of where wireless devices are situated. Environments that require more granular location services can optionally license additional location-based services capabilities within WCS and take advantage of Cisco RF Fingerprinting technology, which is capable of providing accuracy to 10 meters or better. To scale the use of location tracking beyond single threaded device localization, Cisco WCS with location can be deployed in conjunction with the Cisco Wireless Location Appliance for real-time simultaneous tracking of up to 2500 wireless devices.

- Wireless LAN planning and design

  Integrated RF prediction tools are available to create detailed wireless LAN designs, including lightweight access point placement, configuration, and performance/coverage estimates. Floor plans can be imported into Cisco WCS and RF characteristics assigned to building components to increase design accuracy. Graphical heat maps help visualize anticipated wireless LAN behavior to facilitate planning and deployment.

- Policy management and enforcement

  A full suite of tools is provided for the management and enforcement of security policies within a Cisco wireless infrastructure, including the following:

  - *Support for the Cisco Unified Intrusion Detection System/Intrusion Prevention System*—When used with a Cisco Unified IDS/IPS (part of the Cisco Self-Defending Network), the IDS/IPS device detects when an associated client sends malicious traffic through the Cisco Unified Wireless Network and sends shun requests to Cisco Wireless LAN Controllers. These controllers then in turn disassociate the client device.
  - *RF attack signatures and wireless intrusion prevention*—Customizable attack signature files can be used to rapidly detect common RF-related attacks such as denial of service (DoS), Netstumbler, and FakeAP. Cisco WCS is capable of raising alarms and generating notifications if an attack is detected. Detailed trending reports enable network administrators to identify recurring security threats before they can cause significant harm to the network.
  - *Rogue detection, location, and containment*—Cisco WCS maintains a constant vigil for unauthorized "rogue" access points, ad-hoc networks, and clients. If unauthorized rogue devices appear, Cisco WCS can be used to determine their location and assess the level of threat. If deemed malicious, containment procedures can be initiated by the WCS operator to limit the potential threat posed by these devices.
  - *Policy creation and enforcement*—Cisco WCS contains a service policy engine that allows network administrators to easily create and enforce a wide variety of network policies including virtual LAN (VLAN), RF, quality of service (QoS), and security policies. Multiple WLANs can be created with unique service set identifiers (SSIDs) and individualized security parameters. These security policies can be applied across an entire Unified Wireless Network, to specific wireless LAN controllers, or even to individual lightweight access points.
  - *User exclusion lists*—Cisco WCS can be used to proactively exclude specific users from associating with the wireless network. If unusual activity is detected, offending devices can quickly be flagged and excluded if considered to be malicious. These devices cannot access wireless LAN services until a pre-configured timer has expired or a manual override is initiated to grant wireless LAN access once again.

- Secure guest access

  Cisco WCS allows customizable guest access capabilities that allow organizations to keep their wireless networks secure while providing customers, vendors, and partners with controlled access to their WLANs. Organizations can enable the *Guest Access Lobby Ambassador* feature on the wireless LAN controller to allow for the creation of local usernames and passwords and for local or RADIUS-based authentication of guest users.

- General wireless LAN systems management
  - *Configuration*—Configuration of network components can be done via traditional manual methods on an individual basis, or WCS administrators can assign a template to one or all of the wireless LAN controllers or access points in a mobility group.
  - *Troubleshooting*—Important network information is consolidated and reported on, such as noise levels, signal-noise ratio, interference, and signal strength. This facilitates isolation and resolution of problems at all layers of a wireless network.
  - *Software updates*—Upgrades to software contained on components within the Cisco Unified Wireless Network can be performed from a centralized location.
  - *Customized reports*—Numerous reports are available that document network and system activity. These include client statistics, radio usage data, 802.11 counters, RF management configuration history, and device alarms.

Role of WCS Within the Unified Wireless Network Architecture

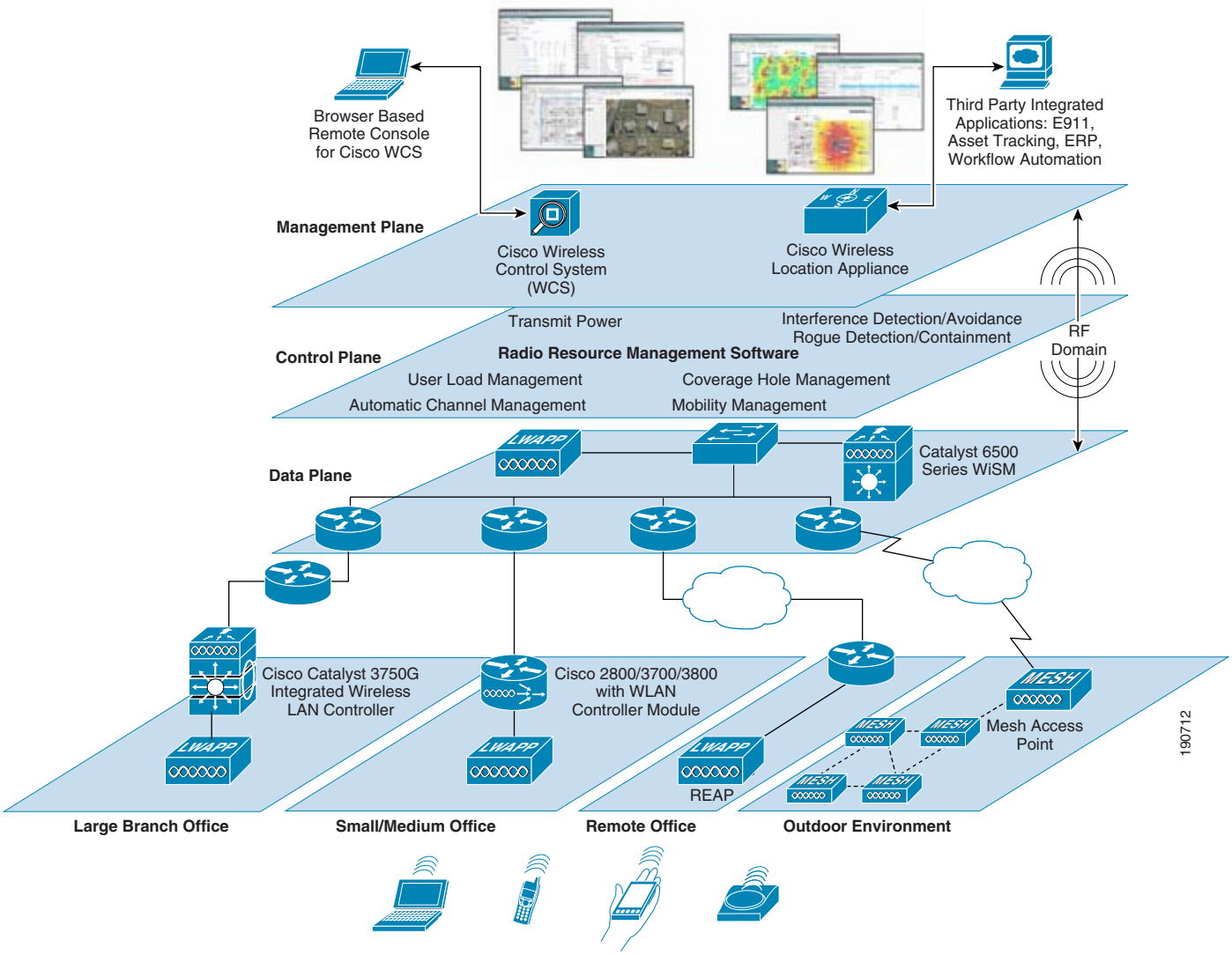
The Cisco Unified Wireless Network is designed to provide robust 802.11 wireless networking solutions for large enterprises, branch, and remote offices as well as outdoor areas. The system manages all data client communications and system administration functions, performs radio resource management (RRM), and manages system-wide mobility policies.

In this solution, the various Cisco WLAN controllers (embedded and standalone) together with their registered lightweight access points may be managed via the following:

- A controller web and command line interface (CLI)
- The Cisco Wireless Control System (WCS), which can be used to configure and monitor one or more controllers and registered access points. All Cisco wireless LAN controller models can be managed by Cisco WCS including enterprise-class standalone wireless LAN controllers such as the 4400 and 2000 Series; as well as the Cisco Catalyst 6500 Series Wireless Services Module (WiSM), the Cisco Catalyst 3750G Integrated Wireless LAN Controller, and the Cisco Wireless LAN Controller Module (WLCM) for Integrated Services Routers (ISRs)
- Other management software compliant with industry-standard SNMP v1, v2c, and v3 interfaces

Figure 8-1 shows the interoperation of WCS along with the other components of the Cisco Wireless LAN Solution when deployed in a Cisco Unified Wireless Network.

Figure 8-1 Overall Wireless Network Architecture with WCS



Various communication protocols (SNMP, SMTP, HTTP/HTTPS, FTP, TFTP, SOAP/XML, and so on) are implemented between these components to provide the management, alerting, and notification functionality necessary to efficiently manage modern enterprise wireless infrastructures.

Figure 8-2 shows the typical client/server communication flows between WCS, the client workstation browser, and the infrastructure components comprising the enterprise wireless LAN. WCS does not directly manage lightweight access points but rather communicates with SNMP agents contained within the wireless LAN controllers to which lightweight access points have been assigned. Configuration changes, inquiries, monitoring, and reporting are all handled via the exchange of SNMP traps, commands, and responses between WCS and the WLC SNMP agents. Any information or configuration requests concerning controller or access point resources are sent by WCS to these WLC SNMP agents. Working in conjunction with other controller hardware and software, these SNMP agents participate in the initiation of appropriate actions on internal controller resources, or communicate such actions to assigned lightweight access points via the lightweight access point protocol (LWAPP).

Figure 8-2 Management Data Flows within the Cisco Unified Wireless Network

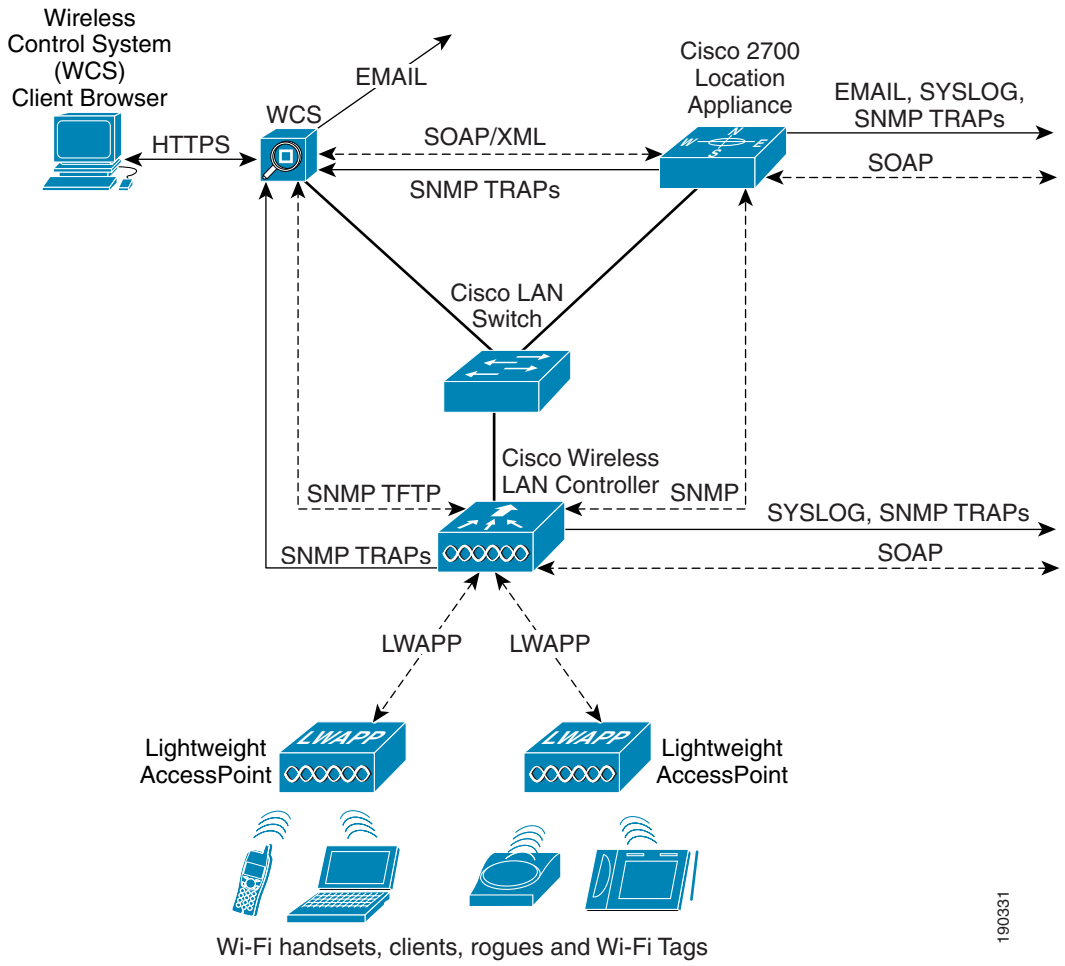


Figure 8-2 also shows the ability of controllers to transmit SNMP *traps* to up to six *trap receivers* as well as transmitting *syslog messages* to a remote syslog receiver. The ability to send traps to multiple trap receivers is useful in networks that, in addition to WCS, possess an overall enterprise network management system (NMS) that you would like to inform when traps are generated by the wireless network devices. The multiple trap capability in WLCs allow you to send traps to WCS and the enterprise NMS.

The information contained within SNMP traps and polling responses are the foundation of *events,* and based on their severity, these events can result in the triggering of WCS *alarms*. Depending on the configuration of WCS alarm *notification*, WCS can generate messages to e-mail destinations such as desktop and laptop clients, pagers, PDAs, and other systems notifying them of newly-triggered critical and coverage hole alarms.

File transfer protocols are used to update a variety of WLC software and configuration information. WCS readily accommodates this by providing for integrated TFTP and FTP server capability. WCS can also be used to configure TFTP file transfer between wireless LAN controllers and other TFTP servers that may be located closer on the network to the managed devices.

Real-time RF management is a hallmark feature of the Cisco lightweight wireless solution, and a unique product differentiator. Each WLAN controller uses dynamic algorithms to create an environment that is completely self-configuring, self-optimizing, and self-healing, making a Cisco-powered WLAN ideal for the delivery of secure and reliable business applications. This is done via specific *radio resource management (*RRM*)* functions such as the following:

- Radio resource monitoring
- Dynamic channel assignment
- Interference detection and avoidance
- Dynamic transmit power control
- Coverage hole detection and correction
- Client and network load balancing

Note Further information about RRM can be found in the RF Design chapter of this SRND. Additional information on this topic can also be found at the following URL: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml.

The Cisco WCS allows for straightforward configuration of RRM parameters that can be applied to multiple WLAN controllers using the policy template facility. If controllers detect that one or more various predefined RRM thresholds are violated, a trap is sent to the Cisco Wireless Control System (WCS). WCS provides multiple reporting facilities that can be used to view the RF environment in real time, aiding greatly in understanding what is happening in the air space and facilitating the troubleshooting process.

WCS provides both the user and control interfaces to the Cisco Wireless LAN Location Appliance, allowing simultaneous location display of WLAN clients, asset tags, rogue access points, and rogue clients. Additionally, WCS provides the ability to configure the location appliance to send various forms of user notification when changes occur in client or asset location. In this way, the location appliance can be defined to transmit messages using SOAP, SMTP, SNMP traps, or syslog messaging if clients or assets become missing, enter or leave coverage areas, or stray beyond a set distance from a pre-determined marker.

For complete information about WCS hardware and software requirements, and for complete step-by-step guidance on installing and accessing the WCS server, see the following documents:

- *Cisco Wireless Control System Configuration Guide, Release 4.0*— http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscfg40.html
- *Cisco Wireless Control System Release Notes, Release 4.0*— http://www.cisco.com/en/US/docs/wireless/wcs/release/notes/wcsrn_MR2.html

Defining Network Devices to WCS

Before being able to manage WLAN controllers and location appliances, these devices must be defined to WCS. You need to specify the IP and SNMP information necessary to communicate with each device that you wish to include in the management domain of your WCS server. After these devices are defined, they are considered to be within the *management domain* of that WCS. WCS implicitly learns of the existence of any lightweight access points registered to any WLAN controllers defined to it.

When using commands in the following subsections that allow multiple objects to be selected as targets, the selected objects must all be present on one display page. This is important, for example, if the total population of controllers displayed spans several pages and requires paging forward and backward. The selected objects cannot be present across multiple pages.

Adding Controllers to WCS

Adding Controllers

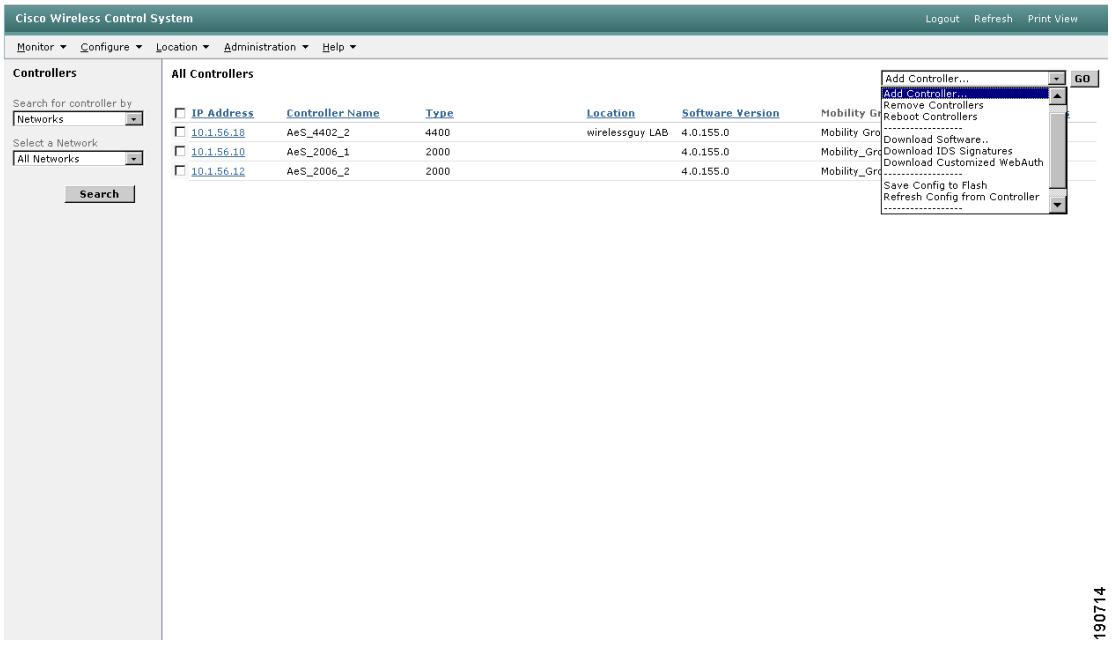
Before being defined to WCS, all WLAN controllers should be properly configured as per the *Cisco Wireless Control System Configuration Guide, Release 4.0*. Basic communication settings for each deployed WLAN controller such as IP addressing, SNMP communities, strings and passwords, SNMP version in use, and so on, should be noted before attempting to define these resource to WCS.

Define properly configured WLAN controllers to WCS as follows:

Step 1 Click **Configure > Controllers** to display the All Controllers page.

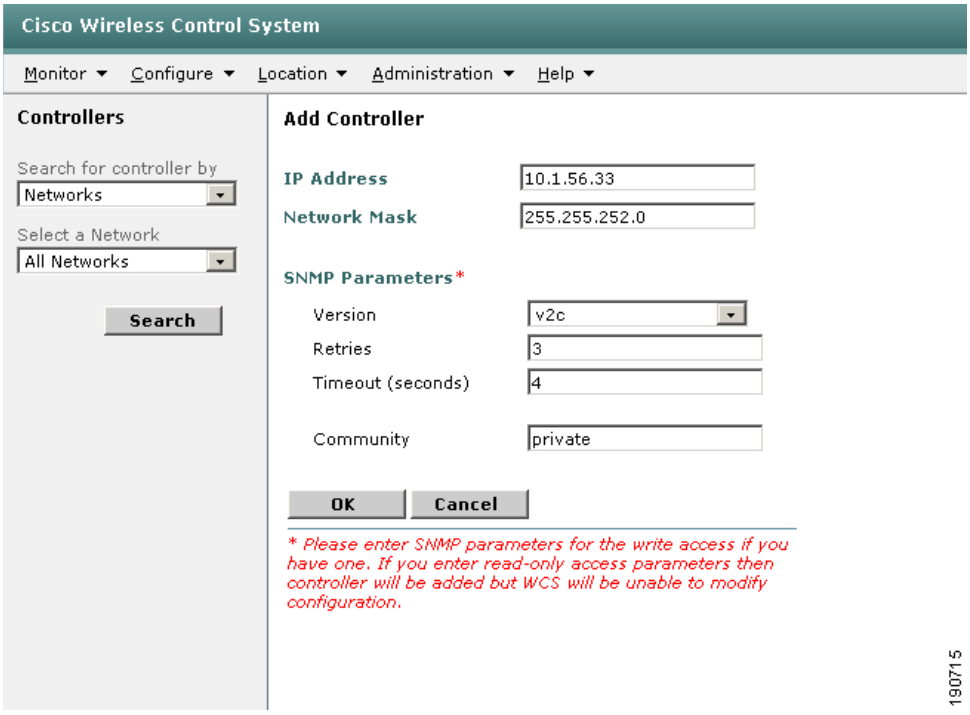
Step 2 From the command drop-down menu in the right-hand upper corner of the screen, choose **Add Controller** and click **GO,** as shown in Figure 8-3.

Figure 8-3 Adding a Controller to WCS



Step 3 On the Add Controller page, enter the controller IP address, network mask and required SNMP settings as shown in Figure 8-4.

Figure 8-4 Defining New Controller IP and SNMP Parameters



Note that if you use the SNMP read-only community string on this screen, you are able to query (but not modify) controller configurations using WCS. With SNMPv3, read-only access is achieved by specifying the name of a user profile that has been defined in the WLAN controller with an authentication password and privacy password to which read-only access has been permitted. In either case, the use of read-only credentials when attempting to modify a configuration results in a "MIB Access Failed" error message. This occurs whenever WCS attempts to modify the value of a parameter in a controller but SNMP read-only access has been specified. Note that WCS still modifies its internal database with the change even though the WLAN controller itself could not be modified because of the read-only community string. Therefore, if you receive a "MIB Access Failed" message, be sure to back out any changes made to the WCS database, either manually or by using the selective or non-selective synchronization methods described in Synchronizing WCS with Controller and Access Point Configurations, page 8-35.

Step 4 Click **OK**.

WCS displays a "Please Wait" dialog box while it contacts the controller and adds the current controller configuration to the WCS database. It then returns you to the Add Controller page.

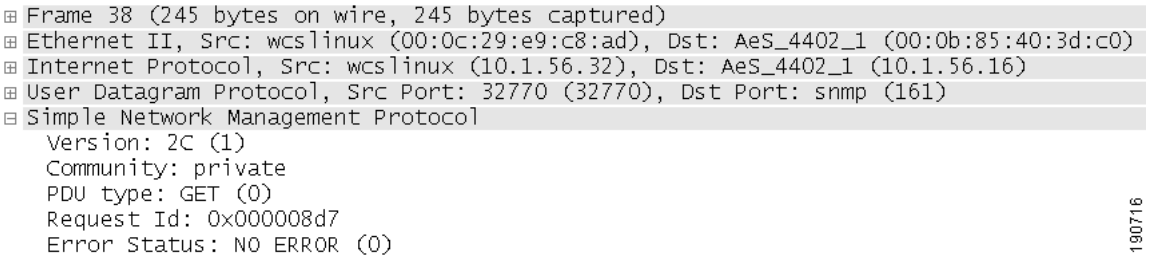
- If WCS does not find a controller at the IP address that you entered for the controller, the Discovery Status dialog displays this message: "No response from device, check SNMP communities, version or network for issues". Check these settings to correct the problem:
- The controller port IP address might be incorrect. Check the port setting on the controller.
- WCS might not have been able to contact the controller. Make sure that you can ping the controller from the WCS server operating system.
- The SNMP settings on the controller might not match the SNMP settings that you entered in WCS. To verify this, login to the controller using the web interface or the CLI and make the appropriate corrections as directed in the *Cisco Wireless Control System Configuration Guide, Release 4.0*.

Step 5 Add additional WLAN controllers by repeating these steps if desired.

Restricting SNMP v1/v2c Access using Source IP Address

SNMPv1 and SNMPv2c access to WLAN controllers is typically limited on the basis of whether the management system has been configured with the correct read-only or read-write community strings for the device. Cisco WLAN controllers allow you to add another layer of SNMP access restriction using source IP addresses as well. This makes it more difficult for an unauthorized SNMP manager that somehow has obtained your community strings from gaining control of your WLAN controllers (keep in mind that SNMP v1 and v2c community strings are sent in the clear and can easily be seen using an Ethernet protocol analyzer, as seen in Figure 8-5, where the community string is use is "private".

Figure 8-5 SNMPv2c Ethereal Trace Showing Plainly Visible Community Strings

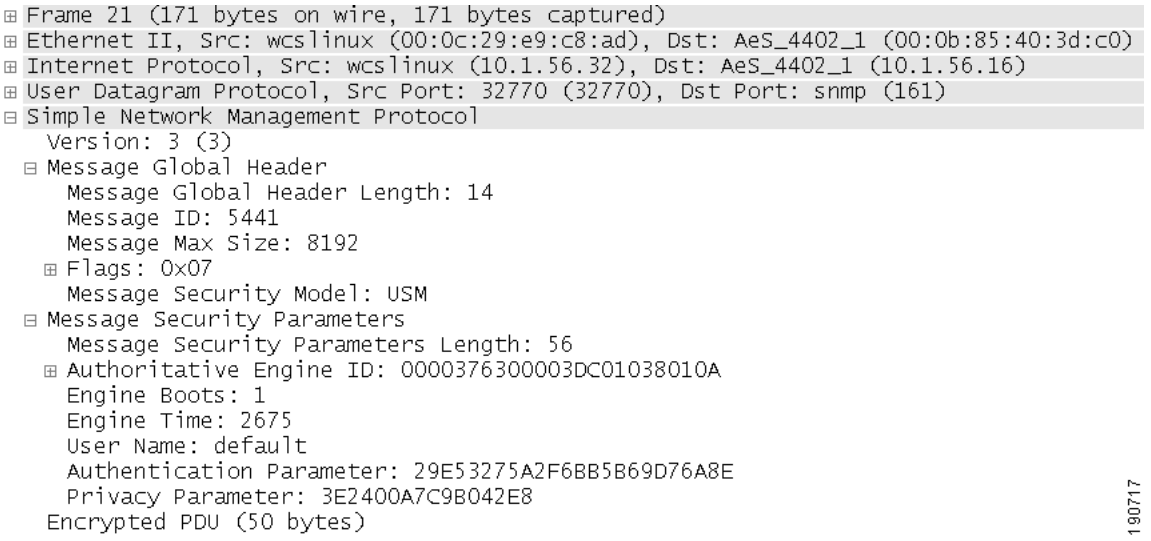


By associating valid IP addresses (or a range of addresses) with each defined community string, only SNMP v1/v2c commands coming from these sources addresses are honored by WLAN controllers so configured, even if the correct community strings are specified.

To configure your controllers in this fashion, use the **Management > Communities** menu option in the controller web interface (*not* WCS) and add IP address and netmask information to your community string definitions. You can also perform this via the controller CLI by using the **config snmp community ipaddr *ip-address ip-mask name*** command.

This source address-based restriction capability is not used with WLAN controllers using SNMPv3. SNMPv3 does *not* use community strings and sends all SNMP Protocol Data Units (PDUs) encrypted between WCS and the WLAN controllers. Figure 8-6 shows an example of a protocol analyzer trace of an encrypted SNMPv3 PDU.

Figure 8-6 Example of Encrypted SNMPv3 PDU



Further information about this capability can be found in the *Cisco Wireless Control System Configuration Guide, Release 4.0*.

Adding Location Appliances To WCS

The Cisco Wireless Location Appliance enhances the capabilities of a location-enabled WCS server by computing, collecting, and storing historical location data and allowing WCS to display graphical location information for multiple clients, tags, and rogue devices simultaneously.

Configuration of the location appliance is performed from WCS using the menus and submenus located under the main menu **Location** tab after initial configuration of IP parameter settings, as described in the *Cisco Wireless Location Appliance—Installation Guide,* available at the following URL: http://www.cisco.com/en/US/docs/wireless/location/2700/quick/guide/li31main.html.

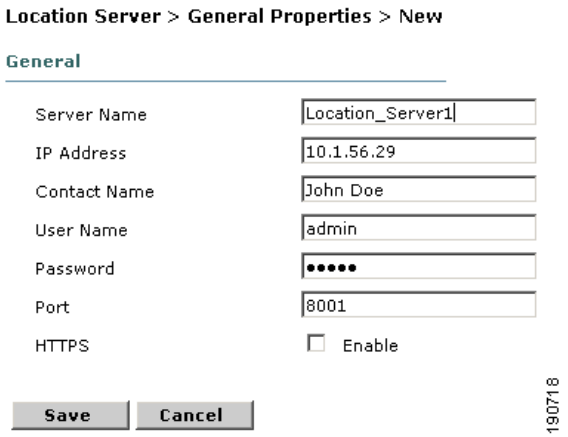
To define a location server(s) to WCS, follow these steps:

Step 1 Click **Location > Location Servers** to display the All Location Servers page.

Step 2 From the command drop-down menu in the right-hand upper corner of the screen, choose **Add Server** and click **GO.**

Step 3 Enter the required information as shown in Figure 8-7.

Figure 8-7 Defining a Location Appliance to WCS



Step 4 If you want to enable HTTPS, enable the check box only *after* completing steps 1 through 3 completely. After enabling the check box, click **GO** again.

Using WCS to Configure Your Wireless Network

Configuring Network Components

After network components have been successfully defined to WCS and two-way communication via SNMP has been established, these devices can be configured and managed centrally as part of the management domain of that WCS server. Of course, WCS allows devices to be configured one parameter screen at a time in a similar fashion to the controller web interface that is available when accessing the WLAN controller individually. However, WCS goes much further and allows for the provisioning of *policy templates* that can be applied to WLAN controllers and lightweight access points. Policy templates are groups of configuration parameters that in most cases are defined once and then applied to multiple controllers without the need to manually re-key each value and send each screen of configuration data to each controller and lightweight access point individually. After being defined and implemented in WCS, the use of policy templates greatly reduces the possibility of controller misconfiguration by ensuring that the proper values are defined once and then saved for future re-application.

When using the commands in the following subsections allowing multiple target objects to be selected, these objects *must* all be present on one display page. This is important if the total population of controllers displayed, for example, spans several pages and requires paging forward and backward.

Configuring WLAN Controllers

WCS allows for the configuration of network components via the **Configure** option on the main menu bar. WLAN controllers can be configured via **Configure > Controllers,** and lightweight access points can be configured via **Configure > Access Points**. In this manner, controller and lightweight access points can be either individually configured or the configuration that was applied to a group of devices via the application of a policy template can be overridden.

To configure a WLAN controller that is currently managed by WCS, perform the following steps:

Step 1 Click **Configure > Controllers** to display the All Controllers page. In large networks, you may find it helpful to use the "Search for Controllers" filter in the left-hand column to narrow the selection of displayed controllers by name, IP address, or network. In large networks, the listing of controllers can be sorted in ascending or descending order by clicking on the appropriate column heading.

Step 2 Click on the hyperlink representing the IP address of the WLAN controller that you want to configure. Note that configuration of a device cannot be performed by simply enabling the check box for the controller; the hyperlink for the particular WLAN controller must be used.

Step 3 On the Controller Properties screen, you may change the name assigned to this WLAN controller as well as the location text string and the controller SNMP properties.

There are also three check box fields available on the **Controller Properties** screen:

- Restore on Cold Start Trap—When this check box is enabled, WCS initiates the **Restore Config to Controller** function on reception of a SNMP cold-start trap, indicating that a WLAN controller has rebooted.

Note For further information, see section 13.7 CSCsc59232 —4400 and 2006 Controllers Not Issuing Cold Start Traps.

This procedure entails WCS refreshing the configuration in the controller from the current contents of the WCS database. This is a valuable feature designed to ensure that the configuration loaded into a freshly-booted WLAN controller is indeed the configuration of record currently contained within the WCS database. In this manner, any unauthorized local changes made to the controller configuration via the controller web interface or CLI are overridden with the configuration of record stored in the WCS database.

Note that the configuration programmed into the controller is not implicitly saved when the restore on cold-start feature is used. This means that the controller retains its original configuration in nonvolatile memory and not the changes that were transferred to it in conjunction with the cold-start restore. If this is not desired, after the controller is fully booted and has received its configuration from WCS, perform an explicit save of the running configuration of the controller to nonvolatile (flash) memory using the Save Config to Flash function as shown in Figure 8-10.

See Non-Selective Synchronization, page 8-36, for further details on the **Restore Config to Controller** function.

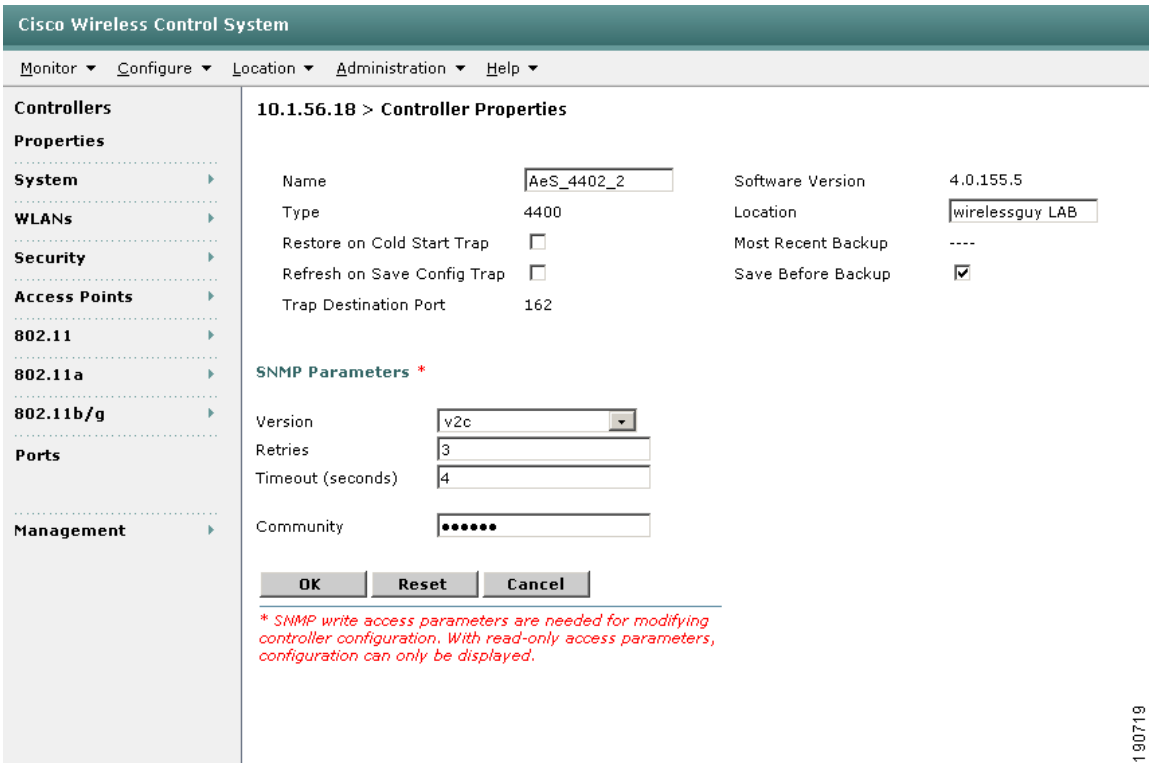
- Refresh on Save Config Trap—When this check box is enabled, WCS initiates the **Refresh Config from Controller** function upon reception of a save-config trap (bsnConfigSaved) indicating that the current configuration in the WLAN controller has been saved to the controller nonvolatile (flash) memory. WCS then refreshes the configuration contained in its databases with the current configuration of the controller. Any configuration objects found in WCS but not found in the controller configuration are retained in the WCS databases. See Non-Selective Synchronization, page 8-36 for further details on the **Refresh Config from Controller** function.

- Save Before Backup—This check box has an effect only when the **Configuration Backup** scheduled task has been enabled and submitted for execution. (An identical but independent check box appears for **Configure > Controllers > *controllerIPadddress* > System > Commands > Upload/Download Commands > Upload/Download Commands > Upload File from Controller**.)

  When enabled, **Save Before Backup** indicates that the running configuration of this controller should be saved to the nonvolatile memory of the controller before the scheduled task archiving the controller-saved configuration. Because the **Configuration Backup** scheduled task archives only the saved configuration of the controller and not the currently running configuration, enabling this check box to ensure that any recent unsaved changes are saved and therefore included in the archive. See Configuration Backup, page 8-117 for further details on the **Configuration Backup** scheduled task.

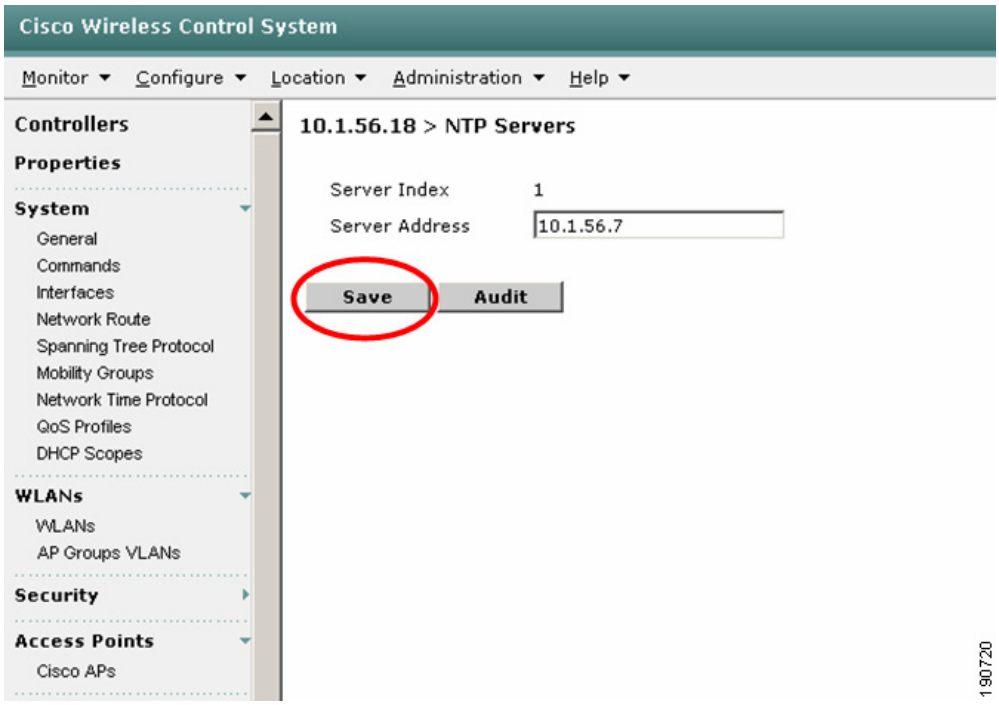
Step 4 You may now select from the list of configuration object categories listed in the column on the left-hand side of the **Controller Properties** screen as shown in Figure 8-8. Guidance on configuring the parameters contained in each of the controller configuration categories can be found in the WCS main menu bar under **Help > Online Help**.

Figure 8-8 Controller Properties



After making your desired changes in each of the various controller configuration object categories, you need to save your changes (as shown in Figure 8-9) **in each category** for your changes to be applied to the current running configuration of the controller.

Figure 8-9 Save and Apply Changes for Configuration Object Category "Network Time Protocol"



Keep in mind that the procedure outlined thus far *does not* save your changes to the nonvolatile memory of the controller (that is, your changes are lost if the controller is rebooted or loses power). To write your newly modified controller running configuration to nonvolatile memory, perform the following steps:

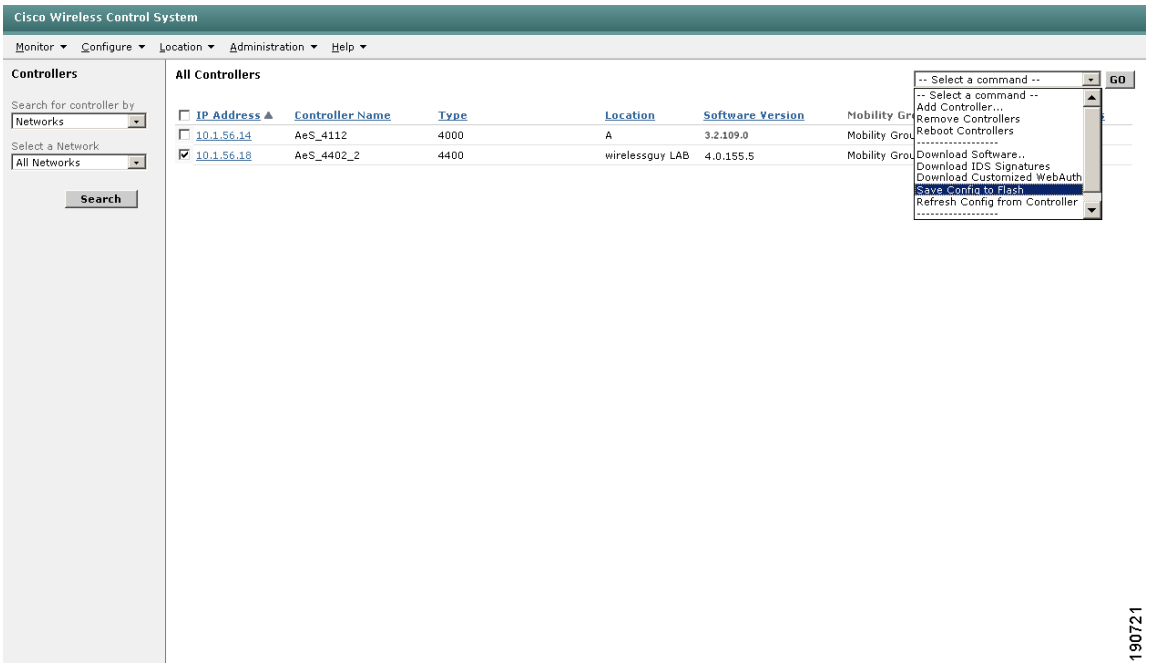
Step 1 Click **Configure > Controllers** to display the All Controllers page.

Step 2 Select the check box(es) for the controller(s) for which you want to write the running configuration to nonvolatile memory.

Step 3 From the command drop-down menu in the right-hand upper corner of the screen, choose **Save Config to Flash** (shown in Figure 8-10) and click **GO.**

The running configuration for each controller selected is written to their respective nonvolatile memories.

Figure 8-10 Saving Configuration to Controller Nonvolatile (Flash) Memory



Further guidance about configuring WLAN controllers can be found in the WCS main menu bar under **Help > Online Help**.

Configuring Lightweight Access Points

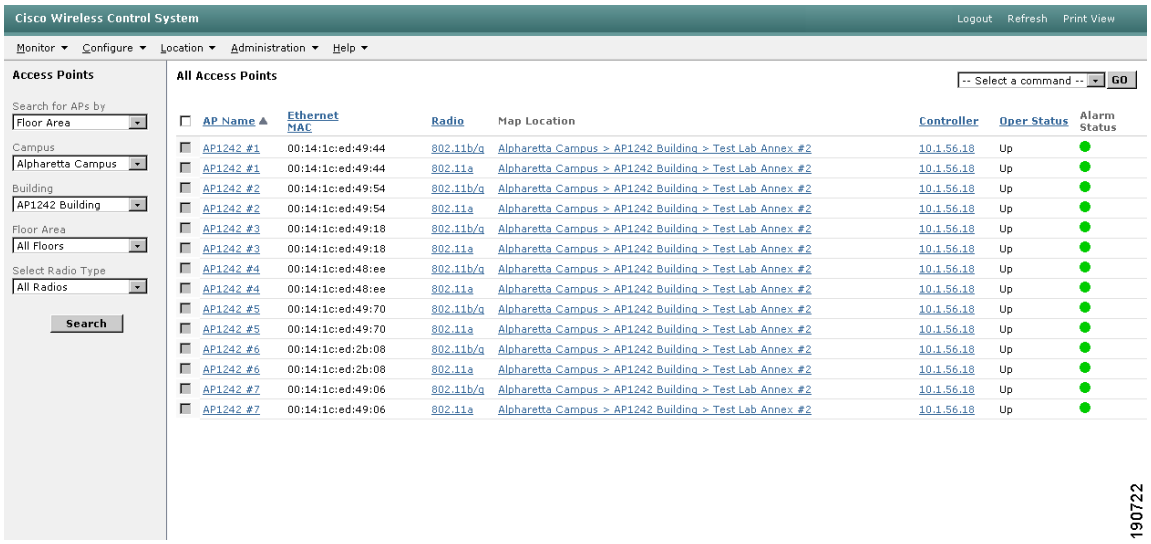
Lightweight access points can be configured using WCS in a similar fashion to that described in the previous section on WLAN controllers. As mentioned previously, WCS does not configure lightweight access points directly but rather does so via the SNMP agent and other software components present in the WLAN controller to which the lightweight access points are currently registered. Thus, only access points that are registered with controllers can ultimately be managed via WCS.

By using the **Configure > Access Points** menu option, lightweight access points can be individually configured or the configuration that was applied to a group of access points using policy templates can be overridden.

Step 1 Click **Configure > Access Points** to display the All Access Points page.

In large networks, it is helpful to narrow the listing by using the "Search for APs By" filter in the left-hand margin of the screen (see Figure 8-11). Access points can be filtered based on several filter types such as MAC addresses, AP name, assigned controller, unassociated or unassigned status and outdoor, campus, building, or floor location.

Figure 8-11 All Access Points Display Menu



Note that the All Access Points page (shown in Figure 8-11) is a bit more involved than the All Controllers page seen in previous sections. Each dual-band lightweight access point is actually represented twice in WCS with a separate line item entry for each radio interface contained within the lightweight access point. Therefore, unless a specific radio type is selected using the display filter in the left-hand column, a typical dual-band lightweight access point has two line item entries on the "All Access Points" menu. Each entry is differentiated by the values listed under the Radio column heading.

Note also that unlike in All Controllers, there is more than just a single hyperlink entry per line item in the All Access Points menu. Clicking on the AP name takes you to the general lightweight access point configuration panel, while the Radio identifier takes you directly to the submenu for a specific radio in that lightweight access point. Clicking on the Location hyperlink immediately links you to the location map where that lightweight access point has been assigned. Clicking on the Controller hyperlink takes you to the Controller Summary screen for the WLAN controller to which this lightweight access point is assigned.

