



Data Sheet

CiscoWorks Wireless LAN Solution Engine

Organizations are adopting wireless LANs (WLANs) to increase business productivity and accessibility. Network managers need an integrated solution that provides them with the control they need to effectively manage and secure their WLANs. The Cisco® Integrated Wireless Network cost-effectively addresses the WLAN security, deployment, and management issues facing enterprises. It integrates and extends wired and wireless networks to deliver scalable, manageable, and secure WLANs with the lowest total cost of ownership. The Cisco Integrated Wireless Network provides the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations expect from their wired LANs.

The Cisco Integrated Wireless Network is an evolution of the Cisco Structured Wireless-Aware Network (SWAN) available from Cisco since 2003. The Cisco Integrated Wireless Network includes two secure, enterprise-class WLAN solutions: the Cisco Distributed WLAN Solution and the Cisco Centralized WLAN Solution.

CiscoWorks Wireless LAN Solution Engine (WLSE) and CiscoWorks WLSE Express play a key role in the Cisco Distributed WLAN Solution for managing Cisco Aironet® access points. CiscoWorks WLSE can centrally manage hundreds to thousands of Cisco Aironet access points for medium-sized to large enterprises and wireless vertical markets. CiscoWorks WLSE helps to simplify and automate the deployment and security of WLANs, to ensure their smooth operation and dependability. CiscoWorks WLSE also provides WLAN IDS capabilities for detecting WLAN intrusions such as rogue access points, ad-hoc networks, and excess management frames on the air that typically signal a WLAN attack.

Also available is the CiscoWorks Wireless LAN Solution Engine Express (WLSE Express), for small and midsize-business or enterprise branch-office WLAN deployments of up to 100 Cisco Aironet access points. CiscoWorks WLSE Express includes the same WLAN management features of CiscoWorks WLSE, plus an integrated and embedded user authentication and authorization server, making it an ideal solution for remote branch-office deployments with limited WAN bandwidth. Please refer to the CiscoWorks WLSE Express data sheet for more details.

