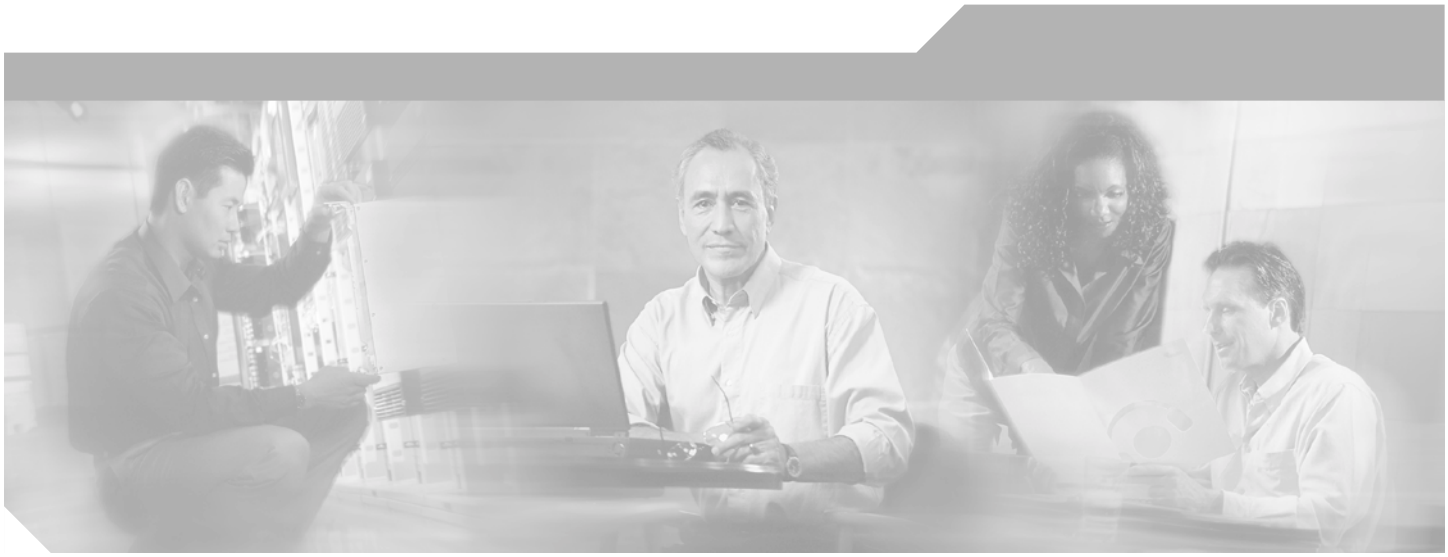


Cisco Wireless Control System Configuration Guide

Software Release 3.2
November 2005

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-8296-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Cisco Wireless Control System Configuration Guide
© 2005 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

The preface provides an overview of the *Cisco Wireless Control System Configuration Guide*, references related publications, and explains how to obtain other documentation and technical assistance, if necessary. It contains these sections:

Audience

This guide describes the Cisco Wireless Control System (WCS). It is meant for networking professionals who use WCS to manage a Cisco Wireless LAN Solution network. To use this guide, you should be familiar with the concepts and terminology associated with wireless LANs.

Purpose

This guide provides the information you need to manage a Cisco Wireless LAN Solution network using WCS.

Note This document pertains specifically to WCS 3.2. Earlier versions of WCS software may look and operate somewhat differently.

Organization

This guide contains the following chapters:

Chapter 1, "Overview," describes the Cisco Wireless LAN Solution and the Cisco Wireless Control System (WCS).

Chapter 2, "Getting Started," describes how to prepare WCS for operation.

Chapter 3, "Configuring Security Solutions," describes security solutions for wireless LANs.

Chapter 4, "Performing System Tasks," describes how to use WCS to add a controller and location appliance to the WCS database, update system software, enable long preambles for SpectraLink NetLink phones, and create an RF calibration model.

Chapter 5, "Adding and Using Maps," describes how to add maps to the Cisco WCS database and use them to monitor your wireless LAN.

Chapter 6, "Monitoring Wireless LANs," describes how to use WCS to monitor your wireless LANs.

Chapter 7, "Managing WCS User Accounts," describes how to add, delete, and change the passwords of WCS user accounts.

Chapter 8, "Maintaining WCS," describes how to check the status of, stop, uninstall, and upgrade WCS. It also provides instructions for backing up and restoring the WCS database.

Appendix A, "End User License and Warranty," provides the end user license and warranty that apply to WCS.

Appendix B, "Supported Country Codes," provides the list of countries in which the Cisco Wireless LAN Solution is supported for use.

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands and keywords are in **boldface** text.
- Variables are in *italicized* text.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Publications

For more information about WCS and related products, refer to the following documents:

- *Quick Start Guide: Cisco Wireless Control System for Microsoft Windows*
- *Quick Start Guide: Cisco Wireless Control System for Linux*
- *Wireless Control System Online Help*
- *Release Notes for Cisco Wireless Control System 3.2 for Microsoft Windows*
- *Release Notes for Cisco Wireless Control System 3.2 for Linux*
- *Cisco Location Application Configuration Guide*
- *Release Notes for Cisco Location Appliance Software 2.0*

Note Click this link to browse to these documents:
http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Overview

This chapter describes the Cisco Wireless LAN Solution and the Cisco Wireless Control System (WCS). It contains these sections:

Overview of the Cisco Wireless LAN Solution

The Cisco Wireless LAN Solution is designed to provide 802.11 wireless networking solutions for enterprises and service providers. It simplifies the deployment and management of large-scale wireless LANs and enables a unique best-in-class security infrastructure. The operating system manages all data client, communications, and system administration functions, performs radio resource management (RRM) functions, manages system-wide mobility policies using the operating system security solution, and coordinates all security functions using the operating system security framework.

The Cisco Wireless LAN Solution consists of Cisco Wireless LAN Controllers (hereafter called *controllers*) and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the operating system user interfaces:

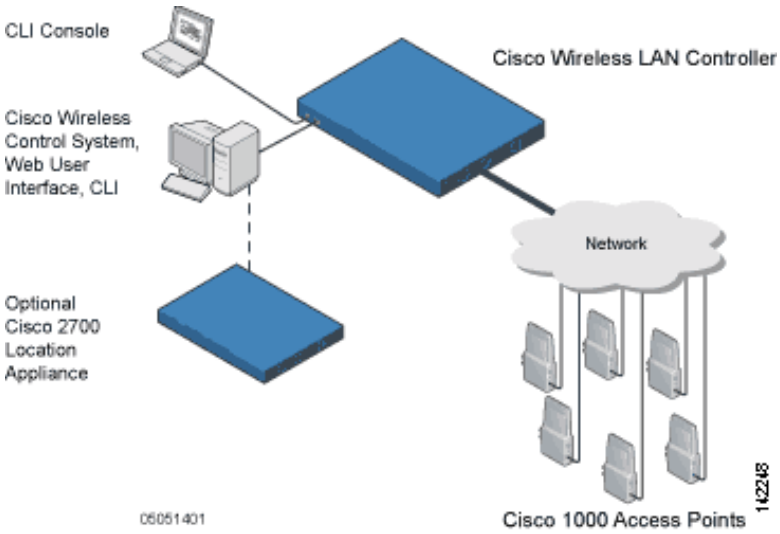
- An HTTPS full-featured web user interface hosted by Cisco controllers can be used to configure and monitor individual controllers.
- A full-featured command line interface (CLI) can be used to configure and monitor individual controllers.
- The Cisco Wireless Control System (WCS) can be used to configure and monitor one or more controllers and associated access points. WCS has tools to facilitate large-system monitoring and control. It runs on Windows 2000, Windows 2003, and Red Hat Enterprise Linux ES 3 servers.
- An industry-standard SNMP V1, V2c, and V3 interface can be used with any SNMP-compliant third-party network management system.

The Cisco Wireless LAN Solution supports client data services, client monitoring and control, and all rogue access point detection, monitoring, and containment functions. It uses lightweight access points, controllers, and the optional WCS to provide wireless services to enterprises and service providers.

Note This document refers to controllers throughout. Unless specified otherwise, the descriptions herein apply to all Cisco Wireless LAN Controllers, including but not limited to Cisco 2000 Series Wireless LAN Controllers, Cisco 4100 Series Wireless LAN Controllers, Cisco 4400 Series Wireless LAN Controllers, and controllers within the Cisco Wireless Services Module (WiSM) and Cisco 26/28/37/38*xx* Series Integrated Services Routers.

Figure 1-1 shows the Cisco Wireless LAN Solution components, which can be simultaneously deployed across multiple floors and buildings.

Figure 1-1 Cisco Wireless LAN Solution Components



Overview of WCS

The Cisco Wireless Control System (WCS) is a Cisco Wireless LAN Solution network management tool that adds to the capabilities of the web user interface and command line interface (CLI), moving from individual controllers to a network of controllers. WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.

WCS runs on Windows 2000, Windows 2003, and Red Hat Enterprise Linux ES 3 servers. On both Windows and Linux, WCS can run as a normal application or as a service, which runs continuously and resumes running after a reboot.

The WCS user interface enables operators to control all permitted Cisco Wireless LAN Solution configuration, monitoring, and control functions through Internet Explorer 6.0 or later. Operator permissions are defined by the administrator using the WCS user interface Administration menu, which enables the administrator to manage user accounts and schedule periodic maintenance tasks.

WCS simplifies controller configuration and monitoring while reducing data entry errors with the Cisco Wireless LAN Controller autodiscovery algorithm. WCS uses the industry-standard SNMP protocol to communicate with the controllers.

WCS Versions

WCS is offered in two versions: WCS Base and WCS Location.

WCS Base

The WCS Base supports wireless client data access, rogue access point detection and containment functions (such as real-time location of rogue access points to the nearest Cisco access point and real-time and historical location of clients to the nearest Cisco access point), and Cisco Wireless LAN Solution monitoring and control. It also includes graphical views of the following:

- Autodiscovery of access points as they associate with controllers
- Autodiscovery and containment or notification of rogue access points
- Map-based organization of access point coverage areas, which is helpful when the enterprise spans more than one geographical area
- User-supplied campus, building, and floor plan graphics, which show the following:
  - Locations and status of managed access points
  - Locations of rogue access points based on the signal strength received by the nearest managed Cisco access points
  - Coverage hole alarm information for access points based on the received signal strength from clients. This information appears in a tabular rather than map format.
  - RF coverage maps

The WCS Base also provides system-wide control of the following:

  - Streamlined network, controller, and managed access point configuration using customer-defined templates
  - Network, controller, and managed access point status and alarm monitoring
  - Automated and manual data client monitoring and control functions
  - Automated monitoring of rogue access points, coverage holes, security violations, controllers, and access points
  - Full event logs for data clients, rogue access points, coverage holes, security violations, controllers, and access points
  - Automatic channel and power level assignment by radio resource management (RRM)
  - User-defined automatic controller status audits, missed trap polling, configuration backups, and policy cleanups

WCS Location

The WCS Location includes all the features of the WCS Base as well as these enhancements:

- On-demand location of rogue access points to within 33 feet (10 meters)
- On-demand location of clients to within 33 feet (10 meters)
- Ability to use location appliances to collect and return historical location data viewable in the WCS Location user interface

Relationship with Cisco Location Appliances

When WCS Location is used, end users can also deploy Cisco 2700 Series Location Appliances. The location appliance enhances the high-accuracy built-in WCS Location capabilities by computing, collecting, and storing historical location data, which can be displayed in WCS. In this role, the location appliance acts as a server to a WCS server by collecting, storing, and passing on data from its associated controllers.

After a quick command line interface (CLI) configuration, the remaining location appliance configuration can be completed using the WCS user interface. After each location appliance is configured, it communicates directly with its associated controllers to collect operator-defined location data. The associated WCS server operators can then communicate with each location appliance to transfer and display selected data.

The location appliance can be backed up to any WCS server into an operator-defined FTP folder, and the location appliance can be restored from that server at any time and at defined intervals. Also, the location appliance database can be synchronized with the WCS server database at any time. Operators can use the location appliance features and download new application code to all associated location appliances from any WCS server.

When WCS is enhanced with a location appliance, it can display historical location data for up to 1,500 laptop clients, palmtop clients, VoIP telephone clients, radio frequency identifier (RFID) asset tags, rogue access points, and rogue clients for each location appliance in the Cisco Wireless LAN Solution. Operators can configure location appliances to collect this data and statistics at defined intervals.

You can also use WCS to configure location appliance event notification parameters. *Event notification* is a feature that enables you to define conditions that cause the location appliance to send notifications to the listeners that you have specified in WCS.

In this way, WCS acts as a notification listener. It receives notifications from the location appliance in the form of the locationNotifyTrap trap as part of the bsnwras.my MIB file. WCS translates the traps into user interface alerts and displays the alerts in the following format:

```
Absence:
- Absence of Tag with MAC 00:0c:cc:5b:e4:1b, last seen at 16:19:45 13 Oct 2005.

Containment:
- Tag with MAC 00:0c:cc:5b:fa:44 is In the Area 'WNBU > WNBU > 4th Floor > wcsDevArea'

Distance:
- Tag with MAC 00:0c:cc:5b:fa:47 has moved beyond the distance configured for the marker
'marker2'.
- Tag with MAC 00:0c:cc:5b:f9:b9 has moved beyond 46.0 ft. of marker 'marker2', located at
a range of 136.74526528595058 ft.
```

Note Refer to the *Location Application Configuration Guide* for more detailed information about the location appliance and its use with WCS.