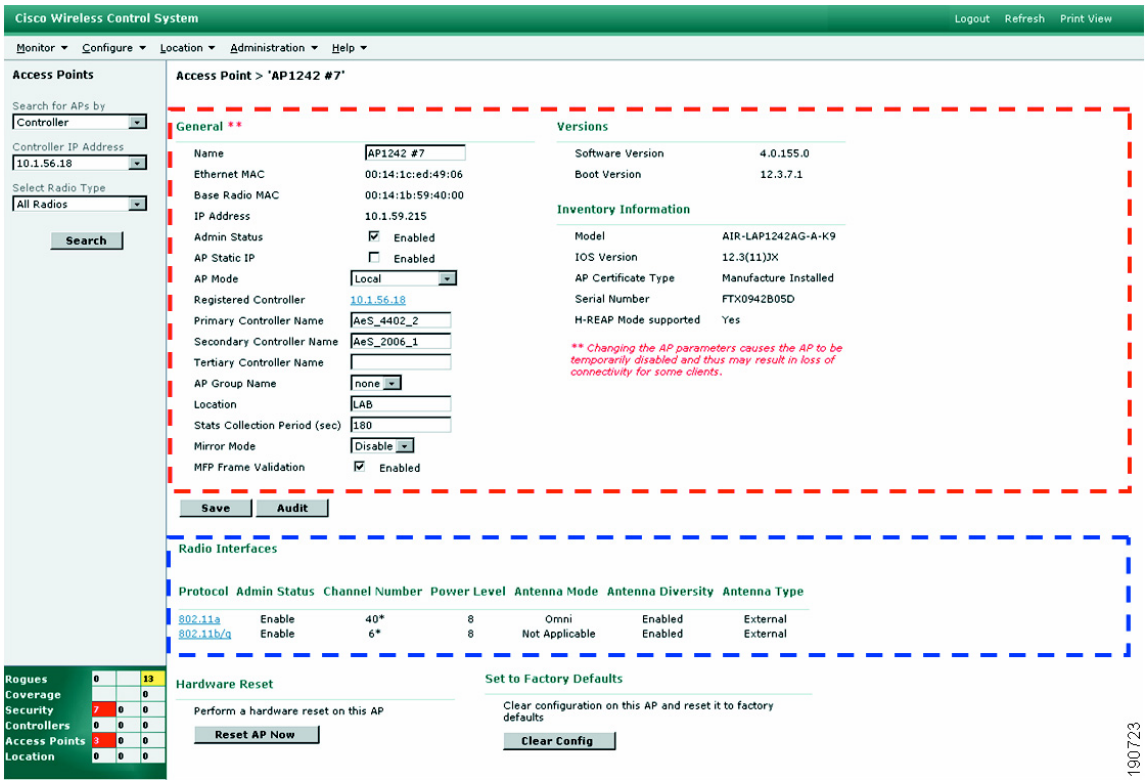
Figure 8-11 shows the All Access Points menu sorted by campus, building, and floor. Access points that are currently registered with controllers show the controller IP address as a hyperlink in the Controller column. Attempting to configure an access point that is not registered results in the error "This AP is not associated with any Controller" being displayed.

You are now ready to select an access point that is registered with a controller and to modify its configuration.

Step 2 Select the desired registered lightweight access point from the All Access Points menu by clicking on the AP name hyperlink.

Step 3 The **Access Point >** ***ap name*** screen is now displayed, as shown in Figure 8-12.

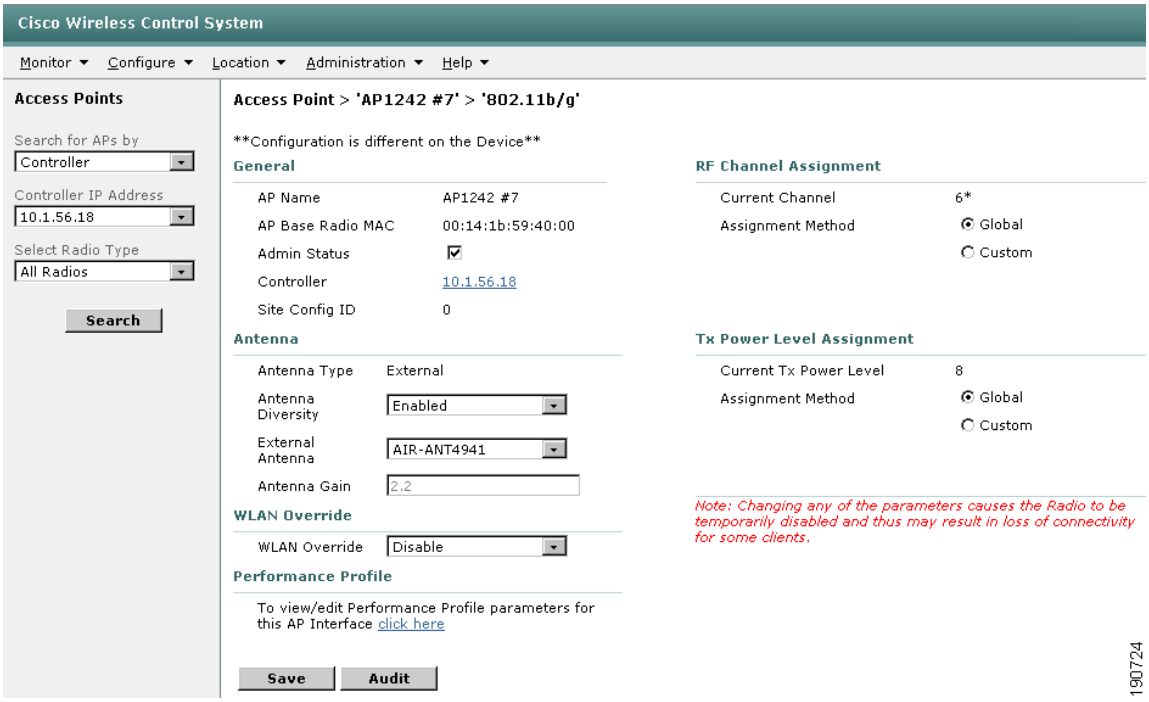
Figure 8-12 Access Point > ap name Configuration Screen



Any parameters modified within the confines of the red dashed rectangle indicate areas that apply to the access point in general. The “Name” parameter shown in this red dashed rectangle is default to the value “AP” concatenated with the MAC address of the access point. You may find it useful to use this field to assign a new name that conveys more meaning within the context of your particular organization, or perhaps to assign a numerical differentiator to each name that assists when sorting and searching the full list of managed access points (seen in Figure 8-12). An example of how this can be used can be seen in Figure 8-11, where access points are named in numerical sequence (“AP1242#1”, “AP1242#2”, and so on) sorted by name in numerical order.

The two radio protocol hyperlinks under the radio interfaces heading (located within the blue dashed rectangle) provide access to **Access Point > *ap name* > 802.11a** and **Access Point > *ap name* > 802.11b/g** radio specific sections (shown in Figure 8-13). Changes to parameters contained within these radio-specific screens affect only the radio interface concerned.

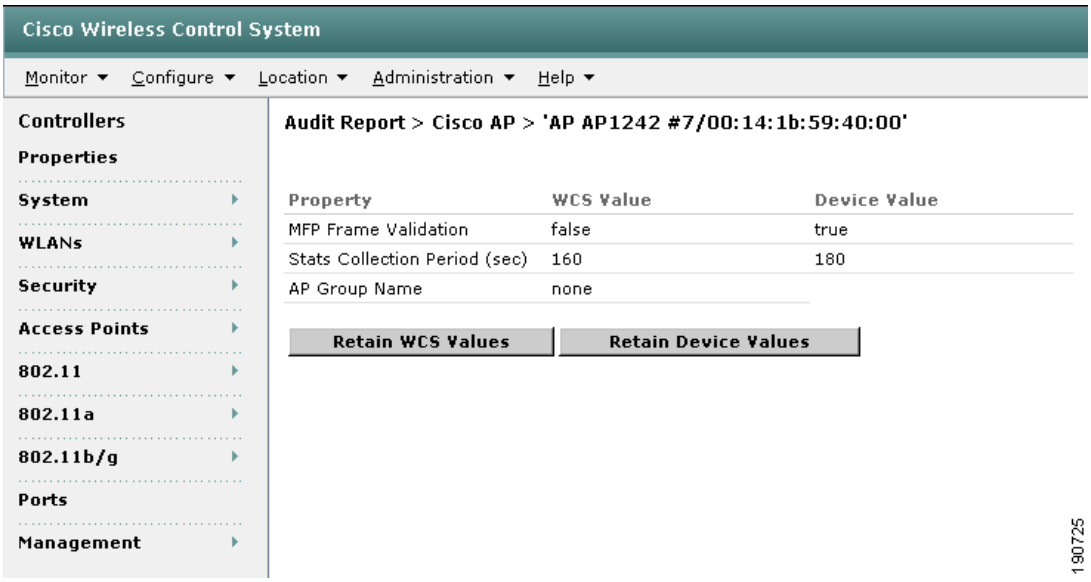
Figure 8-13 Radio-Specific Access Point Configuration



Note that Figure 8-12 also provides a few other options. For example, you find the ability to issue a hardware reset only on the access point or performing a hardware reset and setting the access point configuration to factory defaults. In addition, an option is present to audit configuration parameters. This audit option compares the settings stored in the WCS database to those that are currently resident in the lightweight access point. If they differ, you are presented with a screen similar to that shown in Figure 8-14 asking which set of values (those contained within WCS databases or those contained within the access point/controller) should prevail.

Keep in mind that any parameters changed on this page must be saved to the WCS database (using the **Save** button) before being subject to comparison as part of an audit. If entries are changed and the Audit button is used *before* the changes are saved, the changed entries are discarded. In addition, when an Audit button appears in a configuration-section specific menu such as this, *only* the values contained in the WCS database for the parameters shown on the page are subject to the audit. You are not notified of any discrepancies between the current AP/controller configuration and stored WCS values for parameters other than those shown here.

Figure 8-14 Access Point Audit Report



Step 4 When you are satisfied with your changes on each page, click **Save** and the values are written to both the WCS database as well as the AP/controller configuration.

Configuring WLAN Controllers, page 8-13, showed that when configuring WLAN controllers with WCS, the new configuration is applied as a running configuration and is not automatically saved to nonvolatile memory. However, this is not the case when configuring lightweight access points. When configuring lightweight access points, any changes that are applied from WCS to the access points via the controller are saved to the nonvolatile memory of the access points. Therefore, there is no need for an explicit save procedure to ensure that your changes are still intact after access points are rebooted. In fact, after your changes are applied, they migrate with lightweight access point even if the lightweight access point become registered to a different controller.

Further guidance about configuring lightweight access points can be found in the WCS main menu bar under **Help > Online Help**.

Copying Lightweight Access Point Configurations

In some cases, it may be necessary to copy the configuration that is stored in the WCS database for a lightweight access point to a new lightweight access point. A good example of when this might be necessary is when replacing a lightweight access point that has become damaged in some way with a replacement lightweight access point that has been sent via the Cisco SmartNet program.

WCS makes it possible to copy the configuration-of-record stored in WCS for the original (source) access point and apply it to the replacement (target) access point. When performed, the configuration of the target lightweight access point is overwritten and it assumes the majority of the parameters originally configured for source lightweight access point.

Note Admin Status, Monitor Mode, WLAN Overrides, Channel Assignment, and Antenna Diversity settings are not copied.

Only lightweight access points that are known to WCS but not registered with a WLAN controller can serve as the source of the lightweight access point copy operation. Similarly, only lightweight access points that are known to WCS and currently registered with a controller within this management domain can serve as the target of a lightweight access point copy operation. From the perspective of WCS, it does not matter if the source lightweight access point was originally used on a different WLAN controller than where the target lightweight access point is installed.

To perform this copy operation, follow these steps:

Step 1 Click **Configure > Access Points** to display the All Access Points page. In large networks, it is helpful to narrow the listing by using the "Search for APs By" filter in the left-hand column margin.

Step 2 Select the non-registered source lightweight access point that you want to copy the configuration from by enabling the check box next to its name (notice that the checkboxes for both radio interface line items become enabled).

Note A *non-registered* access point is an access point that had previously been registered to a WLAN controller defined to WCS but is not currently registered to any WLAN controller in this management domain.

Step 3 From the command drop-down menu in the right-hand upper corner of the screen, choose **Copy and Replace AP** and click **GO.**

Step 4 Select the registered target lightweight access point that you want to have serve as the destination for the copied configuration. Enable the check box for "Copy Location Information" if you want the location map information for the source lightweight access point copied as well (that is, this positions the target lightweight access point to the same coordinates on location floor maps as the source lightweight access point).

Step 5 Click **Copy To AP** to copy the configuration. The current configuration of the target lightweight access point is replaced with the configuration of the source lightweight access point.

The copy and replace operation is now complete. Notice that the destination registered AP is now configured with the name of the originating non-registered lightweight access point. To avoid confusion, the name of the source or target lightweight access point should be changed or the source lightweight access point deleted, as described in Removing Lightweight Access Point Configurations, page 8-21.

Additional information on copying lightweight access point configurations can be found in the WCS main menu bar under **Help > Online Help**.

Removing Lightweight Access Point Configurations

After the **Copy and Replace AP** operation in Copying Lightweight Access Point Configurations, page 8-20 is performed, you are still left with the original lightweight access point definition resident in WCS. In the case of the replacement of a damaged lightweight access point, the source definition is no longer used because the replacement lightweight access point has assumed its duties. In this case, Cisco recommends that after the lightweight access point configuration has been copied, the original access point configuration should be removed. Otherwise, you will have the old unused access point configurations simply cluttering up the WCS database and adding unnecessary confusion to WCS screens when displaying lists of all lightweight access points.

You can use the Remove APs command in WCS to remove the configuration for the original lightweight access point. Keep in mind that *only* lightweight access points that are not currently registered with any WLAN controller can be removed from the WCS database via the Remove AP operation.

To remove a non-registered lightweight access point configuration from WCS, perform the following steps:

Step 1 Click **Configure > Access Points** to display the All Access Points page. In large networks, it is helpful to narrow the listing by using the "Search for APs By" filter in the left-hand margin.

Step 2 Select the non-registered access point(s) that you want to remove by enabling the appropriate check box(es).

Step 3 From the command drop-down menu in the right-hand upper corner of the screen, choose **Remove APs** and click **GO.**

Step 4 Confirm your intention to remove the lightweight access points. After doing so, the selected lightweight access point(s) are removed from WCS.

Additional information on removing lightweight access point configurations can be found in the WCS main menu bar under **Help > Online Help**.

Defining and Applying Policy Templates

Policy templates are groups of configuration objects that are typically defined once and then applied to multiple controllers without the need to manually re-key each object value and send each screen of configuration data to each controller, lightweight access point, or radio interface individually. After being defined and implemented in WCS, the use of policy templates greatly reduces the possibility of controller misconfiguration by ensuring that the proper values are defined once and saved for future use when defining subsequent resources.

Policy templates allow for the creation of configuration objects along with a simple means with which to propagate those configuration objects among multiple WLAN controllers, lightweight access points, or access point radios. By using WCS policy templates, uniform QoS, security, and RF management policies can be easily created and enforced across an entire enterprise or outdoor deployment.

The definition of WLAN controller and lightweight access point policy templates is a relatively straightforward task and is similar in many aspects to the procedure described in Configuring WLAN Controllers, page 8-13 and Configuring Lightweight Access Points, page 8-16 for directly configuring managed resources.

Complete guidance concerning how to properly define policy templates within WCS can be found in the *Cisco Wireless LAN Controller Configuration Guide, Release 4.0* and also in the WCS main menu bar under **Help > Online Help**. In addition, the following are key points to keep in mind when planning to use WCS policy templates to assist in managing your wireless LAN enterprise network:

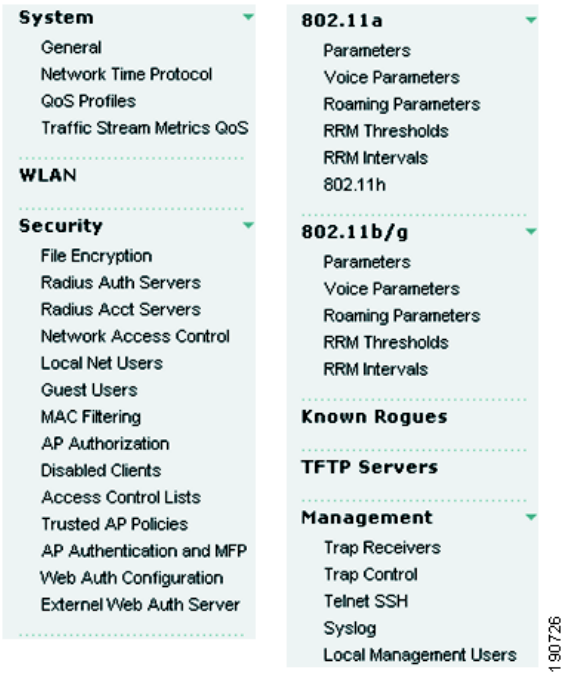
- Policy templates can be applied to WLAN controllers, lightweight access points, and their radio interfaces but not to location appliances.
- Policy templates can be explicitly applied ("pushed") to WLAN controllers, access points, and radios.
- Changes applied to network resources via policy templates can be overridden by authorized operators via WCS or the local controller GUI/CLI interface. The use of the Restore on Cold Start Trap option described in Configuring WLAN Controllers, page 8-13 ensures that the WLAN controller is restored to the WCS configuration of record whenever the controller is rebooted.

Note For further information, see section 13.7 CSCsc59232—4400 and 2006 Controllers Not Issuing Cold Start Traps.

This stored configuration is updated whenever a policy template is successfully applied to a managed resource by WCS.

- Policy templates can be applied to more than a single device at once, making configuration of multiple controllers or lightweight access points easy and efficient. The **Configure > Config Groups** option enables the grouping of multiple templates for application to one or more controllers within the same mobility group (see Using Policy Template Configuration Groups, page 8-25).
- When a controller policy template is created and it is:
  - Saved—This saves the policy template in the WCS database as an unapplied policy template. The template can be applied to managed resources now or at a later time. If you make changes to a policy template but do not save the template or attempt to apply it to at least one controller, the changes are not available on the next use of the policy template. (The policy template is implicitly saved as soon as the **Apply to Controllers** button is clicked, even if no controllers are then subsequently selected for application.)
  - Applied to controllers—This issues an implicit save of the template and applies the policy template to at least one controller. If the application of the template to the controller(s) is successful, the stored configuration for that controller(s) is updated in the WCS database as well.
- Policy templates allow for the definition of the most commonly defined configuration objects (see Figure 8-15 for a listing of available controller policy template configuration object categories).

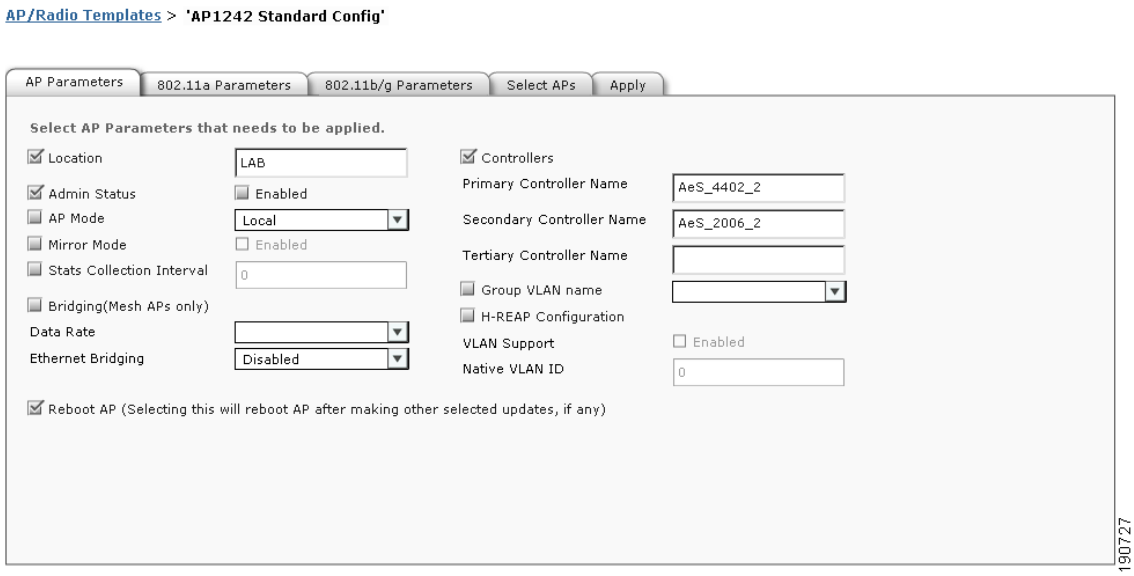
Figure 8-15 Configuration Object Categories Available Via Policy Templates



For some configuration parameters, explicit configuration is required via the WCS **Configure > Controllers** facility. (Some WLAN controller parameters must be configured via the controller web interface or the CLI. Examples of this include SNMP trap destination port, NTP polling interval, and serial port configuration.) The majority of the configuration objects not addressed by policy templates are typically site or controller unique, which tends to exclude them from application as part of a enterprise-wide policy template.

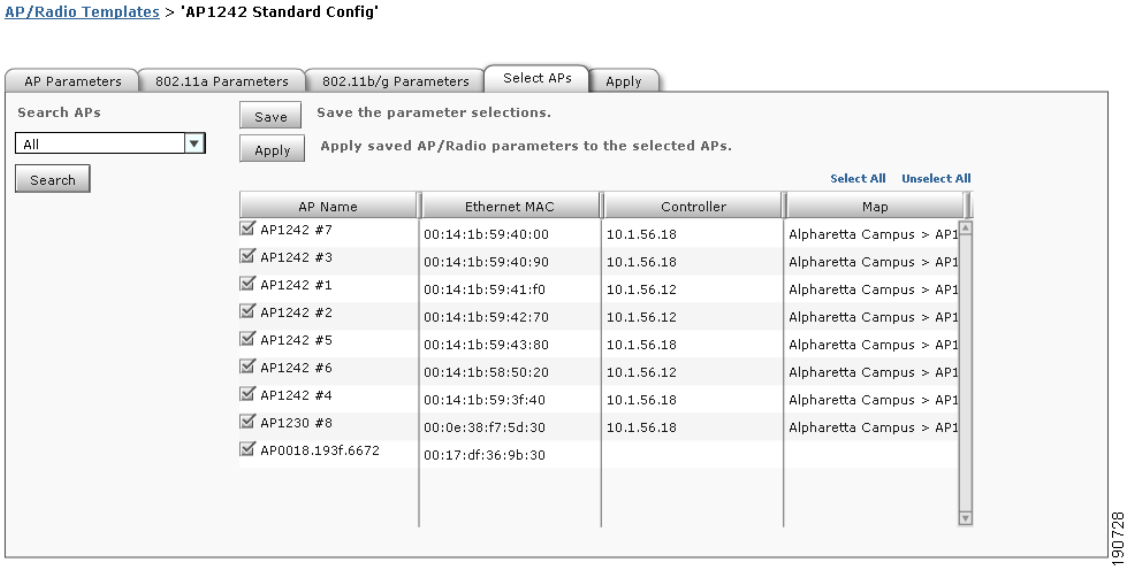
- If you wish to save changes enacted by the application of policy templates in the non-volatile saved configuration of a controller, the save configuration function should be explicitly performed for the controller or group of controllers after the policy templates have been applied. Policy templates are not automatically re-applied to network components after they are re-booted and become reachable from WCS.
- Access points must be registered to WLAN controllers to be eligible to have access point/radio policy templates applied to them via **Configure > Access Point Templates** (shown in Figure 8-16).

Figure 8-16 Access Point/Radio Policy Template



These access points can be on a single controller or spread among two or more controllers (the search parameters in the left-hand margin of Figure 8-17 facilitate choosing access points). Note that after selecting the parameters you wish to configure in all configuration tab areas, you must save the template before applying it to any access points (see red circle in Figure 8-17). Failure to save the template before application results in any changes made being ignored. Beginning with release 4.0 of WCS, access point and radio templates can be saved in WCS for subsequent re-use.

Figure 8-17 Saving and Applying the AP/Radio Template



- After being applied, lightweight access point and radio policy templates are automatically saved in lightweight access points. Lightweight access point and radio configuration changes that have been applied via policy templates are available on a controller or access point re-boot, because the values are saved in the nonvolatile (flash) memory of the lightweight access point. If a controller should fail and the lightweight access point migrate and register to an adjacent controller, the changes that have been applied via the policy template remain with that lightweight access point or its radio interfaces unless changed by policies on the new controller.
- When defining access point and radio policy templates, only configuration objects whose checkboxes are enabled are transmitted to the device. Any configuration objects already existing in the lightweight access point or radio interface are retained if their associated value in the template is not specified. If you want to remove or "blank out" an existing parameter, the configuration object in the access point or radio template must have its check box enabled and the appropriate blank value specified.

Using Policy Template Configuration Groups

By creating a configuration (config) group, you can group controllers that should have the same mobility group name and similar configuration. You can assign templates to the group and push templates to all the controllers in a group. You can add, delete, or remove config groups, and download software, IDS signatures, or a customized web authentication page to controllers in the selected config groups. You can also save the current configuration to the nonvolatile (flash) memory of all controllers in selected config groups.

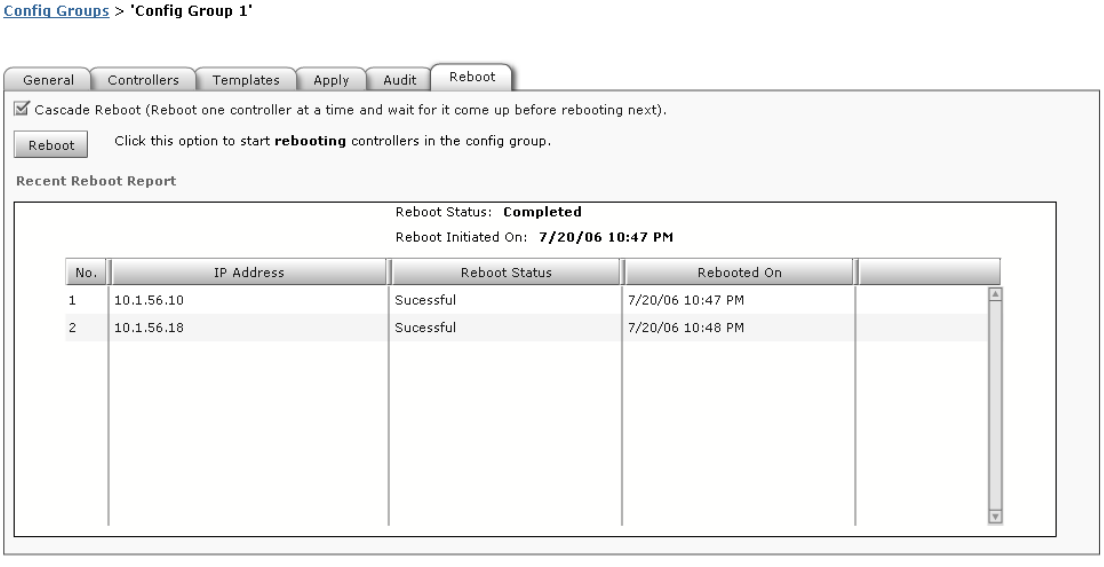
Complete guidance on the use of Configuration > Config Groups can be found in the *Cisco Wireless Control System Configuration Guide, Release 4.0*.

Keep the following points in mind when using policy template configuration groups:

- The mobility group already assigned to a controller is changed by the function of the configuration groups when changes are applied.

- Templates that are applied to controllers via the Config Groups mechanism are not saved to the nonvolatile memory of the controllers by default unless the controllers are rebooted using the Reboot tab, as shown in Figure 8-18.

Figure 8-18 Config Groups Reboot Menu



If you wish to save the updated configuration of all controllers in the configuration group to their respective nonvolatile memories without rebooting them, perform the following:

Step 1 From Configure > Config Groups, click the check box(es) to choose one or more config groups on the Config Groups window.

Step 2 Choose **Save Config to Flash** from the Select a command drop-down menu and click **GO.**

You can perform other utility functions on the controllers in the configuration group in a similar fashion, such as downloading controller software, IDS signatures, and web authentication credentials. Complete details about how to perform these tasks and more can be found in the *Cisco Wireless Control System Configuration Guide, Release 4.0*.

Configuring Location Appliances

When a Cisco Wireless Location Appliance is introduced and configured for use within a Cisco Unified Wireless Network that contains a location-enabled WCS server, the location appliance assumes responsibility for several important tasks. Key among these are the execution of location positioning algorithms for multiple devices, the ongoing processing of historical location and statistical information, the issuance of location notifications, and the provisioning of a defined SOAP/XML Application Programming Interface (API) for other business applications wishing to make use of the device positioning information available in the location appliance.

WCS acts in concert with the location appliance by serving as the user interface (UI) for the enhanced services provided by the location appliance. Other than during the initial installation and shutdown, direct user interaction with the location appliance via the CLI is typically not required.

Integrating a Cisco Wireless Location Appliance into a Cisco Unified Wireless Network architecture immediately enables key operational advantages, such as the following:

- Scalability—Adding a location appliance greatly increases the scalability of the Cisco LBS solution from on-demand tracking of a single device to a maximum capacity of 2500 devices (WLAN clients, RFID tags, rogue access points, and rogue clients). For deployments requiring location tracking of greater than 2500 tracked devices, additional location appliances can be deployed as part of the Unified Wireless Network and managed under a common WCS.
- Historical and statistics trending—The appliance records and maintains historical location and statistics information, which are available for viewing via WCS.
- Location notifications—Location-based alarms and notifications can be triggered through area boundary definitions, allowed areas, and distances. These alarms and notifications can also provide advanced warning of rogue movement and appearance/disappearance.
- SOAP/XML API—The location appliance interfaces to WCS using a very rich and robust SOAP/XML API interface. These same capabilities allow for integration with other business applications that can use the location information contained within the location appliance in a variety of creative value-added applications. Asset tracking, inventory management, location-based security, and automated workflow management are just a few examples of this.

Complete guidance about how to use the Location menu option under WCS to properly configure the Cisco Wireless Location Appliance is available in the *Cisco Wireless Location Appliance—Configuration Guide*.

Managing Network Component Software

An often-overlooked but nevertheless critical feature of any effective enterprise network management system is the ability to inventory and update the operating software levels of the various components comprising the network. An effective enterprise wireless network management system must be able to regularly inventory software levels and facilitate their upgrade by authorized personnel from either centralized or distributed software repositories.

It is generally regarded as standard industry best practice for network architects and network management staff to be aware of current operating software levels throughout the network. Periodic reviews of http://www.cisco.com and regular discussions with your Cisco account team should be conducted to keep abreast of new features, feature improvements, and bug fixes as they become available and posted. Software updates should be applied to your network only after a careful analysis of new enhancements and bug fixes has been performed and a determination made of the applicability of these software updates to your specific environment. This may be done in conjunction with your local Cisco account systems engineering representative or the Cisco Technical Assistance Center.

WCS offers the ability to effectively manage device operating software such as device operating systems, web certificates, and IDS signatures across various components of the Cisco Unified Wireless Network. In addition, WCS makes it possible to routinely archive controller configurations (as well as the WCS database itself) to protect against potential inadvertent loss of data. The subsections that follow describe how WCS provides effective management of these categories of operating software in wireless LAN controllers, lightweight access points, and location services appliances.

Keep in mind that the level of operating software in registered lightweight access points is automatically managed by the WLAN controller. The version of operating software loaded into any registered lightweight access points is dependent on the level of operating software present in the controller. Although WCS clearly displays the current software levels in each lightweight access point, there is no need (and therefore no ability exists in WCS) to explicitly manage the level of operating software present in lightweight access points.

Managing Controller Operating Software, Web Authentication Bundles, and IDS Signatures

Cisco WCS allows for WLAN controller operating software to be updated via two approaches. Each of these involves the use of the TFTP file transfer protocol, but there are differences in the source server that is used to update the controller.

The actual data transfer can be configured to occur between one of the following:

- The internal WCS TFTP server and the controller
- An external TFTP server and the controller

The use of the internal WCS TFTP server is probably the easiest and most straightforward method for most users. This option allows for the file to be loaded onto the TFTP server via one of the following two ways:

- Via the use of a TFTP client (the traditional approach)
- Using your client browser to transfer the file to the TFTP server home directory via HTTPS. With this method, a two-stage transfer is used between a directory on your local workstation and the WCS TFTP server to load the file onto the network device.

If you are updating multiple controllers in multiple download sessions throughout the day, it is more efficient to transfer the file from your desktop to a TFTP server only once and then specify a single stage transfer from the home directory of the WCS TFTP server for all subsequent controller downloads. (This is because when the source of a downloaded file is your local client workstation (“local machine”), the amount of traffic is increased twofold. The reason for this is because the software file is transferred twice: once between your desktop and WCS server using HTTPS, and then again between the controller and the WCS server using TFTP.)

The remainder of this section describes how to do this along with other options.

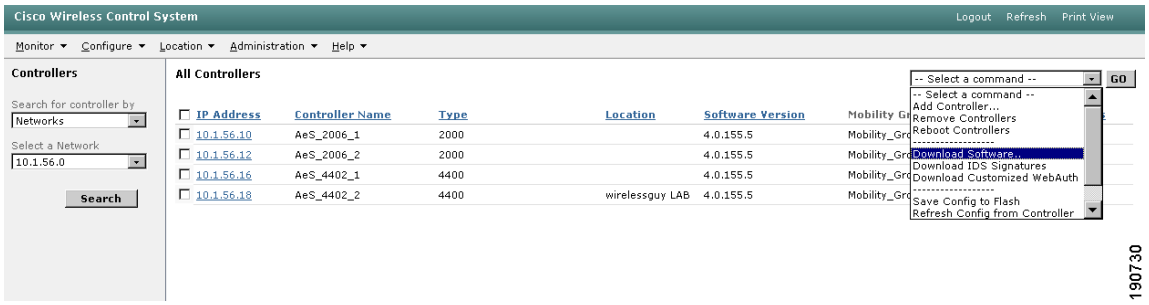
In the majority of centralized WLAN management implementations, the network traffic that results from the maintenance of controller software should not represent a major traffic component, especially with modern high-bandwidth campus LAN implementations. In larger implementations that may use slower or more congested WAN links between campus network and remote sites, it may be beneficial to transfer controller software files across the WAN to local TFTP servers during off-peak periods, especially if it is forecast that controller upgrades might need to be performed during peak traffic periods. By placing software files on TFTP servers that may be local to the network devices that require upgrading, transferring the files across the WAN during periods of peak traffic can be avoided.

In rarer cases of very large networks (such as those considered in Using WCS to Efficiently Deploy Your Wireless Network, page 8-93), additional considerations may be warranted. Given that controller operating software files are typically 25 MB in size, Cisco recommends that the performance impact of initiating multiple simultaneous controller operating software downloads during periods of peak network usage be more carefully examined. Multiple controller selections result in the initiation of multiple TFTP sessions (up to any limitation imposed by the TFTP server being used). The WCS administrator should keep this behavior in mind and limit the number of controllers selected, considering the underlying network topology, the bandwidth available, and other users on the network. As with other WCS displays, all controllers selected for software download must be present on one WCS display page when using the **Configure > Controllers** menu selection.

Perform the follow steps to download new software to WLAN controllers:

Step 1 Click **Configure > Controllers** to display the All Controllers page (shown in Figure 8-19). In large networks, you may find it helpful to use the “Search for Controllers” filtering feature in the left-hand margin to narrow the selection of displayed controllers by name, IP address, or network.

Figure 8-19 All Controllers WCS Page



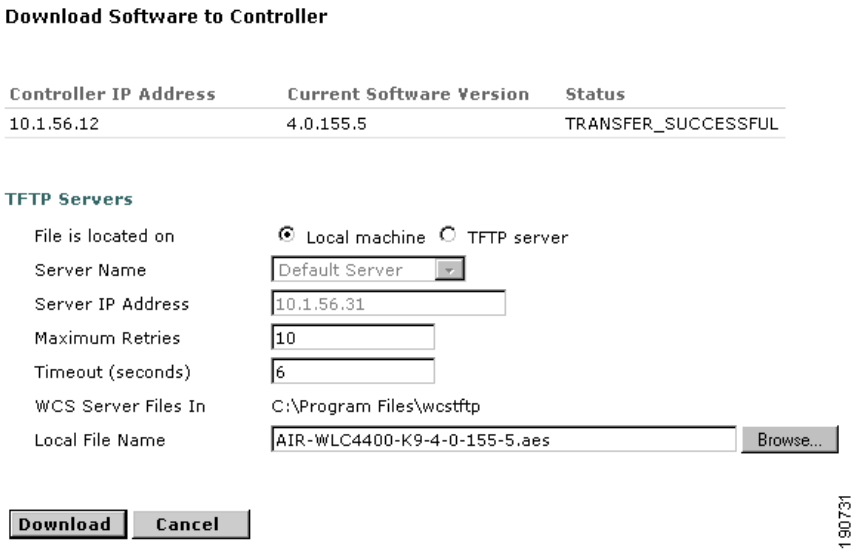
Step 2 The current version of controller software in each controller is listed under the column heading "Software Version". Enable the check box(es) to select the desired controller(s), choose **Download Software** from the command drop-down menu selector in the upper right-hand corner, and click **GO**. WCS displays the "Download Software to Controller" page.

Step 3 There are three choices with regard to transferring the software file to the WLAN controller(s) with the best choice being dependent on where the software file is resident:

- The software file is resident on your local computer—The file is resident on the client workstation that you are currently using to access WCS. In this case, you may use the two-stage process described previously to easily transfer the software file from your workstation to the WLAN controller.

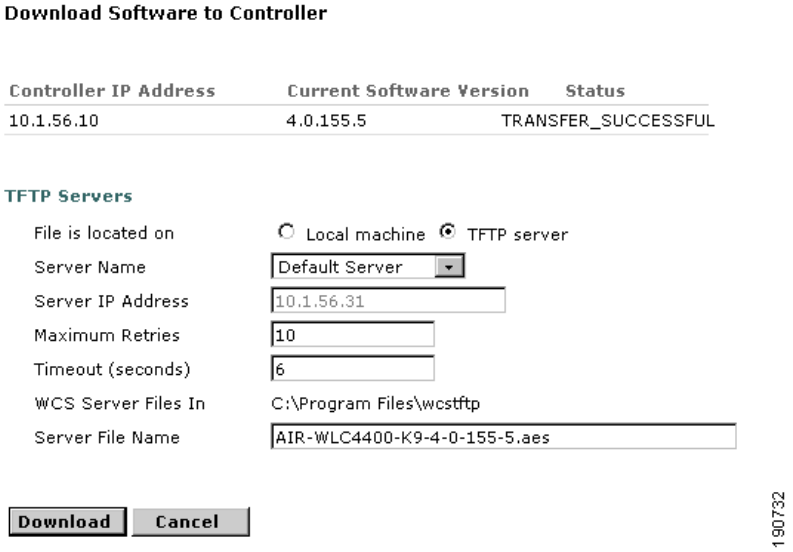
  To do this, ensure that **Local Machine** is selected for the "File is Located on" option, as shown in Figure 8-20. Then click **Browse** to select the software file on your local computer. The file is transferred from your local machine to the internal WCS TFTP server, and then transferred to the controller.

Figure 8-20 Downloading Controller Software From the Local Machine



- The software file is already resident in the TFTP directory on WCS—This is the directory that you specified during the installation of WCS. Under this option, the software file is simply transferred from the WCS TFTP directory to the WLAN controller using TFTP only. To accomplish this ensure that:
  - The **TFTP server** option is selected for the "File is Located on" option.
  - "Default Server" is selected for the server name.
  - The server IP address specified is the IP address of your WCS server. If it is not, it can be changed by modifying the template located at **Configure > Controller Templates > TFTP Server > Default Server**.
  - The exact name of the file you want to load into the WLAN controller (such as *AIR-WLC4400-K9-4.0.155.5.aes*) is specified as shown in Figure 8-21. This filename needs to match the name of the file on the WCS TFTP server.

Figure 8-21 Downloading Controller Software from WCS TFTP Server



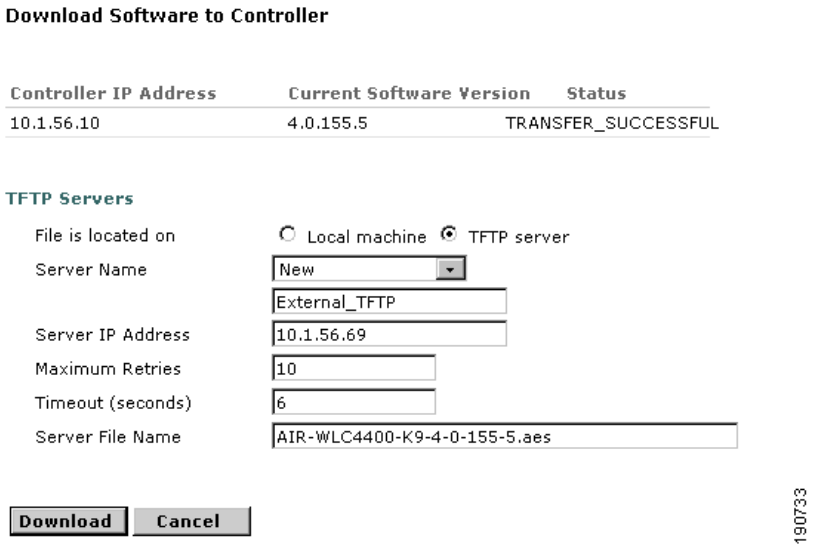
  - The use of this option is an efficient choice if you have already used option (3a) once before and the software file is now already resident on the WCS TFTP server, because it avoids re-transmitting the software file from the local machine to the WCS TFTP server unnecessarily.
- The software file is already resident in the TFTP directory of an external TFTP server—In this case, the file is transferred from the external TFTP server to the WLAN controller using TFTP.

Note Note that WCS cannot transfer a file from the local machine to an external TFTP server using HTTPS. Therefore, ensure that the file is already resident on the external TFTP server.

To accomplish this, ensure the following:

- The **TFTP server** option is selected for the "File is Located on" option.
- The external server of choice is selected from the drop-down menu for server name. If the external TFTP server you wish to use has not been defined on this WCS previously, it can be defined at this time by using "New" as the selection for the server name, typing in a name for this TFTP server definition and entering the server IP address.
- The exact name of the file you want to load into the WLAN controller (such as *AIR-WLC4400-K9-4.0.155.5.aes*) is specified as shown in Figure 8-22. This filename needs to match the name of the file on the WCS TFTP server.

Figure 8-22 Downloading Controller Software From an External TFTP Server



Step 4 After selecting the appropriate option in step 3, click **Download**. WCS downloads the software to the controller, and the controller initiates a process that ultimately results in the new software being written to nonvolatile (flash) memory. As WCS performs this function, it displays its progress in the Status field.

Step 5 After the download is complete, you need to save the current controller configuration (if desired) and reboot the controller for the new software to take effect. This can be easily performed by returning to the All Controllers screen shown in Figure 8-3, selecting the controller(s) you wish to reboot, selecting **Reboot Controllers** from the upper right-hand drop-down menu, and clicking **GO**.

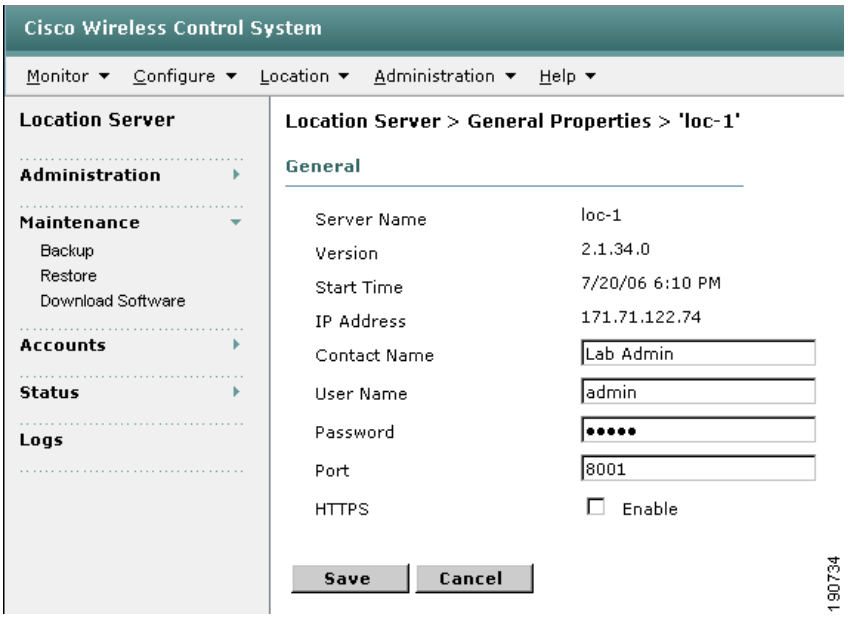
Using the same basic steps outlined above, WCS also allows for web authentication bundles and intrusion detection (IDS) signatures to be downloaded to the controller as well in an analogous fashion. The commands to perform these functions can be accessed from the **Configure > Controllers > All Controllers** screen shown in Figure 8-19.

Further guidance concerning how to download controller operating software, web authentication bundles, and IDS signatures can be found in the *Cisco Wireless LAN Controller Configuration Guide, Release 4.0* and also in the WCS main menu bar under **Help > Online Help**.

Managing Location Server Software Level

As mentioned previously, WCS is the user interface to the location appliance and as such provides the control mechanism through which the location application and history databases on the location appliance are managed. All such software level management is performed for the location appliance from the **Location > Location Servers > Maintenance** screen shown in Figure 8-23. The Maintenance category shown provides several sub-category options for downloading new operating system software to the location appliance as well as performing a backup and restore of historical data on the appliance.

Figure 8-23 Location Server Maintenance



Complete step-by-step guidance about the updating of operating system software as well as how to perform appliance database backup and restore using WCS is available in the *Cisco Wireless Location Appliance—Configuration Guide*.

Ensuring Configuration Integrity

To ensure consistency, Cisco recommends that WCS be used whenever possible to configure and maintain the components of your Cisco Unified Wireless Network instead of direct CLI and GUI device access. As part of their configuration management functionality, many network management systems (including WCS) possess both an internal database structure where the last known configurations of network components are stored as well as the ability to query those components for their actual current configuration. Under normal operating circumstances, in an ideal environment where configuration access to network components is tightly controlled and only allowed from authorized network management stations, there should be little if any discrepancy between the actual configuration information contained in each network component and the configuration contained in the management system database.

In the real world, such discrepancies can and do arise. Whether from access by another group within the organization performing troubleshooting or from misconfiguration during hardware replacement, such situations may occur more often than is desirable in real-world deployments. To maintain integrity and value, an enterprise wireless network management system must possess a configuration management subsystem with which such discrepancies can be quickly identified and efficiently resolved.

When using the **Configuration > Controllers** function under the WCS main menu bar to manage WLAN controller configurations, the configuration object values that are displayed originate from the WCS internal database, not the controllers themselves.

Because WCS stores its representation of current WLAN controller configurations apart from the actual values present in the devices, the state of synchronization should occasionally be validated between the WCS databases and the actual managed device and if necessary, a re-synchronization should be initiated. WCS provides the network administrator with several tools to accomplish this. The subsections that follow describe these tools, which include the following:

- Configuration audit reporting
- Configuration synchronization
- WCS configuration refresh
- WLAN controller and access point configuration restoration

Configuration Audit Reporting

Configuration audit reports compare the complete current running configuration of a controller and its registered access points with the configuration stored in the WCS databases. Any exceptions are noted and brought to the attention of the network administrator via screen reports.

WCS offers both an on-demand as well as a periodically scheduled configuration audit reporting feature.

On-Demand Configuration Audit Reporting

To initiate an on-demand configuration audit report on behalf of a WLAN controller and its registered lightweight access points, follow these steps:

Step 1 Click **Configure > Controllers** to display the All Controllers page. In large networks, you may find it helpful to use the “Search for Controllers” feature in the left-hand margin to narrow the selection of displayed controllers by name, IP address, or network.

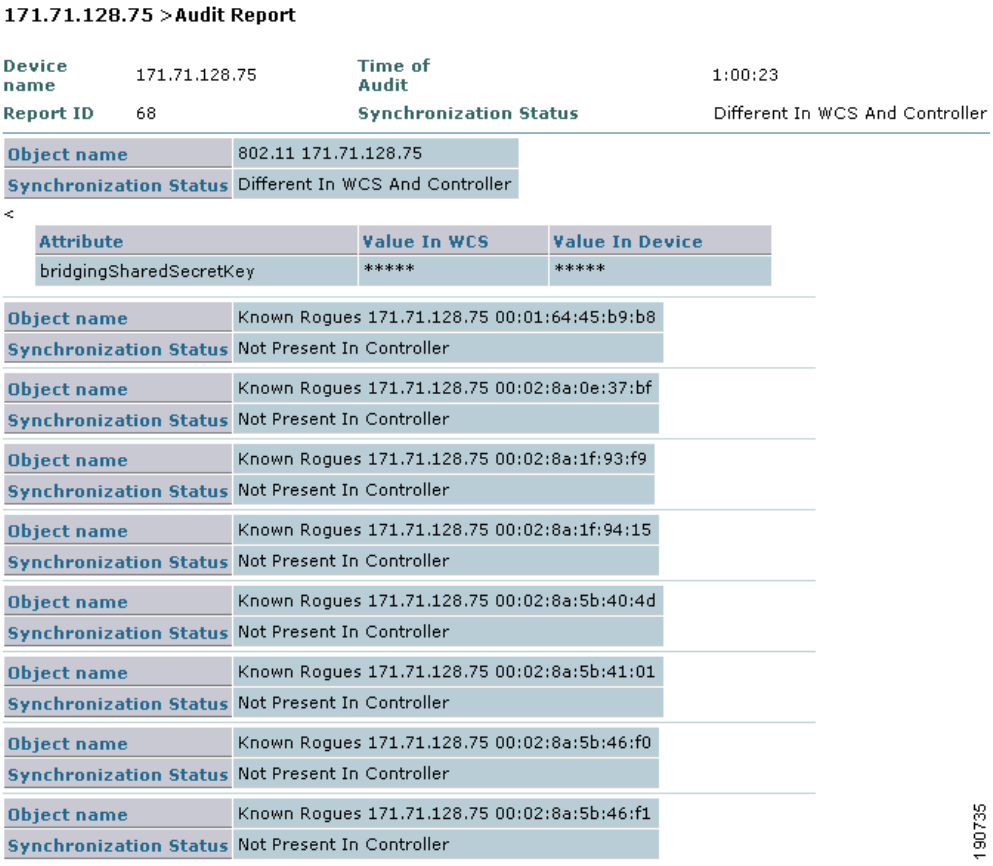
Step 2 Click on the hyperlink representing the IP address of the WLAN controller that you want to report. Note that a controller cannot be selected for this function by simply enabling the check box.

Step 3 Expand the **System** category selection in the left-hand column of the Controller Properties page. Click on the **Commands** subcategory, which brings up the Controller Commands page.

Step 4 Select **Audit Config** from the **Configuration Commands** drop-down selector and click on **GO.**

The result is a configuration audit report listing any discrepancies found, as shown in Figure 8-24.

Figure 8-24 On Demand Audit Report



171.71.128.75 >Audit Report

Device name	171.71.128.75	Time of Audit	1:00:23
Report ID	68	Synchronization Status	Different In WCS And Controller

Object name	802.11 171.71.128.75
Synchronization Status	Different In WCS And Controller

<

Attribute	Value In WCS	Value In Device
bridgingSharedSecretKey	*****	*****

Object name	Known Rogues 171.71.128.75 00:01:64:45:b9:b8
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:0e:37:bf
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:1f:93:f9
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:1f:94:15
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:40:4d
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:41:01
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:46:f0
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:46:f1
Synchronization Status	Not Present In Controller

190735

Scheduled-Task Network Audit Reporting

WCS can also produce configuration audit reports automatically on a routine basis without user intervention. The output of this report is very similar to what has just been described. Known as the network audit report, this runs as a scheduled task and reports on discrepancies found between the configuration values in WCS databases and *all* WLAN controllers defined to WCS and their currently registered lightweight access points. Unlike the on-demand configuration report, the network audit report is non-selective and reports against all defined controllers that are SNMP reachable.

The network audit report can be configured to execute at a pre-defined time and with a pre-defined repetition interval. Alternatively, it can also be executed on a one-time “execute now” basis (which is equivalent in function to what was discussed in On-Demand Configuration Audit Reporting, page 8-33). The network audit report facilitates running unattended reports at times when network utilization is low and allows the viewing of report output to be deferred.

For further information on this scheduled task configuration audit report capability, see Network Audit, page 8-119.

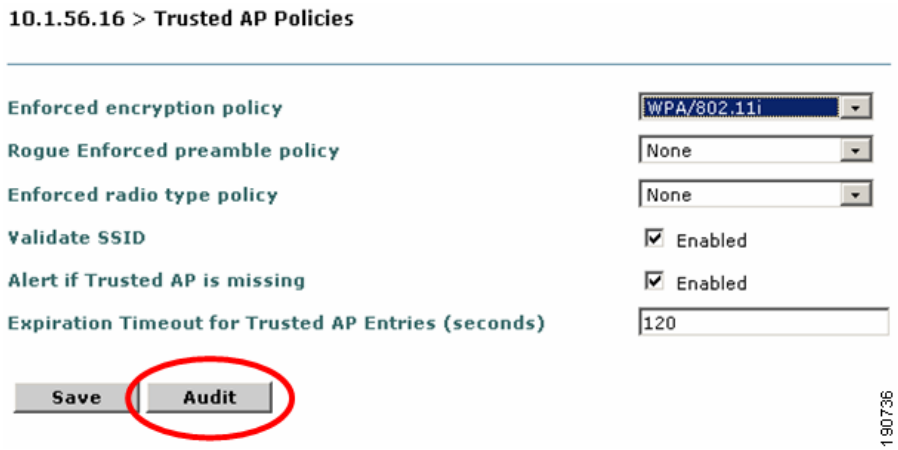
Synchronizing WCS with Controller and Access Point Configurations

Synchronization in WCS is performed as a distinctly separate operation in relation to the identification of discrepancies. WCS offers several mechanisms through which configuration discrepancies between WCS, controllers, and lightweight access points can be resolved without requiring the operator to initiate a manual configuration change. These options can be broken into two groups. The first of these is a selective synchronization option where the administrator may individually audit and synchronize select portions of controller and lightweight access point configurations. Access is via the same controller and lightweight access point configuration menus used to edit the configurations as described in Configuring WLAN Controllers, page 8-13 and Configuring Lightweight Access Points, page 8-16. The second group of options are non-selective one-way mechanisms that can either refresh the content of the WCS database from the controller configuration or restore the controller configuration from the information contained in the WCS databases.

Selective Synchronization

Selective synchronizations options are available on the same WCS menu panels that are used to specify parameters for controller and lightweight access point configuration. To initiate selective synchronization, access the screen of interest for the particular parameter category you want to audit by following the procedures already outlined in Configuring WLAN Controllers, page 8-13 and Configuring Lightweight Access Points, page 8-16. When you arrive at the parameter definition screen, you should notice that an "Audit" option is available alongside the option to save the configuration objects. An example is shown in Figure 8-25.

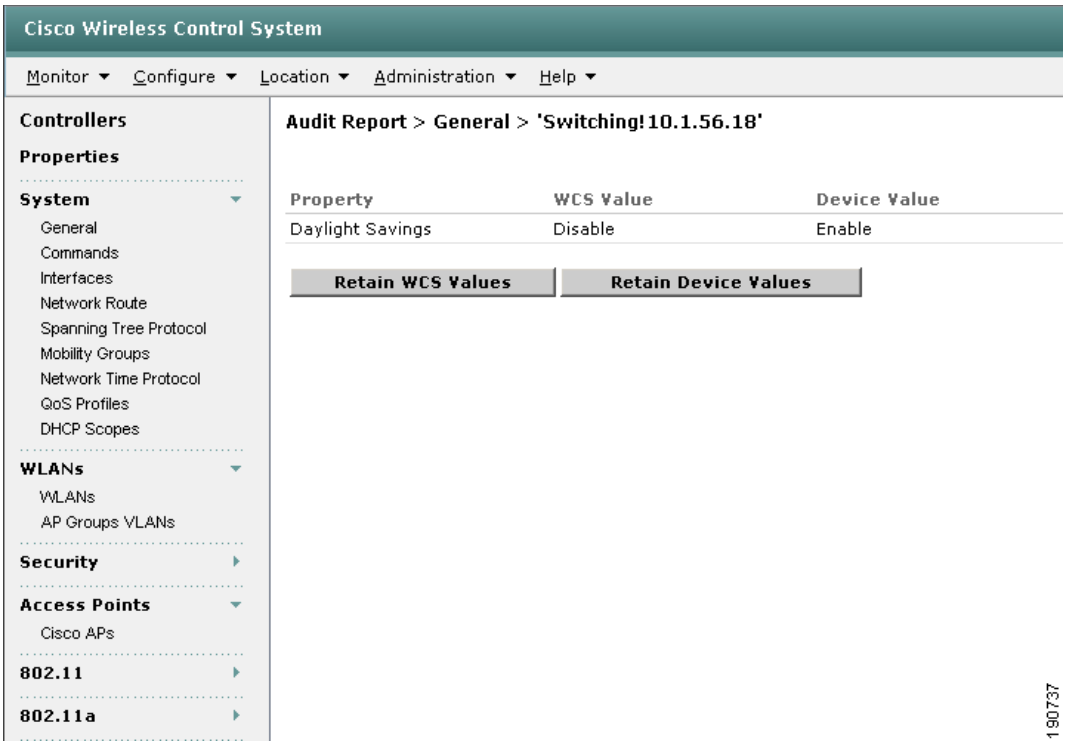
Figure 8-25 Selective Audit Option Example



Selecting "Audit" in this case does not perform simple audit reporting, as was discussed in previous sections, but rather initiates the process of synchronizing the values of the displayed configuration parameters between the WCS database and the actual device running configuration. When a selective synchronization audit is performed, WCS queries the WLC and requests the audit parameter values contained in the WLC for the specified Management Information Base (MIB) objects. WLC responds with the current values for the audit parameters. When the responses are received, WCS compares the values contained in its databases to the values received from the device.

If the results of the comparison indicate that the device is in synchronization with WCS, WCS indicates that no differences exist. However, if there are any discrepancies found during the comparison, WCS presents the operator with a screen similar to that shown in Figure 8-26.

Figure 8-26 Auditing a Configuration Category



Clicking on one of the two options in Figure 8-26 causes one of the following to occur:

- Retain Device Values—The information in WCS that conflicts with the information shown in the device is overwritten with the information specified in the device.
- Retain WCS Values—The information in the device that conflicts with the information shown in WCS is overwritten with the information specified in WCS.

In either case, WCS presents confirmation of the selection and the action performed as a result.

In this way, WCS allows the operator to review as little or as much of the device configuration as desired, and synchronize only selected parts of the configuration.

This same procedure can be used to perform selective synchronization of lightweight access point configurations as well. See Configuring Lightweight Access Points, page 8-16 for information about the configuration of lightweight access points.

Non-Selective Synchronization

In some cases, you may wish to perform synchronization between WCS and its managed resources on a grander scale than that which is available via selective synchronization. WCS offers the capability of performing one-way non-selective synchronizations of the WCS database with the entire running configuration contained within the controller (or vice-versa).

- Refresh Config from Controller—When the **Refresh Config from Controller** feature is selected, a one-way (WLC -> WCS) synchronization of all configuration objects for the selected WLAN controller is performed. A one-way synchronization in this case implies that all configuration information pertaining to the controller on WCS is overwritten with the running configuration of the WLAN controller. This feature is useful in correcting a situation where the WCS database has become out of sync with the configuration contained in the controller in multiple configuration

categories. This can result, for example, if changes are made to the WLAN controller configuration in WCS but because of a communication or other errors in the controller, the changes were not completely applied. WCS and the WLC operate perform such updates in unison and with close monitoring of error status to preclude the occurrence of such events. But if this type of situation should occur, **Refresh Config from Controller** provides a simple way to completely re-synchronize the controller information contained within WCS to the current running configuration of the device.

Refresh Config from Controller can be performed against either a single WLAN controller or multiple WLAN controllers simultaneously. To perform the refresh, follow these steps:

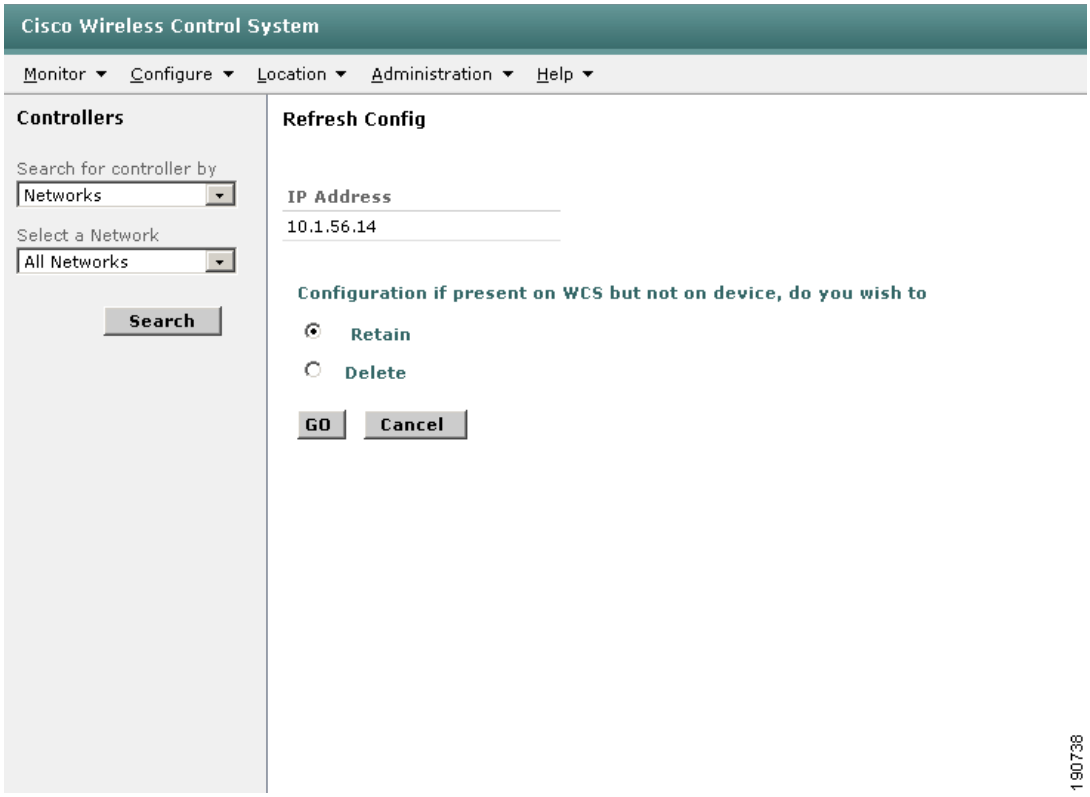
Step 1 Click **Configure > Controllers** to display the All Controllers page. In large networks, you may find it helpful to use the "Search for Controllers" filter in the left-hand margin to narrow the selection of displayed controllers by name, IP address, or network.

Step 2 Enable the check box(es) for each WLAN controller(s) whose configuration(s) you want to restore to the WCS database. Keep in mind that for each controller selected, WCS sends a series of SNMP PDUs to retrieve the running configuration of each controller.

Step 3 From the command drop-down menu selector in the right-hand upper corner of the screen, choose **Refresh Config from Controller** and click **GO.**

The page shown in Figure 8-27 is presented.

Figure 8-27 Refresh Config from Controller Conflict Resolution



This information displayed concerns itself with what to do in the event that a configuration object exists in the WCS database for the controller but does not exist in the running configuration of the controller.

Step 4 Do one of the following:

a. Select **Retain** if you want the value found in the WCS database to prevail.

b. Click **Delete** if you want to remove the existing value found in the WCS database and replace it with the value found in the controller.

Step 5 Click **GO** after you have made your selection.

- Restore Config to Controller—This provides for a one-way, non-selective synchronization of all applicable controller configuration objects from the WCS database to the running configuration of the selected WLAN controller is performed. All information contained in the controller is overwritten with the information contained in the WCS databases.

  Unlike **Refresh Config from Controller**, **Restore Config to Controller** can only be applied on an individual basis against specific controllers.

  To refresh the running configuration of a WLAN controller from the WCS database using **Restore Config to Controller,** perform the following procedure:

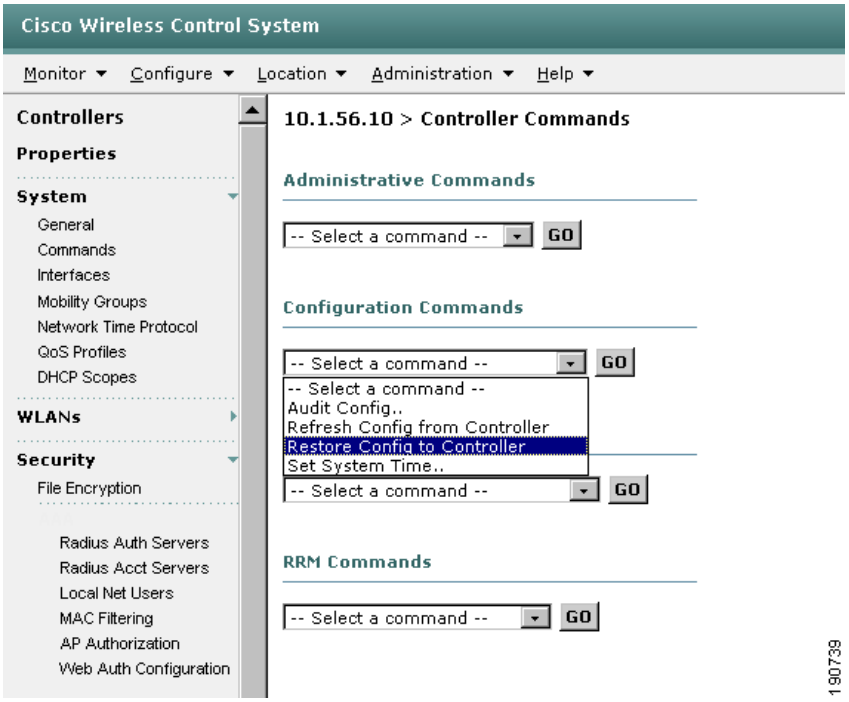
Step 1 Click **Configure > Controllers** to display the **All Controllers** page.

In large networks, you may find it helpful to use the "Search for Controllers" feature in the left-hand margin column to narrow the selection of displayed controllers by name, IP address, or network.

Step 2 Click the hyperlink representing the IP address of the WLAN controller that you want to configure.

Step 3 Expand the **System** category selection in the left-hand column of the **Controller Properties** page, as shown in Figure 8-28. Click the **Commands** subcategory, which brings up the **Controller Commands** menu.

Figure 8-28 Controller Commands



Step 4 Select **Restore Config to Controller** from the **Configuration Commands** drop-down selector and click **GO**.

Be careful not to inadvertently select **Refresh Config from Controller** instead of **Restore Config to Controller** because both options appear in the drop-down menu selector.

Step 5 Confirm the action by clicking **OK** on the confirmation screen.

Controller Configuration Archival

The ability to identify discrepancies between the contents of WCS and the actual configuration of network devices, coupled with two powerful mechanisms allowing for re-synchronization is usually sufficient to recover from most accidental or unintentional out-of-sync situations. In some cases, however, the out-of-sync situation can become somewhat aggravated because of the passage of time or the inadvertent operator acceptance of controller configuration changes into the WCS database that are later found not to have been valid. To address these situations and others, WCS also provides the ability for archival and restoration from external configuration archive files that are independent of the WCS database itself.

Note WCS also provides the ability to backup and restore the WCS databases themselves to protect against the rare occurrence of WCS database failure or corruption. This section concerns itself more with isolated cases of single controller configuration corruption, and not cases of widespread WCS database corruption.

Regular archiving of device configuration is a best practice because it allows the recovery of lost configuration, and it also provides an audit trail of when changes occurred in device configuration. This section describes how WCS provides for controller configurations to be archived to individually named and time-stamped files on a designated TFTP server. The archival process can be initiated either on-demand or via a scheduled task.

Archiving of Individual Controller Configuration Files

WCS provides the ability to manually archive the configuration of a WLAN controller to a file on a designated TFTP server via the following process.

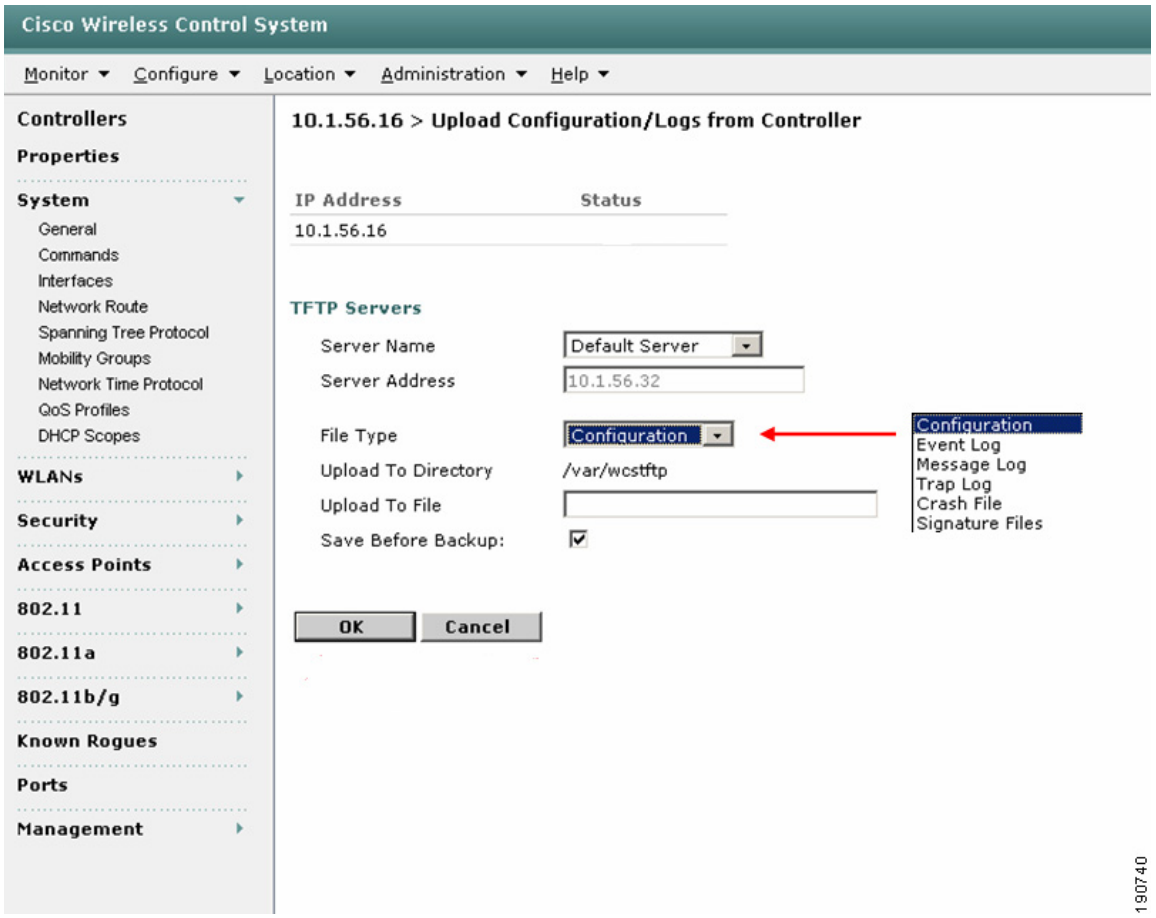
Step 1 Click **Configure > Controllers** to display the All Controllers page. In large networks you may find it helpful to use the "Search for Controllers" feature in the left-hand margin to narrow the selection of displayed controllers by name, IP address, or network.

Step 2 Click the hyperlink representing the IP address of the WLAN controller for which you want to archive the configuration. Note that for this function the controller cannot be selected by simply enabling the check box.

Step 3 Expand the **System** category selection in the left-hand column of the Controller Properties page. Click on the **Commands** subcategory, this brings up the Controller Commands page shown in Figure 8-28.

Step 4 Select **Upload File From Controller** from the **Upload/Download Commands** drop-down selector and click on **GO**. This displays the screen shown in Figure 8-29.

Figure 8-29 Manually Archiving Controller Configurations, Logs, and Signature Files



Step 5 Select a server that has been already configured from the Server Name drop-down selector, or select "New" to define a new TFTP server and enter the IP address. For file type, select **Configuration**. Note that this same mechanism can be used to archive other controller files such as IDS signature files and logs.

Step 6 Enter the file name that you want the archive saved as on the TFTP server.

Step 7 You may wish to enable the **Save Before Backup** check box. When this check box is enabled, it indicates that the running configuration of this controller should be saved to the internal nonvolatile (flash) memory of the controller before the archiving begins. Because the scheduled task archives only the *saved configuration of the controller and not the currently running configuration*, enabling this check box ensures that any recent unsaved changes are included in the archive.

Step 8 Click **OK**.

You may see a warning about enabling file encryption on this page. AES file encryption can be configured using **Configure > Controllers > Security > File Encryption**. File encryption is highly recommended when archiving controller configurations over WANs and other public communications facilities.

Automatic Archival of Controller Configurations

WCS also provides a automated routine (known as the **Configuration Backup** scheduled task) that automatically archives the configuration of each reachable controller that has been defined to WCS.

Note For further information, see section 13.6 CSCsd54800—Config Backup Scheduled Task Fails if One Controller is Unreachable.

The Configuration Backup scheduled task can be configured to run at a pre-defined time of day and with a pre-defined repetition interval. It can also be submitted for execution on a on-demand basis.

See Configuration Backup, page 8-117 for further details on the **Configuration Backup** scheduled task.

Restoring Controller Configuration Archives

WCS provides the ability to manually restore an individual configuration archive to a controller via **Configure > Controllers > Commands > Upload/Download Commands > Download Config**. Note that controller configuration archives can only be restored on an individual, one-at-a-time basis.

Configuring WCS Campus, Building, Outdoor, and Floor Maps

Cisco WCS allows for the addition of *maps* to its internal database that can then be used to assist in the visualization of client, asset tag, and rogue location as well as estimated coverage during the monitoring of your wireless LAN. Adding maps to the Cisco WCS database enables you to view your managed system on realistic outdoor, campus, building, and floor plans that you have defined that allow more meaning to be imparted to the viewer. Maps can originate from actual floor plans that are imported into WCS using .PNG, .JPEG, .JPG, or .GIF graphic file formats (AutoCAD .DXF file formats are not supported at this time). After they are imported and sized, RF characteristics can be added to various building components to increase coverage prediction and design accuracy.

Maps are usually added in campus, building, and floor sequence; however, the existence of a campus map is not mandatory (buildings can be freestanding and not part of a campus in smaller designs). Floor maps cannot exist independently of building maps. Outdoor areas are typically associated with campus maps and do not exist independently.

The WCS *map editor* can be used to define, draw, and enhance floor plan information. The map editor enables the creation of obstacles that can be taken into consideration when computing RF prediction heat maps for access points. (Although supported, Cisco recommends the use of the map editor to draw walls and other obstacles rather than importing .FPE files from the legacy floor plan editor.) You can also add coverage areas that are used by the location appliance to locate clients and 802.11 active RFID tags and provide alarm notifications on their movement.

WCS *planning mode* is a feature that enables you to calculate the number of access points required to cover an area by placing fictitious access points on a map and allowing you to view the coverage area that they would yield. Based on the throughput specified for each protocol (802.11a or 802.11b/g), planning mode calculates the total number of access points required to provide optimum coverage in your network.

Detailed step-by-step guidance on how to define, add, and edit campus, building, and outdoor floor maps can be found in the *Cisco Wireless Control System Configuration Guide, Release 4.0*.

Configuring WCS to Manage the Cisco Wireless Location Appliance

The location appliance enhances the high-accuracy location capabilities that are integrated into location-enabled WCS servers. The location appliance enhances WCS location capabilities by computing, collecting, and storing historical location data and allowing WCS to display location data for multiple tracked devices at a time. In addition, the location appliance handles the dispatch of location notifications and provides the SOAP/XML API to which third-party applications can interface to the location information stored within the location appliance databases. Before use, the location appliance must be configured and defined to the WCS server that has been licensed for location services.

After initial IP parameter settings as described in the *Cisco Wireless Location Appliance—Installation Guide* and the *Cisco Wireless Location Appliance—Configuration Guide*, all configuration of the location appliance is performed from WCS using the menus and submenus located under the **Location** tab.

Complete guidance in configuring and managing the location appliance via the menus located under the WCS **Location** tab can be found in the *Cisco Wireless Location Appliance—Configuration Guide*. This includes step-by-step configuration instructions on the following topics:

- Adding and deleting location servers
- Synchronizing Cisco WCS and location servers
- Editing location server properties
- Managing location server users and groups
- Configuring location event notifications
- Monitoring location servers
- Performing location server maintenance

In addition, extensive coverage of location-based services and positioning technologies, location-aware design, deployment best practices and RFID tag technology are available in the following documents:

- Wi-Fi Location Based Services 4.1Design Guide—
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html
- Cisco Wireless Location Appliance: Deployment Guide—
  http://www.cisco.com/en/US/docs/wireless/technology/location/deployment/guide/depgd.html

Using WCS to Monitor Your Wireless Network

WCS facilitates the monitoring of device status within its management domain via several avenues. Whether looking at the omnipresent alarm counters that appear in the lower left-hand corner of every WCS screen or the detailed status information available under the **Monitor** tab, information about the current status of your enterprise network is presented to the operator in a clear, efficient, and visually attractive manner. Access to this information and more starts with a simple mouse click on the **Monitor** tab on the main menu bar (or the *Alt-M* keyboard shortcut).

The following sections briefly describe the information available to you under each of the selections in the **Monitor** menu tree. Keep in mind that as seen in the **Configuration** menus discussed previously, the majority of device status information in the WCS databases is accessible via multiple paths in the GUI. For example, although information about controller and lightweight access point status is readily available by clicking on **Monitor > Devices > Controllers** or **Monitor > Devices > Access Points** respectively, much of the same information is accessible via strategically located hyperlinks on many other **Monitor > Device** submenus as well.

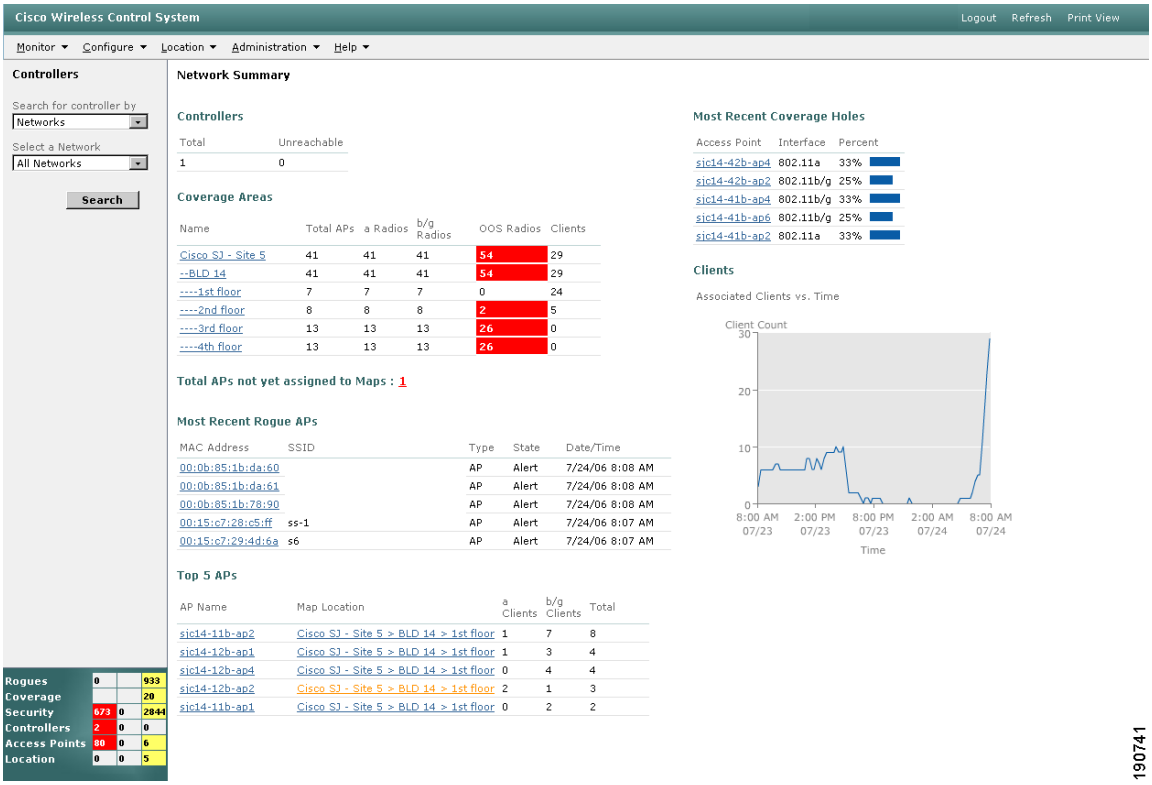
WCS also provides a northbound notification system that can dispatch e-mails to specified destinations (pager, cell phone, PDA, laptop, and so on) whenever certain types of alarms occur.

The following sections describe the monitoring capabilities of WCS and how these can be put to use in monitoring the enterprise wireless network.

Network Summary

WCS typically presents a summary page at the top of the Monitoring menu tree called the *Network Summary***.** Network Summary is presented immediately after clicking on the **Monitoring** main menu selection (or using the keyboard shortcut Alt-M). As shown in Figure 8-30, Network Summary shows what is currently taking place in your wireless network that may warrant your immediate attention.

Figure 8-30 Network Summary



Along with the information that is presented via the alarm summary panel in the lower left-hand corner of the screen, you are shown a cross-sectional view into the status of several key areas that may affect not only the operational and performance characteristics of your wireless LAN but its overall security as well.

The following can be learned from the Network Summary panel:

- Controllers—Total number of WLAN controllers defined to WCS and the number of controllers that WCS has determined to be unreachable (that is, time-outs to SNMP queries from WCS). For more details on precisely which controllers are unreachable, click **Monitor > Devices > Controllers**.

- Coverage Areas—Up to ten "coverage areas" that have been defined to WCS along with the total number of lightweight access points, access point radios, and clients found. Any access point radios that have been administratively disabled or down for other reasons are listed in the Out-Of-Service (OOS) column.

Note The use of "coverage areas" in the context of the Network Summary page should not be confused with the coverage areas that are defined in the location appliance.

  The coverage areas listing may consist of a combination of campuses, buildings, floors, or outdoor areas. If WCS determines that ten or more campus or standalone building maps have been defined, it displays a "View All Maps" hyperlink that enables you to jump to the **Monitor > Maps** page where the entire list of defined maps can be seen.

  Clicking on any of the hyperlinks shown in this area allows you to move to the associated map screen where you are able to obtain detailed information on which lightweight access points in that area are experiencing difficulties and what those difficulties may be. In some cases, a hyperlink may appear indicating the total number of lightweight access points that have not been assigned to any maps.

- Most Recent Rogue Access Points—This area lists information concerning the five most recently detected rogue access point alarms and provides hyperlink access to the **Alarm > Rogue AP** page. The **Alarm > Rogue AP** page lists more detail about the detected rogue access point such as its location, event history, and any rogue clients that may be associated with it.
- Top Five Access Points—The current list of the top five lightweight access points ranked by the total number of client associations. From this list, an AP Name hyperlink provides access to the associated **Monitor > Devices > Access Points** panel for each lightweight access point. The location hyperlink takes you to the floor level map where the lightweight access point has been placed.
- Most Recent Coverage Holes—The names of the lightweight access points that have generated the five most recent "coverage hole" alarms. A "coverage hole" is an alarm situation triggered because of the crossing of a minimum signal coverage threshold by a client. When an alarm is triggered, it usually indicates that a client has entered an area where the minimum signal detected by the client from any of the lightweight access points servicing that area is below pre-determined threshold levels. When this is communicated to WCS via SNMP, it normally results in the generation of a coverage hole alarm. Clicking on any one of the AP name hyperlinks found in this area takes you directly to the detailed coverage hole alarms page that displays the current alarm status.

  Keep in mind that although a coverage hole alarm may have already been cleared, the cleared alarm is still listed in this area unless superseded by other coverage hole alarms.

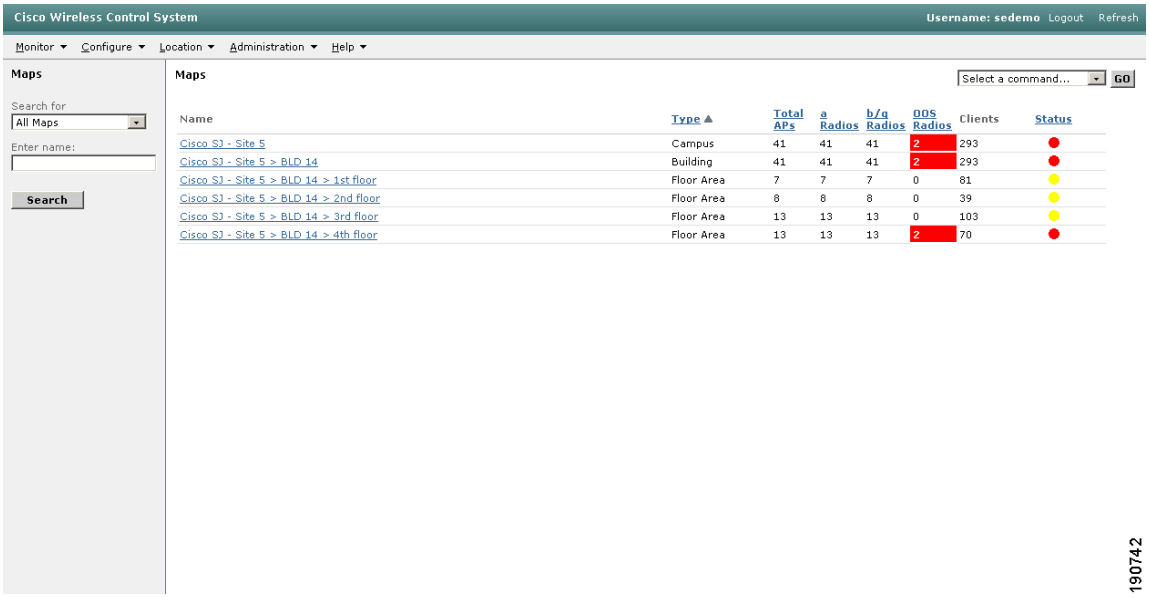
- Associated Clients versus Time—This graph shows the total number of associated clients across the WCS management domain. You can perform a mouse-over of various points on the graph that display additional information in a pop-up bubble about the number of users associated and the date/time that the sample was taken. There are no hyperlinks associated with the points on the graph.
- Critical, Major, and Minor Alarms—Although discussed here, this multi-colored rectangular area is present in the lower portion of the left-hand margin of virtually every WCS display. It contains a tabulation of the number of critical (red), major (orange), and minor (yellow) alarms for each resource category (rogues, coverage, security, controllers, access points, and location). If all alarms of a given type are cleared in a particular category, the count reflects zero and the color changes to white. This feature has been found to be very useful in every network management because it constantly keeps the WCS administrator abreast of all alarm counts while consuming minimal screen real estate.

Monitoring Maps

As discussed in the previous section, WCS allows for visual status of devices to be displayed on campus, building, floor, and outdoor maps. The following examines how **Monitor > Maps** allows the WCS user to fully take advantage of these capabilities in managing the enterprise wireless LAN.

The main page under **Monitor > Maps** (shown in Figure 8-31) contains similar information to what was displayed in the Coverage Areas portion of the Network Summary screen.

Figure 8-31 Monitor > Maps

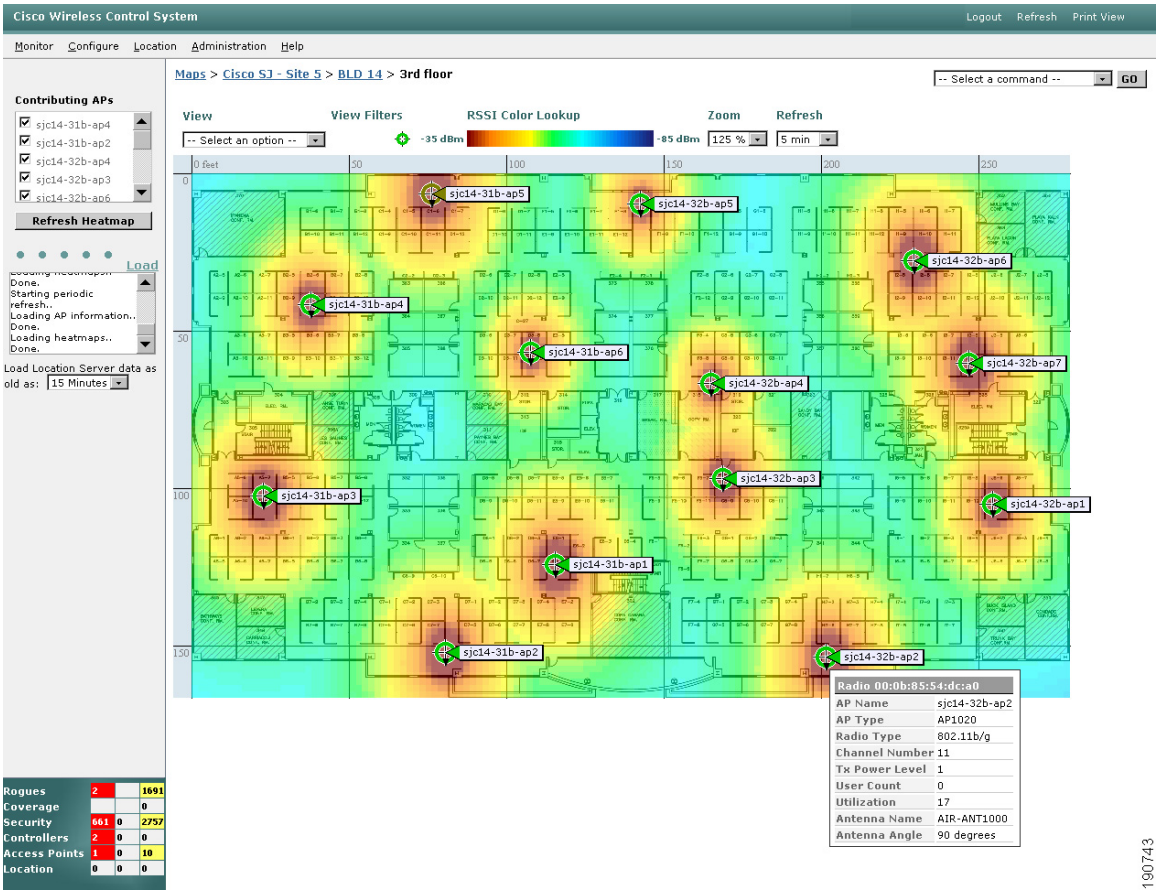


However, here you see the entire listing of all known maps instead of simply a summary excerpt. In large networks comprising more than a single campus with each in turn made up of several buildings with multiple floors, the viewer may find it easier to manage the contents of the display by using the "Search For" selector in the left-hand margin. The display content can also be sorted as per the viewers preference (default sort order is by type). This sort order can be changed by clicking on any of the column headings, which sort the display by the column values in either ascending or descending order.

Figure 8-31 shows that the visual alarm status color indication is provided for the indicated resources. Note that the alarm status of any map in the hierarchy depends not only upon the status of the resources on that map but also on the status of resources located on any lower level maps as well. Thus, if a resource on a floor map generates an event triggering a critical alarm, the campus and building maps as well as the floor map all show a red critical alarm status. In this manner, the presence of an alarm attracts the attention of the WCS administrator no matter what level of the campus hierarchy they happen to browse to in pursuit of the matter.

Clicking on any of the map name hyperlinks results in campus, building, floor, or outdoor area maps being displayed. Floor maps (shown in Figure 8-32) contain icons representing each lightweight access point. The color of these access point icons vary to reflect the state of alarm that has been triggered by events occurring at the lightweight access point.

Figure 8-32 Graphical Floor Map Showing AP Locations and Heat Maps



Floor maps can be viewed at various zoom settings (50–800 percent and full screen) with a screen refresh timer that can be configured from 5 seconds to 15 minutes. The following bullets outline just some of the information that WCS provides graphically using floor maps as shown in Figure 8-32:

- RF coverage predictions (heatmaps) based on current access point settings (with the ability to specify participating access points)
- Lightweight access point locations with antenna orientation and alarm status, and the ability to:
  - Filter by radio type (protocol of 802.11a, 802.11bg or both)
  - Display an icon label for each lightweight access point containing one of the following: channels, TX power, coverage holes, MAC address, AP name, controller IP, utilization percentage, profiles (load, noise, interference, and coverage), or user count
  - Limit heatmaps using an RSSI cutoff (not to be confused with **Location > Location Servers > Location Parameters > RSSI Cutoff**) of between -85 dBm to -60 dBm. This allows you to easily predict where the minimum acceptable RSSI for a particular wireless device (such as an 802.11 wireless phone) likely resides.

Using a version of WCS licensed for location-based services along with a location appliance adds graphical capabilities such as the following:

- Display location coverage areas and coverage markers
- Display the location of multiple clients simultaneously with the ability to:
  - Display as an icon label one of the following: IP address, username, MAC address, asset name, asset group, asset category, or controller IP address
  - Filter the displayed clients by IP address, user name, MAC address, asset name, asset group, asset category, SSID, radio type (protocol), and controller IP address
- Display of 802.11 asset tag locations with the ability to:
  - Display as an icon label one of the following: MAC address, asset name, asset group, and asset category
  - Filter the displayed asset tags by MAC address, asset name, asset group, asset category, and controller IP address
- Display of multiple rogue access point locations with the ability to filter by:
  - MAC address, on-network status (yes/no/either) or state (alert, known, acknowledged, contained, threat, or known contained)
- Display of multiple rogue access point clients with the ability to filter by:
  - Associated rogue access point MAC address
  - State (alert, contained, or threat)

Figure 8-32 also indicates a drop-down menu selector in the left-hand margin that allows all "live" location data retrieved from the location appliance to be filtered by age. In Figure 8-32, this is defaulted to 15 minutes but it can be set from 2 minutes to as long as 24 hours.