Comparison of WCS Base and WCS Location

Table 1-1 compares the WCS Base and WCS Location features.

Table 1-1 WCS Base and WCS Location Features

Features	WCS Base	WCS Location
Location and tracking		
Low-resolution client location	Yes	—
High-resolution client location	—	Yes
Integration with location appliance	—	Yes
Low-resolution rogue access point location	Yes	—
High-resolution rogue access point location	—	Yes
Client data services, security, and monitoring		
Client access via access points	Yes	Yes
Multiple wireless LANs (individual SSIDs and policies)	Yes	Yes
Rogue access point detection and containment using access points	Yes	Yes
802.11a/b/g bands	Yes	Yes
Radio resource management		
Real-time channel assignment and rogue access point detection and containment	Yes	Yes
Real-time interference detection and avoidance, transmit power control, channel assignment, client mobility management, client load distribution, and coverage hole detection	Yes	Yes
Automated software and configuration updates	Yes	Yes
Wireless intrusion protection	Yes	Yes
Global and individual AP security policies	Yes	Yes
Controls Cisco Wireless LAN Controllers	Yes	Yes
Supported workstations		
Windows 2000 or Windows 2003	Yes	Yes
Red Hat Enterprise Linux ES 3 server	Yes	Yes

WCS User Interface

The WCS user interface enables the network operator to create and configure Cisco Wireless LAN Solution coverage area layouts, configure system operating parameters, monitor real-time Cisco Wireless LAN Solution operation, and perform troubleshooting tasks using an HTTPS web browser window. The WCS user interface also enables the WCS administrator to create, modify, and delete user accounts; change passwords; assign permissions; and schedule periodic maintenance tasks. The administrator creates new usernames and passwords and assigns them to predefined permissions groups.

Note Cisco recommends Internet Explorer 6.0 or later on a Windows workstation for full access to WCS functionality.

WCS Features

WCS includes these features: a controller autodiscovery function, alarm email notification, and RF calibration tool.

Controller Autodiscovery

Autodiscovery enables operators to search for a single controller by IP address and facilitates a multiple-controller search across a range of IP addresses. The autodiscovery function finds the controller on the network within the specified IP address range and automatically enters the discovered controller's information into the WCS database.

Note Controller autodiscovery is limited to the Cisco Wireless LAN Solution mobility group subnets that are defined by the operator.

As access points associate with a controller, the controller immediately transmits the access point information to WCS, which automatically adds the access point to the WCS database. After the access point information is in the database, operators can add the access point to the appropriate spot on a WCS user interface map.

Note Because of the large number of addresses in a Class A or Class B range, Cisco recommends that you do not attempt autodiscovery across Class A or Class B ranges.

Alarm Email Notification

WCS includes a built-in email notification function that can notify network operators when critical alarms occur. Refer to the WCS Monitor > All Alarms > Email Notification page to view the current alarm notification settings.

RF Calibration Tool

WCS uses prediction to generate the RF characteristics of the environment in which a Cisco Wireless LAN Solution is being deployed. If the user wants to fine-tune the RF characteristics to match the actual attentuation characteristics of that environment, WCS includes a calibration tool that enables operators to measure the actual signal strength and attenuation in RF coverage areas being surveyed. The tool can be used to create a calibration model customized to the actual environment and stored in the WCS database. This calibration model allows the user to fine-tune location measurements for more precise client and rogue access point location. To save effort, the calibration model can also be reused for areas with an identical access point layout and an identical wall layout.

The calibration tool is used much like a site survey tool. It enables a technician to take a WCS-equipped laptop to multiple locations on a floor or outdoor area and measure actual signal strength at selected locations on the floor or outdoor area map. The technician then uses the calibration tool in WCS to process the collected data points for the floor or outdoor area. Refer to the WCS Monitor > Maps > RF Calibration Models page to view the current calibration models.

Getting Started

This chapter describes how to prepare WCS for operation. It contains these sections:

Installing WCS

Refer to one of these documents for instructions on installing WCS on a server:

- *Quick Start Guide: Cisco Wireless Control System for Microsoft Windows*
- *Quick Start Guide: Cisco Wireless Control System for Linux*

Note Click this link to browse to these documents:
http://www.cisco.com/en/US/products/ps6305/prod_installation_guides_list.html

Starting WCS

This section provides instructions for starting WCS on either a Windows or Linux server.

Note You can check the status of WCS at any time. To do so, follow the instructions in the "Checking the Status of WCS" section on page 8-2.

Starting WCS on Windows

Follow these steps to start WCS when it is installed as a Windows application or Windows service.

Note When WCS is installed as a Windows service, WCS runs automatically upon system bootup.

Step 1 Log into the system as administrator.

Step 2 Perform one of the following:

- From the Windows Start menu, click **Programs** > **Wireless Control System** > **StartWCS**.
- From the command prompt, navigate to the WCS installation directory (C:\Program Files\WCS32\bin) and enter **WCSAdmin start**.

The WCSAdmin window appears and displays messages indicating that WCS is starting.

Note If WCS is installed as a service, messages also appear to indicate that the Nms_Server service is starting.

Step 3 Close the WCSAdmin window when the Close button becomes active.

Step 4 WCS is now ready to host WCS user interfaces (clients). Go to the "Logging into the WCS User Interface" section on page 2-3 to use a web browser to connect to the WCS user interface.

Starting WCS on Linux

Follow these steps to start WCS when it is installed as a Linux application or Linux service.

Note When WCS is installed as a Linux service, WCS runs automatically upon system bootup.

Step 1 Log into the system as root.

Step 2 Using the Linux command line interface (CLI), perform one of the following:

- Navigate to the /opt/WCS32 directory (or the directory chosen during installation) and enter **./StartWCS**.
- Navigate to the opt/WCS32/bin directory and enter **WCSAdmin start**.

The CLI displays messages indicating that WCS is starting.

Step 3 WCS is now ready to host WCS user interfaces (clients). Go to the "Logging into the WCS User Interface" section below to use a web browser to connect to the WCS user interface.

Logging into the WCS User Interface

Follow these steps to log into the WCS user interface through a web browser.

Step 1 Launch Internet Explorer 6.0 or later on a different computer than the one on which you installed and started WCS.

Note Some WCS features may not function properly if you use a web browser other than Internet Explorer 6.0 on a Windows workstation.

Step 2 In the browser's address line, enter **https://*wcs-ip-address***, where *wcs-ip-address* is the IP address of the computer on which you installed and started WCS.

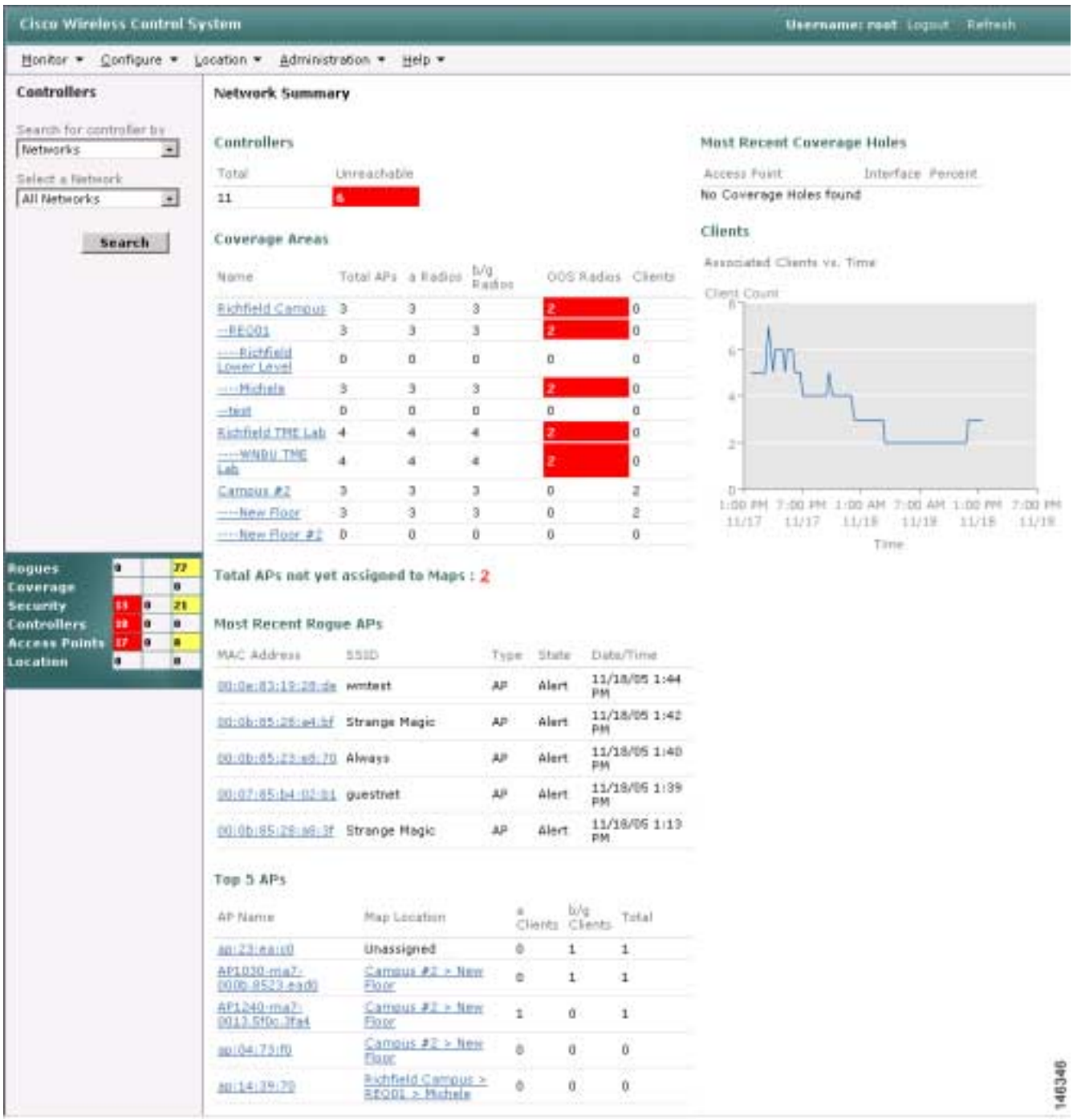
Step 3 When the WCS user interface displays the Login window, enter your username and password. The default username is **root**, and the default password is **public**.

Note All entries are case sensitive.

Step 4 Click **Submit** to log into WCS. The WCS user interface is now active and available for use. The Network Summary page appears. This page provides a summary of the Cisco Wireless LAN Solution, including coverage areas, the most recently detected rogue access points, access point operational data, reported coverage holes, and client distribution over time. Figure 2-1 shows a typical Network Summary page.

Note When you use WCS for the first time, the Network Summary page shows that the Controllers, Coverage Areas, Most Recent Rogue APs, Top 5 APs, and Most Recent Coverage Holes databases are empty. It also shows that no client devices are connected to the system. After you configure the WCS database with one or more controllers, the Network Summary page provides updated information.

Figure 2-1 Network Summary Page



Step 5 Refer to the *Wireless Control System Online Help* for a description of the Network Summary page's menus, fields, and buttons.

Note To exit the WCS user interface, close the browser window or click **Logout** in the upper right corner of the page. Exiting a WCS user interface session does not shut down WCS on the server.

Note When a system administrator stops the WCS server during your WCS session, your session ends, and the web browser displays this message: "The page cannot be displayed." Your session does not reassociate to WCS when the server restarts. You must restart the WCS session.

Configuring Security Solutions

This chapter describes security solutions for wireless LANs. It contains these sections:

Cisco Wireless LAN Solution Security

The Cisco Wireless LAN Solution security solution bundles potentially complicated Layer 1, Layer 2, and Layer 3 802.11 access point security components into a simple policy manager that customizes system-wide security policies on a per wireless LAN basis. It provides simple, unified, and systematic security management tools.

One of the biggest hurdles to wireless LAN deployment in the enterprise is wired equivalent privacy (WEP) encryption, which is a weak standalone encryption method. A more recent problem is the availability of low-cost access points that can be connected to the enterprise network and used to mount man-in-the-middle and denial-of-service attacks. Also, the complexity of add-on security solutions has prevented many IT managers from embracing the benefits of the latest advances in wireless LAN security.

Layer 1 Solutions

The Cisco Wireless LAN Solution operating system security solution ensures that all clients gain access within an operator-set number of attempts. Should a client fail to gain access within that limit, it is automatically excluded (blocked from access) until the operator-set timer expires. The operating system can also disable SSID broadcasts on a per wireless LAN basis.

Layer 2 Solutions

If a higher level of security and encryption is required, the network administrator can also implement industry-standard security solutions such as 802.1X dynamic keys with Extensible Authentication Protocol (EAP) or Wi-Fi Protected Access (WPA) dynamic keys. The Cisco Wireless LAN Solution WPA implementation includes Advanced Encryption Standard (AES), Temporal Key Integrity Protocol + message integrity code checksum (TKIP + Michael MIC) dynamic keys, or static WEP keys. Disabling is also used to automatically block Layer 2 access after an operator-set number of failed authentication attempts.

Regardless of the wireless security solution selected, all Layer 2 wired communications between controllers and access points are secured by passing data through Lightweight Access Point Protocol (LWAPP) tunnels.

Layer 3 Solutions

The WEP problem can be further solved using industry-standard Layer 3 security solutions such as virtual private networks (VPNs), Layer 2 Tunneling Protocol (L2TP), and IP security (IPSec) protocols. The Cisco Wireless LAN Solution L2TP implementation includes IPSec, and the IPSec implementation includes Internet Key Exchange (IKE), Diffie-Hellman (DH) groups, and three optional levels of encryption: ANSI X.3.92 Data Encryption Standard (DES), ANSI X9.52-1998 Data Encryption Standard (3DES), or Advanced Encryption Standard/Cipher Block Chaining (AES/CBC). Disabling is also used to automatically block Layer 3 access after an operator-set number of failed authentication attempts.

The Cisco WLAN Solution IPSec implementation also includes industry-standard authentication using Message Digest Algorithm (MD5) or Secure Hash Algorithm-1 (SHA-1).

The Cisco Wireless LAN Solution supports local and RADIUS media access control (MAC) filtering. This filtering is best suited to smaller client groups with a known list of 802.11 access card MAC addresses. The Cisco Wireless LAN Solution also supports local and RADIUS user/password authentication. This authentication is best suited to small to medium client groups.

Single Point of Configuration Policy Manager Solutions

When the Cisco Wireless LAN Solution is equipped with WCS, you can configure system-wide security policies on a per wireless LAN basis. Small-office, home-office (SOHO) access points force you to individually configure security policies on each access point or use a third-party appliance to configure security policies across multiple access points. Because the Cisco Wireless LAN Solution security policies can be applied across the whole system from WCS, errors can be eliminated, and the overall effort is greatly reduced.

Rogue Access Point Solutions

This section describes security solutions for rogue access points.

Rogue Access Point Challenges

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain text or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as passwords and usernames. The hacker can then transmit a series of clear-to-send (CTS) frames, which mimics an access point informing a particular wireless LAN client adapter to transmit and instructing all others to wait. This scenario results in legitimate clients being unable to access the wireless LAN resources. Thus, wireless LAN service providers have a strong interest in banning rogue access points from the air space.

The operating system security solution uses the radio resource management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points, and locate them as described in the "Tagging and Containing Rogue Access Points" section below.

Tagging and Containing Rogue Access Points

When the Cisco Wireless LAN Solution is monitored using WCS, WCS generates the flags as rogue access point traps and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the access points closest to each rogue access point. The next step is to mark them as Known or Acknowledged rogue access points (no further action), Alert rogue access points (watch for and notify when active), or Contained rogue access points (have between one and four access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

Integrated Security Solutions

The Cisco Wireless LAN Solution also provides these integrated security solutions:

- Cisco Wireless LAN Solution operating system security is built around a robust 802.1X authorization, authentication, and accounting (AAA) engine, which enables operators to rapidly configure and enforce a variety of security policies across the Cisco Wireless LAN Solution.
- The controllers and access points are equipped with system-wide authentication and authorization protocols across all ports and interfaces, maximizing system security.
- Operating system security policies are assigned to individual wireless LANs, and access points simultaneously broadcast all (up to 16) configured wireless LANs. These policies can eliminate the need for additional access points, which can increase interference and degrade system throughput.
- The controllers securely terminate IPSec VPN clients, which can reduce the load on centralized VPN concentrators.
- Operating system security uses the RRM function to continually monitor the air space for interference and security breaches and notify the operator when they are detected.
- Operating system security works with industry-standard AAA servers, making system integration simple and easy.
- The operating system security solution offers comprehensive Layer 2 and Layer 3 encryption algorithms, which typically require a large amount of processing power. Rather than assigning the encryption tasks to yet another server, the controller can be equipped with a VPN/enhanced security module that provides extra hardware required for the most demanding security configurations.

Using WCS to Convert a Cisco Wireless LAN Solution from Layer 2 to Layer 3 Mode

Follow these steps to convert a Cisco Wireless LAN Solution from Layer 2 to Layer 3 LWAPP transport mode using the WCS user interface.

Note This procedure causes your access points to go offline until the controller reboots and the associated access points reassociate to the controller.

Note Layer 3 mode requires that all subnets to which the controllers are connected include at least one DHCP server. When you have completed this procedure, the controller stores its IP address in its associated access points. When each access point is powered up, it obtains an IP address from the local DHCP server and connects to its primary, secondary, or tertiary controller.

Note Layer 3 mode requires that all subnets that contain controllers and access points are routable to each other.

Step 1 To use the Cisco Wireless LAN Solution in Layer 3 mode, you must create an access point manager interface, which manages communications between each controller and its associated access points. This interface requires a fixed IP address, which must be different from the management interface IP address but can be on the same subnet as the management interface.

Step 2 Make sure that all controllers and access points are on the same subnet (that they are connected only through Layer 2 devices).

Note You must configure the controllers and associated access points to operate in Layer 3 mode before completing the conversion.

Step 3 Log into the WCS user interface.

Step 4 Click **Configure > Access Points** to navigate to the All Access Points page.

Step 5 For each access point, click the access point name and verify that the primary, secondary, and tertiary controller names are correct. If you change any of these names, click **Save** to save your changes.

Step 6 On the All Access Points page, make sure that the access points are associated to the controller before you continue to the next step.

Note If you do not complete this step, the access points may not associate to the controllers after completing the conversion.

Step 7 Follow these steps to change the LWAPP transport mode from Layer 2 to Layer 3:

a. Click **Configure > Controllers** to navigate to the All Controllers page.

b. Click the desired controller's IP address to display the *IP Address* > Controller Properties page.

c. In the sidebar, click **System > General** to display the *IP Address* > General page.

d. Change LWAPP transport mode to **Layer3** and click **Save**. The following message appears:

```
Please reboot the system for the LWAPP Mode change to take effect.
```

e. Click **OK**.

Step 8 Follow these steps to create a new access point manager interface:

a. Click **Configure > Controllers** to navigate to the All Controllers page.

b. Click the desired controller's IP address to display the *IP Address* > Controller Properties page.

c. In the sidebar, click **System > Interfaces** to display the *IP Address* > Interface page.

d. From the Select a Command drop-down menu, choose **Add Interface** and click **GO**.

e. Enter the following information on the *IP Address* > Interface page:

- An ap-manager interface name
- A VLAN identifier, if desired
- The access point manager IP address obtained in Step 1
- A gateway IP address
- The physical port number for the distribution system connection to the controller

- A primary DHCP server IP address
- A secondary DHCP server IP address

Note This address can be the same as the primary DHCP server IP address if you do not have a second DHCP server on this subnet.

f. If desired, choose an access control list (ACL) name from the drop-down menu.

g. Click **Save** to add the access point manager interface to the list of interfaces.

h. On the *IP Address* > Interface page, verify that WCS has added the ap-manager interface name to the list of interfaces.

i. Also verify that the management interface is properly configured with a different IP address than the ap-manager interface.

Step 9 Follow these steps to save the new configuration and restart the controller:

a. Click **Configure > Controllers** to navigate to the All Controllers page.

b. Click the desired controller's IP address to display the *IP Address* > Controller Properties page.

c. In the sidebar, click **System > Commands** to display the *IP Address* > Controller Commands page.

d. Under Administrative Commands, choose **Save Config To Flash** and click **GO** to save the changed configuration to the controller.

e. Under Administrative Commands, choose **Reboot** and click **GO** to reboot the controller.

f. Click **OK** to confirm the save and reboot.

Step 10 After the controller reboots, follow these steps to verify that the LWAPP transport mode is now Layer 3:

a. Click **Monitor > Devices** > **Controllers** to navigate to the Controllers > Search Results page.

b. Click the desired controller's IP address to display the Controllers > *IP Address* > Summary page.

c. Under General, verify that the current LWAPP transport mode is Layer3.

Step 11 Click **Configure > Access Points** to navigate to the All Access Points page.

Step 12 Make sure that the access points are associated to the controller before you continue to the next step.

Note If you do not complete this step, the access points may fail to associate to the desired controller after completing the conversion.

Step 13 Power down each access point to save the Layer 3 configuration to nonvolatile memory.

Step 14 Connect each access point to its final location in the network. Each access point connects to its primary, secondary, or tertiary controller; downloads a copy of the latest operating system code; and starts reporting its status to the controller. This process can take a few minutes for each access point.

You have completed the LWAPP transport mode conversion from Layer 2 to Layer 3. The ap-manager interface now controls all communications between controllers and access points on different subnets.

Using WCS to Convert a Cisco Wireless LAN Solution from Layer 3 to Layer 2 Mode

Follow these steps to convert a Cisco Wireless LAN Solution from Layer 3 to Layer 2 LWAPP transport mode using the WCS user interface.

Note This procedure causes your access points to go offline until the controller reboots and the associated access points reassociate to the controller.

Step 1 Make sure that all controllers and access points are on the same subnet.

Note You must configure the controllers and associated access points to operate in Layer 2 mode before completing the conversion.

Step 2 Log into the WCS user interface. Then follow these steps to change the LWAPP transport mode from Layer 3 to Layer 2:

a. Click **Configure > Controllers** to navigate to the All Controllers page.

b. Click the desired controller's IP address to display the *IP Address* > Controller Properties page.

c. In the sidebar, click **System > General** to display the *IP Address* > General page.

d. Change LWAPP transport mode to **Layer2** and click **Save**.

e. If WCS displays the following message, click **OK**:

```
Please reboot the system for the LWAPP Mode change to take effect.
```

Step 3 Follow these steps to restart your Cisco Wireless LAN Solution:

a. Return to the *IP Address* > Controller Properties page.

b. Click **System > Commands** to display the *IP Address* > Controller Commands page.

c. Under Administrative Commands, choose **Save Config To Flash** and click **GO** to save the changed configuration to the controller.

d. Click **OK** to continue.

e. Under Administrative Commands, choose **Reboot** and click **GO** to reboot the controller.

f. Click **OK** to confirm the save and reboot.

Step 4 After the controller reboots, follow these steps to verify that the LWAPP transport mode is now Layer 2:

a. Click **Monitor > Devices** > **Controllers** to navigate to the Controllers > Search Results page.

b. Click the desired controller's IP address to display the Controllers > *IP Address* > Summary page.

c. Under General, verify that the current LWAPP transport mode is Layer2.

You have completed the LWAPP transport mode conversion from Layer 3 to Layer 2. The operating system software now controls all communications between controllers and access points on the same subnet.

Configuring a Firewall for WCS

When a WCS server and a WCS user interface are on different sides of a firewall, they cannot communicate unless the following ports on the firewall are open to two-way traffic:

- 21 (ftp)
- 69 (tftp)
- 169 (trap port)
- 443 (https)

Open these ports to configure your firewall to allow communications between a WCS server and a WCS user interface.

Performing System Tasks

This chapter describes how to use WCS to perform system-level tasks. It contains these sections:

Adding System Components to the WCS Database

This section describes how to add a controller and a location appliance to the WCS database.

Adding a Controller to the WCS Database

Follow these steps to add a controller to the WCS database.

Note Cisco recommends that you manage controllers through the controller dedicated service port for improved security. However, when you manage controllers that do not have a service port (such as 2000 series controllers) or for which the service port is disabled, you must manage those controllers through the controller management interface.

Step 1 Log into the WCS user interface.

Step 2 Click **Configure** > **Controllers** to display the All Controllers page.

Step 3 From the Select a Command drop-down menu, choose **Add Controller** and click **GO**.

Step 4 On the Add Controller page, enter the controller IP address, network mask, and required SNMP settings.

Step 5 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.