This is only a brief overview of the many capabilities available under WCS and its graphical monitoring facilities. Additional information pertaining to the entire range of information viewable under **Monitor > Maps** can be found in the *Cisco Wireless Control System Configuration Guide, Release 4.0*. Additional information can also be found in the WCS menu bar under **Help > Online Help**.

Information specific to the configuration of WCS floor maps for displaying the location of clients, asset tags, rogue access points, and rogue access point clients when using WCS with the Wireless Location Appliance can be found in the following documents:

- Wi-Fi Location-Based Services 4.1 Design Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html
- Cisco Wireless Location Appliance: Deployment Guide—http://www.cisco.com/en/US/docs/wireless/technology/location/deployment/guide/depgd.html

Monitoring Devices

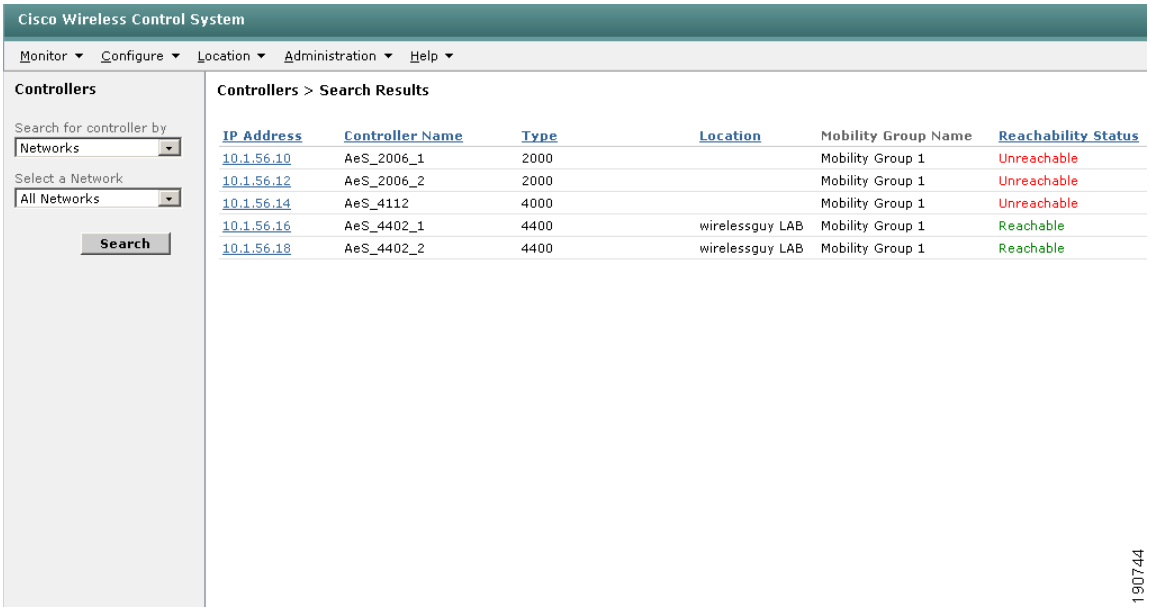
Thus far, this guide has examined the monitoring capabilities of WCS based primarily based on network geography. This section describes the capabilities available that are indexed instead by device category. This proves useful when you are primarily interested in seeing current alarm status for all devices comprising a resource category, regardless of where they may be located within the management domain (although you can filter the listings on location as well).

Clicking on **Monitor > Devices** on the main WCS menu bar shows that device status is grouped into four main device categories: Controllers, Access Points, Clients, and Tags. The subsections that follow take a brief look at each of these.

Monitoring WLAN Controllers

Clicking on **Monitor > Devices > Controllers** displays the page shown in Figure 8-33.

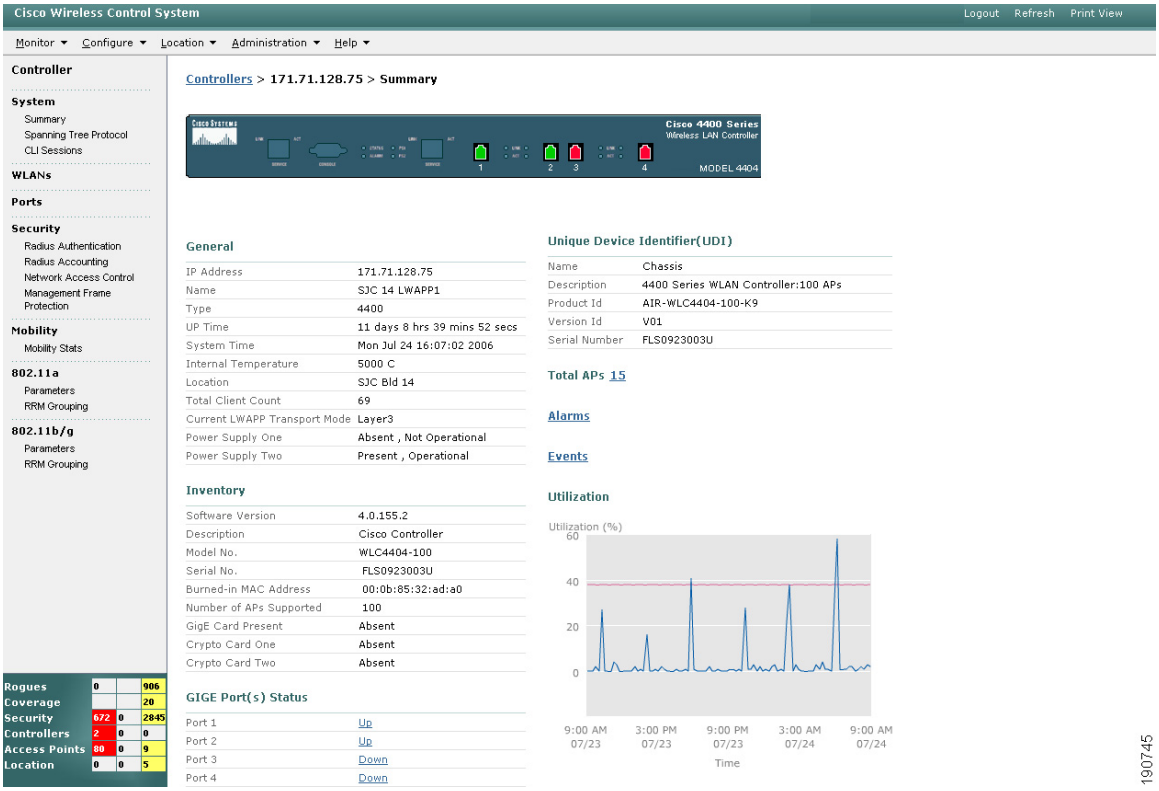
Figure 8-33 Monitor > Devices > Controllers



As seen previously in **Configure > Controllers**, Figure 8-33 indicates whether all controllers managed by this WCS indicate are SNMP reachable. A controller becoming unreachable is an event that triggers a critical alarm, so in this monitor screen it is shown in red. Clicking on the hyperlink for any controller IP address leads the WCS user to the **Controller > Summary** page, as shown in Figure 8-34. The **Controller > Summary** page is the main launching point from which you can drill down into more in-depth status information about a particular controller within the WCS management domain.

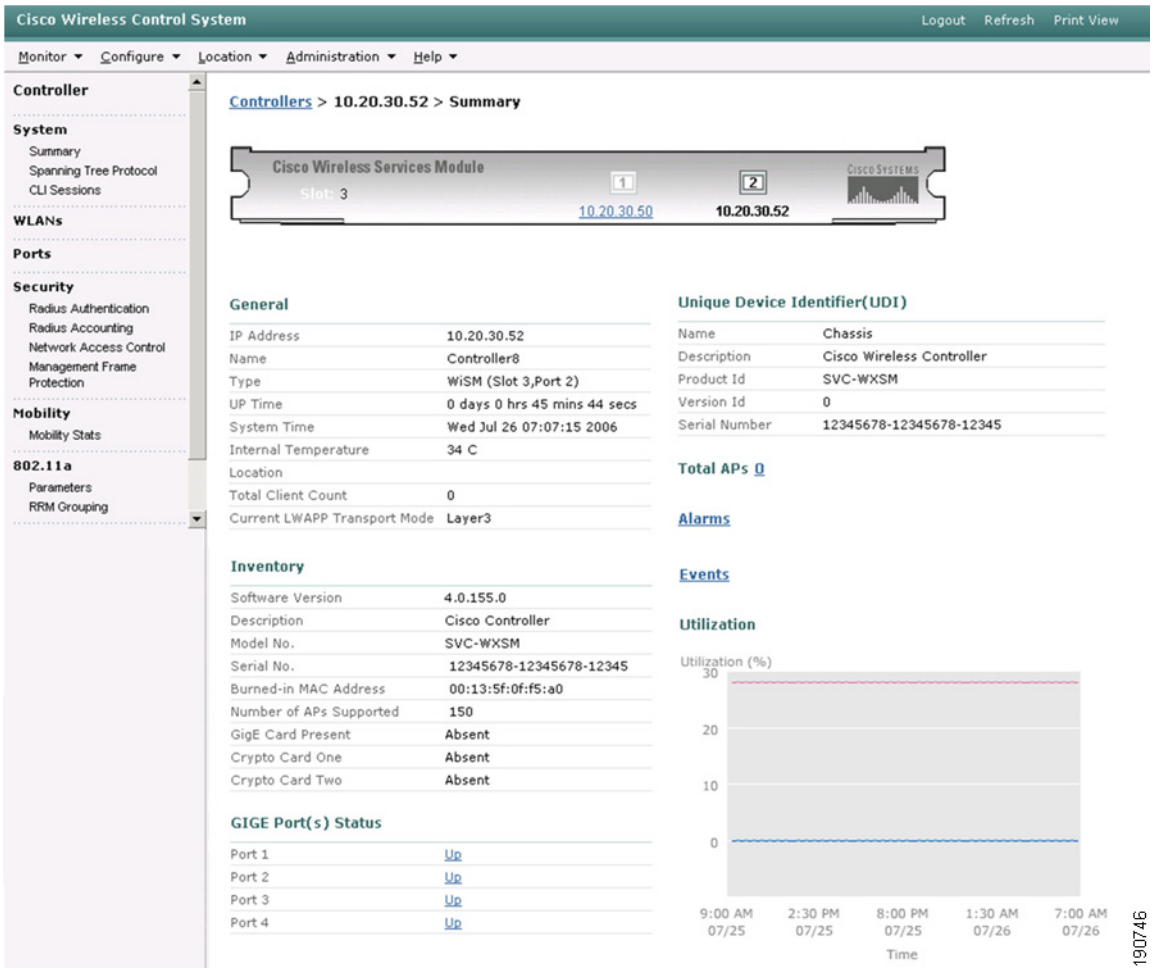
Figure 8-34 illustrates and example of a controller summary display for a Cisco WLAN controller model 4400 with 100 lightweight access point capacity.

Figure 8-34 Monitor > Devices > Controller Summary for 4400 Series WLAN Controller



The graphic that appears varies depending on the model of the controller hardware (4400, 2000, Cat6500/WiSM, ISR/WLCM, and so on). For example, the Cisco Catalyst 6500 Wireless Solutions Module (WiSM) and its two onboard controllers can be visually represented as shown in Figure 8-35.

Figure 8-35 Monitor > Controller > Summary for Catalyst WiSM



Note that in all cases, however, the screen format used in **Controller > Summary** is very similar with pertinent summary information in the main body of the screen and visual color representation used for the status of the physical Ethernet ports. Clicking on any of the red or green port graphics summons the **Monitor > Devices > Controllers > Ports** panel for the port in question, where a full range of Ethernet port performance information is available. Links are also available to applicable Alarms, Events, and AP Status pages from the controller summary display.

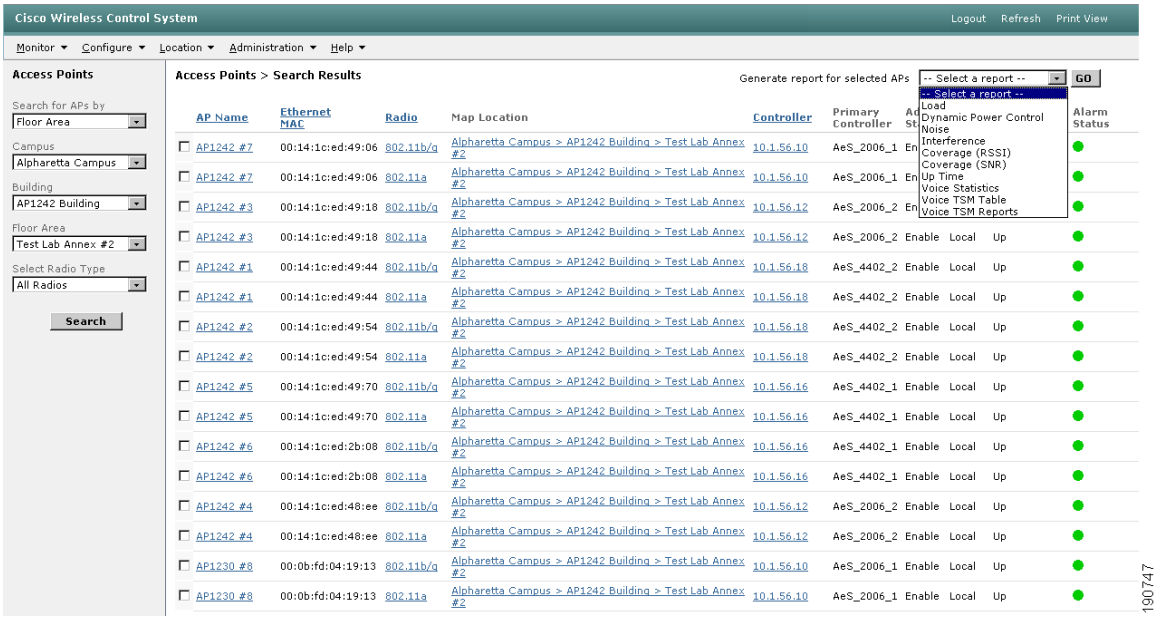
The left column of both Figure 8-34 and Figure 8-35 indicates the complete range of controller-specific information available from the controller summary page. WCS makes it possible to click on one category after another without requiring you to use the "back" browser function, thereby saving time and effort.

Monitoring Access Points

In addition to obtaining information about access point status indirectly via the **Monitor > Maps** and **Monitor > Devices > Controller** menu trees, WCS allows immediate and direct access the same information via the **Monitor > Devices > Access Points** menu selection. After clicking on **Monitor > Devices > Access Points**, you are presented with the **Access Point > Search Results** menu shown in Figure 8-36. Depending on the number of access points that WCS has discovered, the complete list of

search results menu may be quite long. Therefore, the "Search for APs" and "Select Radio Type" filters in the left-hand margin can be especially useful in narrowing down the total number of access points displayed.

Figure 8-36 Monitor > Devices > Access Points > Search Results



The various hyperlinks available from this screen allow access to a wide variety of information about the lightweight access point and its radio interfaces, the location map that it is currently assigned to, the controller to which it is currently registered as well as detailed information concerning the alarms that are currently active regarding it. Note that the Alarm Status indicator on this page is actually a hyperlink to detailed information about the alarm.

As was seen with **Configure > Access Points**, the search results page shown in Figure 8-36 displays *all* lightweight access points known to this WCS including any lightweight access points that are not currently registered to any WLAN controllers in the management domain. However, WCS *only* allows you to display detailed current status for lightweight access points that are currently registered to a WLAN controller (as indicated by the IP address of a WLAN controller appearing in the "Primary Controller" display column).

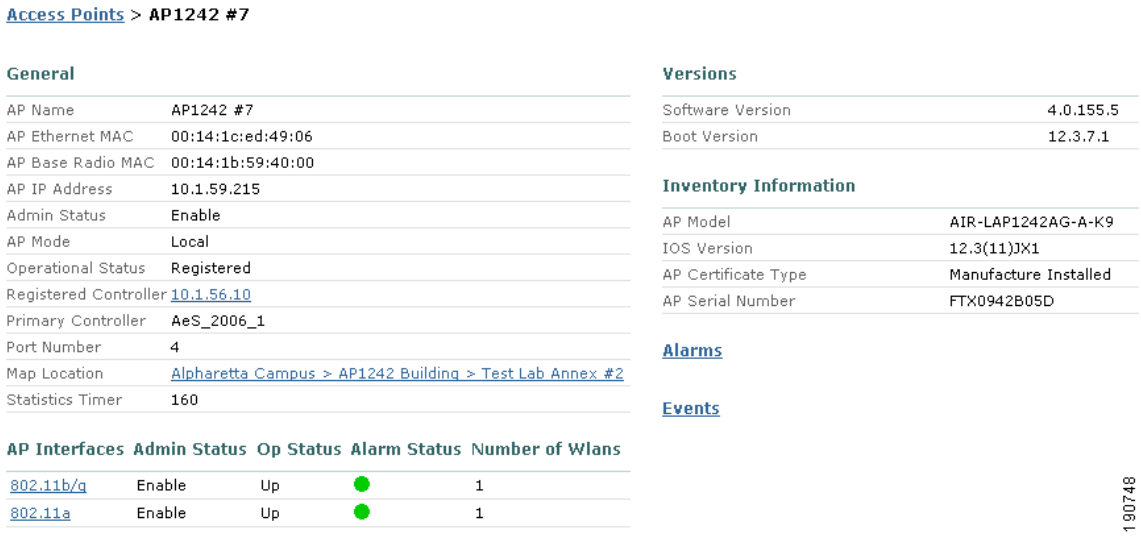
The drop-down command selector in the upper right-hand corner of Figure 8-36 indicates that several useful reporting functions are available from the search results page. Here you see the ability to generate load, dynamic power control, noise, interference, client distribution by RSSI / SNR, total uptime, and voice statistics, and traffic stream metrics reports for selected access points. This can be done by selecting up to five access point radio interfaces shown on the **Access Points > Search** Results screen, selecting a report type from the "Select a Report" menu drop-down at the top right-hand corner of the screen, and then clicking on **GO**.

Note All five selected access points *must* be displayed on the same screen to be selected for reporting (paging forward or backward for additional selections is not allowed). The uptime report allows only one access point to be selected.

Samples of the reports that are generated by these seven options can be seen in Appendix E, "Sample Monitor > Devices > Access Points Reports."

Clicking on any of the AP Name hyperlinks yields the AP detail screen shown in Figure 8-37. This provides hyperlinks to the WLAN controller information found in **Monitor > Controllers** and the map information found in **Monitor > Maps** as well as hyperlinks to any alarms or events that concern this access point. On this screen, you can verify general operational parameters, software levels, access point model, serial number as well as the type of certificate with which it was provisioned. In addition, this page provides hyperlinks to 802.11a and 802.11b/g radio interfaces along with alarm status hyperlinks.

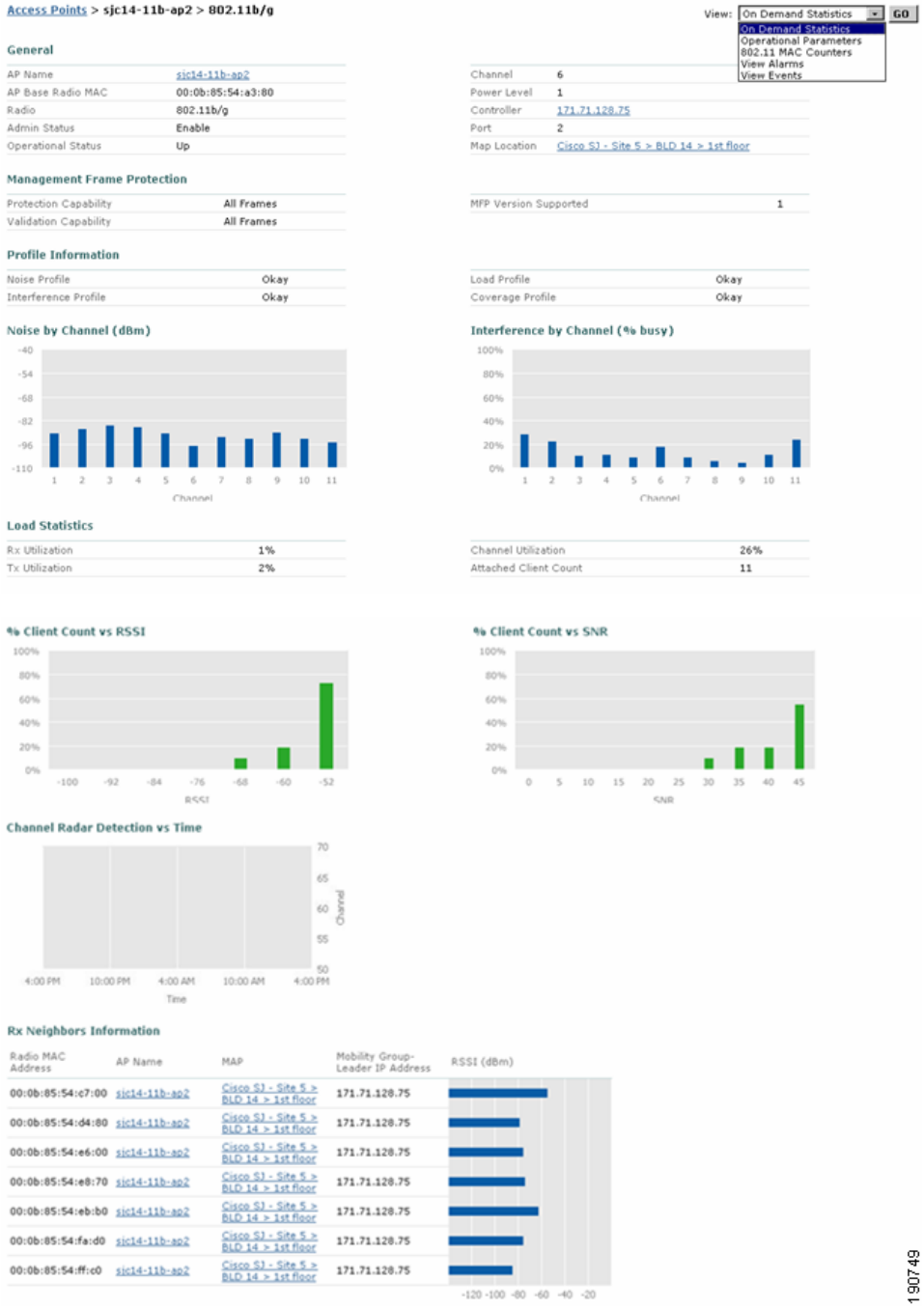
Figure 8-37 Access Point Detail



Clicking on one of the AP interface hyperlinks at the bottom of Figure 8-37 brings up the on-demand statistics page for the access point (Figure 8-38) where information about the status of the four radio resource management (RRM) profiles can be found (load, coverage, noise, and interference) along with information about the status of Management Frame Protection (MFP) on that access point. In addition, graphical charts displaying noise and interference by channel, percentage of client count, and channel radar detection along with receive, transmit, and channel utilization metrics can be found here and are illustrated in Figure 8-38. A bar-chart displaying the RSSI of neighboring lightweight access points as last detected by the lightweight access point you are monitoring is also shown.

Using the selector in the upper right-hand corner of the on-demand statistics page shown in Figure 8-38, considerable detail is available about access point operational parameters, 802.11 MAC counters, and any outstanding alarms and events associated with this access point.

Figure 8-38 Access Point On-Demand Statistics Display



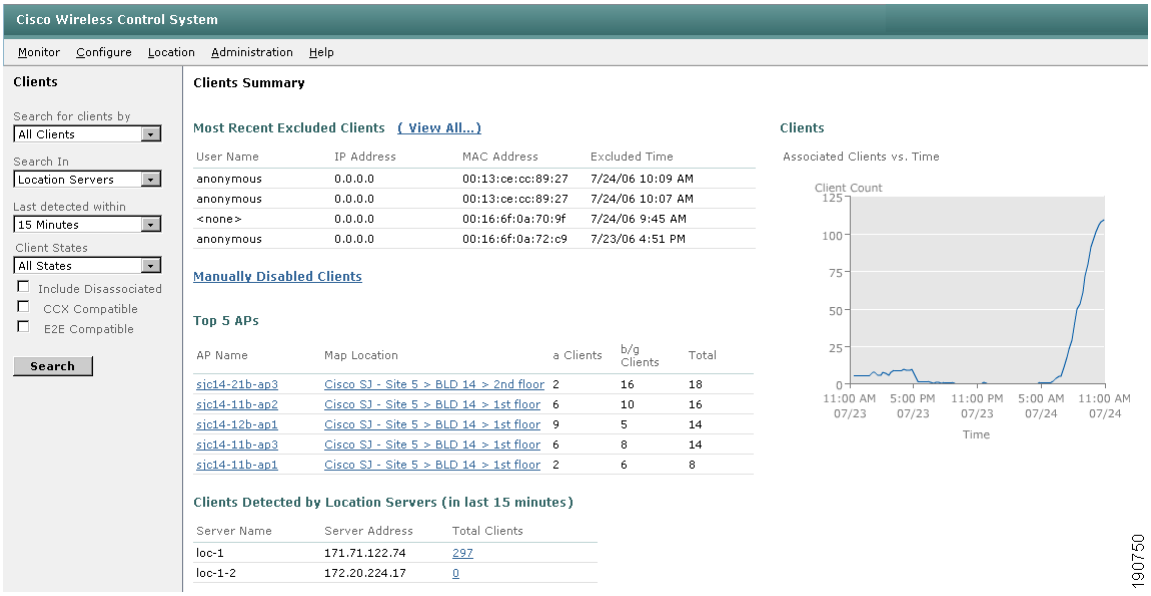
Monitoring Clients

As seen in the previous sections, WCS indirectly makes information available about clients associated to lightweight access points and controllers via the **Monitor > Devices > Controllers** and **Monitor > Devices > Access Points** menu options. WCS provides for direct access to an even larger base of client information via **Monitor > Devices > Clients**.

Although WCS is not a "client manager," it does allow you to configure and manage the various aspects of how client devices are permitted to interact with the network infrastructure. Through its tight integration with the various controllers, lightweight access points, and location servers comprising the wireless network, WCS accumulates a lot of information about the activities of clients on the network, regardless of whether they are probing, associated, or currently disassociated. This section briefly describes some of the information available via the **Monitor > Devices > Clients** selection.

After clicking on **Monitor > Devices > Clients,** the Clients Summary screen (seen in Figure 8-39) is immediately presented.

Figure 8-39 Monitor > Devices > Clients Summary



As seen in other summary screens, Client Summary attempts to display an overall view of client activity in your wireless LAN by displaying information in the following basic areas:

- Most Recent Excluded Clients—This area lists the clients that have been excluded from using the wireless LAN (also known as "blacklisted") because of the detection of one or more policy violations. For example, the client may have attempted association or 802.1x authentication and failed multiple times in succession. Security policies in the system normally exclude such a client from associating with the WLAN for a period of time as a security precaution against a possible intruder mounting an attack. Exclusion rules such as this are configurable via the WLAN template available at **Configure > Templates > WLAN**.

  Additional information regarding configuring client exclusion and the timeouts that are available can be found in the WCS menu bar under **Help > Online Help**.

  To view additional information about any of the excluded clients listed in this section, click on the **View All** hyperlink. This displays an Alarms screen where all the excluded clients are listed. The text of the reason for exclusion can be viewed by performing a mouse-over of the failure object name. Clicking on the failure object name hyperlink of any client displays detailed information about the alarm including hyperlinks to view the event history.

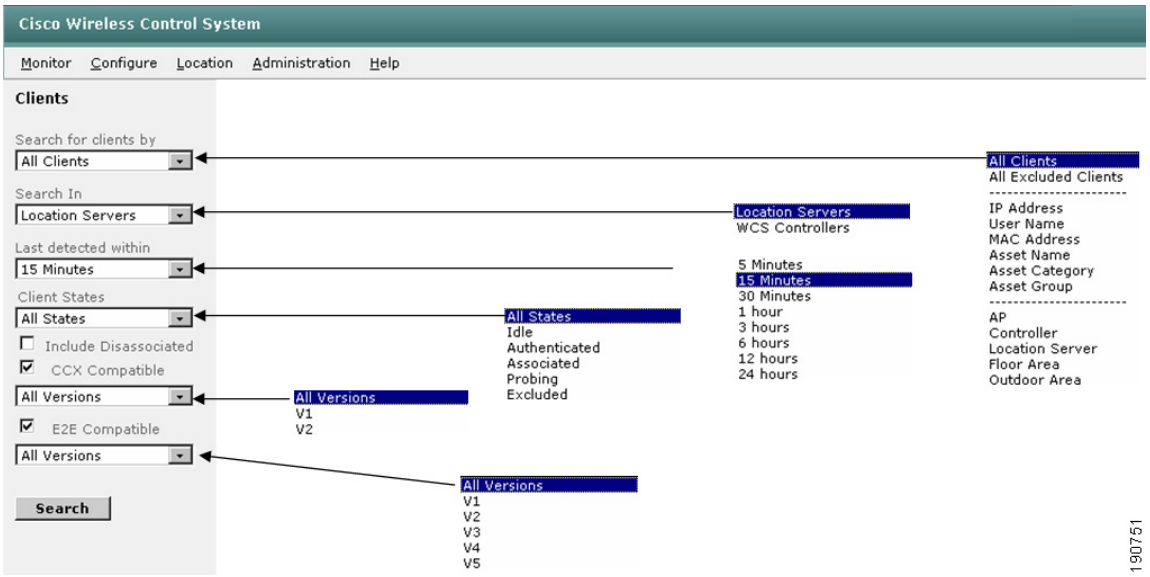
- Manually Disabled Clients—This hyperlink takes you to the **Configuration > Templates > Security > Disabled Clients** page where the current listing of clients that have been administratively excluded can be viewed.

- Top Five Access Points—This area refers to the same information as was shown on the Network Summary screen. See Network Summary, page 8-44 for further details.
- Clients Detected by Location Servers (with Fifteen Minutes)—This area indicates each location server that has been defined to WCS along with a hyperlink enumerating the total number of clients that have been detected within the last fifteen minutes. Note that if a location server is not defined to WCS, this area is still present; however, no entries for location servers are shown. Similarly, if location servers are defined but unreachable, the total client column shows a red "unreachable" alarm indicator.

  The total count of clients is a hyperlink that links the WCS user to the same information available by manually configuring the left-hand margin "Search For" feature. In this case, the hyperlink displays all clients found in all states in that particular location server within the last fifteen minutes.
- Associated Clients vs. Time—A graphical depiction of the number of associated clients plotted against time. By performing a mouse-over of various points on the graph, you can read the number of clients that were detected as associated at that particular sampling interval. The data points on the graph do not provide any hyperlink capability.

Control over the data displayed in **Monitor > Devices > Clients** is provided by the "Search For" selection bar in the left-hand margin. Figure 8-40 illustrates the full range of search criteria that are available to the WCS administrator when using this selection bar.

Figure 8-40 Search Criteria Available under Monitor > Devices >Clients



After selecting the appropriate criteria as shown in Figure 8-40, WCS returns a detailed listing of results in which several fields (user, AP, Map Location, and Link Test) are hyperlink-enabled as shown in Figure 8-41. Note the display of the miniature location floor map when performing a mouse-over of the user name hyperlink. Although small in size, this location floor map does indeed indicate the approximate location of the client. This handy method of quickly scanning each client in the list for their approximate location is available only when using a location-enabled version of WCS with the Wireless Location Appliance.

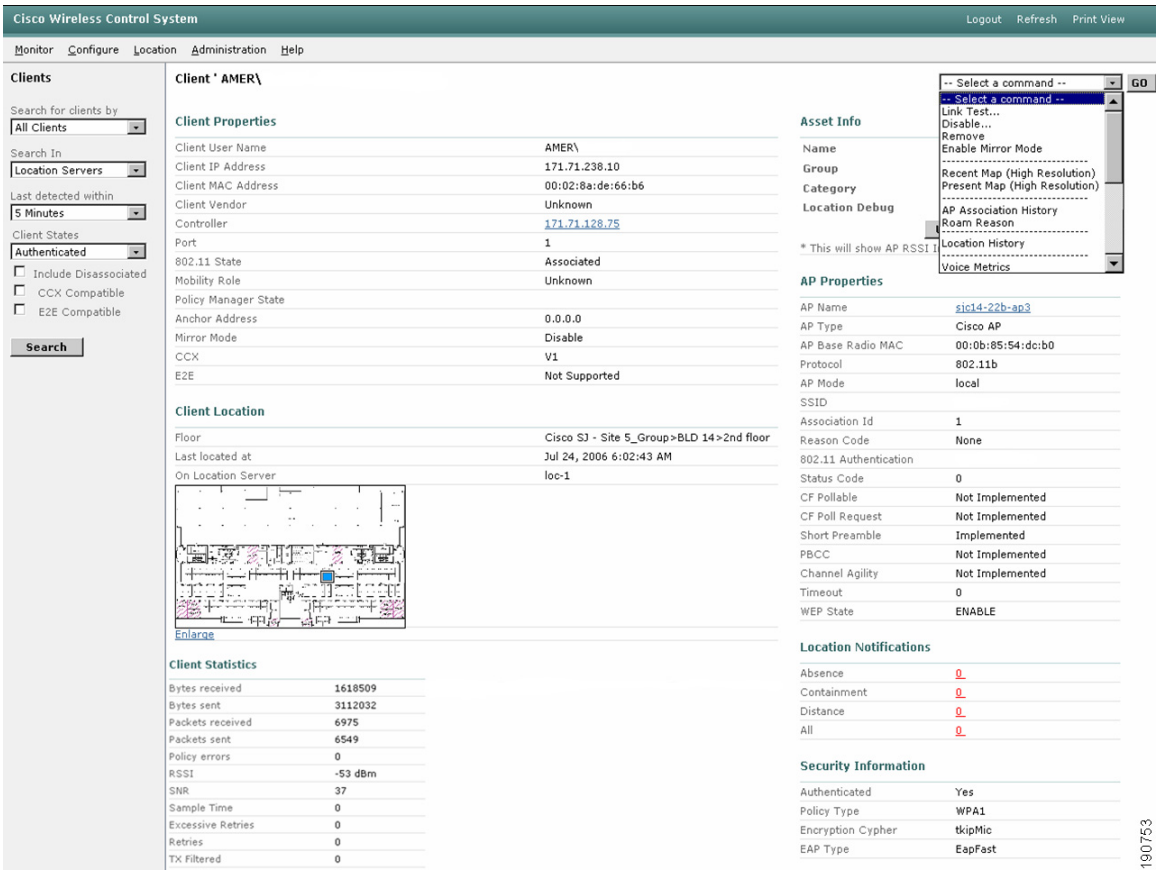
Figure 8-41 Monitor > Devices > Clients Listing

User	Vendor	IP Addr	MAC Addr	AP	Loc Server	802.11 State	SSID	Authenticated	Protocol	Map Location	
<none>	Unknown	0.0.0.0	00:02:8a:a2:2e:a0	00:0b:85:54:dc:b0	TME Loc2	Probing		No	802.11b	Cisco SJ - Site 5 Group>BLD 14>2nd floor	Link Test
one>	Unknown	0.0.0.0	00:02:8a:dc:40:74	00:0b:85:54:e5:70	TME Loc2	Probing		No	802.11b	Cisco SJ - Site 5 Group>BLD 14>3rd floor	Link Test
<no			e:44:1d:36	00:15:c7:a9:43:10	TME Loc2	Probing		No	802.11b	Cisco SJ - Site 5 Group>BLD 14>4th floor	Link Test
<no			e:45:65:e3	00:15:c7:a9:0b:20	TME Loc2	Probing		No	802.11a	Cisco SJ - Site 5 Group>BLD 14>4th floor	Link Test
<none>	Netgear	0.0.0.0	00:09:5b:2f:dc:9f	00:15:c7:a9:43:10	TME Loc2	Probing		No	802.11a	Cisco SJ - Site 5 Group>BLD 14>4th floor	Link Test
<none>	Netgear	0.0.0.0	00:09:5b:68:7f:c7	00:0b:85:54:e8:70	TME Loc2	Probing		No	802.11a	Cisco SJ - Site 5 Group>BLD 14>2nd floor	Link Test
<none>	Netgear	0.0.0.0	00:09:5b:a2:75:eb	00:0b:85:54:dc:b0	TME Loc2	Probing		No	802.11b	Cisco SJ - Site 5 Group>BLD 14>2nd floor	Link Test
<none>	Unknown	0.0.0.0	00:0a:5e:4b:74:a1	00:15:c7:a9:08:40	TME Loc2	Probing		No	802.11a	Cisco SJ - Site 5 Group>BLD 14>4th floor	Link Test
<none>	Unknown	0.0.0.0	00:0b:5f:6e:5b:74	00:0b:85:54:c7:00	TME Loc2	Probing		No	802.11b	Cisco SJ - Site 5 Group>BLD 14>1st floor	Link Test
<none>	Unknown	0.0.0.0	00:0b:fc:ff:af:30	00:0b:85:54:d1:c0	TME Loc2	Probing		No	802.11a	Cisco SJ - Site 5 Group>BLD 14>2nd floor	Link Test
<none>	Unknown	0.0.0.0	00:0b:fc:ff:af:50	00:0b:85:54:dc:b0	TME Loc2	Probing		No	802.11a	Cisco SJ - Site 5 Group>BLD 14>2nd floor	Link Test
<none>	Unknown	0.0.0.0	00:0b:fc:ff:af:b0	00:0b:85:54:ea:40	TME Loc2	Probing		No	802.11a	Cisco SJ - Site 5 Group>BLD 14>2nd floor	Link Test
<none>	Unknown	0.0.0.0	00:0b:fd:01:06:08	00:0b:85:54:e6:00	TME Loc2	Probing		No	802.11a	Cisco SJ - Site 5 Group>BLD 14>1st floor	Link Test
<none>	Intel	0.0.0.0	00:0c:f1:15:f3:94	00:15:c7:a9:42:60	TME Loc2	Probing		No	802.11b	Cisco SJ - Site 5 Group>BLD 14>4th floor	Link Test

190752

Clicking on the username hyperlink produces the Client Detail page (shown in Figure 8-42) that contains a wealth of information about the properties and statistics associated with the monitored client. Associated access point properties and security summary information for the client is also available from this page. If a location-enabled version of WCS is used with the location appliance present, a current floor map (which can be enlarged) showing the estimated location of the client is displayed under the Client Location heading.

Figure 8-42 Monitor > Devices > Clients Detail Page



The location notification alarm display, AP name, and controller IP address are all hyperlinks leading to further detail about location notification alarms that may have been generated based on the movement of this client, the lightweight access point to which this client is associated, and the controller to which the lightweight access point is registered. The asset name, group, and category of the client device can also be updated in this location. Asset information entered for WLAN clients here can be used to define client filters in other WCS functions. For example, asset information can be used when large groups of WLAN clients must be quickly narrowed down by asset group or category and displayed as icons when viewing devices on location maps via the **Monitor > Maps** facility.

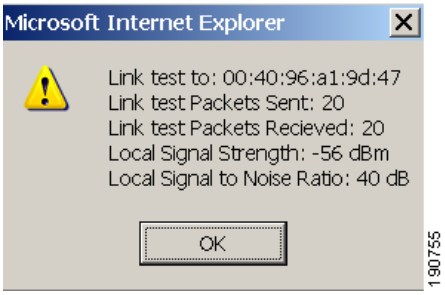
The client detail page also provides graphical trending displays for client RSSI, SNR, packets sent, and packets received, as shown in Figure 8-43.

Figure 8-43 Monitor > Devices > Clients Detail Graphical Displays

Using the command drop-down selector in the upper right-hand corner of the client detail screen in Figure 8-42, you can select from the following options:

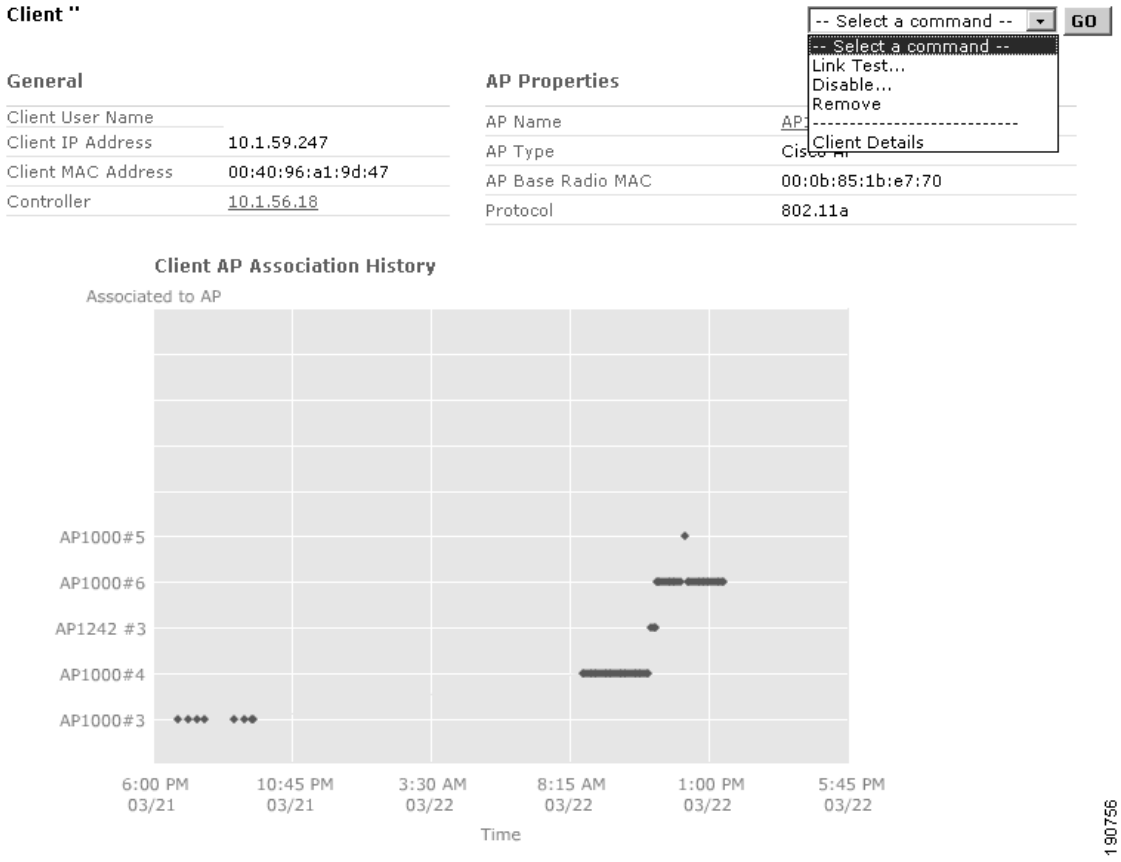
- Link Test—Performs a test of the client wireless link and displays the results as shown in Figure 8-44.

Figure 8-44 Link Test Results



- Disable—Manually adds the client to the client exclusion list. Performing this action immediately de-authenticates/disassociates the client. Its newly-added presence on the exclusion list then prevents it from re-connecting.
- Remove—Disassociates/de-authenticates the client but does not place it on the exclusion list.
- Enable Mirror Mode—Enables this client as a candidate for the mirroring of all data originating from or destined to it. The data is mirrored to a spare Ethernet port on the WLAN controller that you select (you cannot use the service port interface for mirror mode). To use this function, you must enable port mirroring on the WLAN controller via **Configure > Controllers > Ports > General Config > Mirror Mode** and use an Ethernet protocol analyzer to capture the mirrored data. One method of accomplishing this is to connect the mirrored port on the controller to a standalone Ethernet switch (not part of the network to which the controller is already attached so as to prevent any spanning tree loops) and logically connect that switchport to a port on the standalone switch to which the Ethernet protocol analyzer is to attached, using the Cisco Catalyst Switched Port Analyzer (SPAN) feature. Information about how to configure the SPAN feature for various models of Catalyst switches can be found by performing a search at the following URL: http://www.cisco.com.
- Recent Map and Present Map—These two functions cause WCS (rather than the location appliance) to display the location of a client on the appropriate floormap, using either recent location history data or current client RSSI data. Note that when choosing to have WCS locate the client using current RSSI data, client wireless connectivity is briefly interrupted while the data is gathered. The client should reconnect and resume service with minimal disruption. For further information about using these two functions, see On-Demand Location of WLAN Clients, page 8-83.
- AP Association History—Selecting this function displays a graphical plot of the access points with which this client has associated versus time (shown in Figure 8-45). Note that there is a drop-down command selector in the upper right-hand corner that offers many of the same options just discussed as well as a link back to the client details screen.

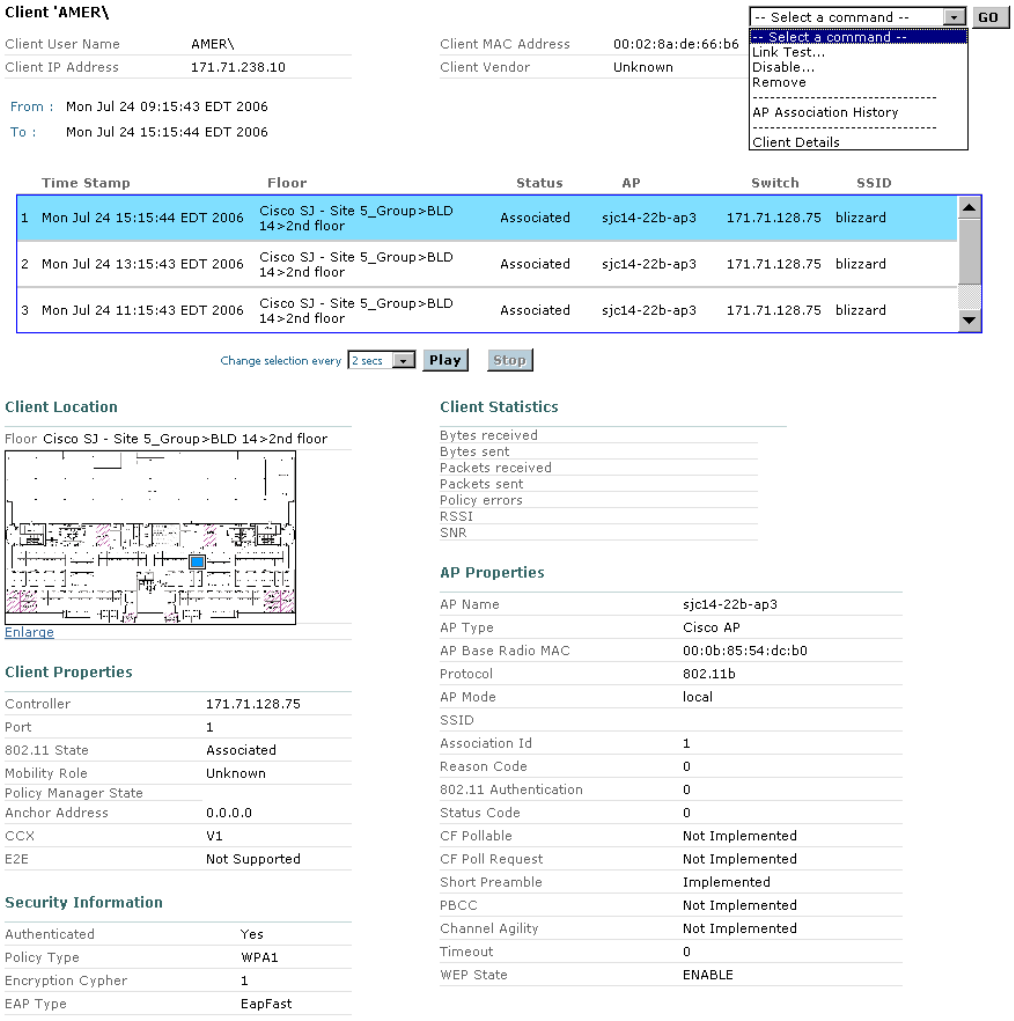
Figure 8-45 Monitor > Clients > AP Association History



- Roam Reason—Using this option, information about when and why a client roamed within the environment can be found. A "Roam Reason" Report is generated that lists the following:
  - MAC addresses of the current as well as the immediately previous access point to which the client associated
  - The previous access point SSID and channel
  - The roam transition time
  - The reason why the client roamed
- Location History—This option appears with versions of WCS licensed for location use and is only functional when a location appliance is installed. It allows for the sequential display of the location history associated with a client device to better visualize and trace the movement of the client throughout the environment over time. This can be very useful, for example, in security and monitoring applications. WCS and the location appliance make it possible to view each location history record sequentially in this fashion, played back with a configurable time delay. The granularity of the "movement" shown depends on the interval with which client history records are recorded in the database. To see location history played back in this fashion, click the **Play** button as shown in Figure 8-46. Past location history should be displayed both in tabular and graphical form. Large amounts of location history data may be more readily viewed by reducing the "Change Selection Every" interval from 2 seconds to 1 second.