Step 6 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.
```

Check these settings to correct the problem:

- The controller service port IP address might be set incorrectly. Check the service 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.
- The SNMP settings on the controller might not match the SNMP settings that you entered in WCS. Make sure that the SNMP settings configured on the controller match the settings that you entered in WCS.

Step 7 Add additional controllers if desired.

Adding a Location Appliance to the WCS Database

To add a location appliance to the WCS database, follow the instructions in Chapter 2 of the *Cisco Location Appliance Configuration Guide*.

Using WCS to Update System Software

Follow these steps to update controller (and access point) software using WCS.

Note When you use WCS to update the software on a 2000, 4100, or 4400 series controller, the controller within the Cisco Wireless Services Module (WiSM), or the controller within the Cisco 26/28/37/38*xx* Series Integrated Services Routers, the WCS server must be on the same subnet as the controller management interface because these controllers either do not have a service port or the service port is not routable.

Step 1 Enter **ping *ip-address*** to be sure that the WCS server can contact the controller. If you use an external TFTP server, enter **ping *ip-address*** to be sure that the WCS server can contact the TFTP server.

Note When you are downloading through a controller distribution system (DS) network port, the TFTP server can be on the same or a different subnet because the DS port is routable.

Step 2 Click the **Configure** > **Controllers** to navigate to the All Controllers page.

Step 3 Check the check box of the desired controller, choose **Download Software** from the Select a Command drop-down menu, and click **GO**. WCS displays the Download Software to Controller page.

Step 4 If you use the built-in WCS TFTP server, check the **TFTP Server on WCS System** check box. If you use an external TFTP server, uncheck this check box and add the external TFTP server IP address.

Step 5 Click **Browse** and navigate to the software update file (for example, AS_2000_*release*.aes for 2000 series controllers). The path and filename of the software appear in the File Name box.

Note Be sure that you have the correct software file for your controller.

Step 6 Click **Download**. WCS downloads the software to the controller, and the controller writes the code to flash RAM. As WCS performs this function, it displays its progress in the Status field.

Using WCS to Enable Long Preambles for SpectraLink NetLink Phones

A radio preamble (sometimes called a *header*) is a section of data at the head of a packet. It contains information that wireless devices need when sending and receiving packets. Short preambles improve throughput performance, so they are enabled by default. However, some wireless devices, such as SpectraLink NetLink phones, require long preambles.

To optimize the operation of SpectraLink NetLink phones on your wireless LAN, follow these steps to use WCS to enable long preambles.

Step 1 Log into the WCS user interface.

Step 2 Click **Configure > Controllers** to navigate to the All Controllers page.

Step 3 Click the IP address of the desired controller.

Step 4 In the sidebar, click **802.11b/g > Parameters**.

Step 5 If the *IP Address* > 802.11b/g Parameters page shows that short preambles are enabled, continue to the next step. However, if short preambles are disabled, which means that long preambles are enabled, the controller is already optimized for SpectraLink NetLink phones, and you do not need to continue this procedure.

Step 6 Enable long preambles by unchecking the **Short Preamble** check box.

Step 7 Click **Save** to update the controller configuration.

Step 8 To save the controller configuration, click **System > Commands** in the sidebar, **Save Config To Flash** from the Administrative Commands drop-down menu, and **GO**.

Step 9 To reboot the controller, click **Reboot** from the Administrative Commands drop-down menu and **GO**.

Step 10 Click **OK** when the following message appears:

```
Please save configuration by clicking “Save Config to flash”. Do you want to continue
rebooting anyways?
```

The controller reboots. This process may take some time, during which WCS loses its connection to the controller.

Note You can use a CLI session to view the controller reboot process.

Creating an RF Calibration Model

If you would like to further refine WCS Location tracking of client and rogue access points across one or more floors of a building, you have the option of creating an RF calibration model that uses physically collected RF measurements to fine-tune the location algorithm. When you have multiple floors in a building with the same physical layout as the calibrated floor, you can save time calibrating the remaining floors by using the same RF calibration model for the remaining floors. To perform an RF calibration, follow the RF calibration procedures included in the *Wireless Control System Online Help* to create an RF prediction model.

Adding and Using Maps

This chapter describes how to add maps to the Cisco WCS database and use them to monitor your wireless LAN. It contains these sections:

Creating Maps

Adding maps to the Cisco WCS database enables you to view your managed system on realistic campus, building, and floor plan maps. Follow the instructions in the sections below to add a campus, buildings, outdoor areas, floor plans, and access points to maps in the Cisco WCS database:

Adding a Campus

Follow these steps to add a single campus map to the Cisco WCS database.

Step 1 Save the map in .PNG, .JPG, .JPEG, or .GIF format.

Note The map can be any size because WCS automatically resizes the map to fit its working areas.

Step 2 Browse to and import the map from anywhere in your file system.

Step 3 Click **Monitor** > **Maps** to display the Maps page.

Step 4 From the Select a Command drop-down menu, choose **New Campus** and click **GO**.

Step 5 On the Maps > New Campus page, enter the campus name and campus contact name.

Step 6 Browse to and choose the image filename containing the map of the campus and click **Open**.

Step 7 Check the **Maintain Aspect Ratio** check box to prevent length and width distortion when WCS resizes the map.

Step 8 Enter the horizontal and vertical span of the map in feet.

Note The horizontal and vertical span should be larger than any building or floor plan to be added to the campus.

Step 9 Click **OK** to add this campus map to the Cisco WCS database. WCS displays the Maps page, which lists maps in the database, map types, and campus status.

Adding Buildings

You can add buildings to the Cisco WCS database regardless of whether you have added campus maps to the database. This section explains how to add a building to a campus map or a standalone building to the Cisco WCS database.

Adding a Building to a Campus Map

Follow these steps to add a building to a campus map in the Cisco WCS database.

Step 1 Click **Monitor > Maps** to display the Maps page.

Step 2 Click the desired campus. WCS displays the Maps > *Campus Name* page.

Step 3 From the Select a Command drop-down menu, choose **New Building** and click **GO**.

Step 4 On the *Campus Name* > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:

a. Enter the building name.

b. Enter the building contact name.

c. Enter the number of floors and basements.

d. Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

Note The horizontal and vertical span should be larger than or the same size as any floors that you might add later.

Tip You can also use Ctrl-click to resize the bounding area in the upper left corner of the campus map. As you change the size of the bounding area, the Horizontal Span and Vertical Span parameters of the building change to match your actions.

e. Click **Place** to put the building on the campus map. WCS creates a building rectangle scaled to the size of the campus map.

f. Click on the building rectangle and drag it to the desired position on the campus map.

g. Click **Save** to save this building and its campus location to the database. WCS saves the building name in the building rectangle on the campus map.

Note A hyperlink associated with the building takes you to the corresponding Map page.

Adding a Standalone Building

Follow these steps to add a standalone building to the Cisco WCS database.

Step 1 Click **Monitor > Maps** to display the Maps page.

Step 2 From the Select a Command drop-down menu, choose **New Building** and click **GO**.

Step 3 On the Maps > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:

a. Enter the building name.

b. Enter the building contact name.

c. Enter the number of floors and basements.

d. Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

Note The horizontal and vertical span should be larger than or the same size as any floors that you might add later.

e. Click **OK** to save this building to the database.

Adding Outdoor Areas

Follow these steps to add an outdoor area to a campus map.

Note You can add outdoor areas to a campus map in the Cisco WCS database regardless of whether you have added outdoor area maps to the database.

Step 1 If you want to add a map of the outdoor area to the database, save the map in .PNG, .JPG, .JPEG, or .GIF format. Then browse to and import the map from anywhere in your file system.

Note You do not need a map to add an outdoor area. You can simply define the dimensions of the area to add it to the database. The map can be any size because WCS automatically resizes the map to fit the workspace.

Step 2 Click **Monitor** > **Maps** to display the Maps page.

Step 3 Click the desired campus. WCS displays the Maps > *Campus Name* page.

Step 4 From the Select a Command drop-down menu, choose **New Outdoor Area** and click **GO**.

Step 5 On the *Campus Name* > New Outdoor Area page, follow these steps to create a manageable outdoor area:

a. Enter the outdoor area name.

b. Enter the outdoor area contact name.

c. If desired, enter or browse to the filename of the outdoor area map.

d. Enter an approximate outdoor horizontal span and vertical span (width and depth on the map) in feet.

Tip You can also use Ctrl-click to resize the bounding area in the upper left corner of the campus map. As you change the size of the bounding area, the Horizontal Span and Vertical Span parameters of the outdoor area change to match your actions.

e. Click **Place** to put the outdoor area on the campus map. WCS creates an outdoor area rectangle scaled to the size of the campus map.

f. Click on the outdoor area rectangle and drag it to the desired position on the campus map.

g. Click **Save** to save this outdoor area and its campus location to the database. WCS saves the outdoor area name in the outdoor area rectangle on the campus map.

Note A hyperlink associated with the outdoor area takes you to the corresponding Map page.

Adding and Enhancing Floor Plans

This section explains how to add floor plans to either a campus building or a standalone building in the Cisco WCS database. It also provides instructions on using the WCS map editor to enhance floor plans that you have created and the WCS planning mode to calculate the number of access points required to cover an area.

Adding Floor Plans to a Campus Building

After you add a building to a campus map, you can add individual floor plan and basement maps to the building. Follow these steps to add floor plans to a campus building.

Step 1 Save your floor plan maps in .PNG, .JPG, or .GIF format.

Note The maps can be any size because WCS automatically resizes the maps to fit the workspace.

Step 2 Browse to and import the floor plan maps from anywhere in your file system.

Step 3 Click **Monitor > Maps** to display the Maps page.

Step 4 Click the desired campus. WCS displays the Maps > *Campus Name* page.

Step 5 Move your cursor over the name within an existing building rectangle to highlight it.

Note When you highlight the name within a building rectangle, the building description appears in the sidebar.

Step 6 Click on the building name to display the Maps > *Campus Name* > *Building Name* page.

Step 7 From the Select a Command drop-down menu, choose **New Floor Area** and click **GO**.

Step 8 On the *Building Name* > New Floor Area page, follow these steps to add floors to a building in which to organize related floor plan maps:

a. Enter the floor or basement name.

b. Enter the floor or basement contact name.

c. Choose the floor or basement number.

d. Choose the floor or basement type.

e. Enter the floor-to-floor height in feet.

f. Check the Image File check box; then browse to and choose the desired floor or basement image filename and click **Open**.

Note When you choose the floor or basement image filename, WCS displays the image in the building-sized grid.

g. Click **Next**.

h. Either leave the **Maintain Aspect Ratio** check box checked to preserve the original image aspect ratio or uncheck the check box to change the image aspect ratio.

i. Enter an approximate floor or basement horizontal span and vertical span (width and depth on the map) in feet.

Note The horizontal and vertical span should be smaller than or the same size as the building horizontal span and vertical span in the Cisco WCS database.

j. If desired, click **Place** to locate the floor or basement image on the building grid.

Tip You can use Ctrl-click to resize the image within the building-sized grid.

k. Click **OK** to save this floor plan to the database. WCS displays the floor plan image on the Maps > *Campus Name* > *Building Name* page.

Step 9 Click any of the floor or basement images to view the floor plan or basement map.

Note You can zoom in and out to view the map at different sizes, and you can add access points. See the "Adding Access Points" section on page 5-9 for instructions.

Adding Floor Plans to a Standalone Building

After you have added a standalone building to the Cisco WCS database, you can add individual floor plan maps to the building. Follow these steps to add floor plans to a standalone building.

Step 1 Save your floor plan maps in .PNG, .JPG, or .GIF format.

Note The maps can be any size because WCS automatically resizes the maps to fit the workspace.

Step 2 Browse to and import the floor plan maps from anywhere in your file system.

Step 3 Click **Monitor > Maps** to display the Maps page.

Step 4 Click the desired building. WCS displays the Maps > *Building Name* page.

Step 5 From the Select a Command drop-down menu, choose **New Floor Area** and click **GO**.

Step 6 On the *Building Name* > New Floor Area page, follow these steps to add floors to a building in which to organize related floor plan maps:

a. Enter the floor or basement name.

b. Enter the floor or basement contact name.

c. Choose the floor or basement number.

d. Choose the floor or basement type.

e. Enter the floor-to-floor height in feet.

f. Check the Image File check box; then browse to and choose the desired floor or basement image filename and click **Open**.

Note When you choose the floor or basement image filename, WCS displays the image in the building-sized grid.

g. Click **Next**.

h. Either leave the **Maintain Aspect Ratio** check box checked to preserve the original image aspect ratio or uncheck the check box to change the image aspect ratio.

i. Enter an approximate floor or basement horizontal span and vertical span (width and depth on the map) in feet.

Note The horizontal and vertical span should be smaller than or the same size as the building horizontal span and vertical span in the Cisco WCS database.

j. If desired, click **Place** to locate the floor or basement image on the building grid.

Tip You can use Ctrl-click to resize the image within the building-sized grid.

k. Click **OK** to save this floor plan to the database. WCS displays the floor plan image on the Maps > *Building Name* page.

Step 7 Click any of the floor or basement images to view the floor plan or basement map.

Note You can zoom in and out to view the map at different sizes, and you can add access points. See the "Adding Access Points" section on page 5-9 for instructions.

Using the Map Editor to Enhance Floor Plans

You can use the WCS map editor to define, draw, and enhance floor plan information. The map editor enables you to create obstacles so that they can be taken into consideration when computing RF prediction heat maps for access points. You can also add coverage areas for location appliances that locate clients and tags in that particular area. Follow these steps to use the map editor.

Note Cisco recommends that you use the map editor to draw walls and other obstacles rather than importing an .FPE file from the legacy floor plan editor. If necessary, however, you can still import .FPE files. To do so, navigate to the desired floor area, choose **Edit Floor Area** from the Select a Command drop-down menu, click **GO**, check the **FPE File** check box, and browse to and choose the .FPE file.

Step 1 Click **Monitor > Maps** to display the Maps page.

Step 2 Click the desired campus. WCS displays the Maps > *Campus Name* page.

Step 3 Click on a campus building.

Step 4 Click on the desired floor area. WCS displays the Maps > *Campus Name* > *Building Name* > *Floor Area Name* page.

Step 5 From the Select a Command drop-down menu, choose **Map Editor** and click **GO**. WCS displays the Map Editor page.

Step 6 Refer to the *Wireless Control System Online Help* for instructions on using the map editor.

Using Planning Mode to Calculate Access Point Requirements

The WCS planning mode 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. 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. Refer to the *Wireless Control System Online Help* for instructions on using the planning mode.

Adding Access Points

After you add the .PNG, .JPG, .JPEG, or .GIF format floor plan and outdoor area maps to the Cisco WCS database, you can position lightweight access point icons on the maps to show where they are installed in the buildings. Follow these steps to add access points to floor plan and outdoor area maps.

Step 1 Click **Monitor > Network Summary** to display the Network Summary page.

Step 2 Under Coverage Areas, click the desired floor plan or outdoor area map. WCS displays the associated coverage area map.

Step 3 From the Select a Command drop-down menu, choose **Add Access Points** and click **GO**.

Step 4 On the Add Access Points page, choose the access points to add to the map.

Step 5 Click **OK** to add the access points to the map and display the Position Access Points map.

Note The access point icons appear in the upper left area of the map.

Step 6 Click and drag the icons to indicate their physical locations.

Step 7 Click each icon and choose the antenna orientation in the sidebar.

Note The antenna angle is relative to the map's X axis. Because the origin of the X and Y axes is in the upper left corner of the map, 0 degrees points side A of the access point to the right, 90 degrees points side A down, 180 degrees points side A to the left, and so on.

Note Make sure each access point is in the correct location on the map and has the correct antenna orientation. Accurate access point positioning is critical when you use the maps to find coverage holes and rogue access points.

Step 8 Click **Save** to store the access point locations and orientations. WCS computes the RF prediction for the coverage area. These RF predictions are popularly known as *heat maps* because they show the relative intensity of the RF signals on the coverage area map. Figure 5-1 shows an RF prediction heat map.

Note This display is only an approximation of the actual RF signal intensity because it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

Figure 5-1 RF Prediction Heat Map

Monitoring Maps

This section describes how to use maps to monitor your wireless LANs. You can use maps to monitor the following information:

- Predicted coverage, page 5-11
- Channels, page 5-12
- Transmit power levels, page 5-13
- Coverage holes, page 5-13
- Client devices, page 5-14

Follow the instructions on the page indicated for the information you want to monitor.

Monitoring Predicted Coverage

Follow these steps to monitor the predicted wireless LAN coverage on a map.

Step 1 Click **Monitor > Maps** to display the Maps page.

Step 2 Click an item in the Name column and click the floor map.

Step 3 Click the **View Filters** icon. The AP Filter window appears.

Step 4 From the Protocol drop-down menu, choose one of the following 802.11 protocols to display on the coverage map:

- **802.11a & b/g**—Displays all the access points in the area.
- **802.11a**—Displays a colored overlay depicting the coverage patterns for the 802.11a radios. The colors show the received signal strength from red (-35 dBm) through dark blue (-85 dBm).
- **802.11b/g**—Displays a colored overlay depicting the coverage patterns for the 802.11b/g radios. The colors show the received signal strength from red (-35 dBm) through dark blue (-85 dBm). This is the default value.

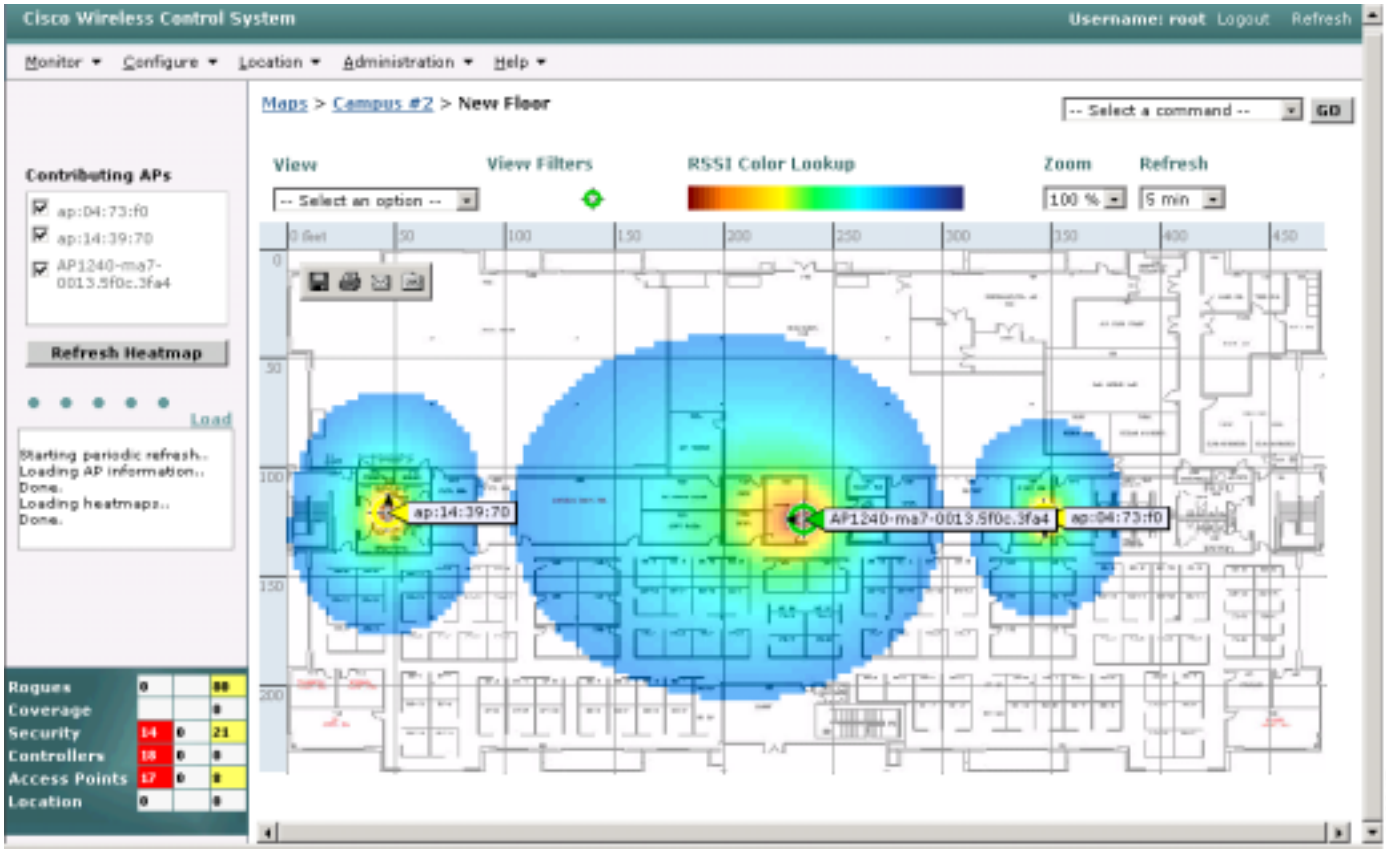
Step 5 From the Display drop-down menu, choose one of the following options to specify the information that appears in the flag next to each access point on the map:

- **Names**—Displays the access point name. This is the default value.
- **MAC Addresses**—Displays the MAC address of the access point, regardless of whether the access point is associated to a controller.
- **Controller IP**—Displays the IP address of the controller to which the access point is associated or “Not Associated” for disassociated access points.
- **Utilization**—Displays the percentage of bandwidth used by the associated client devices, “Unavailable” for disassociated access points, or “MonitorOnly” for access points in monitor-only mode.

Step 6 Click **OK**.

Figure 5-2 shows a typical RF prediction heat map with access points covering one floor of a building.

Figure 5-2 RF Prediction Heat Map



Monitoring Channels on a Floor Map

Follow these steps to monitor channels on a floor map.

Step 1 Click **Monitor** > **Maps** to display the Maps page.

Step 2 Click an item in the Name column and click the floor map.

Step 3 Click the **View Filters** icon. The AP Filter window appears.

Step 4 From the Display drop-down menu, choose **Channels** and click **OK**. The number of the channel being used by each radio appears in the flag next to each access point. “Unavailable” appears for disassociated access points.

Note The available channels are defined by the country code setting and are regulated on a country by country basis. Refer to Appendix B, “Supported Country Codes,” for the channels supported in each country.

Monitoring Transmit Power Levels on a Floor Map

Follow these steps to monitor transmit power levels on a floor map.

Step 1 Click **Monitor** > **Maps** to display the Maps page.

Step 2 Click an item in the Name column and click the floor map.

Step 3 Click the **View Filters** icon. The AP Filter window appears.

Step 4 From the Display drop-down menu, choose **Tx Power Level** and click **OK**. The number of the transmit power level being used by each radio appears in the flag next to each access point. "Unavailable" appears for disassociated access points.

Table 5-1 lists the transmit power level numbers and their corresponding power settings:

Table 5-1 Transmit Power Level Values

Transmit Power Level Number	Power Setting
1	Maximum power allowed per country code setting
2	50% power
3	25% power
4	12.5 to 6.25% power
5	6.25 to 0.195% power

Note The power levels are defined by the country code setting and are regulated on a country by country basis. Refer to Appendix B, "Supported Country Codes," for the maximum transmit power levels in each country.

Monitoring Coverage Holes on a Floor Map

Coverage holes are areas where clients cannot receive a signal from the wireless network. When you deploy a wireless network, there is a trade-off between the cost of the initial network deployment and the percentage of coverage hole areas. A reasonable coverage hole criterion for launch is between 2 and 10 percent. This means that between two and ten test locations out of 100 random test locations might receive marginal service. After launch, Cisco Wireless LAN Solution radio resource management (RRM) identifies these coverage hole areas and reports them to the IT manager, who can fill holes based on user demand.

Follow these steps to monitor coverage holes on a floor map.

Step 1 Click **Monitor** > **Maps** to display the Maps page.

Step 2 Click an item in the Name column and click the floor map.

Step 3 Click the **View Filters** icon. The AP Filter window appears.

Step 4 From the Display drop-down menu, choose **Coverage Holes** and click **OK**. The percentage of clients that have lost their connection to the wireless network appears in the flag next to each access point. "Unavailable" appears for disassociated access points, and "MonitorOnly" appears for access points in monitor-only mode.

Monitoring Clients on a Floor Map

Follow these steps to monitor client devices on a floor map.

Step 1 Click **Monitor** > **Maps** to display the Maps page.

Step 2 Click an item in the Name column and click the floor map.

Step 3 Click the **View Filters** icon. The AP Filter window appears.

Step 4 From the Display drop-down menu, choose **Users** and click **OK**. The number of client devices associated to each radio appears in the flag next to each access point. "Unavailable" appears for disassociated access points, and "MonitorOnly" appears for access points in monitor-only mode.

Step 5 Click the number of clients to display a list of specific client devices and parameters. Table 5-2 lists the parameters that appear.

Table 5-2 Client Parameters

Parameter	Description
User	The username of the client
Vendor	The manufacturer of the client
IP Address	The IP address of the client
MAC Address	The MAC address of the client
Access Point	The name of the access point to which the client is associated
Controller	The IP address of the controller to which the access point is connected
Port	The port number of the controller to which the access point is connected
802.11 State	Indicates whether the client is associated or disassociated
SSID	The service set identifier (SSID) being broadcast by the access point
Authenticated	Indicates whether authentication is enabled or disabled
Protocol	Indicates whether the 802.11a or 802.11b/g protocol is being used

Monitoring Wireless LANs

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

Monitoring Rogue Access Points

Because unauthorized rogue access points are inexpensive and readily available, employees sometimes plug them into existing LANs and build ad hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. Even more alarming, wireless users frequently publish unsecure access point locations, increasing the odds of having the enterprise security breached.

Rather than having a person with a scanner manually detect rogue access points, the Cisco Wireless LAN Solution automatically collects information on rogue access points detected by its managed access points (by MAC and IP address) and allows the system operator to locate, tag, and contain them. It can also be used to discourage rogue access point clients by sending them deauthenticate and disassociate messages from one to four access points.

Rogue Access Point Location, Tagging, and Containment

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take appropriate action:

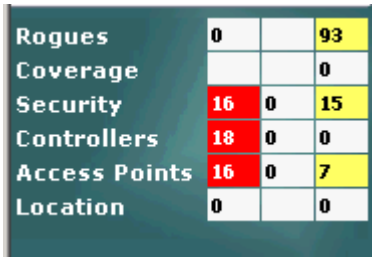
- Locate rogue access points
- Receive new rogue access point notifications, eliminating hallway scans
- Monitor unknown rogue access points until they are eliminated or acknowledged
- Determine the closest authorized access point, making directed scans faster and more effective
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
  - Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or wireless LAN security
  - Accept rogue access points when they do not compromise the LAN or wireless LAN security
  - Tag rogue access points as unknown until they are eliminated or acknowledged
  - Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Detecting and Locating Rogue Access Points

When the access points on your wireless LAN are powered up and associated with controllers, WCS immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies WCS, which creates a rogue access point alarm.

When WCS receives a rogue access point message from a controller, an alarm monitor appears in the lower left corner of all WCS user interface pages. The alarm monitor in Figure 6-1 shows 93 rogue access point alarms.

Figure 6-1 Alarm Monitor for Rogue Access Points



Follow these steps to detect and locate rogue access points.

Step 1 Click the **Rogues** indicator to display the Rogue AP Alarms page. This page lists the severity of the alarms, the rogue access point MAC addresses, the rogue access point types, the date and time when the rogue access points were first detected, and their SSIDs.

Step 2 Click any **Rogue MAC Address** link to display the associated Alarms > Rogue - *AP MAC Address* page. This page shows detailed information about the rogue access point alarm.

Step 3 To modify the alarm, choose one of these commands from the Select a Command drop-down menu and click **GO**.

- **Assign to me**—Assigns the selected alarm to the current user.
- **Unassign**—Unassigns the selected alarm.
- **Delete**—Deletes the selected alarm.
- **Clear**—Clears the selected alarm.
- **Event History—**Enables you to view events for rogue alarms.
- **Detecting APs** (with radio band, location, SSID, channel number, WEP state, short or long preamble, RSSI, and SNR)—Enables you to view the access points that are currently detecting the rogue access point.
- **Trend**—Shows a trend of recent RSSI signal strength.
- **Rogue Clients**—Enables you to view the clients associated with this rogue access point.
- **Set State to 'Unknown - Alert'**—Tags the rogue access point as the lowest threat, continues to monitor the rogue access point, and turns off containment.

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

  Set State to 'Known - External'—Tags the rogue access point as external, adds it to the known rogue access points list, and turns off containment.
- **1 AP Containment** through **4 AP Containment—**When you select level 1 containment, one access point in the vicinity of the rogue unit sends deauthenticate and disassociate messages to the client devices that are associated to the rogue unit. When you select level 2 containment, two access points in the vicinity of the rogue unit send deauthenticate and disassociate messages to the rogue's clients and so on up to level 4.

Step 4 From the Select a Command drop-down menu, choose **Map (High Resolution)** and click **GO** to display the current calculated rogue access point location on the Maps > *Building Name* > *Floor Name* page.

If you are using WCS Location, WCS compares RSSI signal strength from two or more access points to find the most probable location of the rogue access point and places a small skull-and-crossbones indicator at its most likely location. If you are using WCS Base, WCS relies on RSSI signal strength from the rogue access point and places a small skull-and-crossbones indicator next to the access point receiving the strongest RSSI signal from the rogue unit. Figure 6-2 shows a map that indicates that location of a rogue unit.

Figure 6-2 Map Indicating Location of Rogue Unit

Acknowledging Rogue Access Points

Follow these steps to acknowledge rogue access points.

Step 1 Navigate to the Rogue AP Alarms page.

Step 2 Check the check box of the rogue access point to be acknowledged.

Step 3 From the Select a Command drop-down menu, choose **Set State to 'Known - Internal'** or **Set State to 'Known - External'**. In either case, WCS removes the rogue access point entry from the Rogue AP Alarms page.

Finding Clients

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

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

Step 2 In the sidebar, choose **All Clients** in the Search For Clients By drop-down menu and click **Search** to display the Clients page.

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

Step 3 Click the username of the client that you want to locate. WCS displays the corresponding Clients *Client Name* page.

Step 4 To find the client, choose one of these options from the Select a Command drop-down menu and click **GO**:

- **Recent Map (High Resolution)**—Finds the client without disassociating it.
- **Present Map (High Resolution)**—Disassociates the client and then finds it after reassociation. When you choose this method, WCS displays a warning message and asks you to confirm that you want to continue.

If you are using WCS Location, WCS compares the RSSI signal strength from two or more access points to find the most probable location of the client and places a small laptop icon at its most likely location. If you are using WCS Base, WCS relies on the RSSI signal strength from the client and places a small laptop icon next to the access point that receives the strongest RSSI signal from the client. Figure 6-3 shows a heat map that includes a client location.

Figure 6-3 Map with Client Location

Finding Coverage Holes

Coverage holes are areas where clients cannot receive a signal from the wireless network. The Cisco Wireless LAN Solution radio resource management (RRM) identifies these coverage hole areas and reports them to WCS, enabling the IT manager to fill holes based on user demand. Follow these steps to find coverage holes on your wireless LAN.

Step 1 Click the **Coverage** indicator on the bottom left of the WCS user interface page (or click **Monitor > Alarms** and search for **Coverage** under Alarm Category) to display the Coverage Hole Alarms page.

Step 2 Click **Monitor > Maps** and search for access points by name (this search tool is case sensitive). WCS displays the Maps > Search Results page, which lists the floor or outdoor area where the access point is located.

Step 3 Click the floor or outdoor area link to display the related Maps > *Building Name* > *Floor Name* page.

Step 4 Look for areas of low signal strength near the access point that reported the coverage hole. These areas are the most likely locations of coverage holes. If there does not appear to be any areas of weak signal strength, make sure that the floor plan map is accurate.

Pinging a Network Device from a Controller

Follow these steps to ping network devices from a controller.

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

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

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

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

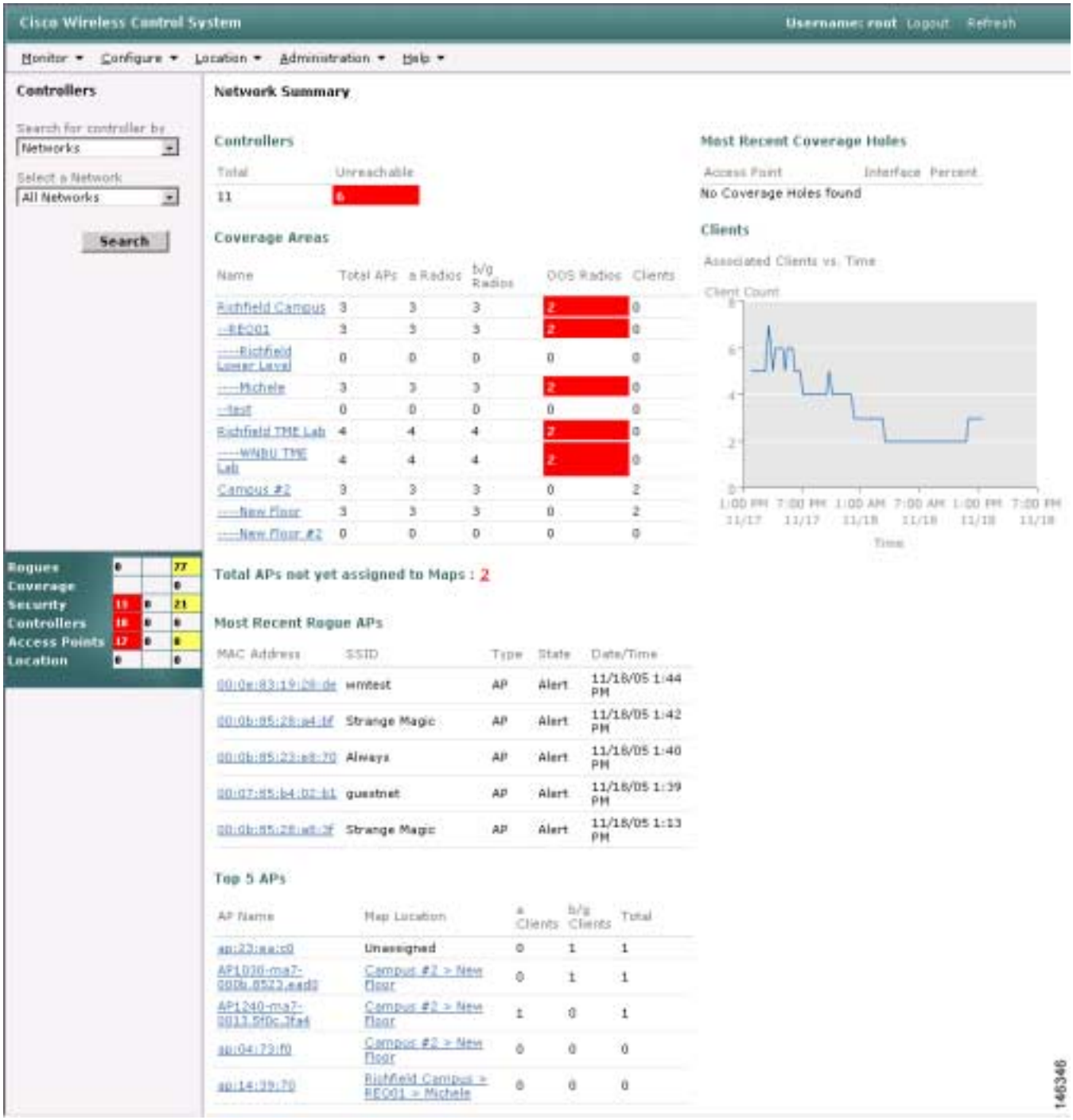
Step 5 In the Enter an IP Address (x.x.x.x) to Ping window, enter the IP address of the network device that you want the controller to ping and click **OK**.

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

Viewing Controller Status and Configurations

After you add controllers and access points to the WCS database, you can view the status of the Cisco Wireless LAN Solution. To view the system status, click **Monitor > Network Summary** to display the Network Summary page (see Figure 6-4).

Figure 6-4 Network Summary Page



Viewing WCS Statistics Reports

WCS periodically collects statistics such as client counts, radio utilization, transmit power and channel information, and profile status and organizes them into reports. To view these reports, click **Monitor** > **Reports**.

Managing WCS User Accounts

This chapter describes how to manage WCS user accounts. It contains these sections:

Adding WCS User Accounts

Follow these steps to add a new user account to WCS.

Step 1 Start WCS by following the instructions in the "Starting WCS" section on page 2-2.

Step 2 Log into the WCS user interface as Super1.

Note Cisco recommends that you create a new superuser assigned to the SuperUsers group and delete Super1 to prevent unauthorized access to the system.

Step 3 Click **Administration** > **Accounts** to display the All Users page.

Step 4 From the Select a Command drop-down menu, choose **Add User** and click **GO** to display the User administration page.

Step 5 Enter the username and password for the new WCS user account. You must enter the password twice.

Note These entries are case sensitive.

Step 6 Under Groups Assigned to this User, check the appropriate check box to assign the new user account to one of four user groups supported by WCS:

- **System Monitoring**—Allows users to monitor WCS operations.
- **ConfigManagers**—Allows users to monitor and configure WCS operations.
- **Admin**—Allows users to monitor and configure WCS operations and perform all system administration tasks except administering WCS user accounts and passwords.
- **SuperUsers**—Allows users to monitor and configure WCS operations and perform all system administration tasks including administering WCS user accounts and passwords.

Step 7 Click **Submit**. The name of the new user account appears on the All Users page and can be used immediately.

Step 8 In the sidebar, click **Groups** to display the All Groups page.

Step 9 Click the name of the user group to which you assigned the new user account. The Group > *User Group* page shows a list of this group's permitted operations.

Step 10 Make any desired changes by checking or unchecking the appropriate check boxes.

Note Any changes you make will affect all members of this user group.