For additional details about location history features and the location appliance, see *Wi-Fi Location Based Services 4.1Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html.

Figure 8-46 Monitor > Clients > Client Detail > Location History



- Voice Metrics—This displays the voice stream metrics report and requires that voice traffic stream metrics (**Configure > Controller > ipaddress > 802.11bg > Voice Parameters > Enable Voice Metrics**) be enabled on the WLAN controller. See the *Cisco Wireless LAN Controller Configuration Guide, Release 4.0* and *Cisco Wireless Control System Configuration Guide, Release 4.0* for further information about enabling voice stream metrics and voice metric reporting.

Monitoring Asset Tags

Information about asset tags that have been detected by lightweight access points and controllers can be accessed indirectly via the **Monitor > Controllers** and **Monitor > Access Points** menu selections. When WCS has been installed and licensed for location-based services, the WCS user is able to directly access this information via the **Monitor > Devices > Tags** function. Note that the **Monitor > Devices > Tags** submenu does not appear for a WCS that has been licensed only for base level functionality (WCS-Base).

Only 802.11 active RFID Layer 2 asset tags (such as those from AeroScout) are displayed under **Monitor > Devices > Tags**. Asset tags acting in Layer 2 mode typically do not associate or authenticate to the WLAN but rather communicate their payload information via Layer 2 multicasts. Other types of 802.11 active RFID asset tags that associate/authenticate to the wireless infrastructure are detected as WLAN clients and are not listed under **Monitor > Devices > Tags** (instead, they can be found under **Monitor > Devices > Clients**).

Note For a detailed discussion of Layer 2 and other types of asset tag technologies, see the *Wi-Fi Location-Based Services 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html.

After clicking on **Monitor > Devices > Tags,** the Tag Summary screen (seen in Figure 8-47) displays the total number of asset tags detected by the location appliance within the previous fifteen minutes as a hyperlink. Clicking on this hyperlink allows you to quickly initiate a search in the associated location server for all tags from all vendors detected within the last fifteen minutes.

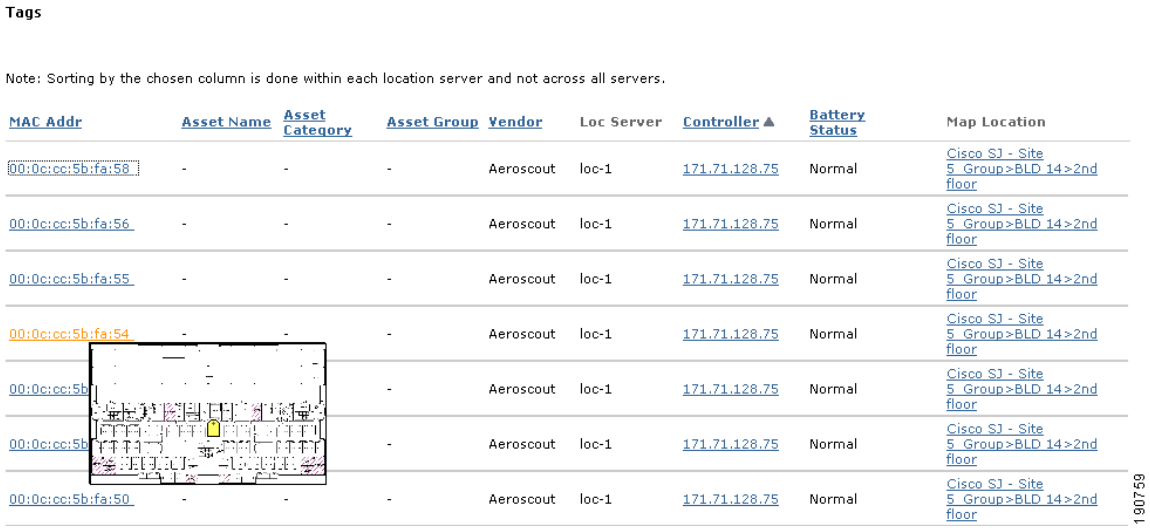
Figure 8-47 Monitor > Tags Tag Summary Screen

If you want to modify the terms of the search (that is, to specify a different search time frame, vendor, or other tag search criteria) use the drop-down menus in the left-hand margin of Figure 8-47.

The tag search results page, tag detail page, and asset tag location history display all have a very similar look and feel to their respective client page counterparts discussed in the previous section. On the Tag Search Results page, you can see tag-specific information such as tag asset information, tag vendor, location server, and tag battery status. Of the displayed fields, tag MAC address, switch IP address, and tag map location are hyperlink-enabled.

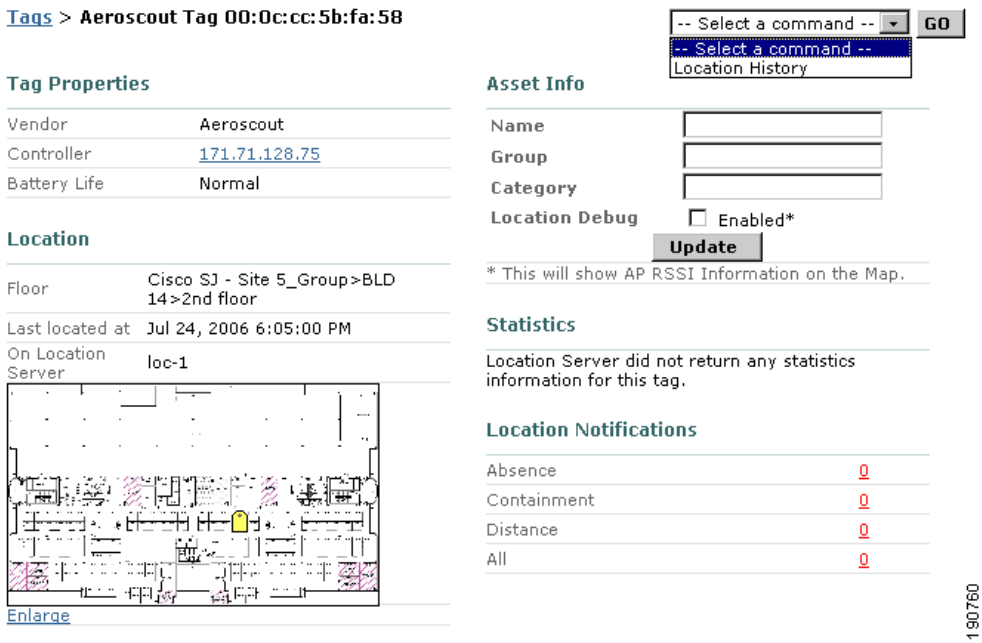
Note that performing a mouse-over of the tag MAC addresses shows a miniature location map with the asset tag located estimated using a yellow tag icon, as shown in Figure 8-48.

Figure 8-48 Tag Search Results



The tag detail page is similar to what has been seen before for clients, and allows for only the Location History option via the right-hand command drop-down menu selector (see Figure 8-49).

Figure 8-49 Tag Detail Page

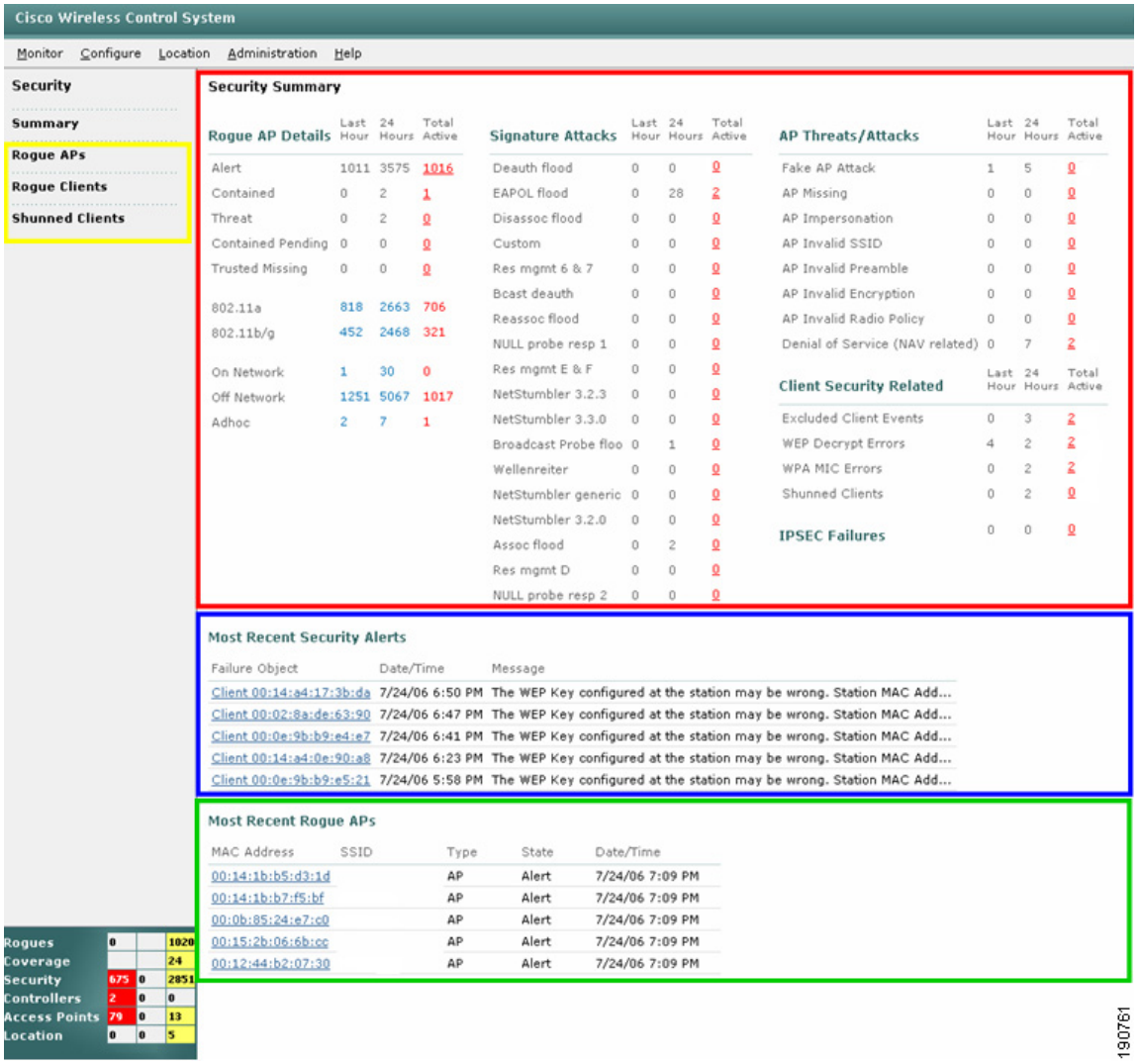


The format and function of the asset tag location history display is similar to that described for clients as well. Note the check box for "Location Debug" that enables WCS to display graphically the RSSI at which each access point has detected the asset along with an indication of how much time has passed since the asset tag has been detected. The enabling of Location Debug and how it can be used to facilitate the proper design and maintenance of a location-aware Cisco WLAN is discussed further in the *Wi-Fi Location-Based Services 4.1 Design Guide*.

Monitoring Security

WCS provides a summarization of security-related events in the network via the Security Summary page (shown in Figure 8-50), which is available from the main menu bar via **Monitor > Security**. Although every page in WCS displays the latest tally of critical, major, and minor alarms via the lower left-hand corner (the alarm monitor), the Security Summary page provides an especially detailed view of the security-related events that have recently transpired in the wireless network.

Figure 8-50 Monitor > Security Summary Page with Main Information Groups Emphasized



Because consumer-grade 802.11 access points are so readily available, maintaining constant vigilance against the proliferation of unauthorized rogue access points and rogue clients in the enterprise is typically one of the top priorities of security staff. Employees, contractors, and sometimes even visiting customers and guests commonly plug these unauthorized access points into existing LANs or build *ad hoc* wireless networks to facilitate their own mobility without the knowledge or consent of corporate IT or security departments.

These rogue access points can be a serious breach of network security because they can be very easily plugged into a network port behind the corporate firewall. Because these products often ship configured for easy wireless connectivity, security is usually disabled, and their owners often leave these settings at factory defaults. This being the case, it is very easy for malicious third-party users or outside hackers to gain access to the corporate intranet by using these unauthorized rogue access points as an easy entry point to the corporate intranet. After being discovered, the location of these unsecured portals can be published on the Internet, thereby drawing even greater attention to them from an unscrupulous community and increasing the odds of an enterprise security breach.

Rather than having a technician with a wireless analyzer constantly patrolling physical sites for new rogue access points, the Cisco Unified Wireless Network offers the ability to automatically collect information on these unauthorized devices via its managed access points. This allows the system administrator to determination the location of these rogues and make conscious decisions about their status.

These integrated anti-rogue client and access point capabilities allow WCS system administrators and other authorized users to do the following:

- Receive new rogue access point and client notifications and establish the location of these rogues, eliminating the need for a technician to periodically visit each site with a wireless network analyzer
- Monitor unknown rogue access points until they are eliminated or consciously acknowledged as benign
- Initiate containment actions against rogue access points and their clients by sending the clients deauthenticate and disassociate messages, discouraging further communication
- Acknowledge the presence of benign rogue access points when they are not attached to the enterprise wired LAN and can be seen to be located outside of the physical premises of the enterprise
- Acknowledge the presence of benign rogue access points when they are not attached to the enterprise wired LAN and can be seen to be located within the physical premises of the enterprise. These types of rogues typically operate in testing labs or other standalone networks that are not attached to the enterprise intranet. Rogue operation of this nature is typically for legitimate business purposes and is performed under the full knowledge and approval of corporate security departments.
- Tag other rogue access points as unknown until they are eliminated or acknowledged
- Tag rogue access points as contained, which implies that the containment process has been successful

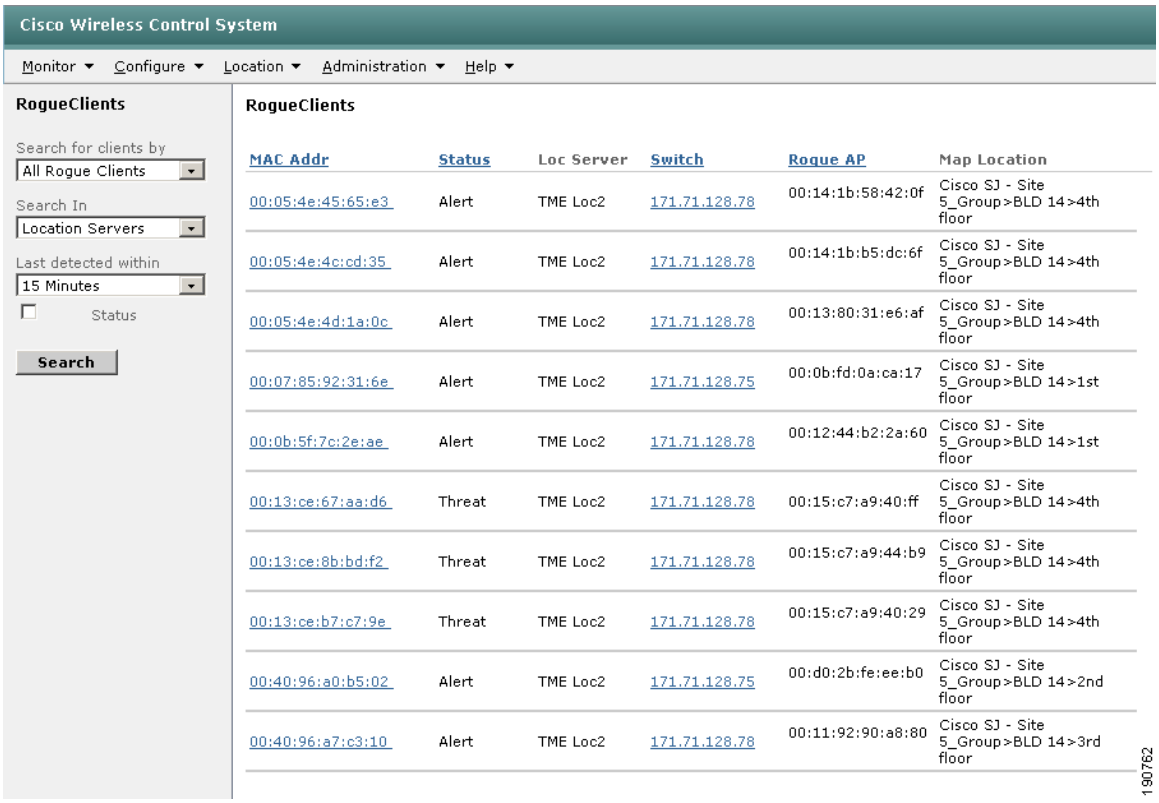
Figure 8-50 shows the Security Summary page divided into four key areas:

- *Fast access hyperlinks* (shown within the yellow rectangular area in the left-hand column):
  - Listing of rogue access point alarms of all severities and categories

    See Monitoring Events, page 8-75 for a further discussion of the rogue access point alarm detail page.
  - Rogue Client search screen

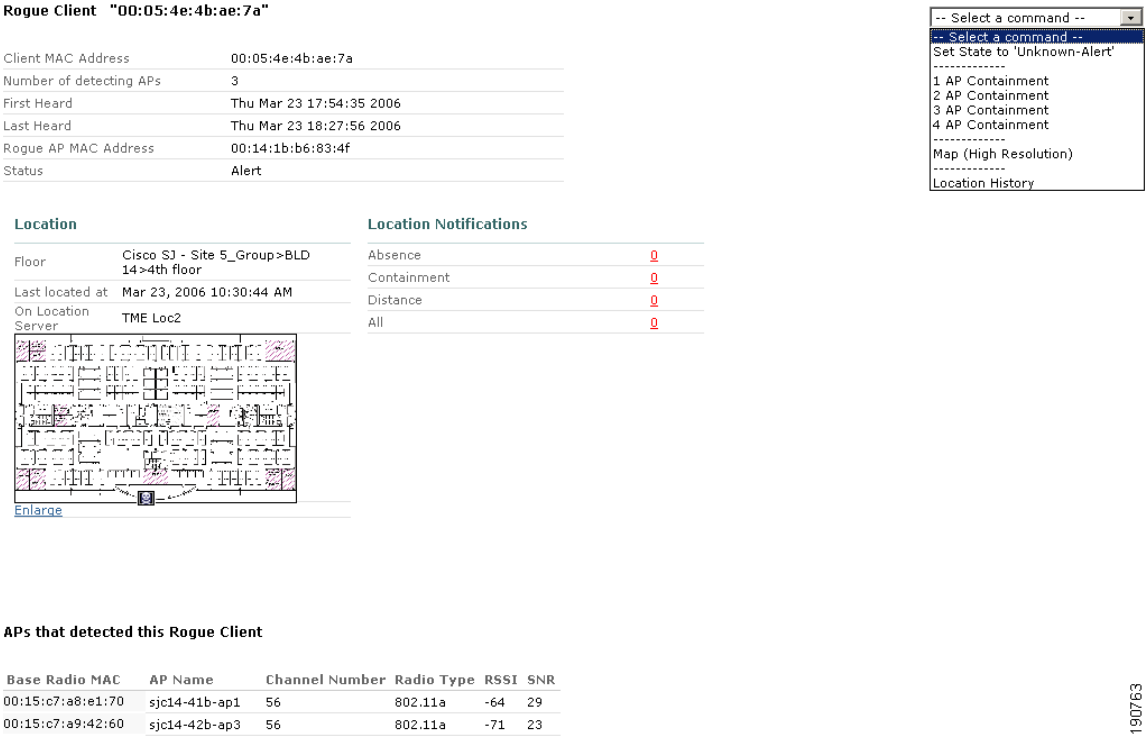
    To use this facility, the search criteria in the left-hand column of the Rogue Client search screen must be configured to search for desired rogue clients in either the databases of WCS or the location appliance. When this is performed, a listing of rogue clients such as that displayed in Figure 8-52 can be viewed.

Figure 8-51 Monitor > Security > Rogue Clients



Clicking on any of the rogue client MAC addresses yields the rogue client detail screen (shown in Figure 8-52) providing detailed information about the rogue client such as which and how many lightweight infrastructure access points have detected it, when it was first and last heard, and its location.

Figure 8-52 Rogue Client Detail



The drop-down menu selector in the upper right-hand portion of the rogue client detail screen shown in Figure 8-52 allows the WCS user to perform additional functions concerning the rogue client such as displaying its location history and current location, changing its status, or initiating containment of the rogue client. When you select level 1 containment, one lightweight infrastructure access point in the vicinity of the rogue client sends de-authenticate and disassociate frames to the client. When you select level 2 through 4 containment, two through four lightweight infrastructure access points participate in containing the rogue client.

- The Shunned Clients search screen.

  Using this facility, a search can be conducted of all associated clients that have been detected by a Cisco IDS device as sending malicious traffic through the network. The IDS device detects such activity and sends “shun” requests to Cisco Wireless LAN Controllers, which in turn disassociate the client device. This search facility provides access to a listing of shunned clients by client IP address, IDS sensor address, and controller.

- *Security Alarms*—This area typically occupies the upper half of the security summary page (shown in Figure 8-50 within the red rectangular area). It is subdivided into subgroups that provide last hour, 24 hour, and active alarm counts pertaining to rogue access points, signature attacks, AP threats/attacks, IPsec failures, and client-related security alarms. The total active alarm counters in this area are hyperlinks to a common list of alarms that pertain to the particular category. For example, clicking on the total active alarms counter for rogue AP alerts takes you to the appropriate listing of alarms.

Note Note that there is no implied relationship of (Last hour alarms) + (Last 24 hour alarms) = Total Active Alarms. Last hour and last 24 hour alarm counters are a tally of *all* alarms received in those time frames. The Total Active Alarms counter is the sum total of alarms received *net any corresponding clear alarms received*. Therefore, it is not unusual to see (Last hour alarms) + (Last 24 hour alarms) > Total Active Alarms.

Most of the categories in the Security Alarms area are self-explanatory, but a few are clarified as follows:

- *Threats*—Any rogue APs detected as being on the same wired network as your infrastructure lightweight access points are considered a threat. The detection of a threat is always considered a critical event/alarm.
- *Contained Pending*—This is a transitory state for a rogue AP that is in the process of being contained.
- *Trusted Missing*—A rogue AP that has been marked as Known Internal or Known External but is now determined to be missing from the management domain.

- *Most Recent Security Alerts*—This area is shown within the blue rectangle in Figure 8-50 and displays up to five of the most recent security alerts detected. The entire text of each alert can be seen by simply performing a mouse-over of the listed failure objects. Each failure object is itself a hyperlink to the associated alarm detail page.
- *Most Recent Rogue APs*—Shown within the green rectangular area in Figure 8-50, this portion of the Security Summary page displays up to five of the most recent rogue APs detected. Details are displayed during a mouse-over of each MAC address, and each address is a hyperlink to the Alarm Details page associated with the rogue AP.

Monitoring Events and Alarms, and Generating Notifications

WCS contains an alarm and notification subsystem that maintains an automated watch over the network, alerting the administrator (or anyone else with an e-mail account) even when they are not logged into WCS. Multiple recipients can be alerted about potential issues as they are discovered and before they turn into full-fledged problems.

Relationship Between Traps, Events, Alarms, and Notifications

In the Cisco Unified Wireless Network:

- The WLAN controllers and lightweight access points monitor activity that involves RF.
- Controllers monitor the status of lightweight access points and enforce defined policies.
- Location appliances monitor the movement of clients and assets.
- WCS monitors all the location servers, controllers, and lightweight access points that are within its management domain.

If operational exceptions (access point not found, controller unreachable, location appliance not responding, and so on) or other changes in state are deemed to have taken place within the domain of control of the controller (excessive interference, rogue access point detected, and so on), an *event* is registered as having occurred within the WLAN controller. An event is an occurrence or detection of some condition in and around the network. It can be a report about radio interference crossing a threshold, the detection of a new rogue access point, a controller rebooting, or some situation which takes places at a particular time.

Events are communicated to WCS via one of two ways:

- SNMP traps
- Normally scheduled polling

SNMP traps enable WLAN controllers and location appliances to notify WCS of significant changes in condition within the network by way of an unsolicited SNMP message known as a *trap*. Traps are normally sent to *trap receivers* at UDP port 162. Controllers can be configured to send traps to multiple trap receivers. The trap port to which a controller sends traps cannot be changed via WCS (it must be changed via the controller web interface or CLI). Traps are sent to the same trap port for all trap receivers defined in a controller.

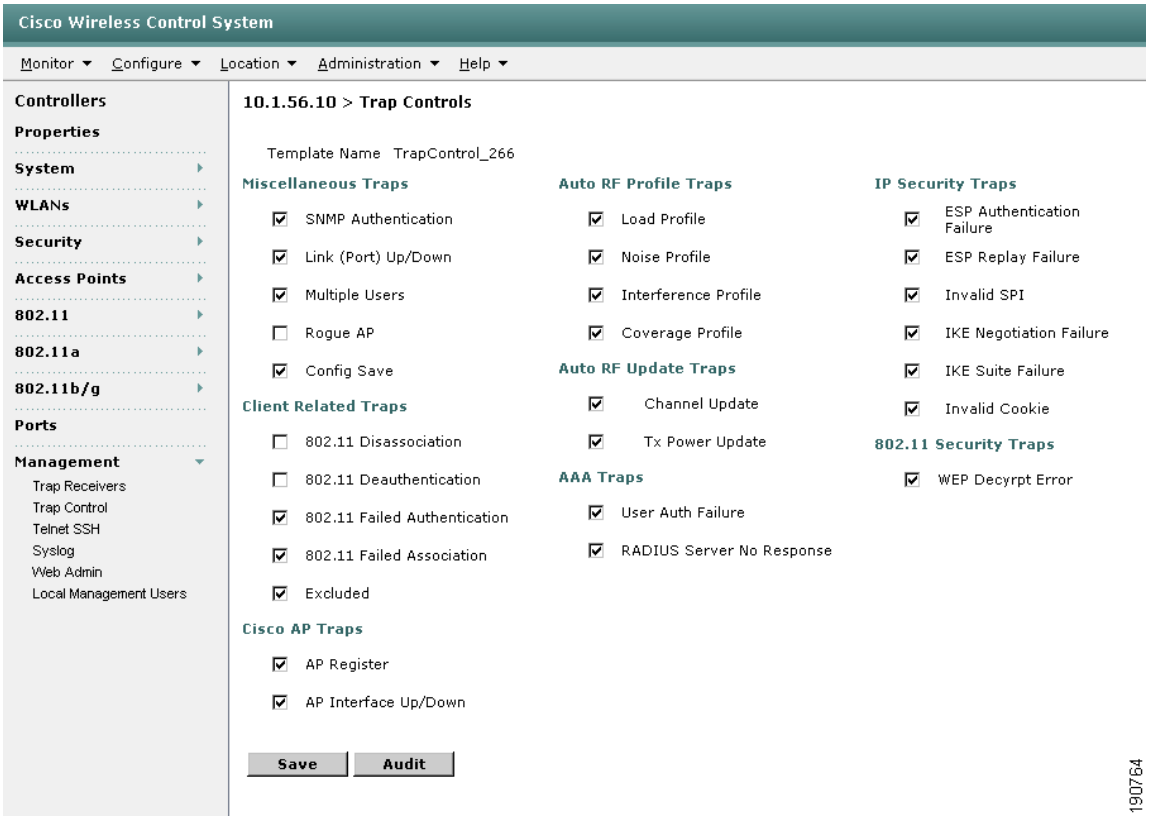
Controller traps can be enabled or disabled in WCS via **Configure > Controllers > Management > Trap Control**.

Depending on the nature of the condition detected by the controller, a system log (*syslog*) message may also be generated. An example of this is the automatic addition of a client to an exclusion list because of repeated authentication failures or the loss of connectivity to a lightweight access point that was formerly associated with this controller. Note that traps and syslog messages do not necessarily duplicate one another. Events may not always be severe enough to generate syslog messages but may trigger pre-configured traps, and conditions that are severe enough to trigger a message to be sent to the system log may not be addressed by any configured traps.

SNMP traps and UDP syslog messages are logged internally at the controller and can be sent to external destinations. Both SNMP traps and syslog messages are sent using UDP; controllers can send traps to multiple IP destinations but they send syslog messages only to a single IP destination. Traps should always be sent to WCS for proper management function, but there is no need to send syslog messages to WCS because WCS does not natively run a remote syslog server to process them.

Figure 8-53 illustrates the various individual trap categories for a WLAN controller.

Figure 8-53 Configure > Controllers > Management > Trap Control



Trap categories are as follows:

- Miscellaneous traps
  - Multiple Users Traps—When enabled, this trap notifies all trap receivers when more one user logs into the CLI of a WLAN controller using a particular user credential. The value for this threshold is hardcoded in the controller and is currently set to one. When WCS receives this trap from the WLAN controller, a critical event is logged as shown in Appendix B, "WCS Event and Alarm Severities.".
- Auto RF profile traps
  - Load, noise, interference, and coverage profiles—When enabled, these traps notify all trap receivers when 802.11a or 802.11b/g load, noise, interference, and coverage threshold violations have been detected by any RF interface of any lightweight access point registered with the WLAN controller. These profiles are specified in WCS using **Configure > Controllers > 802.11a > RRM Thresholds** and **Configure > Controllers > 802.11b/g > RRM Thresholds.** Thresholds can also be specified using Policy Templates as discussed in Defining and Applying Policy Templates, page 8-22. When WCS is notified that one or more of these thresholds have been violated, a minor severity event is logged as shown in Appendix B, "WCS Event and Alarm Severities.".

In addition to the traps defined in Figure 8-53, there are a few others that are associated with thresholds to consider. The thresholds associated with these traps are not configurable:

- Too Many Unsuccessful Login Attempts—This trap notifies all trap receivers when a user using the WLAN controller CLI fails to successfully login after five attempts. When WCS receives this trap from the WLAN controller, a critical event is logged as shown in Appendix B, "WCS Event and Alarm Severities.".

- Maximum Rogue Count Exceeded—This trap notifies all trap receivers when the total number of rogue APs detected exceeded certain prescribed thresholds. The thresholds are as follows:
  - For WLCM and 2006 WLAN controllers—A maximum of 30 rogue APs detected per infrastructure AP; maximum of 125 rogue APs detected per WLAN controller.
  - For all other WLAN controllers including WiSM—A maximum of 30 rogue APs detected per infrastructure AP; maximum of 625 rogue APs detected per WLAN controller.

When WCS receives any of these traps from the WLAN controller, a critical event referring to a potential "Fake AP or other attack" is logged as shown in Appendix B, "WCS Event and Alarm Severities.".

WCS should always be configured as a trap receiver to ensure proper function. Trap receivers may be defined and removed for controllers via the **Configure > Controllers > Management > Trap Receivers** menu selections. WLAN controllers allow the definition of up to six trap receivers, and WCS allows the application of up to six trap receiver templates to a WLAN controller.

Appendix D, "Examples of SNMP Traps," contains several examples of SNMP traps captured during lab testing. Although not an exhaustive list of all traps available from Cisco WLAN controllers, this appendix does show actual received traps and decodes much of their content for easier viewing. Complete trap definitions for 4400, 4100, and 2000 Series WLAN controllers are defined in MIB files that are available to registered users on the Cisco Connection Online (CCO) at http://www.cisco.com.

Although WCS itself is not a syslog server, it does enable the configuration of syslog receivers for controllers via **Configure > Controllers > Management > Syslog**. If you have a system in your network that can function as a syslog server and accept remote syslog updates, you can define that system as the recipient of syslog messages from WLAN controllers using this feature.

Note Syslog message error level (that is, Critical, Error, Informational, and so on) is not configurable via WCS but can be set via the controller GUI.

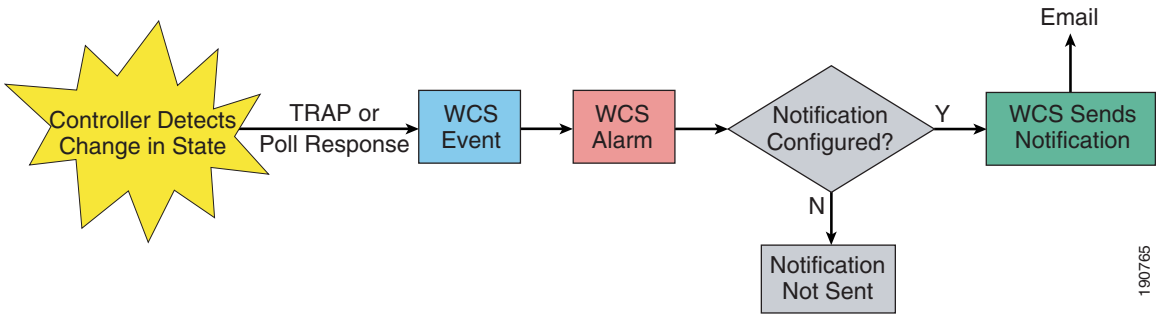
All syslog messages are sent to UDP port 514 using facility level Local0; therefore, you should ensure that your syslog server is configured appropriately for UDP port 514. Only UDP is supported as a transport for syslog traffic at this time.

After receiving and processing a received trap, WCS logs the fact that an event has occurred at the trap originator. Events are filtered into assigned classes of severities. These events trigger *alarms* of corresponding severity at WCS. An alarm is a WCS response to one or more related events. If an event is considered of high enough severity (critical, major, minor warning, clear, or informational), the WCS raises an alarm until the condition that resulted in the alarm is judged to be no longer occurring. For example, an alarm may be raised while a rogue access point is detected, but the alarm terminates after the rogue has not been detected for several hours. A WCS administrator currently has no control over which events generate alarms, when they time out, or what severity they are.

One or more events can result in a single alarm being raised. Certain classes of alarms are deemed of utmost importance and when they occur, WCS can generate a outbound notification to alert critical personnel that events have occurred that may warrant their immediate attention.

Figure 8-54 illustrates the logic behind this event-driven alarm and notification system in more detail. This example is that of a WLAN controller, but this same process is used by all members of the Cisco Unified Wireless Network that wish to enlist the alarming and notification services of WCS.

Figure 8-54 High-Level WCS Event, Alarm, and Notification Flow Diagram



The following sequence takes place:

1. The controller detects that a change in state has occurred within the portion of the wireless network that the controller and its lightweight access points are monitoring. This can be the sudden unavailability of a network resource such as one of the lightweight infrastructure access points registered with the controller, or the identification of a potential security breach such as the detection of a rogue access point. Controllers can send information about such state changes in their environment to WCS, either via an unsolicited SNMP trap, a poll response, or both.
2. On reception of the trap, WCS registers an event and the event is filtered according to one of the following five severities: critical, major, minor, clear, or informational. Appendix C, "Example of Wireless LAN Controller Initial Setup," contains a listing of the various event and alarm messages that comprise these severity classfications.

Note There is actually a *sixth* severity class for "warning" events and alarms. However, as of this writing, the warning severity class is reserved for potential future use. There are no traps, events, or alarms currently classified as warnings.

- As Figure 8-54 illustrates, the reception of a trap or a poll response leads WCS to log an event that in turn can lead to the triggering of an alarm. It is very important to distinguish WCS *events* (which represent occurrences or a change in condition on a network device) from WCS *alarms* (which are states that occur only on WCS that are the direct result of an event). The alarm state can be cleared either manually or by an administrator. It can also be cleared automatically by an event indicating that the condition responsible for the original alarm state for a managed device has been resolved.

  Active alarms (that is, alarm status of other than "clear") have an indefinite lifetime while cleared alarms linger within WCS for 24 hours. Events, on the other hand, remain in the WCS database for up to seven days. The current set of active and cleared alarms can be viewed at **Monitor > Alarms** while the WCS event log can be viewed at **Monitor > Events** (these are examined in more detail in Monitoring Events, page 8-75 and Monitoring Alarms and Configuring E-mail Notifications, page 8-76).

  Alarms are assigned to severity classes in a similar fashion to events. For the majority of non-critical alarm severities, WCS logs the alarm, changes displayed icon colors appropriately, and increments the alarm monitor counters displayed in the lower left-hand corner of each WCS screen. Indication of the alarm can be seen on the **Monitor > Alarms** screen and by changes in the color of icons seen on campus, building, and floor maps; pictorial displays of network equipment; and other screens within WCS.

- Alarms classified as critical have the potential for immediate service impact and as such offer the option for external notification of key personnel. (As is discussed subsequently, coverage hole alarms are a special case in that they also provide the option for external notification even though they are not classified as “critical alarms”.)

  Recipients of WCS-generated notifications commonly include organizational team members such as network administrators, lead technicians, operations management, and perhaps those members of management responsible for mission-critical applications that depend on wireless services. You can see from the event flow in Figure 8-54 that if notifications have been enabled and properly configured, WCS ultimately issues an email notification. This is performed via one or more Simple Mail Transfer Protocol (SMTP) servers defined to WCS.

  In determining whether an e-mail notification should be sent when a particular alarm is triggered, WCS uses alarm severity in conjunction with alarm categories. There are currently the following seven alarm categories:

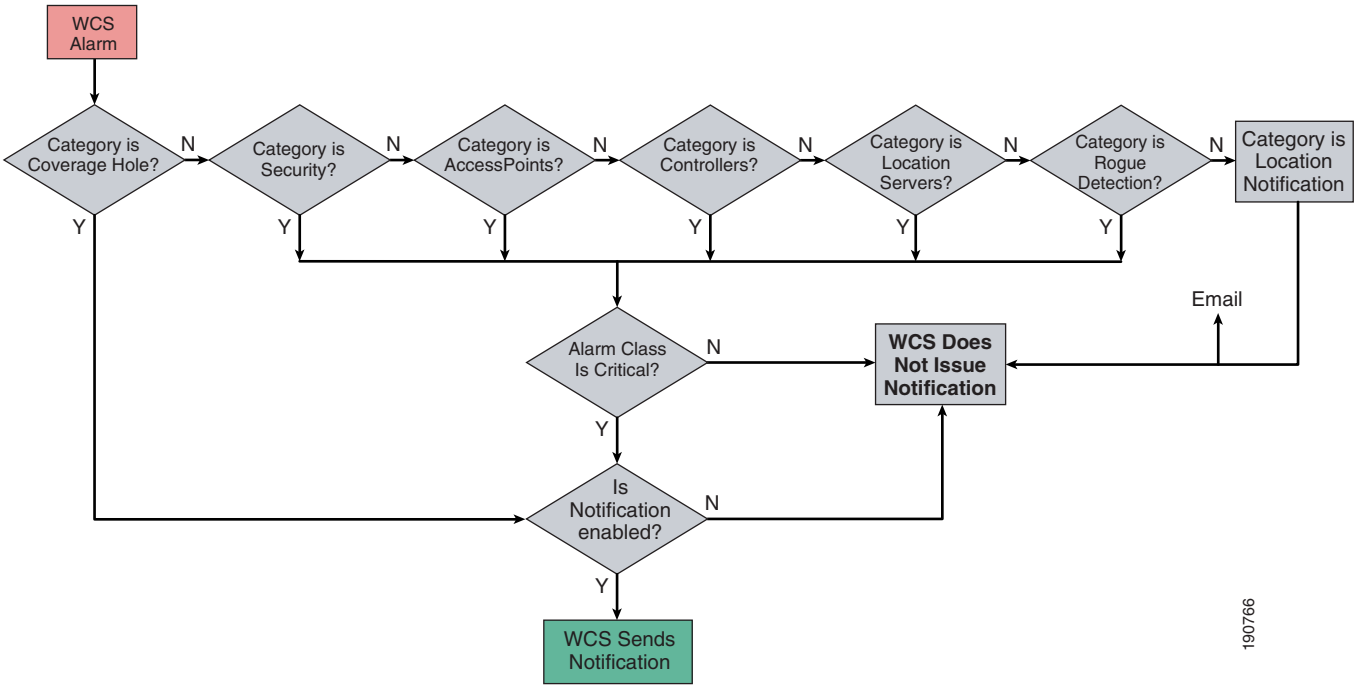
  - Rogue detection
  - Coverage holes
  - Security
  - Access points
  - Controllers (switches)

  Note The use of the term “switches” here is not intended to refer to Ethernet LAN switches such as the Cisco Catalyst Series. Instead, it is a legacy reference to a WLAN controller (WLC) such as the Cisco 2006, 4400, ISR/WLCM, or Catalyst 6500 WiSM.)

  - Location servers
  - Location notifications

  Figure 8-55 presents a conceptual flow diagram that illustrates how WCS decides whether or not a notification is sent.

Figure 8-55 E-Mail Notification Logic Flow



- If e-mail notification has been properly configured and enabled, the flow diagram indicates that WCS dispatches e-mails for triggered alarms if those alarms are either coverage holes alarms, or critical alarms. See Appendix B, "WCS Event and Alarm Severities." for a listing of alarms that are classified as critical alarms. Coverage hole alarms are classified as minor alarms and can also be found in Appendix B, "WCS Event and Alarm Severities.".

  The special case of the Location Notification alarm should be noted in Figure 8-55. Location Notification alarms are alarms that have been generated because of the reception of absence, containment, movement from marker, location changes, or battery level events from a location appliance. Because the location appliance itself is responsible for generating e-mail, syslog, SOAP/XML, and SNMP trap notification for these types of events, WCS does not provide for redundant notification capabilities and does not issue email notifications for Location Notification alarms.

Monitoring Alarms and Configuring E-mail Notifications, page 8-76 discusses how to configure WCS to successfully dispatch e-mail notifications.

Monitoring Events

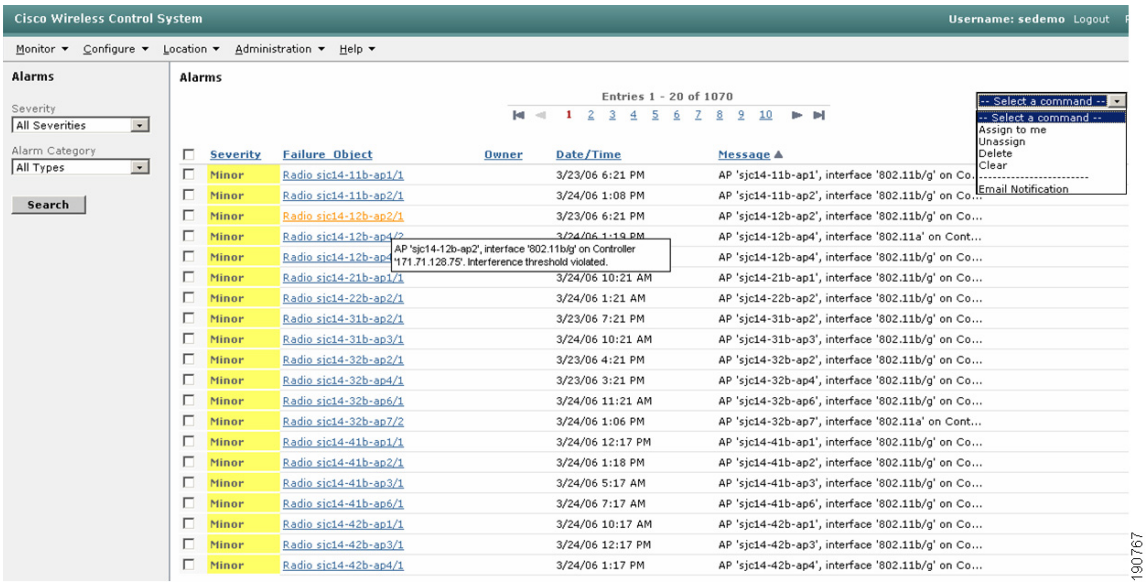
As discussed previously, WCS maintains a log of all received events for a fixed seven-day retention period. These can be displayed by selecting **Monitor > Events** from the main menu selection bar. Because of the number of events that can be present in the event log in large networks, WCS provides the ability to filter the displayed events using the filter selector located in the left-hand margin of the **Monitor > Events** page. Using this tool, the displayed selection of events can be limited to a combination based on severity class and category.

Each column of the event display can be sorted by clicking on the column heading and choosing either ascending or descending sort sequence. Note that this can be very helpful not only in ensuring that the data you are viewing is in the proper date order but also in helping spot repeated patterns of events (that is, sorting on message or failure type). There is only one hyperlink available in the event log data for further information and that is for the failure object. Clicking on any of the failure objects brings up additional information about the event in question.

Monitoring Alarms and Configuring E-mail Notifications

WCS maintains a log of all triggered alarms (shown in Figure 8-56) that can be displayed by selecting **Monitor > Alarms** from the main menu selection bar.