Step 11 Click **Submit** to save your changes or **Cancel** to leave the settings unchanged.

Changing Passwords

Follow these steps to change the password for a WCS user account.

Step 1 Start WCS by following the instructions in the "Starting WCS" section on page 2-2.

Step 2 Log into the WCS user interface as a user assigned to the SuperUsers group.

Step 3 Click **Administration** > **Accounts** to display the All Users page.

Step 4 Click the name of the user account for which you want to change the password.

Step 5 On the User > *Username* page, enter the new password in both the New Password and Confirm New Password fields.

Step 6 Click **Submit** to save your changes. The password for this user account has been changed and can be used immediately.

Deleting WCS User Accounts

Follow these steps to delete a WCS user account.

Step 1 Start WCS by following the instructions in the "Starting WCS" section on page 2-2.

Step 2 Log into the WCS user interface as a user assigned to the SuperUsers group.

Step 3 Click **Administration** > **Accounts** to display the All Users page.

Step 4 Check the check box to the left of the user account(s) to be deleted.

Step 5 From the Select a Command drop-down menu, choose **Delete User(s)** and click **GO**.

Step 6 When prompted, click **OK** to confirm your decision. The user account is deleted and can no longer be used.

Maintaining WCS

This chapter provides routine procedures for maintaining WCS. It contains these sections:

Checking the Status of WCS

This section provides instructions for checking the status of WCS on either a Windows or Linux server.

Checking the Status of WCS on Windows

Follow these steps to check the status of WCS when it is installed as a Windows application or Windows service. You can check the status at any time.

Step 1 Log into the system as administrator.

Step 2 Perform one of the following:

- From the Windows Start menu, click **Programs** > **Wireless Control System > WCSStatus**.
- From the command prompt, navigate to the WCS installation directory (C:\Program Files\WCS32\bin) and enter **WCSAdmin status**.

The WCSAdmin window appears and displays messages indicating the status of WCS.

Step 3 Close the WCSAdmin window when the Close button becomes active.

Checking the Status of WCS on Linux

Follow these steps to check the status of WCS when it is installed as a Linux application or Linux service. You can check the status at any time.

Step 1 Log into the system as root.

Step 2 Using the Linux CLI, perform one of the following:

- Navigate to the /opt/WCS32 directory (or the directory chosen during installation) and enter **./WCSStatus**.
- Navigate to the /opt/WCS32/bin directory and enter **WCSAdmin status**.

The CLI displays messages indicating the status of WCS.

Stopping WCS

This section provides instructions for stopping WCS on either a Windows or Linux server.

Stopping WCS on Windows

Follow these steps to stop WCS when it is installed as a Windows application or Windows service. You can stop WCS at any time.

Note If any users are logged in when you stop WCS, their WCS sessions stop functioning.

Step 1 Log into the system as administrator.

Step 2 Perform one of the following:

- From the Windows Start menu, click **Programs** > **Wireless Control System > StopWCS**.
- From the command prompt, navigate to the WCS installation directory (C:\Program Files\WCS32\bin) and enter **WCSAdmin stop**.

The WCSAdmin window appears and displays messages indicating that WCS is stopping.

Note If WCS is installed as a service, messages also appear to indicate that the Nms_Server service is stopping.

Step 3 Close the WCSAdmin window when the Close button becomes active.

Stopping WCS on Linux

Follow these steps to stop WCS when it is installed as a Linux application or Linux service. You can stop WCS at any time.

Note If any users are logged in when you stop WCS, their WCS sessions stop functioning.

Step 1 Log into the system as root.

Step 2 Using the Linux CLI, perform one of the following:

- Navigate to the /opt/WCS32 directory (or the directory chosen during installation) and enter **./StopWCS**.
- Navigate to the /opt/WCS32/bin directory and enter **WCSAdmin stop**.

The CLI displays messages indicating that WCS is stopping.

Backing Up the WCS Database

This section provides instructions for backing up the WCS database. You can schedule regular backups through the WCS user interface or manually initiate a backup on either a Windows or Linux server.

Scheduling Automatic Backups

Follow these steps to schedule automatic backups of the WCS database.

Step 1 Log into the WCS user interface.

Step 2 Click **Administration > Scheduled Tasks** to display the Scheduled Tasks page.

Step 3 Click **WCS Server Backup** to display the Task > WCS Server Backup page.

Step 4 Check the **Admin Status: Enabled** check box.

Step 5 In the Max Backups to Keep field, enter the maximum number of backup files to be saved on the server.

Range: 7 to 50

Default: 7

Note To prevent the WCS platform from running out of disk space, the server automatically deletes old backup files when the number of files exceeds the value entered for this field.

Step 6 In the Interval (Days) field, enter a number representing the number of days between each backup. For example, 1 = a daily backup, 2 = a backup every other day, 7 = a weekly backup, and so on.

Range: 1 to 360

Default: 7

Step 7 In the Time of Day field, enter the time when you want the backup to start. It must be in this format: *hh*:*mm* AM/PM (for example: 03:00 AM).

Note Backing up a large database affects the performance of the WCS server. Therefore, Cisco recommends that you schedule backups to run when the WCS server is idle (for example, in the middle of the night).

Step 8 Click **Submit** to save your settings. The backup file is saved as a .zip file in the *ftp-install-dir*/ftp-server/root/WCSBackup directory using this format: *dd-mmm-yy_ hh-mm-ss*.zip (for example, 11-Nov-05_10-30-00.zip).

Performing a Manual Backup

This section provides instructions for backing up the WCS database on either a Windows or Linux server.

Backing Up the WCS Database on Windows

Follow these steps to back up the WCS database on a Windows server.

Step 1 Log into the system as administrator.

Step 2 Create a backup directory for the WCS database with no spaces in the name, such as C:\WCS32_Backup.

Note Make sure that the directory name does not contain spaces. Spaces can generate errors.

Step 3 Perform one of the following:

- Follow these steps from the Windows Start menu:
  a. Click **Programs** > **Wireless Control System > Backup**. The Enter Information window appears.
  b. Enter the full path of the backup directory that you created and a name for the backup file (such as C:\WCS32_Backup\Nov11) and click **OK**.
- Follow these steps from the command prompt:
  a. Navigate to the WCS installation directory (C:\Program Files\WCS32\bin).
  b. Enter **DBAdmin backup *backup-filename***, where *backup-filename* is the full path of the backup directory that you created plus a name for the backup file (such as C:\WCS32_Backup\Nov11).

The DBAdmin window appears and displays messages indicating the status of the backup.

Step 4 Close the DBAdmin window when the Close button becomes active.

Note In the example above, the backup file would appear in the C:\WCS32_Backup directory as Nov11.nmsbackup.

Backing Up the WCS Database on Linux

Follow these steps to back up the WCS database on a Linux server.

Step 1 Log into the system as root.

Step 2 Using the Linux CLI, navigate to the /opt/WCS32 directory (or any other directory).

Step 3 Create a backup directory for the WCS database with no spaces in the name (for example, **mkdir WCS32_Backup**).

Note Make sure that the directory name does not contain spaces. Spaces can generate errors.

Step 4 Perform one of the following:

- Navigate to the /opt/WCS32 directory (or the directory chosen during installation) and enter **./Backup**. Enter a name for the backup file when prompted (such as WCS32_Backup/Nov11).
- Navigate to the /opt/WCS32/bin directory and enter **DBAdmin backup *backup-filename***, where *backup-filename* is the full path of the backup directory that you created plus a name for the backup file (such as WCS32_Backup/Nov11).

The CLI displays messages indicating the status of the backup.

Note In the example above, the backup file would appear in the WCS32_Backup directory as Nov11.nmsbackup.

Restoring the WCS Database

This section provides instructions for restoring the WCS database on either a Windows or Linux server.

Restoring the WCS Database on Windows

Follow these steps to restore the WCS database from a backup file on a Windows server.

Step 1 If possible, stop all WCS user interfaces to stabilize the database.

Step 2 Log into the system as administrator.

Step 3 Perform one of the following:

- Follow these steps from the Windows Start menu:
  a. Click **Programs** > **Wireless Control System > Restore**. The Enter Information window appears.
  b. Enter the full path and filename of the backup file (such as C:\WCS32_Backup\Nov11.nmsbackup) and click **OK**.
- Follow these steps from the command prompt:
  a. Navigate to the WCS installation directory (C:\Program Files\WCS32\bin).
  b. Enter **DBAdmin restore *backup-filename***, where *backup-filename* is the full path and filename of the backup file (for example, C:\WCS32_Backup\Nov11.nmsbackup).

Step 4 Click **Yes** if a message appears indicating that WCS is running and needs to be shut down.

Step 5 The DBAdmin window appears and displays messages indicating that WCS is shutting down (if applicable) and the WCS database is being restored. Close the DBAdmin window when the Close button becomes active.

Restoring the WCS Database on Linux

Follow these steps to restore the WCS database from a backup file on a Linux server.

Step 1 If possible, stop all WCS user interfaces to stabilize the database.

Step 2 Log into the system as root.

Step 3 Using the Linux CLI, perform one of the following:

- Navigate to the /opt/WCS32 directory (or the directory chosen during installation) and enter **./Restore** to start the restoration process. Enter the backup filename when prompted (such as WCS32_Backup/Nov11.nmsbackup).
- Navigate to the /opt/WCS32/bin directory and enter **DBAdmin restore *backup-filename***, where *backup-filename* is the full path and filename of the backup file (such as WCS32_Backup/Nov11.nmsbackup).

The CLI displays messages indicating that the WCS database is being restored.

Uninstalling WCS

This section provides instructions for uninstalling WCS on either a Windows or Linux server. You can uninstall WCS at any time, even while WCS is running.

Uninstalling WCS on Windows

Follow these steps to uninstall WCS on a Windows server.

Step 1 Log into the system as administrator.

Step 2 From the Windows Start menu, click **Programs** > **Wireless Control System** > **Uninstall WCS**.

Step 3 When the Uninstall Wireless Control System window appears, click **Uninstall**.

Step 4 Follow the instructions on the screen to continue the uninstall process.

Step 5 When the WCS Uninstaller window indicates that the program is uninstalled, click **Finish** to close the window.

Note If any part of the C:\Program Files\WCS32 folder remains on the hard drive, manually delete the folder and all of its contents. If you fail to delete the previous WCS installation, this error message appears when you attempt to reinstall WCS: “Cisco WCS already installed. Please uninstall the older version before installing this version.”

Uninstalling WCS on Linux

Follow these steps to uninstall WCS on a Linux server.

Step 1 Log into the system as root.

Step 2 Using the Linux CLI, navigate to the /opt/WCS32 directory (or the directory chosen during installation).

Step 3 Enter **./UninstallWCS**.

Step 4 Click **Yes** to continue the uninstall process.

Step 5 Click **Finish** when the uninstall process is complete.

Note If any part of the /opt/WCS32 directory remains on the hard drive, manually delete the directory and all of its contents. If you fail to delete the previous WCS installation, this error message appears when you attempt to reinstall WCS: "Cisco WCS already installed. Please uninstall the older version before installing this version."

Upgrading WCS

This section provides instructions for upgrading WCS on either a Windows or Linux server.

Upgrading WCS on Windows

Follow these steps to upgrade WCS on a Windows server.

Step 1 If possible, stop all WCS user interfaces to stabilize the database.

Step 2 Back up the WCS database by following the instructions in the "Backing Up the WCS Database on Windows" section on page 8-5.

Step 3 Uninstall the WCS application by following the instructions in the "Uninstalling WCS on Windows" section on page 8-7.

Step 4 Install the new version of WCS by following the instructions in the *Quick Start Guide: Cisco Wireless Control System for Microsoft Windows*.

Step 5 Restore the WCS database by following the instructions in the "Restoring the WCS Database on Windows" section on page 8-6.

Upgrading WCS on Linux

Follow these steps to upgrade WCS on a Linux server.

Step 1 If possible, stop all WCS user interfaces to stabilize the database.

Step 2 Back up the WCS database by following the instructions in the "Backing Up the WCS Database on Linux" section on page 8-5.

Step 3 Uninstall the WCS application by following the instructions in the "Uninstalling WCS on Linux" section on page 8-8.

Step 4 Install the new version of WCS by following the instructions in the *Quick Start Guide: Cisco Wireless Control System for Linux*.

Step 5 Restore the WCS database by following the instructions in the "Restoring the WCS Database on Linux" section on page 8-7.

End User License and Warranty

This appendix provides the end user license and warranty that apply to the Cisco Wireless Control System (WCS). It contains these sections:

End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

The following terms of this End User License Agreement ("Agreement") govern Customer's access and use of the Software, except to the extent (a) there is a separate signed agreement between Customer and Cisco governing Customer's use of the Software or (b) the Software includes a separate "click-accept" license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the signed agreement, (2) the click-accept agreement, and (3) this End User License Agreement.

License. Conditioned upon compliance with the terms and conditions of this Agreement, Cisco Systems, Inc. or its subsidiary licensing the Software instead of Cisco Systems, Inc. ("Cisco"), grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) specifically pertaining to the Software and made available by Cisco with the Software in any manner (including on CD-ROM, or on-line).

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or that number of agent(s), concurrent users, sessions, IP addresses, port(s), seat(s), server(s) or site(s), as set forth in the applicable Purchase Order which has been accepted by Cisco and for which Customer has paid to Cisco the required license fee.

Unless otherwise expressly provided in the Documentation, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer and used for Customer's internal business purposes. NOTE: For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Cisco retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Cisco, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Accordingly, except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

(i) transfer, assign or sublicense its license rights to any other person or entity, or use the Software on unauthorized or secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;

(ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

(iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction;

(iv) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Cisco; or

(v) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Cisco. Customer shall implement reasonable security measures to protect such trade secrets; or

(vi) use the Software to develop any software application intended for resale which employs the Software.

To the extent required by law, and at Customer's written request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Cisco makes such information available. Customer is granted no implied licenses to any other intellectual property rights other than as specifically granted herein.

Software, Upgrades and Additional Copies. For purposes of this Agreement, “Software” shall include (and the terms and conditions of this Agreement shall apply to) computer programs, including firmware, as provided to Customer by Cisco or an authorized Cisco reseller, and any upgrades, updates, bug fixes or modified versions thereto (collectively, “Upgrades”) or backup copies of the Software licensed or provided to Customer by Cisco or an authorized Cisco reseller. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Cisco.