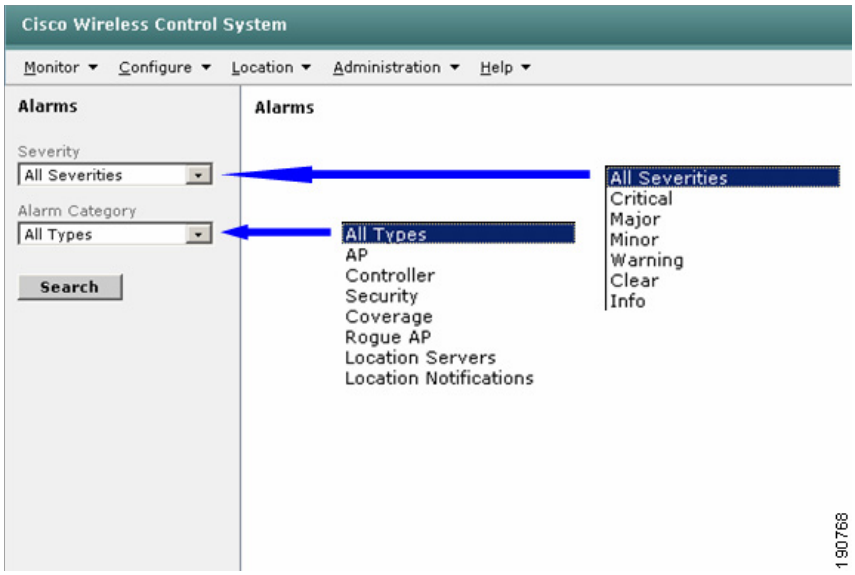
Figure 8-56 Monitor > Alarms



When performing a mouse-over of the failure object hyperlinks listed in the alarm display list, the alarm text associated with each message is displayed as shown in Figure 8-56. This mouse-over capability is useful when quickly scanning the list of alarms because it avoids the necessity of opening each alarm line item to simply determine the details. Each column of the alarm display list can be sorted by clicking on the column heading and choosing either ascending or descending sort sequence. This can be very helpful, not only in ensuring that the data you are viewing is in the proper date order but also in helping to spot repeated patterns in alarms.

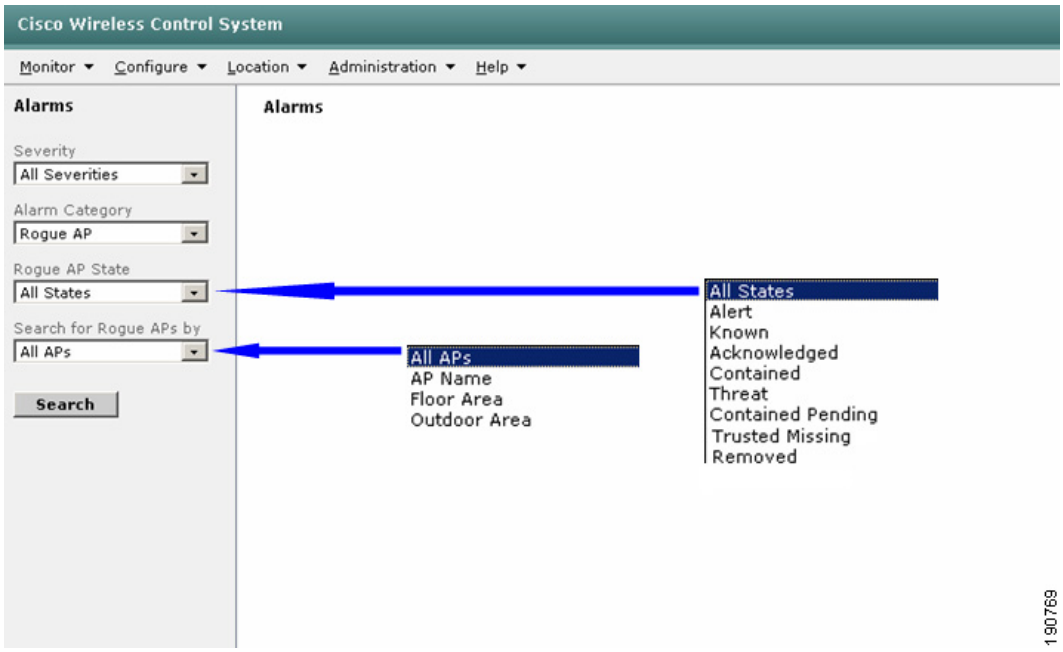
As mentioned previously, alarms that have not been cleared (or manually deleted) remain in the database indefinitely. Cleared alarms remain in the database for a fixed period of 24 hours. In the case of very large networks, many alarms can be displayed; thus, WCS provides the ability to filter the displayed alarms using the selectors located in the left-hand margin of the alarms listing page. This allows the displayed selection of alarms to be limited by severity class and category, as shown in Figure 8-57.

Figure 8-57 Setting Display Filters in Monitor > Alarms



Depending on the alarm category, additional filtering options may be available. For example, when selecting the Rogue AP category, the filtering options shown in Figure 8-58 are available. Additional options become available when the AP Name, Floor Area, and Outdoor Area filters are selected to further qualify the rogue AP list.

Figure 8-58 Rogue AP Alarm Filtering Options



The options shown in Figure 8-58 for rogue AP state are defined as follows:

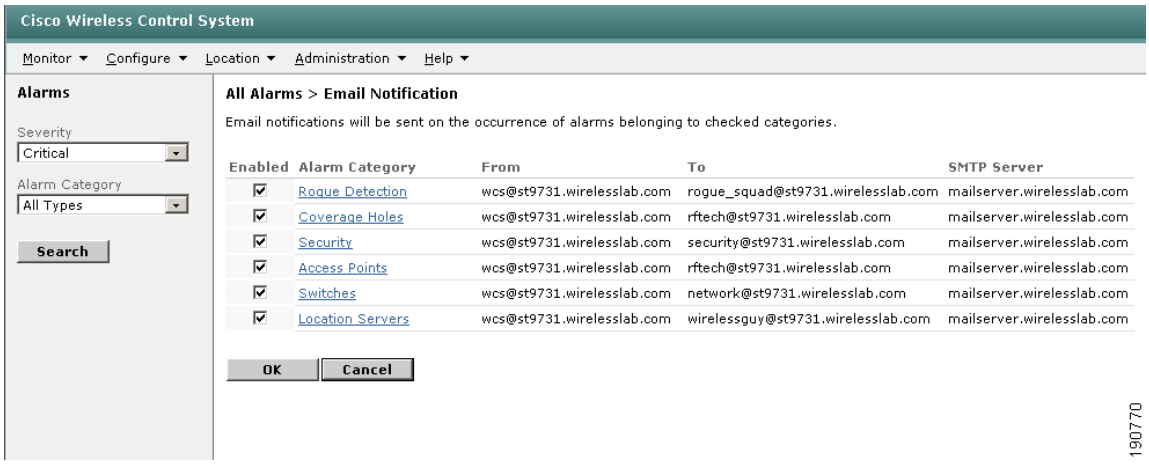
- Alert—Rogue access points that have been identified by the system as potential threats
- Known—Rogue access points identified as known internal rogues

- Acknowledged—Rogue access points identified as known external rogues
- Contained—Rogue access points that have been successfully contained by the system
- Threat—Rogue access points that are confirmed threats to the security of your network. An example of a confirmed threat is a rogue access point that has been identified by the system as physically attached to your internal wired network.
- Contained Pending—Rogue access points that are in the process of being contained by the system
- Trusted Missing—Known or acknowledged rogue access points that are no longer found
- Removed—Untrusted rogue access points that are no longer found

The drop-down command selector in the upper right-hand corner of the **Monitor > Alarms** alarms listing page provides the following options for most alarm categories:

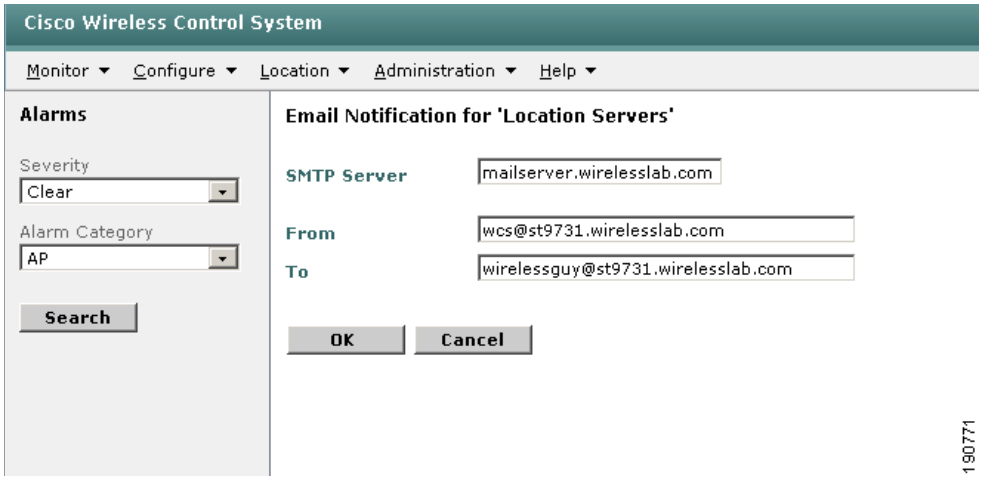
- Assign to me—This command allows the WCS user to select alarms via their check boxes and to assign themselves as the "owner" of the alarm. Assigning owners to alarms is a useful administrative tool that can assist in managing alarm resolution by clearly indicating which person has agreed to take ownership of resolving the alarm. After you assign an alarm to yourself, the user name with which you are currently logged into WCS is displayed as the owner in the **Monitor > Alarms** display as well as in the alarm detail display. Alarms can be assigned only to the user name that you used when logging into WCS; you may not assign alarms to other users.
- Unassign—A complement to "Assign to me", this option allows you to remove the owner of an alarm.
- Delete—Removes the alarm from the alarm database entirely (that is, as if the alarm never existed). Note that although this command removes the alarm, the underlying events that caused the alarm are not removed. In the rare circumstance of an entry persisting in the database even after a manual clearing of the alarm has been performed, the delete command can be used to forcibly remove the alarm. The deletion of an alarm is not reversible except via restoration of the WCS database. Use of the delete command can be restricted via permissions assigned in **Administration > Accounts > Groups**.
- Clear—Manually clears a currently active alarm by issuing a clear alarm that replaces the original alarm severity in much the same manner as a clear alarm received from a network component clears the corresponding active alarm. After an alarm is cleared, only the clear alarm remains listed in **Monitor > Alarms** (the original alarm severity is replaced by the clear alarm). 24 hours after the alarm is cleared, the clear alarm is removed from the database. Note that clearing an alarming does not affect the underlying events that caused the alarm (that is, the events are still present in the event log for seven days).
- E-mail notification—Opens the page shown in Figure 8-59, and is where the communication parameters are configured for e-mail notification. Note that as mentioned in Relationship Between Traps, Events, Alarms, and Notifications, page 8-69, there are seven categories of alarms and each category allows you to configure different e-mail settings.

Figure 8-59 Monitor > Alarms > E-mail Notification



To configure the parameters for one of the seven categories, click on the hyperlink for the alarm category. This displays the page shown in Figure 8-60.

Figure 8-60 Specifying E-mail Parameters



Within each category, only one SMTP server can be specified (either as a fully qualified domain name or IP address); however, multiple e-mail destination addresses can be specified and separated by commas. When specifying multiple e-mail destinations, be aware that there is a 56-byte total length limitation on the "To" field.

Notice that there is no e-mail notification configurable for the Location Notifications alarm category, as described in Relationship Between Traps, Events, Alarms, and Notifications, page 8-69 and Figure 8-55.

When you have specified the e-mail notification parameters, click **OK** and return to the e-mail notifications screen. Before your e-mail notifications become active, you must enable them as shown in Figure 8-59 by checking the applicable check box(es) in the Enabled column and clicking **OK**. Your e-mail notification configuration is complete at that point and e-mail notification should be functional.

An example of an actual e-mail alert received can be seen in Figure 8-61.

Figure 8-61 E-mail Notification

Date: Tue, 21 Feb 2006 12:37:29 -0500 (EST)
From: wcs@st9731.wirelesslab.com
To: rftech@st9731.wirelesslab.com
Subject: Access Points Alarm from Radio AP1000#3/2

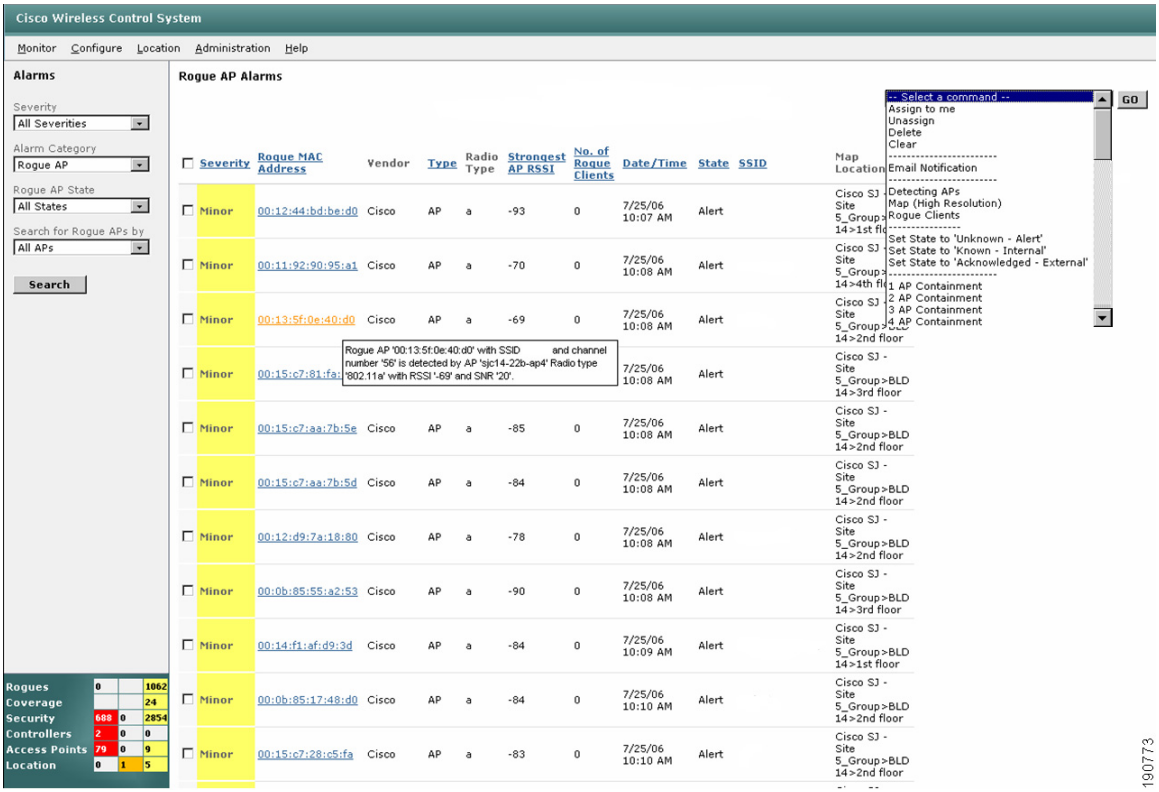
TIME:Tue Feb 21 12:37:29 EST 2006

An Alert of Category AP is generated with severity 1
by Radio AP1000#3/2 .
The message of the alert is AP 'AP1000#3', interface '802.11a' is down on Controller '10.1.56.18'.

190772

Compared to the other alarms categories available under **Monitor > Alarms**, rogue AP alarms are somewhat of a special case in that the options presented under the drop-down command selector are expanded, as shown in Figure 8-62.

Figure 8-62 Monitor > Alarm Rogue AP Alarms



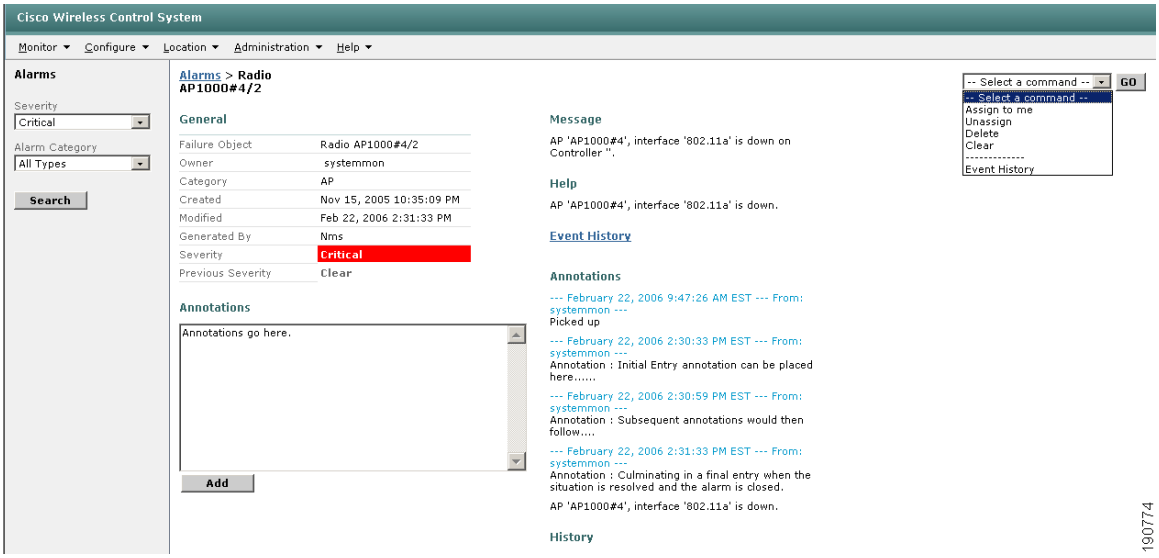
The following additional command options are available under rogue AP alarms:

- Detecting APs—Provides a listing of all lightweight infrastructure access points detecting the selected rogue AP. When using this option, you must select only one rogue access point.
- Map—Provides either a low-resolution or high-resolution on-demand location display of the current location of the rogue AP. See On-Demand Location of Individual Rogue Access Points, page 8-87 for further details about on-demand rogue access point location.

- Rogue Clients—Provides a listing of the rogue clients that are associated to this rogue access point. See Monitoring Security, page 8-65 for more information, and Figure 8-51 for an example of the rogue client detail screen.
- Set State to “Known–Internal”—When searching for rogue APs, this state is referred to as “Known”.
- Set State to “Acknowledged–External”—When searching for rogue APs, this state is referred to as “Acknowledged”.
- AP Containment—Initiates rogue AP containment using from one to four infrastructure access points.

Clicking on the failure object hyperlink of any of the items listed on the **Monitor > Alarms** listing page results in the Alarms Detail page being displayed. The look and feel of the alarm detail page varies somewhat based on the type of alarm being displayed. A common alarm detail format shared among most alarms (except for the rogue AP alarm) is shown in Figure 8-63.

Figure 8-63 Alarm Detail Page—Annotations



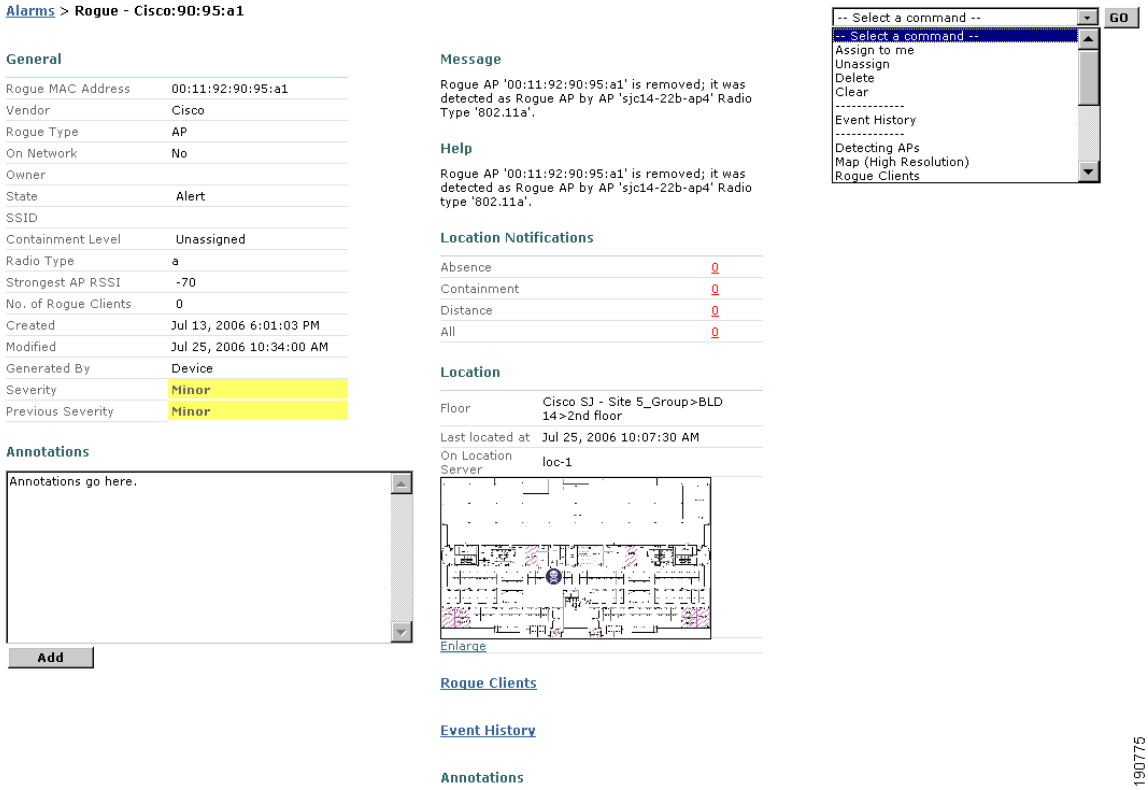
In all cases, the value shown for the “Generated By” field in the alarm detail page shown in Figure 8-63 indicates the source of the information that triggered the alarm or event:

- Device—Indicates that the alarm or event was generated based on information obtained from an SNMP trap received from the device.
- NMS—Indicates that the alarm or event was generated based on information obtained during SNMP polling.

Note the use of the Annotations area for keeping a running log of what has occurred and who has been involved in resolving the alarm. Annotations are added via the entry box on the left-hand side and appear in the order in which they were added in the annotations area on the right. The date and time of the alarm assignment is indicated by the “picked up” entry (if the alarm were to be unassigned, an “unpicked” entry would show up here as well). The clearing of an alarm results in a severity change but no additional entry in the annotations area.

Rogue AP alarms use a somewhat different detail page format, with additional information provided about location, location notification, and any rogue clients that might be associated to this rogue AP available. The rogue AP alarm detail page is shown in Figure 8-64.

Figure 8-64 Rogue AP Alarm Detail



The drop-down menu selector in the upper right-hand corner of the rogue AP alarms page offers an expanded set of command options when compared to other alarms. The majority of the command options are familiar from the discussion of rogue AP alarms listings. Two options found here that are not available when listing rogue AP alarms are event history and location history. Event history is available both as a command drop-down selection and as a hyperlink on the rogue AP alarm detail page. The function in both cases is the same; the list of events that are associated with this alarm are displayed. Location history is available for the rogue access point in a similar fashion to that described for WLAN clients in Monitoring Clients, page 8-54.

Using WCS to Locate Devices in Your Wireless Network

WCS offers the ability to locate rogue client devices, 802.11 active RFID tags, rogue access points, and rogue clients when they are detected within your wireless network. Location of these devices can be provided by WCS on either an on-demand basis for a single device or on a routinely updated basis for multiple devices when used with a location appliance.

For users requiring location services only when the need arises to locate a lost device, the on-demand location capabilities afforded by WCS-Base or WCS-Location may be all that is required. However, for users that rely on the ability to track the movement of devices in their environment on a regular basis, require alarms and notifications when devices move into or out of defined areas, maintain location history for more than seven days, or interface to third-party location client applications, the use of a location-licensed WCS server with the location appliance is a more appropriate choice.

This section describes each of these options in further detail.

On-Demand Device Location

In this section, "on-demand" device location refers to the ability of WCS to display the current position of a single device whenever you explicitly request the system to do so without the use of a location appliance. Although both the base as well as the location-enabled version of WCS can perform on-demand location, they vary both in for which devices each provide positioning information as well as the level of position granularity.

Only a WCS server that is licensed for base-level functions can perform on-demand client and rogue device location, by placing an icon on a floor map nearest the access point that has detected the device with the highest signal strength. Knowing which infrastructure access point detects the device with the highest signal strength usually provides sufficient resolution for casual location services use, especially in cases where the need for location services in a particular business situation may not justify additional investment in software or hardware.

A location-licensed WCS server improves these on-demand capabilities by providing "high-resolution" location of WLAN clients and rogues using Cisco RF Fingerprinting positioning technology. As opposed to simply knowing the lightweight access point that detected the client with the highest signal strength, RF Fingerprinting can provide location accuracy of 10 meters, 90 percent of the time (90 percent precision) in a properly-designed system. A location-licensed WCS server can perform on-demand location of a single device at a time, and is an excellent choice where higher accuracy is desired to reduce the amount of time and effort that must be expended searching for items that are within the range of a particular access point.

The location appliance does not play an active role in establishing on-demand location because it is typically entirely driven using the client and rogue information available in WCS databases and the WLAN controllers. Rather, the Wireless Location Appliance allows WCS to display the location of multiple devices simultaneously by performing location calculations on the data acquired by the location appliance during its polling of WLAN controllers. The location appliance polls based on configured polling parameters and does not poll WLAN controllers on-demand. The information that is used to establish device location during an on-demand location request is supplied by WCS and the WLC.

On-Demand Location of WLAN Clients

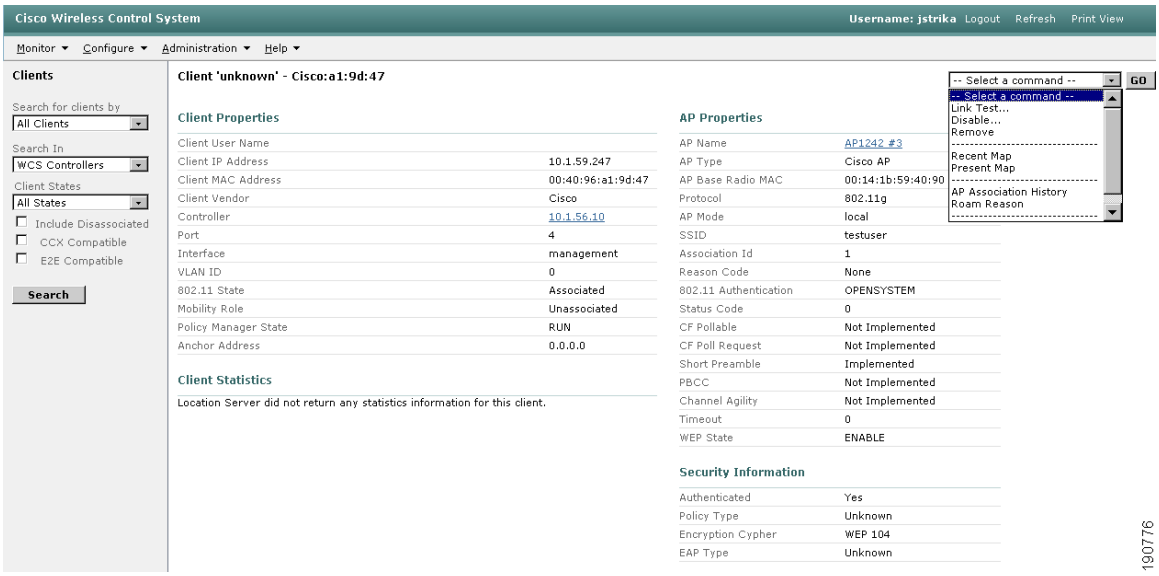
On-demand location of a single WLAN client at a time without the use of a location appliance can be performed from WCS using the **Monitor > Devices > Clients** Summary menu shown in Figure 8-39. To do so, follow these steps:

Step 1 Using the "Search for Clients by" feature in the left-hand margin of the page narrow the search to include only the clients of potential interest. Be sure to specify "WCS Controllers" instead of "Location Servers" if there is not a location appliance present. Click **Search**.

Step 2 Click on the client user name hyperlink of the client for which you want to display location.

WCS displays the client detail screen shown in Figure 8-65 for the client you have selected.

Figure 8-65 Client Details



Step 3 Click on the command drop-down menu in the upper right-hand corner of the screen and choose from either the “Recent Map” or “Present Map” options.

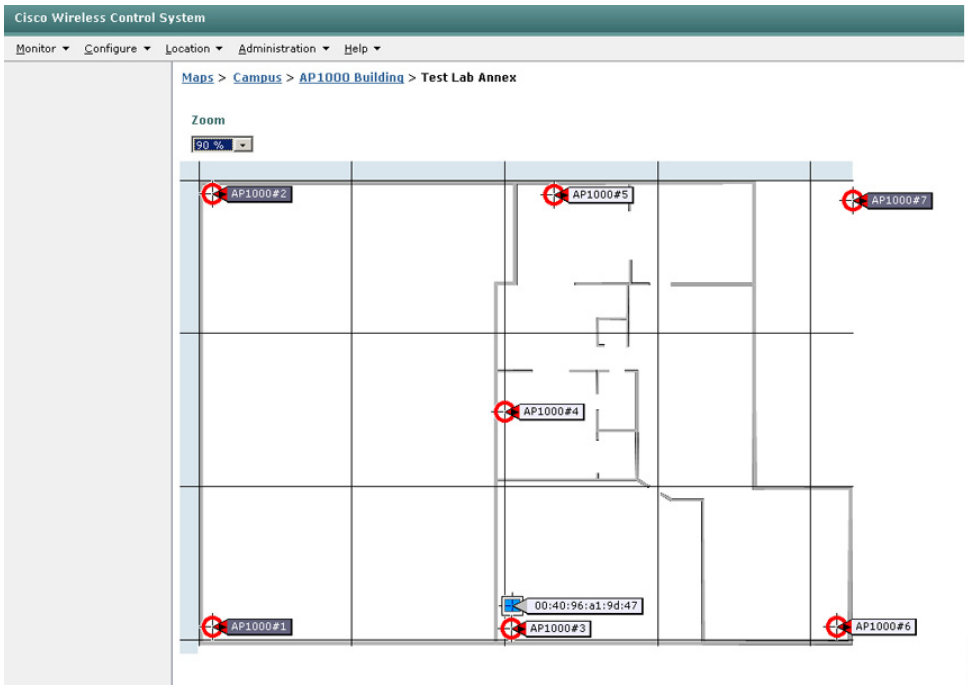
- Recent map—Displays the last recorded historical location of the client from the WCS database and is non-intrusive to the WLAN client. The information that is used to establish device location in this case is garnered via the routine background polling cycles of WLAN controllers by WCS.
- Present Map—Displays the current location of the client and can cause disruption to the existing client session. To gather the current signal strength information of the client, the client is de-authenticated/disassociated very briefly and must then re-associate/re-authenticate. The amount of time this takes depends on the details of the client authentication method being used. Although this disruption is typically quickly recovered, some applications (such as voice and some business data applications) may prove to be more sensitive to the interruption than others. For this reason, Recent Map instead of Present Map is generally preferred when performing on-demand location for active, in-session users unless the impact of any such interruption has been assessed beforehand.

  In most cases, if on-demand location is being used to locate a lost device, this interruption has little impact because if the device is still powered on, it is typically not in use. However, lost devices tend to eventually power down because of battery exhaustion, and in that case the Recent Map option is of much more use in determining the last known location.

Choose either of the mapping options and then click **Go**.

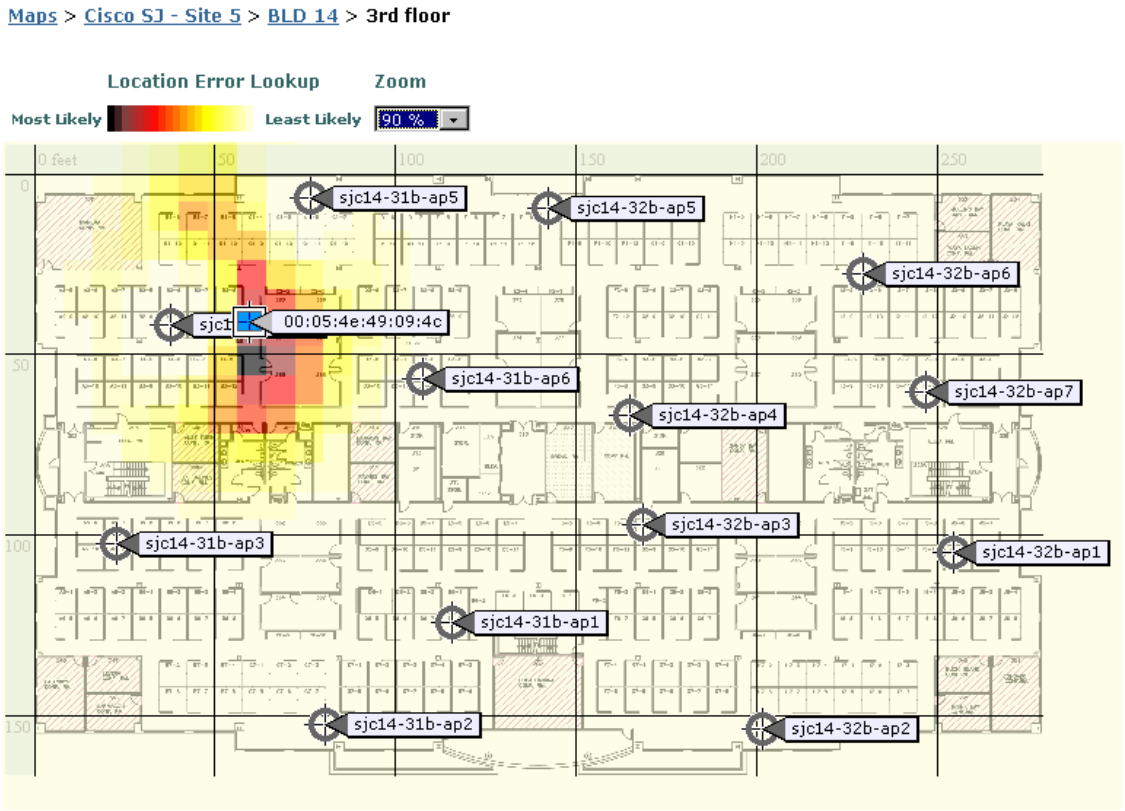
Step 4 WCS systems that are licensed only for base-level functionality (WCS-Base) display on-demand location of clients in a manner similar to what is shown in Figure 8-66. Note that the icon for a WLAN client is placed adjacent to the access point that detects the client with the highest signal level. The location of the client on the map does not indicate the estimated location of the client, just that it has been detected with the highest signal strength by the infrastructure access point that it is adjacent to. In Figure 8-66, that access point is AP1000#3.

Figure 8-66 On-Demand WLAN Client Location (Base Level WCS)



When using a location-licensed WCS server without a location appliance, the process is essentially the same with the exception that WCS uses RF Fingerprinting to derive estimated client location on a "high-resolution" map. In this case, your on-demand location results resemble Figure 8-67 instead of Figure 8-66.

Figure 8-67 High Resolution On-Demand Client Location (Location-Licensed WCS)



The main difference between what Figure 8-66 and Figure 8-67 is that in Figure 8-67, the placement of the blue rectangular WLAN client icon is intended to represent the estimated client position on the map. The various color bands in the display indicate varying location probabilities, as shown in the "Location Error Lookup" legend at the top of the display. Performing a mouse-over of the various colors in the legend itself displays the error probability associated with each color band. In contrast, the positioning of the blue rectangular WLAN client icon in Figure 8-66 is not intended to convey estimated client position on the map, but merely to indicate which access point has detected the WLAN with the greatest signal strength.

On-Demand Location of Individual 802.11 Active RFID Asset Tags

The 802.11 active RFID asset tags that can be tracked by the Cisco Location-Based Services solution can be grouped into two basic categories:

- 802.11 Active RFID asset tags that communicate via Layer 2 (L2) multicasts such as the AeroScout T2 asset tag. These asset tags typically use the WDS frame format and do not associate to the WLAN infrastructure. These asset tags appear as yellow tag icons within WCS floor maps.

Note For a complete discussion of the AeroScout T2 tag and WDS frame formats, see *Wi-Fi Location-Based Services 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html.

- 802.11 Active RFID asset tags that communicate as full WLAN clients and associate/authenticate to the WLAN infrastructure, such as PanGo Locator LAN tags. These types of asset tags are viewed as WLAN clients by WCS and the location appliance, and they appear as blue rectangular icons within WCS floor maps.

To locate 802.11 Active RFID asset tags that are of the latter category, see On-Demand Location of WLAN Clients, page 8-83 because these types of asset tags are technically treated as WLAN clients by the Cisco UWN.

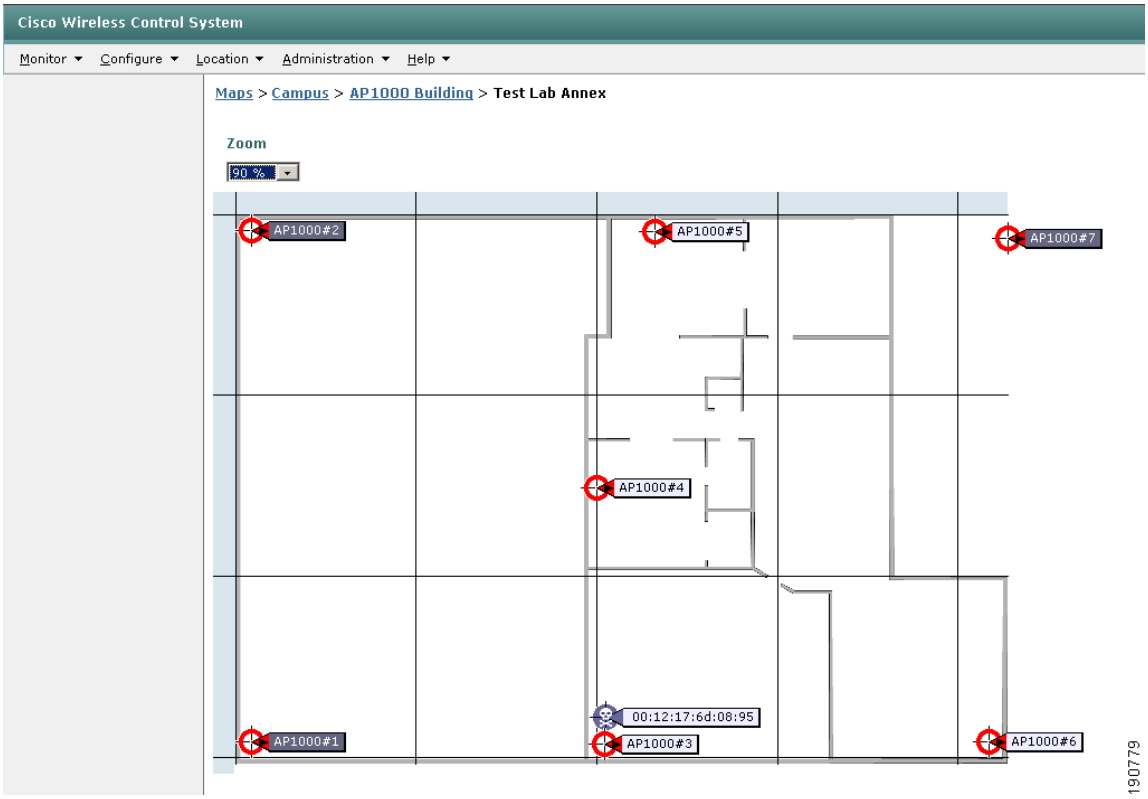
Note that beginning with release 4.0 of WCS, a location appliance is required to determine the position of any Layer 2 multicast-based RFID asset tags. A subsequent maintenance release is expected to reinstate the capability to perform on-demand location of individual Layer 2 multicast-based RFID tags when using a WCS server that is licensed for location use. In addition, beginning with release 4.0, WCS servers that are licensed only for base-level functionality do *not* have the capability to perform *any* type of location determination for Layer 2 multicast-based RFID tags.

On-Demand Location of Individual Rogue Access Points

On-demand location of a single rogue access point at a time without the use of a location appliance can be performed with base-level WCS using the Rogue AP Alarms menu accessible via **Monitor > Security > Rogue APs**. To do so, select a single Rogue AP by enabling its check box. From the command drop-down located at the upper right-hand corner of the screen, select “Map” and then click **GO**.

When using the base-level WCS, the screen shown in Figure 8-68 is displayed.

Figure 8-68 On-Demand Rogue Access Point Location (Base-Level WCS)



Note that the circular black "skull-and-crossbones" icon representing a rogue access point is placed directly adjacent to the lightweight infrastructure access point that has detected it with the highest signal level.

When using a version of WCS that is licensed for high resolution location tracking, the process is identical with the exception that WCS uses RF Fingerprinting to determine the estimated position of the rogue access point and displays it on a "high resolution" map similar to that shown in Figure 8-67. With the exception of the icon used to indicate the location of the rogue AP, the look and feel of the high-resolution on-demand map is the same as that shown in Figure 8-67.

On-Demand Location of Individual Rogue Clients

On-demand location of a single rogue client at a time can be performed from WCS without a location appliance using the **Monitor > Security > Clients** Summary menu shown in Figure 8-39. To do so, follow these steps:

Step 1 Using the "Search for Clients by" feature in the left-hand portion of the screen, specify information to narrow the search to include only rogue clients of potential interest. Be sure to specify "WCS Controllers" instead of "Location Servers" if there is not a location appliance present.

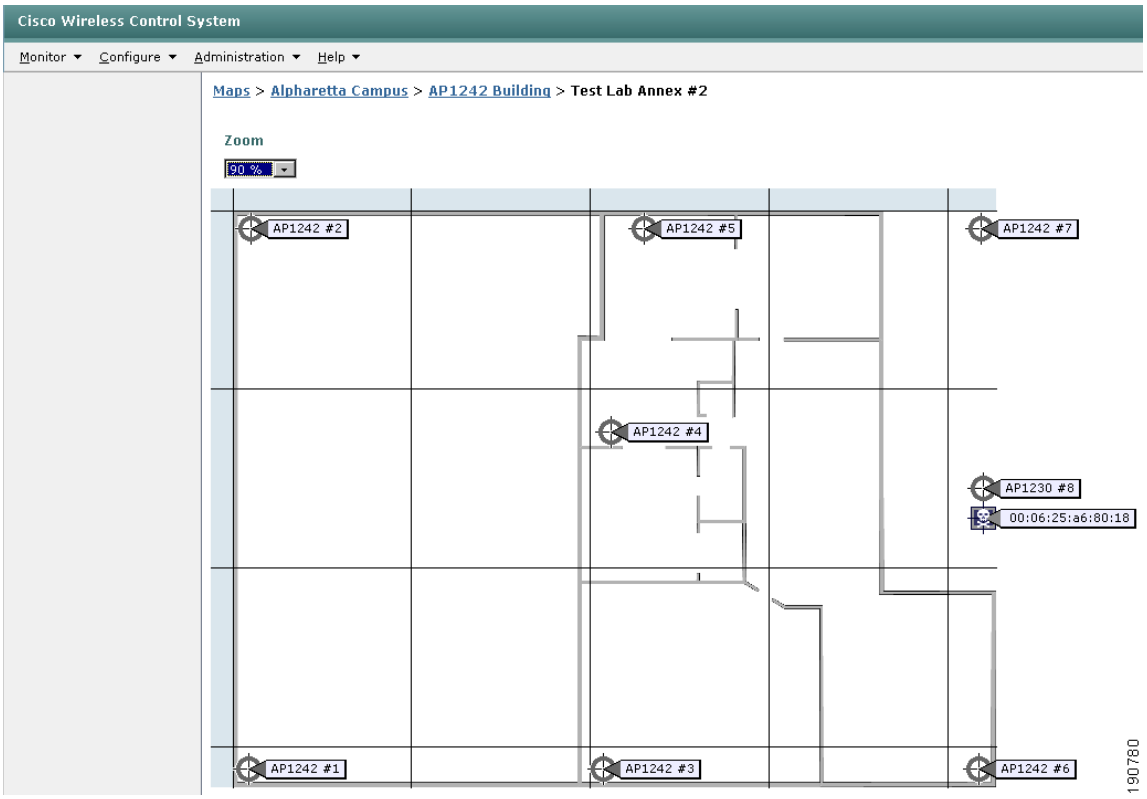
Click **Search**.

Step 2 WCS displays a listing of detected rogue clients that are found in the WCS database. Click on the MAC address hyperlink of the rogue client for which you want to display location.

Step 3 WCS displays detailed information about the rogue client including the time it was detected, which access points detected it, and at what signal levels. Click on the command drop-down menu in the upper right-hand corner of the screen, select "Map", and click **GO**.

The base-level WCS displays a location map with a black rectangular icon representing a rogue client, as shown in Figure 8-69. It is placed nearest the infrastructure lightweight access point that has detected it with the highest signal level.

Figure 8-69 On-Demand Rogue Client Location (Base Level WCS)



When using a version of WCS that is licensed for high resolution location tracking, the process is essentially the same with the exception that WCS uses RF Fingerprinting to determine the estimated position of the rogue client and displays it on a "high resolution" map similar to that shown in Figure 8-67. With the exception of the icon used to indicate the location of the rogue client, the look and feel of the high-resolution on-demand map is the same.

WCS and the Location Appliance

When a Cisco Wireless Location Appliance is added to a location-licensed WCS server, its high-resolution location capabilities are enhanced by the ability of the location appliance to issue location notifications and compute positioning information for multiple devices simultaneously while maintaining a much larger amount of location history data in its internal databases.

The location appliance interfaces to WCS using the SOAP/XML API interface. Via this API, WCS serves in the role of both a *location client* in displaying the location of many simultaneous devices, asset tags, and rogues on location maps as well as a *control client* in acting as the primary user interface to the location appliance and handling its configuration.

This same SOAP/XML API allows for integration with other business applications that can use the location information contained within the location appliance for a variety of creative applications. Asset tracking, inventory management, location-based security, and automated workflow management are just a few examples of this. Third-party location client applications access the location appliance only via the API and typically do not access WLAN controllers or other components of the network directly.

Operators can configure location appliances to collect client RSSI data and statistics from WLAN controllers at defined intervals. The location appliance allows WCS to display the location of multiple devices simultaneously by performing location calculations on the data acquired by the location appliance during its polling of WLAN controllers. The location appliance polls based on configured polling parameters and does not participate in on-demand location display.

The location appliance also provides *location-based event notification*, whereupon it generates e-mail and other notifications directly to specified destinations. These alarms and notifications can be triggered through area boundary, allowed areas, and distance definitions in the location appliance. These alarms and notifications can also provide advanced warning of rogue movement and appearance/disappearance. Using WCS, you can configure location appliance event notification parameters that allow the location appliance to send notifications to destinations configured via the WCS **Location > Notifications** menu option. The location appliance can be defined to transmit messages using SOAP, SMTP, SNMP traps, or syslog messages if clients or assets become missing, enter or leave coverage areas, or stray beyond a set distance from a pre-determined marker.

Architecture Overview

The overall architecture of the Cisco location-based services solution is shown in Figure 8-70.

Figure 8-70 Cisco Location-Based Services Architecture

Access points forward information to WLAN controllers about the detected signal strength of any Wi-Fi clients, 802.11 active RFID tags, rogue access points, or rogue clients. In normal operation, access points collect this information on their primary channel of operation, going off-channel and scanning all channels in their regulatory channel set periodically. The collected information is forwarded to the WLAN controller with which the access point is currently registered. Each controller manages and aggregates all such signal strength information coming from its access points. The location appliance uses SNMP to poll each controller for the latest information for each tracked category of device. In the case of a location tracking system deployed without a location appliance, WCS obtains this information from each controller directly.

WCS and the location appliance exchange information about calibration maps and network designs during a process known as *synchronization*. During a *network design synchronization* between WCS and the location appliance, the up-to-date partner updates the design and calibration information of the out-of-date partner. The location appliance synchronizes with each controller containing access points participating in location tracking during *controller synchronization*. The synchronization of notification schedules and destinations between the location appliance and WCS is handled via a process referred to as *event group synchronization*. Synchronization occurs either on-demand or as a scheduled task, the timing of which is determined by the Administration > Scheduled Tasks main menu option in WCS.

Location information is displayed to the end user using a *location client* application in conjunction with the Cisco Wireless Location Appliance. Typically, this role is fulfilled by the Cisco WCS, which is capable of displaying a wide range of information about the location of clients, asset tags, rogue access points, and rogue clients. However, location client functionality is not limited to WCS, because other third-party applications written in accordance with the Cisco Location Appliance API and using the SOAP/XML protocol can also serve as a location client to the Wireless Location Appliance (as shown in Figure 8-70).

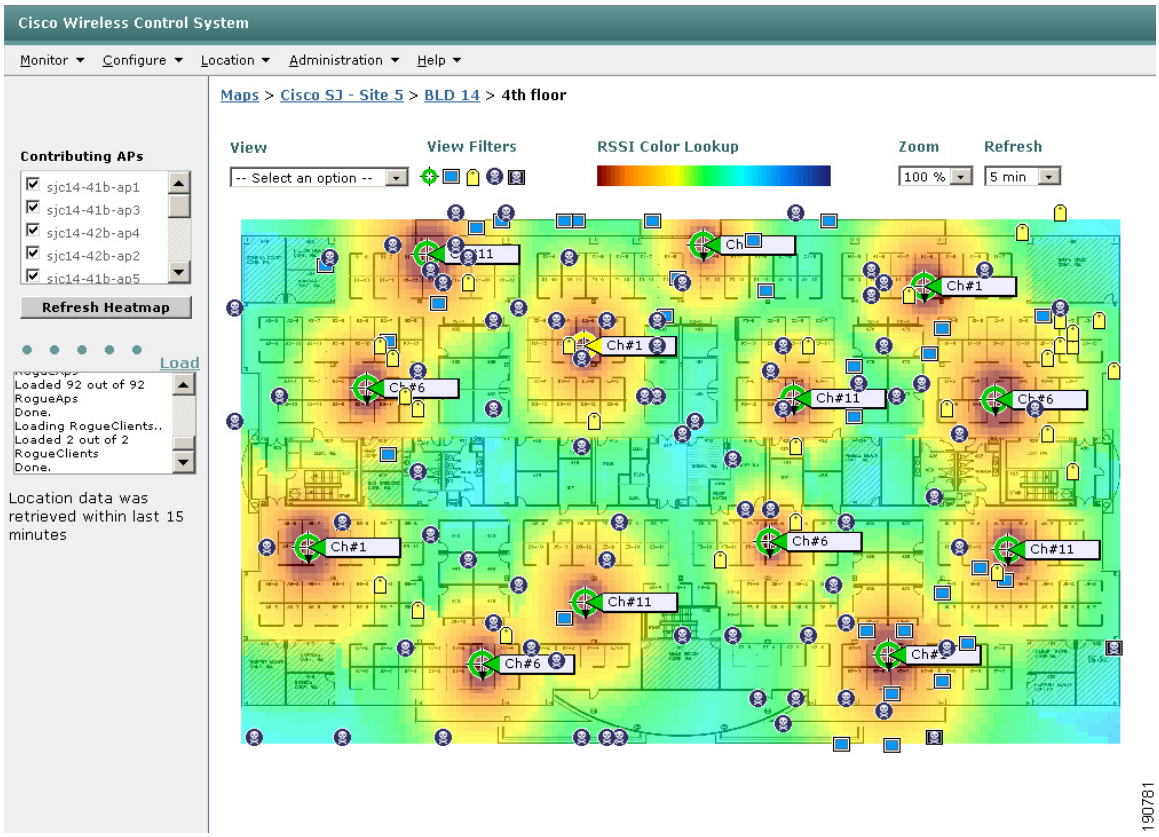
Although it is most common to have a single WCS paired with a single location appliance, variations on this theme are also possible to better support specific configurations. For example, in some cases because of a high number of clients and rogues, the supported device tracking capability of a single location appliance may be exceeded while being substantially under the supported access point and controller limitations of WCS. In this case, you can partition the network from the perspective of location service only and assign one half of the network (for example) to location appliance A, with the other half to location appliance B. Both of these location servers can then be managed under a single common WCS. Using this approach, the WCS administrator is presented with the simplicity of managing a single management domain from a single WCS server, but with the extensibility of multiple location domains that allow for addressing client, asset tag, and rogue counts that exceed the supported capacities of a single location appliance.

Tracking Clients, Asset Tags, and Rogues with the Location Appliance

As mentioned in On-Demand Device Location, page 8-83, WCS can perform on-demand location of clients, rogue access points, and rogue clients regardless of the presence of a location appliance. However, the addition of the location appliance allows you to view the location of multiple devices across all these classes simultaneously and track their history for longer periods than WCS allows.

Figure 8-71 provides a visual example of this multiple device simultaneous tracking capability. It may be helpful to compare the capabilities shown here to those shown in Figure 8-66 and Figure 8-67 for on-demand location. In Figure 8-71, devices from all supported categories are displayed on a floor with a periodic screen refresh set to five minutes. The floor plan loaded by the WCS administrator used as a background onto which is superimposed an RF “heatmap” showing the predicted RF coverage of each access point. Access points are shown on the floorplan along with internally generated channel information tags. Using information contained in the location appliance database, WCS displays icons for each device at locations that were determined by the location appliance using RF Fingerprinting positioning calculations.

Figure 8-71 Floor Map—Simultaneous Tracking of all Device Categories



For a comprehensive discussion of the device tracking capabilities that are available when using WCS with the Wireless Location Appliance, see *Wi-Fi Location-Based Services 4.1 Design Guide* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html.

Using WCS to Efficiently Deploy Your Wireless Network

One of the challenges facing network designers and installers is how to efficiently and rapidly deploy large numbers of lightweight access points and controllers across numerous sites.

In very large deployments, the ability to rapidly deploy and configure the network infrastructure is a key aspect of a successful and economically successful project implementation. It is not always feasible to deploy experienced network technicians to perform configuration, troubleshooting, and software upgrades on-site to each and every site in a large-scale deployment. Often there are simply too many sites being installed simultaneously and not enough personnel available to make this practical.

To address this situation, the wireless networking solution should require only minimal, basic configuration on-site at installation time to allow IP connectivity back to a centralized management site. This allows further configuration to be performed over the network by a central pool of experienced technical personnel. Experienced central site technical staff can make use of configuration efficiencies present within the WCS management system that greatly reduce the number of steps required to configure WLAN controllers and lightweight access points in accordance with all policies and standards set forth for the enterprise.

In the Cisco Unified Wireless Network, each controller requires only basic interface and IP configuration before it is accessible over an IP network. This is typically performed via the controller serial console and is a relatively simple affair. After interfaces are configured and the controller is attached to the IP network, WCS can be used to complete the application of configuration parameters to WLAN controllers as well as the latest software levels. After configuration of WLAN controllers has been completed, there is no need to individually configure lightweight access points because they derive their configuration parameters as well as their internal operating software in a "zero-touch" fashion from the WLAN controllers themselves.

Several WCS features are described in this chapter that can be particularly helpful during the deployment of large wireless networks across numerous sites, allowing far more efficient configuration than would be possible by simply accessing each controller using a web browser or CLI session and performing all configuration manually.

Policy Templates

Policy templates (Defining and Applying Policy Templates, page 8-22) are a key feature of WCS that can reduce the amount of effort required to configure remote site WLAN controllers during a deployment of any size. Policy templates allow for a set of related configuration objects to be defined, applied to selected controllers, and then saved for later use with subsequent controllers awaiting deployment. As each controller is physically installed and made available over the IP network, policy templates can be applied to one or more controllers, access points, or radios by the WCS operator. (Access points and radios must be registered with controllers to be eligible for configuration via templates. See Defining and Applying Policy Templates, page 8-22 for further information.)

When configuring multiple WLAN controllers that are part of the same mobility group, consider using the Configuration Groups facility described in Using Policy Template Configuration Groups, page 8-25 as opposed to applying templates one at a time. The use of configuration groups allows you to assign multiple controllers to a mobility group and apply one or more templates to them, saving a considerable amount of labor.

An example of how policy templates can be used to save both time and effort can be seen in the following steps taken to remotely configure a newly-installed Cisco 4400 WLAN Controller at a remote site.

The WLAN controller to be installed should receive its initial basic configuration via a local CLI session using the serial port. This is typically performed either before shipment at a staging center or at the remote site during installation by on-site installers. Appendix C, "Example of Wireless LAN Controller Initial Setup," indicates an example of the controller Setup Wizard and the type of information that is required for basic setup. Complete guidance and step-by-step instructions for configuring a WLAN controller using the controller Setup Wizard can be found in the document entitled Cisco 4400 Wireless LAN Controller—Quick Start Guide.

Step 1 After the controller has received basic configuration and it has been confirmed that the controller has been successfully attached to the network, it attempts to add the controller to WCS as described in Adding Controllers, page 8-8. If this fails, re-check connectivity and SNMP parameters specified in **Configure > Controllers > Add Controller**.

Step 2 Apply all desired templates to the WLAN controller as described in Defining and Applying Policy Templates, page 8-22 and *Cisco Wireless Control System Configuration Guide, Release 4.0* at the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscfg40.html.

Step 3 Save the controller configuration to nonvolatile (flash) memory as described in Configuring WLAN Controllers, page 8-13 and Figure 8-10.

Step 4 If necessary, upgrade any controller software as described in Managing Controller Operating Software, Web Authentication Bundles, and IDS Signatures, page 8-28. If a controller operating system upgrade was performed, reboot the controller by visiting the All Controllers screen shown in Figure 8-3 and selecting the controller you wish to reboot.

Step 5 Select **Reboot Controllers** from the upper right-hand drop-down menu and click **GO**. After the controller has fully rebooted, verify that it contains the expected software version by viewing **Monitor > Devices > Controllers > Summary** and observing the software version listed under Inventory.

Step 6 Have the lightweight access points at the remote site connected to the local network and allow them to boot up completely as per the detailed guidelines found in either Quick Start Guide LWAPP-Enabled Cisco Aironet Access Points or Cisco Aironet 1240AG Series Lightweight Access Point Hardware Installation Guide, which are both available at the following URL: http://www.cisco.com.

Step 7 After the access points have successfully booted up and can be seen to have registered to the controller as per Monitoring Access Points, page 8-51 and Figure 8-36, proceed to define the AP and radio policy templates for this controller and apply them to the access points as described in Defining and Applying Policy Templates, page 8-22 and *Cisco Wireless Control System Configuration Guide, Release 4.0* at the following URL:
http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscfg40.html.

If the policy templates are successfully applied to the access points and radios, they are automatically saved within those devices and retained during any future reboot.

Step 8 As noted in Defining and Applying Policy Templates, page 8-22, there are a few parameters that can only be configured via the controller web interface or CLI. If any such changes are required, make them at this time via either the controller web interface or a CLI session and save the controller configuration to nonvolatile (flash) memory.

Performing Tasks Across Multiple WLAN Controllers

As has been described in other sections of this document, WCS makes it easy to update WLAN controller resident software such as operating software and IDS signatures from either WCS itself or other TFTP servers in the network. When working with multiple WLAN controllers, especially during a network upgrade or other deployment, WCS makes it possible to perform these types of tasks and others for a group of selected controllers with a minimal amount of keystrokes. The maximum number of WLAN controllers that can be selected for these operations is currently set at the display page size of 20 controller entries. All selected WLAN controllers must be resident on a single WCS display page using the **Configure > Controllers** menu selection. Controllers cannot be included in a selection set if the desired controllers are found on multiple display pages.

For example, if two controllers are being installed at six sites that are located in three different regions of a country, this capability can be used to initiate a download of the latest controller operating software to each of the controllers in each region. Instead of having to initiate twelve separate WCS command sequences to get this done, the ability to specify multiple controllers allows it to be done with three (each sequence specifying a download to all controllers in a single region from a regional TFTP server). If you want to initiate a save to configuration and reboot for all twelve controllers, this can be done via two WCS commands instead of twelve. During a deployment where many controllers may need many of the same functions performed repeatedly, the ability to use WCS to direct such actions at multiple controllers across the management domain saves time and work on the part of the central administration staff.

The types of functions that can be targeted at multiple controllers in this manner include the following:

- Updating operating software to multiple controllers—Allows the administrator to load new controller operating firmware to multiple controllers that have been successfully added to WCS and are currently reachable. It can be accessed via **Configuration > Controllers**, selecting the target controllers from the list presented on the screen and proceeding with the steps detailed in Managing Controller Operating Software, Web Authentication Bundles, and IDS Signatures, page 8-28. It can also be performed on all controllers in a configuration groups via **Configuration > Controllers > Config Groups**.
- Downloading IDS signatures to multiple controllers—Allows the administrator to load new IDS signatures to multiple controllers that have been added to and are currently reachable by WCS. This feature is available by accessing **Configuration > Controllers**, selecting the target controllers from the list presented on the screen, and following the procedure indicated on the screen. It can also be performed on all controllers in a configuration groups via **Configuration > Controllers > Config Groups**.
- Downloading customized web authentication to multiple controllers—Allows the administrator to download a customized web authentication page to multiple controllers. This feature is available by accessing **Configuration > Controllers**, selecting the target controllers from the list presented on the screen and following the procedure indicated on the screen. It can also be performed on all controllers in a configuration groups via **Configuration > Controllers > Config Groups**.
- Saving configuration for flash to multiple controllers—Allows the administrator to initiate writing the current configuration file to nonvolatile (flash) memory on several controllers simultaneously. It is a very useful feature especially immediately after applying policy templates to multiple controllers, because these controllers would normally require this command to be issued individually to save updated configuration information to nonvolatile memory. This feature is available by accessing **Configuration > Controllers**, selecting the target controllers from the list presented on the screen by enabling their checkboxes and then selecting “Save Config to Flash” from the drop-down command selector in the upper right-hand portion of the screen.

  This function can also be performed on all controllers in configuration groups via **Configuration > Controllers > Config Groups**.
- Refreshing WCS configuration from multiple controllers—This feature (described in detail in Non-Selective Synchronization, page 8-36) allows the administrator to initiate the refreshing of the stored configuration contained in the WCS databases from multiple controllers simultaneously. This is useful in correcting situations where it is suspected that the WCS database is no longer in sync with the configuration contained in the controller for multiple categories of configuration objects. Such a situation can result, for example, when changes are made to the WLAN controller configuration in WCS but because of a communication or other error in the controller, these changes did not take effect in the device. A refresh of WCS configuration from multiple controllers can also be performed on all controllers in a configuration groups via **Configuration > Controllers > Config Groups**.
- Initiation of a re-boot in multiple controllers—This feature is also accessible from **Configuration > Controllers** and allows multiple controllers to be re-booted at once. It is a useful feature when updating operating software in multiple controllers, because these updates do not become effective until each controller is re-booted. To initiate a re-boot of multiple controllers, access the **Configuration > Controllers** screen, select the target controllers from the list presented by enabling their check boxes, and then selecting **Reboot Controllers** from the drop-down command selector in the upper right-hand portion of the screen.

- Note that all controllers that are part of a configuration group can be rebooted either sequentially (cascade reboot) or in parallel via the reboot menu tab in **Configuration > Config Groups >*configgroupname*** as shown in Figure 8-18. Rebooting the controllers in a configuration group via this method is an individual action; that is, it does not require that templates be applied to the controllers.
- Configuration Backup Scheduled Task—This feature is useful both as a scheduled task that is executed routinely to archive copies of all known (and currently reachable) controller configurations as well as a method to initiate an immediate archival of those same controller configurations.

Note For more information, see 13.6 CSCsd54800—Config Backup Scheduled Task Fails if One Controller is Unreachable.

Unlike other methods of performing configuration backups, a snapshot of *all* controller configuration in the entire network can be obtained simply by running this one scheduled task. Running this task before making major changes to widespread controller configurations in your network is typically a good idea. See Configuration Backup, page 8-117 for more information about this useful configuration management utility.

Deployment Models

This section discusses two basic deployment models for WCS in the enterprise:

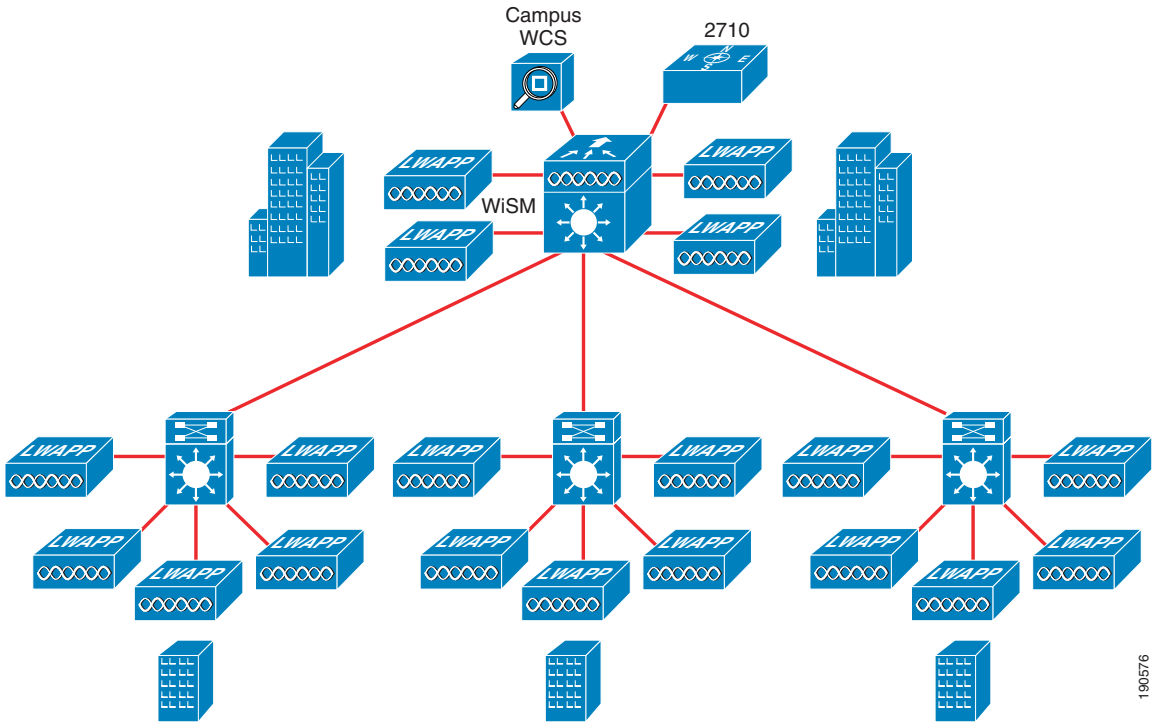
- Campus deployment
- Branch deployment

Note that all illustrations in the following sections have been simplified to focus primarily on the deployment of wireless network management. As such, these illustrations may not illustrate in detail all recommended wired or wireless infrastructure components as specified in other chapters of this SRND.

Campus Deployment

The most common campus deployment model for WCS is as a centralized component managing multiple WLAN controllers (one or more combinations of WLC, WLCM, or WiSMs) interconnected via a modern high-speed campus local area network as shown in Figure 8-72 (optional location appliance is also shown here).

Figure 8-72 Campus WCS Deployment using Single WCS and Location Appliance



In this model, up to 3000 lightweight access points dispersed among a maximum of 250 WLAN controllers are supported as of WCS version 4.0. (This is dependent on the type of system used for WCS deployment and other factors. See *Cisco Wireless Control System Release Notes, Release 4.0* for further details about WCS capacities.)

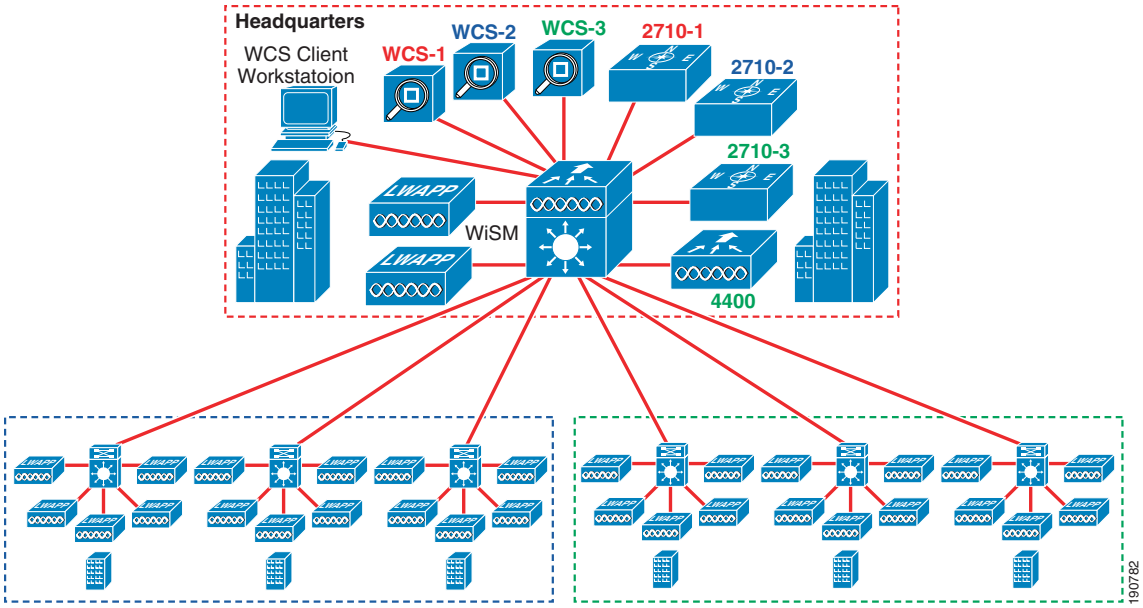
This is not a "hard" limitation but rather a limit to which the solution has been tested and is supported by Cisco Systems.

The campus management model illustrated in Figure 8-72 illustrates the use of the Catalyst 6500 Wireless Services Module (WiSM) at the main campus site that provides WLAN controller services for lightweight access points in the main building complex as well as the other locations shown. This use of a Catalyst 6500 WiSM controller module is not mandatory, and the same design model can be applied using external WLAN controllers located centrally instead if so desired.

The approach shown in Figure 8-72 has been found to be suitable for the vast majority of customer wireless campus deployments. In combination with well-designed modern high speed LANs, it provides excellent performance with a highly scalable centralized management base (including optional location-based services) that can be easily scaled without requiring an extensive re-design of the network as the enterprise grows.

In the few cases of very large campuses, this model can be scaled for even greater capacity by grouping WLAN controllers and placing each group under the control of a different WCS server. This approach is known as the *separation of management domains* and is illustrated in Figure 8-73.

Figure 8-73 Multiple WCS/Location Appliance Campus Deployment



Three WCS servers (WCS1, WCS2, and WCS3) and three location appliances (2710-1, 2710-2, and 2710-3) are co-located at the campus data center and main office building. Each of these WCS/Location Appliance pairs has been configured such that their management and location domains coincide with a different portion of the overall campus (as shown by the red, blue, and green outline boxes). Color-coded text has been used in the illustration provide clarity, indicating that each of the two controllers on the WiSM module are assigned to the management domain of WCS-1 and WCS-2 respectively with the standalone 4400 WLAN controller assigned to WCS-3. Note that each and every WLAN controller is defined to a single WCS management domain (and therefore only one WCS management server).

One or more client workstations (shown in Figure 8-73) can access any of the WCS servers. Each management server can be accessed from a single client workstation using multiple browser windows. It is not uncommon to see client workstations used precisely for this purpose located at the main campus building complex, typically within a network operations center (NOC).

Each WCS server can be configured to generate e-mail notifications (which can be relayed as pager and cell phone text messages) to NOC management staff personnel informing them of critical alarms that have been generated within any of the management domains. NOC personnel can then respond by accessing the proper WCS server from WCS client workstations to investigate and rectify the alarm situation.

To assure that NOC personnel have visibility to all traps issued by WLAN controllers in any of the management domains, the IP address of an overall enterprise network management system such as HP OpenView, Tivoli, and so on, can be entered as an additional trap receiver for each WLAN controller. This assures that all traps can be seen in a central location (in addition to each individual WCS), which facilitates problem resolution in organizations so equipped. Each WLAN controller can also be configured with the address of a NOC remote syslog server. In a similar fashion, this practice provides NOC personnel with visibility to all syslog messages generated by WLAN controllers in each management domain.

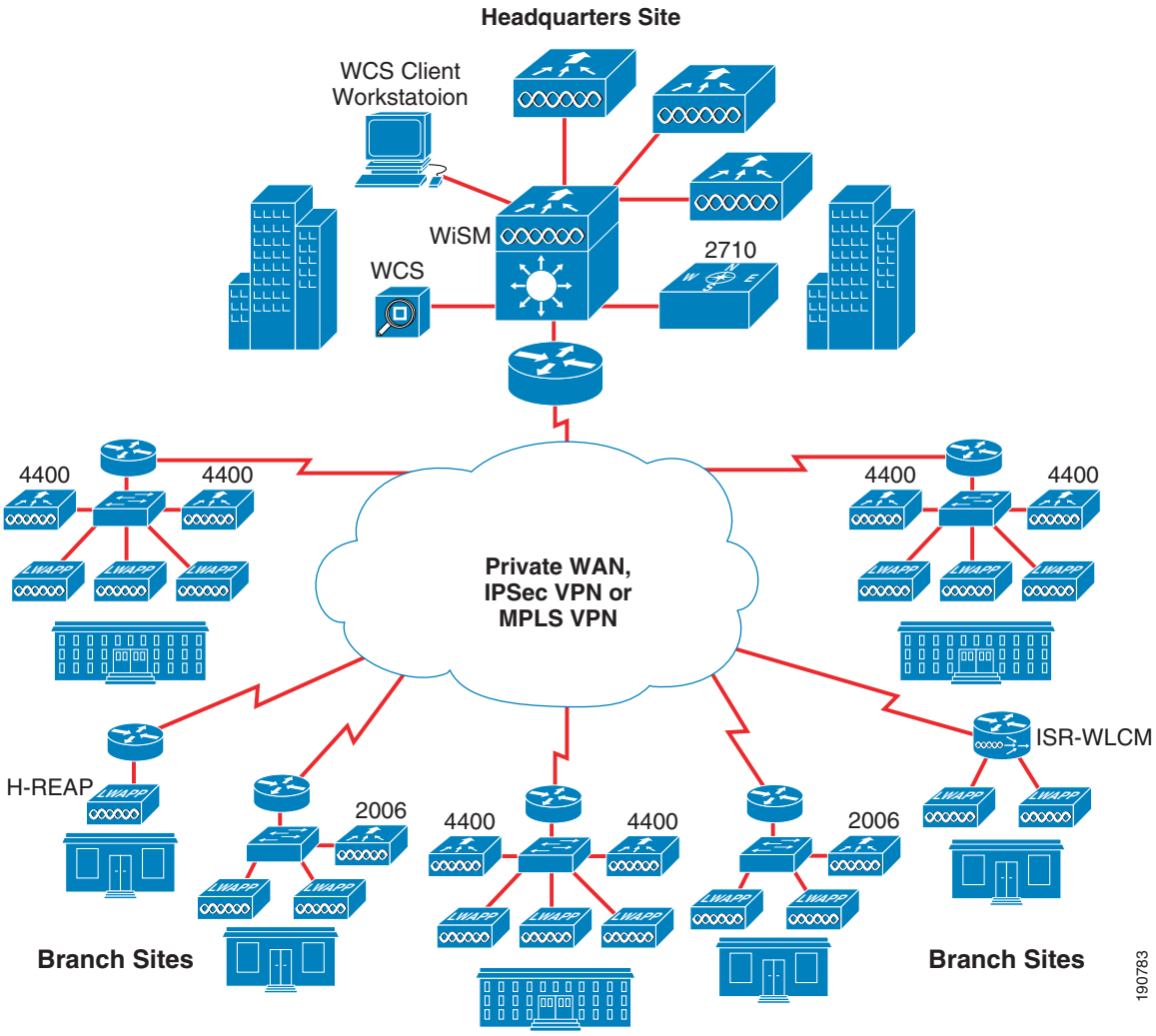
As shown in Figure 8-73, the use of a modular approach allows you to scale the campus model beyond the controller and access point limitations mentioned previously. This provides the ability to manage much larger (albeit much less common) campus networks than would otherwise be the case with a single WCS server but still retain a design that is supported by Cisco.

Branch Deployment

This section describes scenarios where the main corporate campus comprises only a minority presence in terms of installed wireless infrastructure within the enterprise. In these cases, the majority of wireless infrastructure as well as mission-critical wireless usage are found in *remote branch offices*.

Figure 8-74 shows a typical WLAN management deployment model in a network servicing remote branch offices (with optional location appliance included). This design illustrates the most common scenario of a single WCS server at a central headquarters location. As can be seen from the information contained in the *Cisco Wireless Control System Release Notes, Release 4.0*, depending on the choice of hardware and network capacity considerations, this WCS server can support up to 3000 lightweight access points distributed over 250 WLAN controllers (keep in mind that the limit on total tracked devices in the location appliance is 2500).

Figure 8-74 Remote Management of Branch Offices—Single Centralized WCS Server



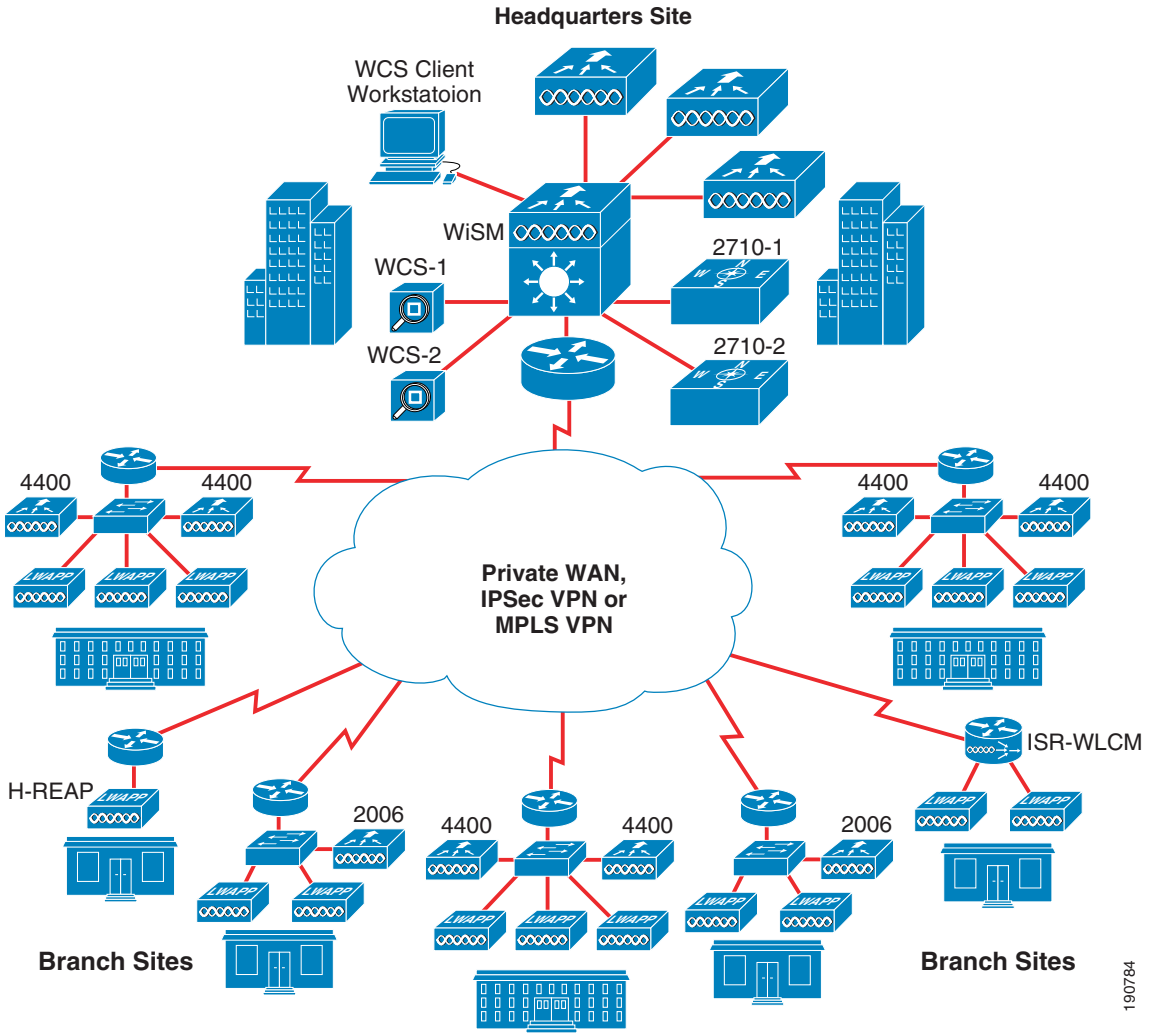
In this type of network design, application computing resources may be located centrally with backup WAN services provisioned in the event of a network outage. In the case of mission-critical application computing resources, these resources may be located in the branch (such as for point-of-sale systems in a retail environment) so as to withstand a complete interruption of primary and backup WAN service. In

the event of a WAN connectivity failure, management and location services are lost but basic wireless connectivity to local resources are preserved. (This availability is for wireless traffic that does not depend on a AAA server located at the central headquarters site, or traffic that is using a AAA server located in the branch.)

Non-mission critical systems (such as accounting systems, personnel records, and so on) are usually centrally located in both cases. As shown in Figure 8-74, the choice of WLAN controller at each site can vary. This can range from a Hybrid REAP (H-REAP) implementation designed to service sites requiring no more than two or three H-REAP lightweight access points per site to those with as many as 50 lightweight access points per site or more, which requires one or more 4400-series WLAN controllers to be deployed.

In some cases, the number of branch locations as well as the number of lightweight access points may be greater than the capacity of a single WCS server, even when deployed on the most robust available hardware. The network illustrated in Figure 8-75 illustrates such a case, where either the total number of lightweight access points is greater than 3000 or the total number of deployed controllers exceeds 250. In those situations, multiple centralized WCS servers can be deployed at the central site, splitting the network into multiple management domains (and multiple location domains).

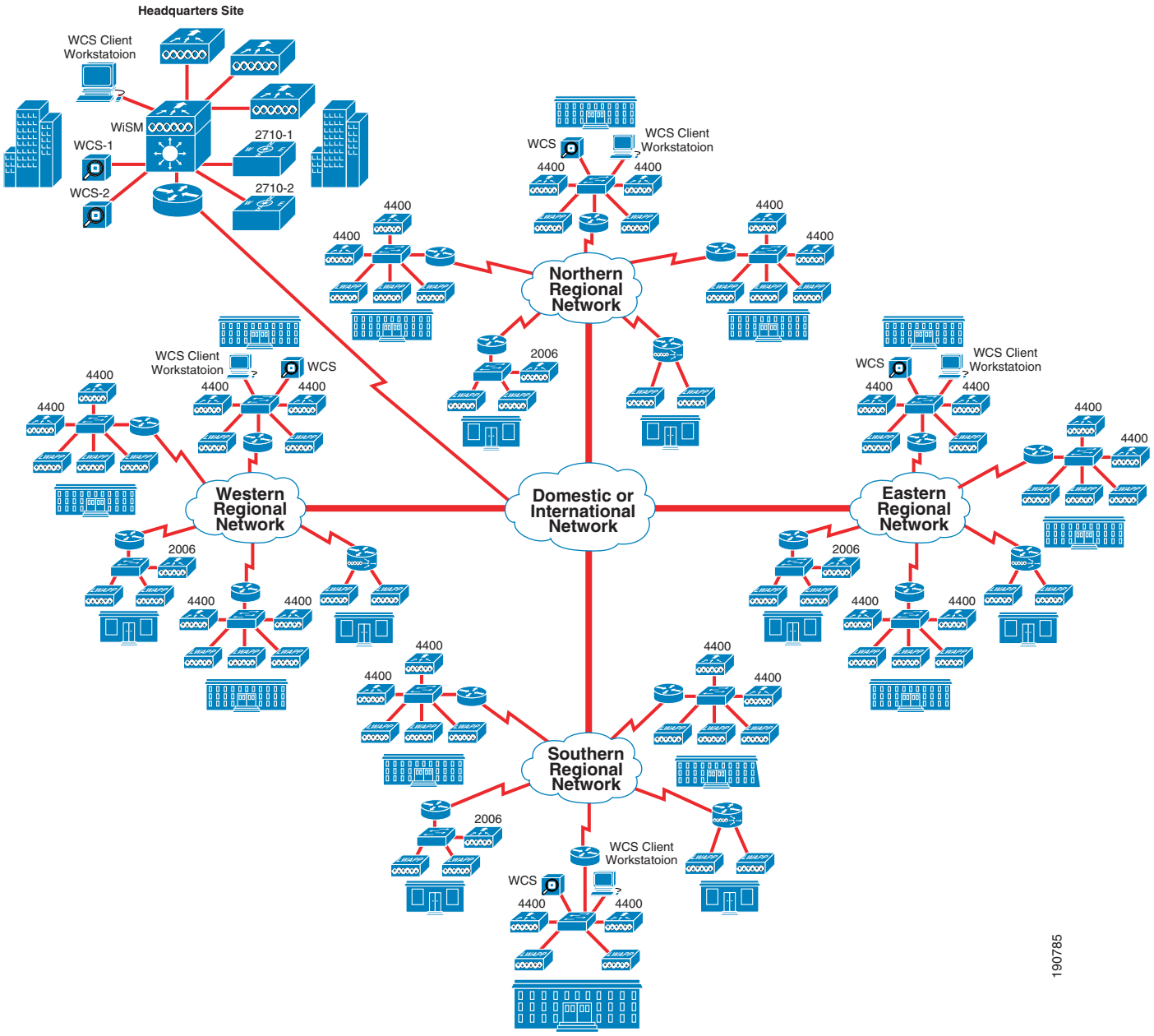
Figure 8-75 Remote Management of Branch Offices—Multiple Centralized WCS Servers



The allocation of WLAN controllers between the WCS servers in Figure 8-75 is the choice of the designer; however, a common approach is to partition the design into at least two WCS management domains. The first management domain you might specify can be for the wireless infrastructure that resides at the headquarters site. One or more additional management domains can then include the branch sites. WCS servers and location appliances can then be allocated to these management domains as appropriate. These WCS servers are then accessible from WCS client workstations located at the headquarters site.

Although the design described in Figure 8-75 may provide satisfactory performance for the majority of large scale wireless branch networks, there are alternatives for even larger (albeit much less common) branch networks that may make more sense depending on the organization itself, the way it is structured, and its underlying WAN topology. Some organizations structured along regional boundaries may find that a network infrastructure more representative of their structure is a better overall fit. In these cases, for example, it is not uncommon to find a central headquarters site along with several regional headquarters sites containing corporate resources in both locations. Figure 8-76 illustrates one such regionalized approach for an enterprise that is sub-divided into four regions plus a headquarters campus site.

Figure 8-76 Remote Management of Branch Offices—Multiple Regionalized WCS Servers



The branch sites in each region are network-managed by regional network operations staff located at each respective regional headquarters location. These regional headquarters locations are also full-time branch locations that, from a business operational standpoint, are peers with the other branch locations in the region. Regional connectivity is provided by one of the WAN networking alternatives already discussed, and the regional networks are connected via very high bandwidth connections to a corporate WAN network that is provided by one or more major service providers.

At the corporate headquarters site, a WCS server and location appliance are present to provide management and location services for the headquarters campus only (these do not interact with branch sites). Headquarters NOC staff can directly manage the wireless network in any branch location via their WCS client workstations (which have access to the WCS server in any region). Each regional WCS

server can be configured to generate e-mail notifications (which in turn can translate into text message notifications to cell phones, pagers, and PDAs) to headquarters network management staff, informing them of critical alarms that have been generated within the region. Headquarters personnel can then respond appropriately via their global WCS client workstations.

The IP address of a headquarters-based enterprise network management system (NMS) can be entered as an additional trap receiver for each WLAN controller in all sites. This ensures that headquarters personnel are made aware via the enterprise NMS of any conditions that trigger trap generation in any of the branch sites.

Note Note that simply defining the IP address of the headquarters WCS server as a trap receiver in the branch WLAN controllers does not provide the desired visibility to branch WLC traps. The headquarters WCS server ignores incoming traps from WLCs that have not been explicitly defined to it via **Configure > Controllers > Add Controller**. Adding a branch controller to the headquarters WCS server then enables polling of the controller by the corporate WCS, which negates one of the advantages of the regional design (reducing polling traffic).

Each branch WLAN controller can be configured with the address of a remote syslog server at the headquarters site to ensure that headquarters personnel have visibility to syslog messages generated by any of the branch WLAN controllers.

The regionalized approach shown in Figure 8-76 and other regionalized designs like it can offer the following key advantages to those customers whose organizational makeup and size allows them to make good use of it:

- A network failure in any one of the regional networks or in the corporate network itself is unlikely to cause a loss of WCS management in the branches outside of the affected region. From a network management perspective, a corporate network interruption affects only the ability of the corporate NOC staff to receive trap, syslog, and e-mail updates as well as their ability to directly manage resources in any of the branch sites. Depending on the degree to which resources are regionalized, each region can retain a fairly high degree of operational autonomy in spite of a corporate network disruption.
- Polling between WCS and each WLAN controller (and optionally between the location appliance and each controller) is confined entirely to each region and does not occur across the corporate network, which may be of interest to those planning to deploy large wireless networks. Assuming an even distribution of polling traffic among regions, the total traffic volume in any of the regional networks would be approximately estimated at only about 25 percent of what would be seen across a single network with all management servers centralized at one location.

Thus far, two remote branch management deployment models have been discussed that provide a very workable solution for the great majority of all wireless network management needs. Even so, there are still some organizations whose sheer scope and size may make even a regionalized solution such as shown in Figure 8-76 less than optimal. For this small group of extraordinarily large (in many cases multi-national) entities, you can institute WCS management at lower levels of the network, further down below even the regional level.

Some of the specialized concerns in these extremely large networks that can require such designs include the following:

- Organizational preferences—Some organizations may grant individual branch offices greater operational autonomy than might otherwise be the case. Although data and programs for many administrative background processes may be contained on corporate or regional servers, computing and network resources deemed “mission-critical” may be located at each branch site. This allows the branch to function with not only a high degree of managerial empowerment but with the capability to act almost as a standalone autonomous business unit when severe environmental events preclude any form of WAN connectivity to corporate or regional headquarters.

  In this type of organization, it may be preferred for the local branch to have the capability of managing its wireless LAN infrastructure in an autonomous fashion more analogous to its operational capabilities, even when situations make it impossible to establish external network connectivity. In both the centralized as well as the regional approaches illustrated in Figure 8-74, Figure 8-75, and Figure 8-76, this type of outage requires local branch personnel lacking access to their WCS servers to manage their WLAN controllers directly via the web or command line interfaces. No location services capabilities are available during any such outage because of the lack of accessibility to WCS and the location appliances located at the corporate or regional headquarters (this includes on-demand location).

- Mission-critical location-based services—Some very large branch enterprises may make use of location-based services applications at each branch location such that normal business functions may be impacted severely if LBS is not available. Looking back at the designs in Figure 8-74, Figure 8-75, and Figure 8-76, the location appliance is located either at a central or regional headquarters site. Any third-party location client-server applications that are located within the branch are not able to display current location information if the location appliance becomes unavailable because of a prolonged WAN failure. An example is a large national hospital corporation that depends on its LBS system to quickly locate critical medical equipment. A sudden disruption in such a system may impact the level of service that the hospital is able to deliver to its patients.

- Polling traffic—Taking into the consideration the information presented in Device Status Polling, page 8-108, there is a potential for very large enterprise networks to produce a significant amount of network polling traffic, especially at the central headquarters or regional headquarters where WCS servers happen to be located. Depending on the current use of existing circuits, this added traffic between WCS and WLAN controllers (as well as between the location appliance and WLAN controllers) can be of concern.

In the few extremely large-scale deployments where these areas must be addressed, the added cost of deploying a WCS server (and location appliance) within each branch may be justified. This approach eliminates the impact of management and location services polling upon the WAN completely by relocating the WCS servers and location appliances to each individual branch. It also adds full management and location-based services survivability to the branch in spite of prolonged WAN interruption, thereby allowing branch wireless management autonomy. In the event of a WAN interruption at either the regional or corporate level, local branch WLAN users continue to have access to branch-resident mission-critical resources located, and local branch technical personnel have complete and unfettered management access to their wireless LAN infrastructure as well.

Traffic Considerations When Using WCS in Large Networks

For customers wishing to deploy large or very large networks, an understanding of the traffic volumes that are involved when routine management polling occurs can be useful in making proper design choices.

Traffic Sources

In a system consisting of a WCS, location appliance, WLAN controllers, and lightweight access points, the following categories are the main sources of network traffic:

- Between WLAN Controllers and WCS:
  - Device status polling
  - Client statistics polling
  - RF statistics polling
  - Rogue access point polling
  - Configuration audit reports and network audits
  - Controller configuration refresh (including cold-start refresh)
  - WCS configuration refresh
  - Controller configuration backups
  - Software, configuration and IDS signature downloads
- Between WLAN controllers and the location appliance:
  - Client polling
  - Asset tag polling
  - Rogue AP/client polling
  - Statistics polling
- Between WCS and the location appliance:
  - Network design synchronization
  - Location appliance backup

WLAN Controllers and WCS

WCS obtains information about the status of WLAN controllers, lightweight access points, WLAN clients, asset tags, and rogues in two ways: via WCS-initiated SNMP polling of the WLAN controllers, and unsolicited SNMP traps generated by WLAN controllers. As mentioned in previous sections, WCS does not poll lightweight access points, WLAN clients, asset tags, or rogue devices directly, but instead relies on information that WLAN controllers proxy to WCS about these entities.

In WCS, configure the various categories of polling as well as the regularity of polling via one of four scheduled tasks:

- Device status polling
- Client statistics polling

- Statistics polling
- Rogue AP polling

The following sections discuss each of these in more detail and provide a brief understanding of the level of traffic impact each polling categories can assess on total network management traffic.

Although SNMP polling makes up the predominant portion of the total management traffic between WCS and WLAN controllers, it is by no means the exclusive source of management traffic. SNMP traps flowing from controllers to WCS and other trap receivers also contribute a traffic component, albeit one that is rarely a concern in most cases. The number of traps enabled, the number of WLAN controllers, the amount of times additional SNMP polling is triggered by the reception of traps, the number of trap receivers, and the frequency at which trap-generating events occur all dictate the impact of SNMP traps on overall management traffic.