Open Source Content. Customer acknowledges that the Software contains open source or publicly available content under separate license and copyright requirements which are located either in an attachment to this license, the Software README file or the Documentation. Customer agrees to comply with such separate license and copyright requirements.

Third Party Beneficiaries. Certain Cisco or Cisco affiliate suppliers are intended third party beneficiaries of this Agreement. The terms and conditions herein are made expressly for the benefit of and are enforceable by Cisco’s suppliers; provided, however, that suppliers are not in any contractual relationship with Customer. Cisco’s suppliers include without limitation: (a) Hifn, Inc., a Delaware corporation with principal offices at 750 University Avenue, Los Gatos, California and (b) Wind River Systems, Inc., and its suppliers. Additional suppliers may be provided in subsequent updates of Documentation supplied to Customer.

Term and Termination. This Agreement and the license granted herein shall remain effective until terminated. Customer may terminate this Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer's rights under this Agreement will terminate immediately without notice from Cisco if Customer fails to comply with any provision of this Agreement. Cisco and its suppliers are further entitled to obtain injunctive relief if Customer's use of the Software is in violation of any license restrictions. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License" shall survive termination of this Agreement.

Customer Records. Customer grants to Cisco and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit.

Export. Software and Documentation, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software and Documentation. Customer's failure to comply with such restrictions shall constitute a material breach of the Agreement.

U.S. Government End User Purchasers. The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which this End User License Agreement may be incorporated, Customer may provide to Government end user or, if this Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in this End User License Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Limited Warranty

Software. Cisco warrants that commencing from the date of shipment to Customer (but in case of resale by an authorized Cisco reseller, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the software warranty period (if any) set forth in the warranty card accompanying the Product (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to its published specifications. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided AS IS. This limited warranty extends only to the Customer who is the original licensee. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers and licensors under this limited warranty will be, at Cisco's option, repair, replacement, or refund of the Software if reported (or, upon request, returned) to Cisco or the party supplying the Software to Customer. In no event does Cisco warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development

of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; or (d) is licensed, for beta, evaluation, testing or demonstration purposes for which Cisco does not charge a purchase price or license fee.

Disclaimer of Warranty

EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

General Terms Applicable to the Limited Warranty Statement and End User License Agreement

Disclaimer of Liabilities. REGARDLESS WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Cisco's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim or if the Software is part of another Product, the price paid for such other Product. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Customer agrees that the limitations of liability and disclaimers set forth herein will apply regardless of whether Customer has accepted the Software or any other product or service delivered by Cisco. Customer acknowledges and agrees that Cisco has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

The Warranty and the End User License shall be governed by and construed in accordance with the laws of the State of California, without reference to or application of choice of law rules or principles. The United Nations Convention on the International Sale of Goods shall not apply. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement shall remain in full force and effect. Except as expressly provided herein, this Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any purchase order or elsewhere, all of which terms are excluded. This Agreement has been written in the English language, and the parties agree that the English version will govern. For warranty or license terms which may apply in particular countries and for translations of the above information please contact the Cisco Legal Department, 300 E. Tasman Drive, San Jose, California 95134.

Additional Open Source Terms

GNU General Public License. Certain portions of the Software are licensed under and Customer's use of such portions are subject to the GNU General Public License version 2. A copy of the license is available at www.fsf.org or by writing to licensing@fsf.org or the Free Software Foundation, 59 Temple Place, Suite 330, Boston, MA 02111-1307. Source code governed by the GNU General Public License version 2 is available upon written request to the Cisco Legal Department, 300 E. Tasman Drive, San Jose, California 95134.

SSH Source Code Statement. © 1995 - 2004 SAFENET, Inc. This software is protected by international copyright laws. All rights reserved. SafeNet is a registered trademark of SAFENET, Inc., in the United States and in certain other jurisdictions. SAFENET and the SAFENET logo are trademarks of SAFENET, Inc., and may be registered in certain jurisdictions. All other names and marks are property of their respective owners.

Copyright (c) 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Components of the software are provided under a standard 2-term BSD license with the following names as copyright holders:

- Markus Friedl
- Theo de Raadt
- Niels Provos
- Dug Song
- Aaron Campbell
- Damien Miller
- Kevin Steves

Supported Country Codes

This appendix provides the list of countries in which the Cisco Wireless LAN Solution is supported for use. It contains this section:

Supported Country Codes

The Cisco Wireless LAN Solution has been approved or is being approved to operate in the countries shown in Table B-1 and fully conforms with current country requirements.

The maximum regulatory transmit power level limits published here are defined by the country code setting and are regulated on a country by country basis. The actual maximum transmit power levels may be less than the published regulatory limits.

Note Some of these entries may change over time. Consult www.cisco.com/go/aironet/compliance for current approvals and regulatory domain information.

Table B-1 Supported Country Codes

Country Code/ Country	1000 Series Access Point Regulatory Domain	802.11 Bands	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Indoor/ Outdoor Use	Frequency Range (GHz)	Regulatory Authority
AT/ Austria	-E	a	36, 40, 44, 48	60 mW EIRP	In	5.15-5.25	BMV/ FSB-LD047
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
AU/ Australia	-N	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.725-5.825	ACA
		b	1-11	200 mW EIRP	Both	2.4-2.4835	
BE/ Belgium	-E	a	36, 40, 44, 48 52, 56, 60, 64	120 mW EIRP 120 mW EIRP	In In	5.15-5.25	BIPT/ Annexe B3 Interface radio HIPERLAN
		b/g	1-12 13	100 mW EIRP 100 mW EIRP	In Out	2.4-2.4835	
BR/ Brazil	-C	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	200 mW EIRP 1 W EIRP	In Both	5.725-5.85	Anatel/ Resolution 305
		b/g	1-11	1 W EIRP	Both	2.4-2.4835	
CA/ Canada	-A	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both Both	5.15-5.25 5.25-5.35 5.725-5.85	Industry Canada RSS-210
		b/g	1-11	1 W+Restricted Antennas	Both	2.4-2.4835	

Table B-1 Supported Country Codes (continued)

Country Code/ Country	1000 Series Access Point Regulatory Domain	802.11 Bands	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Indoor/ Outdoor Use	Frequency Range (GHz)	Regulatory Authority
CH/ Switzerland and Liechtenstein	-E	a	36, 40, 44, 48 52, 56, 60, 64	200 mW EIRP 200 mW EIRP	In In	5.15-5.25 5.25-5.35	OFCOM
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
CN/ China	-C	a	149, 153, 157, 161	150 mW+6 dBi~600 mW	Both	5.725-5.825	RRL/ MIC Notice 2003-13
		b/g	1-13	150 mW+6 dBi~600 mW	Both	2.4-2.4835	
CY/ Cyprus	-E	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both Both	5.15-5.25 5.25-5.35 5.725-5.85	(tbd)
		b/g	1-11	1 W+Restricted Antennas	Both	2.4-2.4835	
CZ/ Czech Republic	-E	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.725-5.825	CTO
		b	1-11	200 mW EIRP	Both	2.4-2.4835	
DE/ Germany	-E	a	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	RegTP/ wlan35
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
DK/ Denmark	-E	a	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	ITST/ Radio interface specification 00 007
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
EE/ Estonia	-E	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both Both	5.15-5.25 5.25-5.35 5.725-5.85	SIDEAMET
		b/g	1-11	1 W+Restricted Antennas	Both	2.4-2.4835	
ES/ Spain	-E	a	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	Ministry of Telecom
		b/g	1-11	100 mW EIRP	In	2.412-2.472	

Table B-1 Supported Country Codes (continued)

Country Code/ Country	1000 Series Access Point Regulatory Domain	802.11 Bands	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Indoor/ Outdoor Use	Frequency Range (GHz)	Regulatory Authority
FI/ Finland	-E	a	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	FICORA/ RLAN Notice
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
FR/ France	-E	a	36, 40, 44, 48 52, 56, 60, 64	200 mW EIRP 200 mW EIRP	In In	5.15-5.25 5.25-5.35	A.R.T./ Decision 01-441
		b/g	1-7 8-11	100 mW EIRP 100 mW EIRP	Both In	2.4-2.4835 2.4-2.454	
GB/ United Kingdom	-E	a	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	UKRA/ IR2006
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
GR/ Greece	-E	b/g	1-11	100 mW EIRP	In	2.4-2.4835	Ministry of Transport & Comm.
HK/ Hong Kong	-N	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	200 mW EIRP 200 mW EIRP 1 W+6 dBi=4 W	Both Both Both	5.15-5.25 5.25-5.35 5.725-5.85	OFTA
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
HU/ Hungary	-E	a	36, 40, 44, 48 52, 56, 60, 64	200 mW EIRP	In	5.15-5.25 5.25-5.35	HIF
		b/g	1-11	1 W EIRP	Both	2.4-2.4835	
ID/ Indonesia	-R	a	N/A	N/A	N/A	5.725-5.875	PDT
		b/g	1-13	100 mW EIRP	In	2.4-2.5	
IE/ Ireland	-E	a	36, 40, 44, 48 52, 56, 60, 64	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	COMREG/ ODTR 00/61, ODTR 0062
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
IL/ Israel	-I	a	36, 40, 44, 48 52, 56, 60, 64	200 mW EIRP 200 mW EIRP	In In	5.15-5.25 5.25-5.35	MOC
		b/g	1-13	100 mW EIRP	Both	2.4-2.4835	
ILO/ Israel OUTDOOR	-I	a	36, 40, 44, 48 52, 56, 60, 64	200 mW EIRP 200 mW EIRP	In In	5.15-5.25 5.25-5.35	MOC
		b/g	5-13	100 mW EIRP	Both	2.4-2.4835	

Table B-1 Supported Country Codes (continued)

Country Code/ Country	1000 Series Access Point Regulatory Domain	802.11 Bands	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Indoor/ Outdoor Use	Frequency Range (GHz)	Regulatory Authority
IN/ India	-N	a	N/A	N/A	N/A	N/A	WPC
		b/g		4 W EIRP	In	2.4-2.4835	
IS/ Iceland	-E	a	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	PTA
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
IT/ Italy	-E	a	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	Ministry of Comm
		b/g	1-11	100 mW EIRP	In	2.4-2.4835	
J1/ Japan	-P	a	36, 40, 44, 48, 52, 56, 60, 64	10 mW/MHz~200 mW	In	5.15-5.25 5.25-5.35	Telec/ARIB STD-T71
		b	1-14	10 mW/MHz~200 mW EIRP	Both	2.4-2.497	Telec/ARIB STD-T66
		g	1-13	10 mW/MHz~200 mW EIRP	Both	2.4-2.497	
JP/ Japan	-J	a	1-3 34, 38, 42, 46	10 mW/MHz~200 mW 10 mW/MHz~200 mW	Both In	5.03-5.09 5.15-5.25	Telec/ARIB STD-T71
		b	1-14	10 mW/MHz~200 mW EIRP	Both	2.4-2.497	Telec/ARIB STD-T66
		g	1-13	10 mW/MHz~200 mW EIRP	Both	2.4-2.497	
KE/ Republic of Korea	-K	a	36, 40, 44, 48 52, 56, 60, 64 100,104,108,112 116, 120, 124 149, 153, 157, 161	2.4 mW/MHz+6 dBi 10 mW/MHz+7 dBi 10 mW/MHz+7 dBi 150 mW+6 dBi~600 mW	In Both Both Both	5.725-5.825	RRL/ MIC Notice 2003-13
		b/g	1-13	150 mW+6 dBi~600 mW	Both	2.4-2.4835	
KR/ Republic of Korea	-C	a	149, 153, 157, 161	150 mW+6 dBi~600 mW	Both	5.725-5.825	RRL/ MIC Notice 2003-13
		b/g	1-13	150 mW+6 dBi~600 mW	Both	2.4-2.4835	

Table B-1 Supported Country Codes (continued)

Country Code/ Country	1000 Series Access Point Regulatory Domain	802.11 Bands	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Indoor/ Outdoor Use	Frequency Range (GHz)	Regulatory Authority
LT/ Lithuania	-E	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both Both	5.15-5.25 5.25-5.35 5.725-5.85	LTR
		b/g	1-11	1 W+Restricted Antennas	Both	2.4-2.4835	
LU/ Luxembourg	-E	a	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	ILR
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
LV/ Latvia	-E	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both Both	5.15-5.25 5.25-5.35 5.725-5.85	(tbd)
		b/g	1-11	1 W+Restricted Antennas	Both	2.4-2.4835	
MY/ Malaysia	-E	b/g	1-13	100 mW EIRP	In	2.4-2.5	CMC
NL/ Netherlands	-E	a	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	Radiocom Agency
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
NO/ Norway	-E	a	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	NPT
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
NZ/ New Zealand	-N	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both Both	5.15-5.25 5.25-5.35 5.725-5.85	RSM
		b/g	1-11	1 W+Restricted Antennas	Both	2.4-2.4835	
PH/ Philippines	-A	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both Both	5.15-5.25 5.25-5.35 5.725-5.85	FCC Part 15
		b/g	1-11	1 W Conducted Output	Both	2.4-2.4835	

Table B-1 Supported Country Codes (continued)

Country Code/ Country	1000 Series Access Point Regulatory Domain	802.11 Bands	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Indoor/ Outdoor Use	Frequency Range (GHz)	Regulatory Authority
PL/ Poland	-E	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	200 mW EIRP 1 W EIRP	In Both	2.4-2.4835	Office of Telecom & Post
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
PT/ Portugal	-E	a	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	NCA
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
SE/ Sweden	-E	a	36, 40, 44, 48 52, 56, 60, 64 104, 108, 112, 116, 120, 124, 128, 132, 140	200 mW EIRP 200 mW EIRP 1 W EIRP	In In Both	5.15-5.25 5.25-5.35 5.47-5.725	PTS
		b/g	1-11	100 mW EIRP	Both	2.4-2.4835	
SG/ Singapore	-S	a	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161	200 mW EIRP 200 mW EIRP 1 W EIRP	Both Both Both	5.15-5.25 5.25-5.35 5.725-5.85	IDA/ TS SSS Issue 1
		b/g	1-13	200 mW EIRP	Both	2.4-2.4835	
SI/ Slovenia	-E	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both Both	5.15-5.25 5.25-5.35 5.725-5.85	ATRP
		b/g	1-11	1 W+Restricted Antennas	Both	2.4-2.4835	
SK/ Slovak Republic	-E	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both Both	5.15-5.25 5.25-5.35 5.725-5.85	Telecom Admin.
		b/g	1-11	1 W+Restricted Antennas	Both	2.4-2.4835	
TH/ Thailand	-R	a	N/A	N/A	N/A	5.725-5.875	PDT
		b/g	1-13	100 mW EIRP	In	2.4-2.5	
TW/ Taiwan	-T	a	56, 60, 64, 100-140 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both	5.25-5.35 5.47-5.725 5.725-5.825	PDT
		b/g	1-13	1 W EIRP	Both	2.4-2.4835	

Table B-1 Supported Country Codes (continued)

Country Code/ Country	1000 Series Access Point Regulatory Domain	802.11 Bands	Channels Allowed	Maximum Transmit Power (Radio Tx + Antenna Gain = EIRP)	Indoor/ Outdoor Use	Frequency Range (GHz)	Regulatory Authority
US/ United States of America	-A	a	36, 40, 44, 48 52, 56, 60, 64 149, 153, 157, 161	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W 1 W+6 dBi=4 W	In Both Both	5.15-5.25 5.25-5.35 5.725-5.85	FCC Part 15
		b/g	1-11	1 W Conducted Output	Both	2.4-2.4835	
USE/ United States of America	-A	a	36, 40, 44, 48 52, 56, 60, 64	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W	In Both	5.15-5.25 5.25-5.35	FCC Part 15
		b/g	1-11	1 W Conducted Output	Both	2.4-2.4835	
USL/ United States of America LOW	-A	a	36, 40, 44, 48 52, 56, 60, 64	50 mW+6 dBi=200 mW 250 mW+6 dBi=1 W	In Both	5.15-5.25 5.25-5.35	FCC Part 15
		b/g	1-11	1 W Conducted Output	Both	2.4-2.4835	
ZA/ South Africa	-E	a	N/A	N/A	N/A	5.25-5.35 5.725-5.825	(tbd)
		b/g	1-13	1 W EIRP	Both	2.4-2.4835	

A

B

C

D

E

F

H

I

L

M

N

O

P

R

S

T

U

V

W