Utility functions such as backup and restores of controller and WCS database configurations can also contribute to network congestion, primarily in very large networks when such functions might be performed on many controllers simultaneously. Taken individually, such actions are typically of minor consequence, but when initiated on large groups of controllers simultaneously, it would not be unusual to see traffic spikes that may become noticeable overall. An example of where this may be commonly seen is with the case of controller software downloads (see Managing Controller Operating Software, Web Authentication Bundles, and IDS Signatures, page 8-28) and controller configuration backups that tend to be the most traffic intensive of the utility functions. Traffic because of other utility functions such as configuration refreshes to and from WLAN controllers (described in Non-Selective Synchronization, page 8-36) are usually not significant and typically should not pose a problem.

Reporting functions (such as the configuration audit reports) cause WCS to inventory the configuration of each selected controller and compare the results against the contents of the WCS database. Configuration Audit Reports and Network Audits, page 8-114 discusses the best practices surrounding the running of these reports and also some detailed analysis of the traffic flows that are involved for both SNMPv2c and SNMPv3. The network audit scheduled task (Network Audit, page 8-119) is a derivative of the configuration audit report except that it runs against all controllers defined to WCS instead of a subset of selected controllers. In large networks comprising many WLAN controllers and lightweight access points, it is always good practice to consider running the network-wide network audit scheduled task at times of low network usage.

Using the discussions of initial and incremental traffic as a guide (described in Device Status Polling, page 8-108 through SNMP Traps, page 8-112), it is possible to gain a general understanding of the traffic volume that might be generated by the various management polling methods in a proposed design. Note that estimates stated in the subsections to follow are based on lab testing under closely controlled circumstances. The number of devices, clients, and rogues detected in your network will likely vary between polling cycles.

This information is provided so that designers and architects of network systems can use the traffic volume information in conjunction with information they already know about network utilization in their own environment to make intelligent design decisions. It is not provided with the intent of serving as a precision prediction tool, but rather to educate readers with large networks as to the magnitude of potential management traffic volumes they may incur in an effort to enable better overall network designs.

Management traffic volumes should be considered not only in conjunction with the present network utilization, but with those traffic loads that can be reasonably expected in the near future because of growth and expansion. If location appliances are to be included in the design, a separate analysis should be conducted focusing on polling traffic between the location appliance and the WLAN controllers (see WLAN Controllers and the Location Appliance, page 8-116).

In the minority of large wireless networks where the impact of SNMP polling on network utilization is deemed to be excessive, the polling intervals for device status, client statistics, radio statistics, and rogue access point polling can be adjusted as described in *Cisco Wireless Control System Release Notes, Release 4.0*, which is available at the following URL: http://www.cisco.com/en/US/docs/wireless/wcs/release/notes/wcsrn_MR2.html.

By staggering and increasing the polling intervals, you can better distribute the aggregate volume of polling traffic that is being introduced into the network and lower increases in peak network utilization that are because of management SNMP polling.

Unless otherwise noted, all traffic quantities in the following sub-sections are UDP byte and packet counts for a single controller that were measured on a 10/100/1000 Ethernet LAN using Ethereal 0.99.0. Measurements were taken for both bidirectional and unidirectional traffic flows, along with a measurement of the total elapsed time required for the polling process to complete. Hardware used in these tests were Cisco Catalyst c3750 Ethernet switches and 4400-12 WLAN Controllers with 4.0.155.5 controller software and AP1242 access points.

Device Status Polling

Device status polling is conducted in WCS by the Device Status scheduled task. WCS is configured by default to conduct device status polling every five minutes. In addition to being responsible for updating device reachability, device status polling provides WCS with information such as the following:

- Controller SysUpTime, total memory, free memory, CPU utilization, and operating software version
- Lightweight access point and radio interface administrative status
- Coverage, load, and interference profile status
- 802.11 privacy options in use
- Beacon periods currently in use
- MAC addresses of AP neighbors

The amount of traffic exchanged during device status polling is not affected by the presence of wireless LAN clients, asset tags, rogue access points, or rogue clients. The volume of polling traffic produced was seen to be tied to the number of lightweight access points registered to the WLAN controller.

Figure 8-77 provides average SNMP v2c/SNMPv3 UDP traffic volumes observed during testing between WCS and a 4400-12 WLAN controller. The tables provide us with baseline device status polling traffic figures for a single 4400-12 controller with zero access points registered, and allows visualization of how this traffic flow increases with additional registered access points.

The table in Figure 8-77 is broken down into ranges. Note that within each range, the traffic quantities listed represent the amount of traffic observed when the number of registered access points was within the range. For example, when device status polling occurs using SNMPv2c between WCS and a controller with four registered infrastructure access points, on average an exchange of approximately 4805 bytes of UDP data was observed each time WCS polled the WLAN controller for device status information. However, if the number of registered infrastructure access points increases to nine, the average number of bytes exchanged between WCS and the WLAN controller increases to approximately 7154 during each iteration of device status polling.

Although not intended as a precision prediction tool, this information can be useful in understanding how device status polling traffic might grow beyond the twelve access points shown.

Figure 8-77 Device Status Polling Traffic

Bytes

	Polling Traffic 0 APs	Each Additional AP
SNMPv2c	2,728	2,561
SNMPv3	5,773	4,291

Number of Packets

SNMP	0 APs	Each Additional AP
v2 or v3c	32	20

190786

Client Statistics Polling

Client statistics polling is conducted in WCS by the clients statistics polling scheduled task (Client Stats Poll). WCS is configured by default to conduct client statistics polling every fifteen minutes. Some of the information that is gathered by WCS via client statistics polling includes but is not limited to the following:

- Average SNR and RSSI of clients
- Number of packets received and sent from/to the client
- Number of bytes received and sent from/to the client
- Number of policy errors that have occurred for the client
- Client status

The amount of traffic exchanged during client status polling is not related to the number of lightweight access points registered to the WLAN controller. It is also not affected by the presence of Layer 2 asset tags, rogue access points, or rogue clients.

Note Asset tags that associate to lightweight access points as WLAN clients (such as PanGo Locator LAN tags) contribute to the amount of traffic produced during client statistics polling. AeroScout asset tags do not associate to access points.

The traffic volume is driven primarily by the number of WLAN clients that have associated to the lightweight access points serviced by the controller being observed. Lightweight access points that do not have WLAN clients associated do not contribute to client statistics polling traffic.

The distribution of clients between lightweight infrastructure access points was seen to have little if any impact on the aggregate amount of client statistics polling traffic produced for that controller. For example, four WLAN clients associated to a single lightweight access point affiliated with a controller result in approximately the same volume of client statistics polling traffic between that controller and WCS as four WLAN clients, each associated to individual lightweight access points on the same controller.

Figure 8-78 provides average SNMP v2c/SNMPv3 UDP traffic volumes observed during testing between WCS and a 4400-12 WLAN controller with a single registered lightweight access point. The tables provide baseline client statistics polling traffic figures for a single 4400-12 controller with zero clients associated, and allows visualization of how this flow might increase with additional clients.

Figure 8-78 Client Statistics Polling Traffic

Bytes

	Polling Traffic 0 Clients	Each Additional Client
SNMPv2c	722	2,419
SNMPv3	1,438	3,160

Number of Packets

SNMP	0 Clients	Each Additional Client
v2 or v3c	8	8

190787

The table in Figure 8-78 is divided into ranges. Note that within each range, the traffic quantities listed represent the amount of traffic observed when the number of clients associated to registered access points is within the range. For example, when client statistics polling occurs using SNMPv2c between WCS and a controller with three associated clients, on average approximately 3950 bytes of UDP data are exchanged between WCS and the WLAN controller. However, if the number of associated clients increases to six, the average number of bytes exchanged between WCS and the WLAN controller increases to approximately 6118 during each iteration of client statistics polling.

Although not intended as a precision prediction tool, this information can be useful in understanding how client statistics polling traffic might grow beyond the six clients shown.

Statistics Polling

Statistics polling is conducted in WCS using the Statistics scheduled task. The statistics that are gathered by this scheduled task concern the lightweight access point radio interfaces. WCS is configured by default to conduct statistics polling every fifteen minutes. Some of the information that is gathered by WCS via statistics polling includes but is not limited to the following:

- Radio interface transmit power level
- Radio interface operational status
- Number of WLAN clients associated to a radio interface
- Percentage of time interface radio receiver/transmitter is receiving/transmitting packets
- Channel utilization
- Number of clients with below-threshold SNR
- Status of whether load, coverage, noise, or interference thresholds have been exceeded

- Transmitted and received fragment counts
- FCS error count

The amount of traffic exchanged during statistics polling is not affected by the presence of wireless LAN clients, asset tags, rogue access points, or rogue clients. Rather, the volume of traffic produced is primarily driven by the number of lightweight access points (and the number of 802.11 radios they contain) that registered with the WLAN controller.

Figure 8-79 provides average SNMP v2c/SNMPv3 UDP traffic volumes observed during testing between WCS and a 4400-12 WLAN controller. The tables provide baseline statistics polling traffic figures for a single 4400-12 controller with zero registered lightweight access points and allows you to visualize how this flow of traffic might increase as the number of registered infrastructure dual-band lightweight access points is increased.

Figure 8-79 Statistics Polling Traffic

Bytes

	Polling Traffic 0 APs	Each Additional AP
SNMPv2c	348	1,848
SNMPv3	716	2,085

Number of Packets

SNMP	0 APs	Each Additional AP
v2 or v3c	4	3

190788

The table in Figure 8-79 is divided into ranges. Note that within each range, the traffic quantities listed represent the amount of traffic observed when the number of registered dual-band access points was within the range. For example, when statistics polling occurs using SNMPv2c between WCS and a controller with four registered dual-band access points, on average approximately 10,279 bytes of UDP data are exchanged each time WCS polls the WLAN controller. However, if the number of registered dual-band access points increases to six, the average number of bytes exchanged between WCS and the WLAN controller increases to approximately 13,229 during each iteration of statistics polling.

Although not a precision prediction tool, this information can be useful in understanding how polling traffic might grow beyond the 12 access points shown.

Rogue Access Point Polling

Rogue access point polling is conducted in WCS via the Rogue AP scheduled task. WCS is configured by default to start rogue AP polling of all controllers every 120 minutes. Some of the information that is gathered by WCS during rogue access point polling includes but is not limited to the following:

- Rogue AP type
- Rogue AP channel, SNR, RSSI, WEP mode, WPA mode, preamble
- Rogue AP SSID, radio type
- Time stamp of rogue AP initial detection
- Total number of rogue clients
- Rogue AP on network status
- Rogue AP containment level
- Total number of detecting APs
- Detecting AP names and MAC addresses

The amount of traffic exchanged between WCS and the WLAN controller during rogue AP polling is not affected by the presence of wireless LAN clients or asset tags. It is driven primarily by the number of rogue access points detected by the lightweight infrastructure access points.

Figure 8-80 provides average SNMP v2c/SNMPv3 IPv4 traffic volumes observed during testing between WCS and a 4400-12 WLAN controller. The tables provide baseline rogue polling traffic figures for a single 4400-12 controller with zero detected rogue APs through 29 detected rogue access points, and allows you to visualize how this flow of traffic might increase as the number of detected rogue access points increases.

Figure 8-80 Rogue AP Polling Traffic

Polling Traffic in Bytes

	1 AP Detecting 1 Rogue AP	Each Additional AP Detecting 1 Rogue AP
SNMPv2c	2,993	1,382
SNMPv3	4,434	1,742

Number of Packets

SNMP	1 AP Detecting 1 Rogue AP	Each Additional AP Detecting 1 Rogue AP
v2 or v3c	16	12

190789

The table in Figure 8-80 is divided into ranges of detected rogue access points. Note that within each range, the traffic quantities listed represents the amount of traffic that was observed when the number of detected rogue access points was within the range. For example, when rogue AP polling occurs using SNMPv2c between WCS and a controller with nine detected rogue access points, on average approximately 2592 bytes of IPv4 data was exchanged between WCS and the WLAN controller each time WCS polls the WLAN controller. However, if the number of detected rogue access points rises to 12, then the average number of bytes exchanged increases to approximately 5158 on each polling iteration.

Although not intended as a precision prediction tool, this information can be useful in understanding how rogue polling traffic might grow beyond the 29 detected rogue access points tested here.

Note that the presence of associated rogue clients was not found to add any appreciable amount of traffic to the results recorded in Figure 8-80.

SNMP Traps

As described in Relationship Between Traps, Events, Alarms, and Notifications, page 8-69, a trap is a notification issued by a managed device to the network management station (WCS) when a significant event occurs at the managed device. WLAN controllers can be configured to send SNMP traps to up to six trap receivers. In contrast to a response to a polling request, the information contained in a trap is typically sent in an unsolicited manner. When traps are configured and enabled in the managed device (WLAN controller), they are sent to WCS as the events that generate them occur.

Traps are enabled or disabled via **Configure > Controllers > Management > Trap Control**, and trap receivers are defined using **Configure > Controllers > Management > Trap Receivers**, as described in Relationship Between Traps, Events, Alarms, and Notifications, page 8-69. Both trap receiver as well as trap control configuration objects can be defined via policy templates. For proper WCS event

notification, it is always required that WCS be defined as one of the trap receivers in each WLAN controller comprising the management domain. You may opt to define other trap receivers as well depending on your organizational policy and any other enterprise management systems in use, but always make sure to include a WCS server as a trap receiver for your WLAN controllers.

Because traps are sent without acknowledgement, it is possible that a transmitted trap is never received by WCS. This can happen, for example, in highly utilized or congested WAN networks because of packet discard algorithms that take place in the service providers network, or simply because of QoS mechanisms doing their job and discarding low-priority traffic. Because trap delivery is not guaranteed, WCS also polls for some of the same information that is available via the trap mechanism. Examples include rogue AP traps and various traps pertaining to the state of the lightweight access point radios. The WLAN controller makes much of this same information available to WCS via rogue access point and statistics polling, thereby ensuring that if this information is not received via the trap mechanism, WCS still learns of any extraordinary conditions during the next polling cycle.

The traps sent from WLAN controllers to WCS can vary in size (during lab testing traps were analyzed that ranged in size from approximately 120 bytes to almost 400 bytes). In most cases, the amount of overall traffic added to the network specifically attributable to SNMP traps is inconsequential. However, for those customers that may be considering deploying very large networks with large numbers of controllers and several WCS servers, a few key points should be kept in mind:

- Depending on the specific trap received, WCS may immediately poll the responsible WLAN controller for additional information.

  An example of this can be seen in the AP Registered trap. After reception of this trap, WCS immediately issues a series of poll requests to the controller that initiated the trap for additional device status information. Other examples include traps indicating that the channel country set or power levels have changed. This is a well-known and perfectly acceptable method of obtaining additional information that has not been included in the trap itself, and it allows WCS to gain a better understanding of precisely what the condition is at the WLAN controller that initiated the trap. The point to keep in mind here is that the net contribution to management traffic in this case is more than simply the traffic volume incurred transmitting the trap itself.

- Out-of-date trap receiver lists can increase the level of network trap traffic by causing unnecessary copies of traps to be sent to non-existent stations, stations that are simply not listening on the trap port any longer, or stations that are listening but really should not be provided with the information any longer.

  The amount of trap traffic generated by a controller increases in direct proportion to the total number of trap receivers specified, up to the maximum of six trap receivers (that is, a fully configured controller with six trap receivers defined generates six times more trap traffic that a controller that has only a single WCS configured as a trap receiver and nothing more). In large networks, trap receivers should be specified strictly on a need-to-know basis and only for stations that are actually active trap receivers. Trap receivers used during troubleshooting, testing, or network diagnostics should be promptly disabled or removed promptly after their usefulness has expired and they are no longer necessary. The use of policy templates can make the assignment and prompt removal of any unnecessary trap receivers much easier.

Additional information about the traps configurable via the **Configure > Controllers > Management > Trap Control** page can be found in online help system available under the WCS main menu bar as **Help > Online Help**.

Appendix D, “Examples of SNMP Traps,” contains several examples of SNMP traps captured during lab testing. Although not a complete listing of all traps available from Cisco WLAN controllers, this appendix does show actual received traps and decodes much of their content for easier viewing. Complete trap definitions for 4400, 4100, and 2000 series WLAN controllers are defined in MIB files that are available to registered users on the Cisco Connection Online (CCO): http://www.cisco.com.

Configuration Audit Reports and Network Audits

The routine examination of periodic configuration audit reports is a useful tool for the WCS administrator toward ensuring that the integrity of the WCS databases is being verified and maintained. This is especially important in organizations where disparate groups may be responsible for various facets of network operation and maintenance. As is often the case when there are service impacting outages in remote field locations, modifications to WLAN controller configurations may sometimes occur outside the auspices of the network operations center and WCS (in the name of expeditious problem resolution and service restoration).

In these cases, an out-of-sync condition can exist between the configuration stored within the WCS databases and the current configuration of the actual WLAN controller or lightweight access point. Adherence to a policy of routine configuration audit report examination can give advanced warning that such activities have occurred, and more importantly prompt the WCS administrator to the fact that re-synchronization or the re-application of uniform policy templates may be justified.

Configuration audit reports can be run for either a single controller in the management domain (see On-Demand Configuration Audit Reporting, page 8-33), or for all controllers in the management domain via the Network Audit scheduled task (see Scheduled-Task Network Audit Reporting, page 8-34). Although there is typically little concern regarding running the standalone configuration audit report for a single controller, customers with very large wireless networks may wish to consider the traffic impact of the Network Audit task before use during peak periods of network use.

When a configuration audit report is run for a controller, WCS basically retrieves the content of the WLAN controller configuration via SNMP. This is done both for the WLAN controller itself as well as the configuration of any currently registered lightweight access points. The amount of data sent is therefore partially determined by the number of lightweight access points currently registered with the WLAN controller. A small excerpt of the entire SNMP v2c exchange that occurs between a WCS and a 4400-series WLAN controller during a configuration audit can be found in Appendix A, “Excerpt of Configuration Audit Exchange, WCS <-> 4400 WLAN Controller.”.

Figure 8-81 provides us with an analysis of the traffic flow observed between WCS and a 4400-12 WLAN controller during the execution of the single controller configuration audit. The number of registered access points varied from zero to the maximum capacity of the controller. Keep in mind that the amount of information transferred during the network audit did not depend on the number of WLAN clients or asset tags associated to the access points registered to the controller, but was very dependent on the complexity of the controller configuration. The data in Figure 8-81 was based on a very minimally (default) configured 4400-12 WLAN controller. More complex controller configurations increases the amount of data transferred during the configuration audit.

Figure 8-81 Configuration Audit Traffic Analysis

Polling Traffic in Bytes

	2 AP Detecting 2 Rogue AP	Each Additional AP Detecting 2 Rogue AP
SNMPv2c	5,520	2,699
SNMPv3	8,053	3,465

Number of Packets

SNMP	2 AP Detecting 2 Rogue AP	Each Additional AP Detecting 2 Rogue AP
v2 or v3c	36	16

190790

As mentioned previously, the primary use for this information is in gauging the amount of traffic to expect if one is planning on running the all-controller-inclusive network audit scheduled task in very large network configurations. In most such cases, the Network Audit configuration should be scheduled to run during off-peak times of operation or other times when any such audit of all controllers in the management domain would have minimal impact on the users of the network. In those very large networks where there are several WCS servers, each managing different portions of the network over a shared network infrastructure, you may wish to stagger scheduling of Network Audit tasks between the WCS servers such that all WCS servers are not attempting to audit their management domains simultaneously.

Configuration Backup

Lab testing has shown that under version 4.0, a controller configuration archive for a controller with a nearly default configuration is approximately 740,000 bytes in size. When the WLAN controller configuration was archived (either on-demand or via the **Configuration Backup** scheduled task) using SNMPv2c the traffic flows shown in Figure 8-82 were observed over a time period of 13.45 seconds.

Figure 8-82 Single WLC Configuration Archival Traffic Analysis, SNMPv2c

Bytes

	Traffic 0 APs	Each Additional AP	Avg Packet Size
SNMPv2c	81,688	8,942	158
SNMPv3	132,564	11,760	248

Number of Packets

The use of SNMPv3 in (Figure 8-83) was shown to have only minimal impact in this case because the bulk of the traffic was because of TFTP and not SNMP components. Elapsed time for the SNMP traffic flow was 13.29 seconds.

Figure 8-83 Single WLC Configuration Archival Traffic Analysis, SNMPv3

Address A	Address B	Protocol	Packets	Bytes	Packets WLC=>WCS	Bytes A->B WLC=>WCS	Packets WLC<=WCS	Bytes A<-B WLC<=WCS	Avg Pkt Size WLC<=> WCS
WLAN Controller	WCS	TFTP	2602	803180	1301	725120	1301	78060	309
WLAN Controller	WCS	SNMP	46	6155	23	2997	23	3158	134

Designers of very large wireless networks may wish to consider the potential traffic associated with the Configuration Backup scheduled task in their environment because it initiates configuration backups of *all* reachable controllers defined to WCS in a serial fashion.

Note For more information, see section 13.6 CSCsd54800—Config Backup Scheduled Task Fails if One Controller is Unreachable.

Although the peak traffic impact of this task is not high (WLCs are archived one at a time in sequence), it can run for some time depending on the number of the controllers that are reachable. It is good practice to schedule this archival tool for execution during off-peak periods of low usage instead of during peak traffic periods.

Non-Selective Configuration Refresh

Lab testing has shown that the traffic volumes experienced under version 4.0 for the Refresh Config from Controller and the Restore Config to Controller operations are nominal. For SNMPv2c, the traffic flow was observed as 372 packets of 129,000 bytes in a time period of about 1.06 seconds. This traffic was allocated as 186 packets in each direction, with 39,000 bytes from WCS to the WLAN controller and

91,000 bytes returned from the WLAN controller to WCS, with an average UDP packet size of 400 bytes. For SNMPv3, the traffic flow increases to about 372 packets of 160,000 bytes in a time period of about 1.77 seconds. This SNMPv3 traffic was observed to be 186 packets in each direction, 55,000 bytes from WCS to the WLAN controller, and 104,000 bytes returned from the WLAN controller to WCS with an average UDP packet size of 475 bytes.

For Restore Config to Controller, lab testing has indicated that under SNMPv2c, the traffic flow was observed as 1244 packets of 316,000 bytes in a time period of about 6.3 seconds. This traffic was allocated as 622 packets in each direction, with 128,000 bytes from WCS to the WLAN controller and 188,000 bytes returned from the WLAN controller to WCS, with an average UDP packet size of 275 bytes. For SNMPv3, the traffic flow increases to 1244 packets of 427,000 bytes in a time period of about 7 seconds. This SNMPv3 traffic was observed to be 622 bytes in each direction, 184,000 bytes from WCS to the WLAN controller and 243,000 bytes returned from the WLAN controller to WCS, with an average UDP packet size of 362 bytes.

Keep in mind that these traffic volumes are affected by the complexity of the controller configuration, which in turn increases the overall size of the controller configuration. The controller configuration used during this test was relatively simple; controllers with much more complex configurations generate more traffic during these operations.

WLAN Controllers and the Location Appliance

The Wireless Location Appliance learns about WLAN controllers in the management domain from WCS and when synchronized, queries these controllers using SNMP for signal strength and other information necessary to properly determine client, asset tag, and rogue location. Note that in terms of determining device location, the location appliance does not obtain device location information or signal strength data from WCS but independently polls each WLAN controller for the information it needs to perform these calculations. This occurs independently of the on-demand location capabilities present in WCS.

Wi-Fi Location Based Services: Design and Deployment Considerations discusses in detail the communication flows between the location appliance and WLAN controllers. Included in this document are traces and analysis of actual traffic flows between controllers and location appliances in both small and large footprint installations. This document is available at the following URL: http://www.cisco.com.

WCS and the Location Appliance

WCS and the location appliance exchange information regarding calibration maps and network designs during the design synchronization process. During a network design synchronization, we are generally transferring network design information from the more current to the less current partner in order to promote a common understanding of the overall design of the network and the environmental factors included in the most recent calibration maps. Lab analysis of the routine communication flows between WCS and the location appliance indicate that peak traffic flows occur during the synchronization and location server backup/restore processes.

The *Wi-Fi Location Based Services 4.1 Design Guide* (see above) discusses in detail the communication flows between WCS and the location appliance as well as best practice recommendations that should be considered in deciding where the location appliance should be placed within your network.

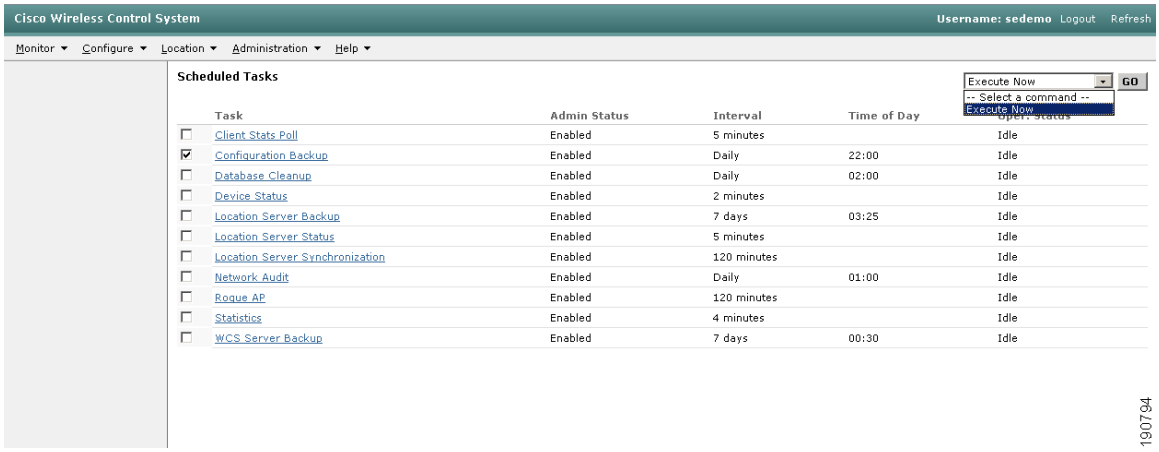
Administering WCS

Administering Scheduled Tasks

WCS provides several pre-defined system tasks that address various areas of configuration and database backup, device status, and synchronization and statistics collection. The currently available scheduled tasks can be accessed via **Administration > Scheduled Task,** as shown in Figure 8-84. These tasks can be scheduled to run at pre-determined times of the day and with varying repetition intervals. When configured, each task can be administratively enabled or disabled. Any task can be submitted for immediate execution (including tasks that have been administratively disabled) by selecting the task check box and then selecting **Execute Now** from the command drop-down menu in the upper right-hand corner of the screen. This immediate execution capability allows the scheduled tasks feature to flexibly serve in dual roles:

- As a time-driven job scheduler, allowing you to accomplish basic system housekeeping chores
- As a method of performing on-demand functions that otherwise would not be accessible to you from within WCS (examples of this are the Database Cleanup and WCS Server Backup tasks).

Figure 8-84 Administration > Scheduled Tasks



The online help system accessible via under the WCS menu bar as **Help > Online Help** contains guidance on how each of the scheduled tasks should be configured for proper operation. The following subsections provide further detail on the Configuration Backup, Network Audit, and WCS Server Backup scheduled tasks.

Configuration Backup

The Configuration Backup scheduled task archives the configurations of all controllers that have been added to WCS and are reachable at the time the task is submitted for execution.

Note For more information, see section 13.6 CSCsd54800—Config Backup Scheduled Task Fails if One Controller is Unreachable.

For each controller that is defined and currently reachable, WCS creates a configuration archive file in the default directory of the TFTP server selected with a filename that is in the format of *nnn_nnn_nnn_nnn_YYMMDD_hhmm.cfg* where *nnn* represents each octet of the IP address of the controller.

For example, a display of the tftp directory on a Linux-based WCS server shows the following files after a successful execution of this task:

```
[root@wcslinux wcs_tftp]# ls
10_1_56_10_060301_2238.cfg  10_1_56_14_060301_2237.cfg  10_1_56_18_060301_2237.cfg
10_1_56_16_060301_2238.cfg  10_1_56_12_060301_2238.cfg
[root@wcslinux wcs_tftp]#
```

To configure this task, perform the following:

Step 1 You must decide whether you desire to save and archive the current running configuration or simply archive the current saved configuration of each controller. Configuration parameters that have not been saved to the nonvolatile memory of each controller are *not* be included in the configuration archives that are produced.

a. For each controller for which you want to save and archive the current *running* configuration, go to **Configure > Controllers > Controller Properties** and ensure that the Save Before Backup check box is enabled. Click on **Save**.

   Note that this option saves the current running configuration of the controller to nonvolatile memory before archiving it. The saved configuration that was present in nonvolatile memory is overwritten. See Configuring WLAN Controllers, page 8-13, for further information on the Save Before Backup check box parameter.

b. For each controller for which you want to archive the current *saved* configuration, go to **Configure > Controllers > Controller Properties** and ensure that the Save Before Backup check box is *not* enabled. Click on **Save**.

Step 2 Go to **Administration > Scheduled Tasks** and click on the **Configuration Backup** hyperlink shown in Figure 8-84, which results in the display of the Modify Task page.

Step 3 Select the time at which you want the configuration backup task to be submitted for execution as well as the daily repetition interval.

Step 4 Choose a destination TFTP server from those provided in the drop-down list. Note that you cannot define a new TFTP server during the configuration of this task. If you want to define another server to be added to the list, use **Configure > Templates > TFTP Servers** and select Add TFTP Server from the drop-down menu in the upper right corner of the screen. When you have added a new TFTP server in this manner, return to the Configuration Backup scheduled task panel and your newly-defined server should now be available to you.

Step 5 Enable the task by clicking on the **Admin Status Enabled** check box.

The task is now enabled for automatic submission at the time and with the daily repetition interval you have selected. If you want to schedule the task for immediate submission, select the task by enabling the check box as shown in Figure 8-84, then select **Execute Now** from the command drop-down menu in the upper right-hand screen corner and click **Go**.

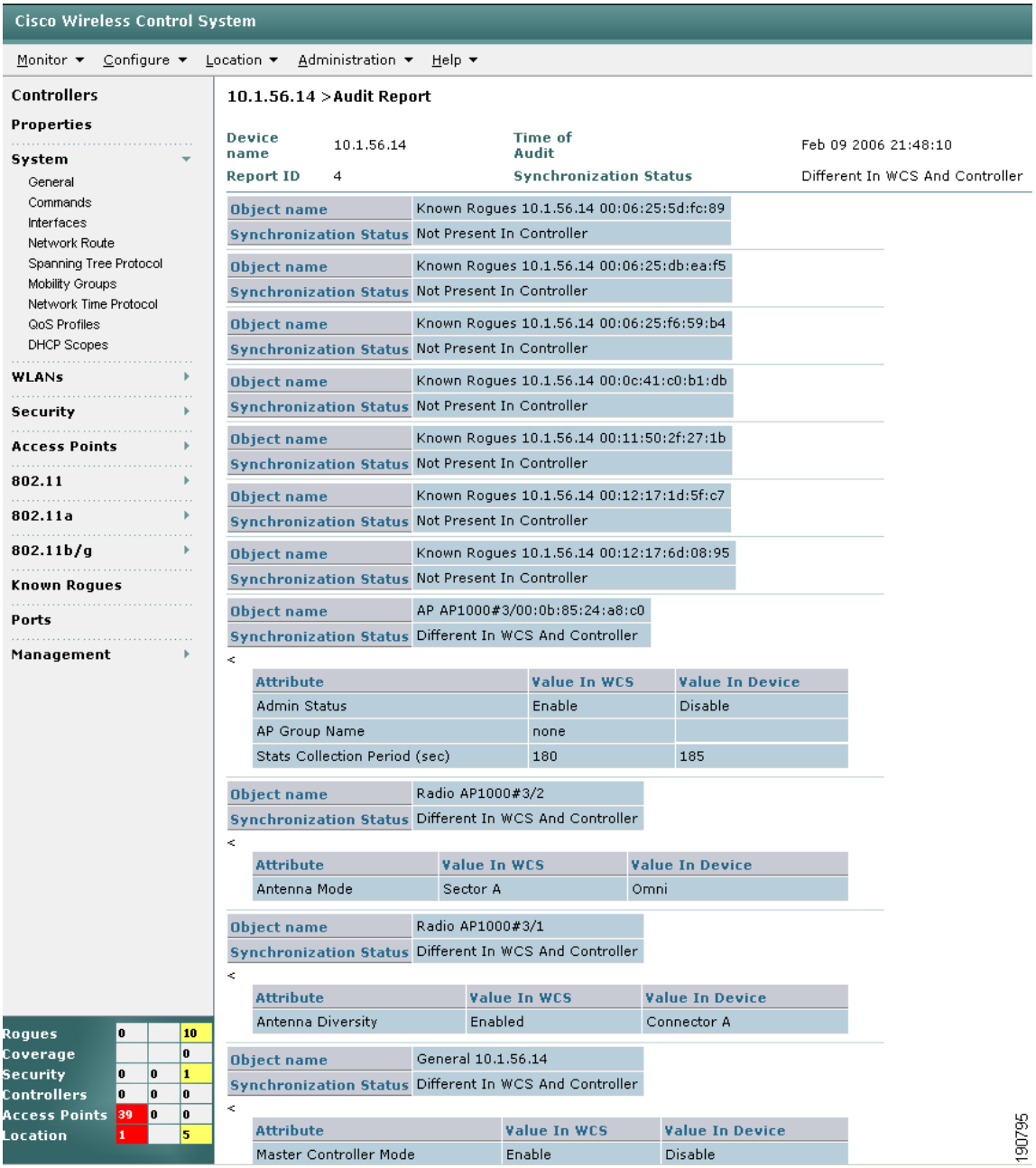
Network Audit

To initiate a network audit report scheduled task, perform the following steps:

Step 1 Click **Administration > Scheduled Tasks** to display the listing of available scheduled tasks.

Step 2 Click on the hyperlink for the Network Audit scheduled task entry. This brings up the **Task > Network** Audit page. At the top of this screen the status of the last network audit is indicated. Set the time of day that you want the network audit to run and set the interval at which you want the network audit to repeat (that is, 1=daily). Finally, enable the check box to enable the network audit as shown in Figure 8-85.

Figure 8-85 Network Audit Configuration



Step 3 Click **Submit**. The **Administration > Scheduled Tasks** screen should re-appear and the network audit task admin status should indicate "enabled" with the scheduled start time and repetition interval that was specified.

To view the results of a network audit that has completed running, perform the following:

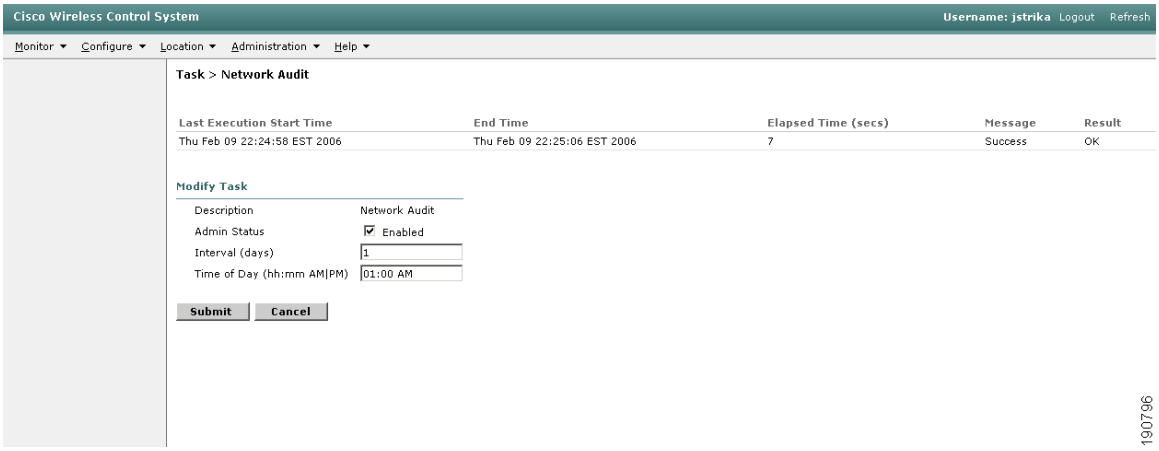
Step 1 Click on **Configure > Controllers** and enable the check box of the controller for which you want to see the configuration audit report.

Step 2 Choose **View Audit Reports** from the command drop-down menu in the upper right-hand corner and click **GO**. WCS displays all available configuration audit reports for the selected WLAN controller.

Step 3 Click on the **Report ID** hyperlink of the Configuration audit report you want to view.

WCS then displays the same format configuration audit report for the WLAN controller and its registered lightweight access points as is shown in Figure 8-86.

Figure 8-86 Configuration Audit Report



Step 4 Network Audit scheduled tasks can also submitted for immediate execution. To do this, click on **Administration > Scheduled Tasks** and then enable the check box beside the Network Audit hyperlink.

Step 5 Choose **Execute Now** from the command drop-down menu in the upper right-hand corner, and click **Go**.

WCS submits the Network Audit task for immediate execution (the status of the network audit changes to “Executing”). You may view the results of this network audit as has been previously described.

WCS Backup

The WCS Backup scheduled task provides a convenient mechanism to ensure that the WCS databases are archived on a regular basis. Unlike the “Backup” script that is executed from the operating system outside the WCS user interface, the WCS Backup scheduled task does not offer a choice of destination system or folder. Rather, the database archive is always placed on the WCS server itself in a “WCSBackup” subdirectory below the directory chosen by you at WCS installation time for the storage of FTP files. Each database archive file is named as per the following format:

DD-mon-YY_hh-mm-ss.nmsbackup.

Thus, for a WCS-Linux installation, if */opt/WCS32/wcs_ftp* was chosen as the FTP directory, the archive files created by the WCS Backup scheduled task is found in */opt/WCS32/wcs_ftp/WCSBackup*. The database archive files that can be found under that directory appears as follows:

```
[root@wcslinux WCSBackup]# ls
02-Mar-06_22-13-11.nmsbackup  02-Mar-06_22-13-47.nmsbackup  02-Mar-06_22-15-06.nmsbackup
02-Mar-06_22-13-21.nmsbackup  02-Mar-06_22-13-55.nmsbackup
02-Mar-06_22-13-30.nmsbackup  02-Mar-06_22-14-05.nmsbackup
[root@wcslinux WCSBackup]#
```

To configure the WCS Backup scheduled task, perform the following steps:

Step 1 Go to **Administration > Scheduled Tasks** and click on the **WCS Backup** hyperlink shown in the screen shown in Figure 8-84. This results in the display of the Modify Task screen.

Step 2 Specify the time at which you desire the task to be submitted for execution as well as the daily repetition interval.

Step 3 Choose the total number of database archives you want WCS to maintain on an ongoing basis (this must be at least seven and cannot exceed fifty).

Step 4 Enable the task by clicking on the **Admin Status Enabled** check box.

The task is now enabled for automatic submission at the time and with the daily repetition interval you have selected.

Step 5 If you want to schedule the task for immediate submission, select the task by enabling the check box for the task on the **Administration > Scheduled Tasks** screen, then select **Execute Now** from the command drop-down menu in the upper right-hand screen corner and click on **GO**.

Note Keep in mind that performing a WCS database backup can be relatively resource-intensive. Therefore, Cisco does not recommend that database backups be performed during peak periods of WCS usage. Schedule WCS database backups for non-busy periods when there is little use of WCS or the WCS databases.

Managing WCS Users

Adding User Accounts

WCS is installed by default with a single user *root* with a password of *public* that is a member of group *SuperUsers*. The password for *root* should be changed to a secure password as soon as possible after installation to prevent unauthorized access.

To add user accounts to WCS, use the following procedure:

Step 1 Log into WCS using the *root* account (or another account with *superuser* privileges).

Step 2 Click **Administration > Accounts** to display the All Users page.

Step 3 From the command drop-down menu in the upper right-hand corner of the page, choose **Add User** and click **GO** to display the User Administration page.

Step 4 Enter the username and password for the new WCS user account. You need to re-enter the password to confirm it.

Step 5 Under **Groups Assigned to this User**, check the appropriate box to assign the new user account to one of the six user groups supported by WCS. Keep in mind that the privileges assigned to each group can be modified further from the defaults by using the **Accounts > Groups** option described in Modifying Group Privileges, page 8-123.

a. User Assistant—Allows users only enough authority to apply an existing template to create local network user accounts for the selected controller. Local network user accounts are used to allow local controller-based authentication of clients using web authentication.

b. Lobby Ambassador—Allows an assigned user only the ability to create, apply, and delete guest user accounts that are assigned a limited lifetime of between 5 minutes and 30 days. These guest user accounts use web authentication to authenticate to the controller. For further information on the guest access capabilities of the Cisco UWN, see the "Cisco Centralized WLAN Architecture Guest Access Services" chapter in this SRND.

c. System Monitoring—Allows users to monitor WCS operations. Most general users of WCS can be assigned system monitoring capabilities. In its default configuration, it allows only general "read-only" viewing of WCS operations without the ability to affect the configuration of WCS or network components.

d. ConfigManagers—Allows users to monitor and configure WCS and network component operations. This should be assigned to users that only require the ability to change the configuration of WCS or network components managed by WCS.

e. Admin—Allows users to monitor and configure WCS operations and also perform all system administration tasks with the exception of administering WCS user accounts and passwords.

f. SuperUsers—Allows users to monitor and configure WCS operations and perform all system administration tasks including administering WCS user accounts and passwords. A SuperUser has *all* rights and privileges on the WCS system. This right should be assigned *very* judiciously.

Step 6 Click **Submit**. The name of the new user account appears on the All Users page and can be used immediately.

Modifying Group Privileges

The default privileges that are assigned to each of the groups described in the previous section are shown in Figure 8-87.

Figure 8-87 Comparison of Default WCS User Group Privileges

In some cases, it may be necessary to modify the specific privileges associated with a specific group (the procedure for accomplishing this is shown below). Keep in mind that any changes made to the group affecting the user in question *affect all users assigned to that group*.

Step 1 Click **Administration > Accounts** to display the All Users page.

Step 2 In the sidebar, click **Groups** to display the All Groups page.

Step 3 Click the name of the user group that you wish to modify. A listing of the permissions currently assigned and those available to assign for the group is displayed.

Step 4 Make any desired changes by checking or unchecking the appropriate check boxes.

Step 5 Click **Submit** to save your changes or **Cancel** to leave the settings unchanged.

Note that although users can be restricted from performing classes of activities from all lightweight access points or WLAN controllers in the WCS management domain, these privileges are not specified on a per-access point or per-controller basis.

Viewing User and Group Audit Trails

WCS allows users that are members of the *SuperUser* group to view the past WCS access audit trail of any user or group defined to WCS and also clear that audit trail if desired. User and group audit trail information is maintained indefinitely by WCS and contains the time, date, and status of authentication attempts made by each user against WCS.

To view the audit trail for a WCS user, perform the following steps:

Step 1 Log into the WCS user interface as a user assigned to the SuperUsers group.

Step 2 Click **Administration > Accounts > Users** to display the All Users page.

Step 3 Locate the user for which you want to display the audit trail information.

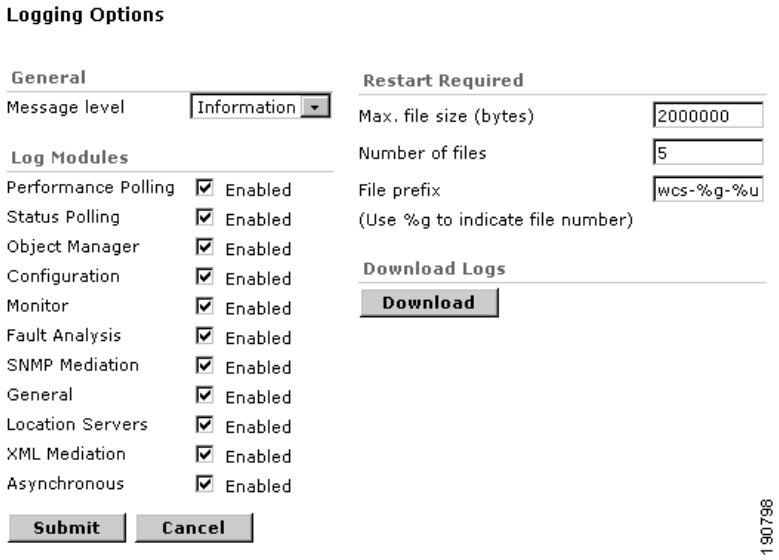
Step 4 Click on the  icon under the extreme right-hand column entitled “Audit Trail”. The audit trail log is displayed.

To view the audit trail for a WCS user group, use the same basic procedure but substitute **Administration > Accounts > Groups** in Step 2.

Logging Options

WCS provides extensive command logging options that are accessed and controlled via the **Administration > Logging** option from the WCS main menu bar. Logging message levels can be configured for Error, Informational, and Trace (in order of increasing detail). The default logging configuration is shown in Figure 8-88 and includes all possible logging modules enabled.

Figure 8-88 Default Logging Configuration



The standard configuration is for WCS to create up to five rotating log files with a maximum size of 2 MB each. The names are specified using the file prefixes listed (for example, wcs-0-0.log through wcs-4-0.log.) Note that a restart is required if log file size, name, or number is changed.

To view WCS log files, use the **Download** selection shown in Figure 8-88 to download the entire set of logs as a .zip compressed archive to your desktop or elsewhere for viewing with one of many popular ASCII text viewing programs, such as Microsoft Notepad, Wordpad, and so on.

There are very many log files contained in the compressed archive. However, the wcs*.log files are the first places to look when inquiring into the reason behind the abnormal termination of scheduled tasks, audit reports, configuration file archivals, and other tasks. This is also the first place to look for information about why other screen functions or commands issued from within WCS may have terminated abnormally or produced unexpected results.

When experiencing difficulties with WCS that you cannot resolve, you will likely be asked to download the compressed zip archive from the screen shown in Figure 8-88 for use by the Cisco Technical Assistance Center in resolving your problem.

Reference Publications

This chapter makes reference to the following Cisco publications:

- Cisco Wireless Control System (WCS) Installation and Upgrade Guides—http://www.cisco.com/en/US/products/ps6305/tsd_products_support_series_home.html
- Cisco Wireless Control System Release Notes, Release 4.0—http://www.cisco.com/en/US/docs/wireless/wcs/release/notes/wcsrn_MR2.html
- Cisco Wireless Control System Configuration Guide, Release 4.0—http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscfg40.html
- Cisco Wireless LAN Controller Configuration Guide, Release 4.0—http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfig40.html

- Cisco Aironet 1240AG Series Lightweight Access Point Hardware Installation Guide—
http://www.cisco.com/en/US/docs/wireless/access_point/1240/installation/guide/1240hig5.html
- Release Notes for Cisco Wireless Location Appliance—
http://www.cisco.com/en/US/docs/wireless/location/2700/release/notes/larn4032.html
- Cisco Wireless Location Appliance—Installation Guide—
http://www.cisco.com/en/US/docs/wireless/location/2700/quick/guide/li31main.html
- Cisco Wireless Location Appliance—Deployment Guide—
http://www.cisco.com/en/US/docs/wireless/technology/location/deployment/guide/depgd.html
- Wi-Fi Location-Based Services 4.1 Design Guide—
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html