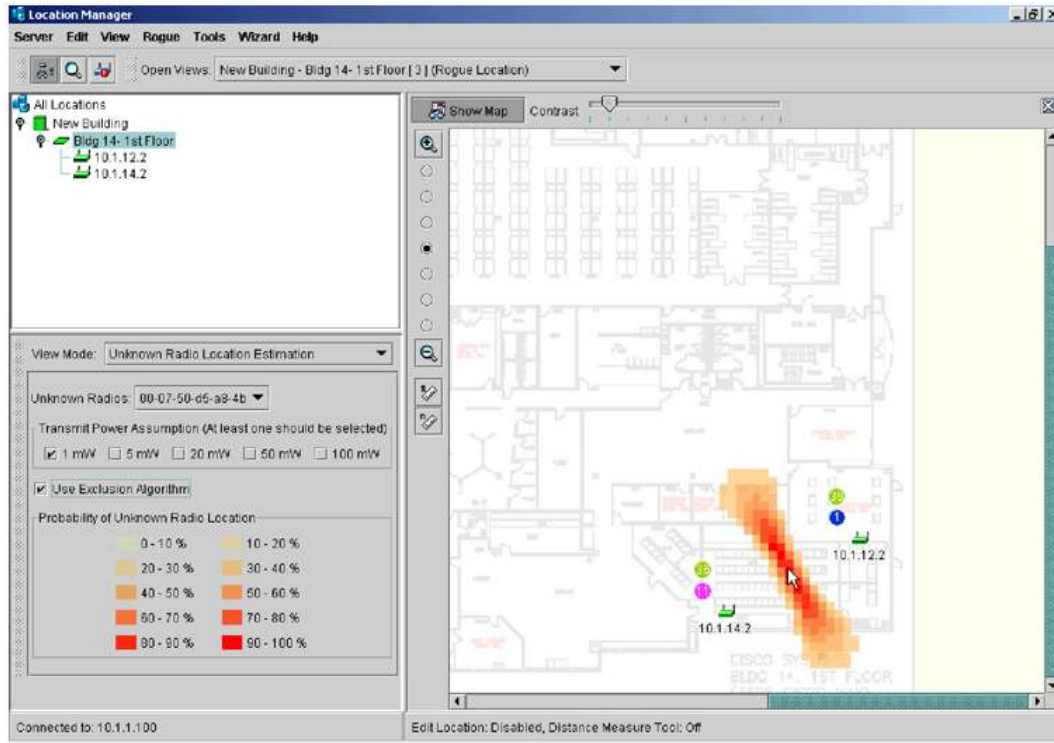
Product Overview

CiscoWorks WLSE is a centralized network management solution for managing the entire Cisco Aironet WLAN infrastructure. As the management component of the Cisco Distributed WLAN Solution, CiscoWorks WLSE provides comprehensive air/radio frequency (RF) and device-management capabilities in ways that simplify deployment, reduce operational complexity, and provide administrators visibility into the WLAN. By automating several RF and device-management tasks, CiscoWorks WLSE reduces the costs and time needed for WLAN deployment, management, and security.

By using Cisco Aironet access points as air/RF monitors, CiscoWorks WLSE provides WLAN intrusion detection and protection. As part of the WLAN Intrusion Detection System (IDS), CiscoWorks WLSE quickly detects, locates (Figure 1), and disables unauthorized (rogue) access points, helping to ensure that security policies are applied consistently throughout the network. CiscoWorks WLSE further enhances the security of the WLAN by monitoring for unplanned (ad-hoc or peer-to-peer) networks, unauthorized WLAN client networks, client spoofing, and other WLAN attacks that may introduce security openings in the network. These capabilities can benefit any organization, including those that have not formally deployed WLANs but want to guard against intruders.

Figure 1

CiscoWorks WLSE Location View Displays Rouge Access-Point Location



CiscoWorks WLSE provides dynamic RF management through self-healing, which enables a Cisco Aironet access point to adjust its cell-coverage area automatically when an adjacent access point becomes disabled or fails. It also helps optimize performance by detecting and locating RF interference while proactively monitoring usage and faults.

CiscoWorks WLSE's deployment wizard allows administrators to effortlessly deploy access points by creating contextual configurations that are automatically installed into access points as they are plugged into the network. Specific access point configurations can be applied depending on flexible deployment criteria. Device (AP/Bridge)-specific settings such as hostname, radio power, and channel can be imported into CiscoWorks WLSE via a comma separated (CSV) file, with unique Ethernet MAC addressing mapping. This allows CiscoWorks WLSE to automatically apply device-specific settings without touching each AP for configuring device-specific parameters. This reduces deployment times, increases security and configuration consistency, while reducing user-caused configuration errors.

CiscoWorks WLSE may be transparently integrated with other network management systems, operations support systems, and CiscoWorks applications through syslog messages, Simple Network Management Protocol (SNMP) traps, and an Extensible Markup Language (XML) interface. CiscoWorks WLSE's secure HTML-based user interface provides access anywhere, including through firewalls.

Key Features and Benefits

Deployment

CiscoWorks WLSE speeds deployment by automating configuration and setup, reducing the overall cost to provision WLANs. The result is superior return on investment and enhanced productivity.

- *Automatic access-point configuration* – CiscoWorks WLSE can automatically discover and configure newly deployed autonomous Cisco Aironet access points using Dynamic Host Configuration Protocol (DHCP), with the flexibility to assign different configurations based on the access-point device type, its source subnet, and its software version. CiscoWorks WLSE provides an easy-to-use deployment wizard to specify the configuration criteria up front. This allows administrators to automate deployment and simultaneously maintain control in rapidly expanding environments. The deployment wizard also simplifies and automates the setup of the Wireless Domain Services (WDS) that plays an important role in the Cisco Distributed WLAN Solution for seamless mobility and RF aggregation services. For deployments that use Cisco Aironet access points as a WDS device, CiscoWorks WLSE can automatically designate a WDS access point and apply the right configuration to it without requiring manual setup.
- *Assisted site surveys* – Complete and reliable WLAN coverage is achieved only with a detailed site survey. Site surveys are essential during deployment, and they should be performed regularly thereafter to address changes in the environment. Site surveys once required special knowledge and were both expensive and time-consuming. Most organizations contracted with outside consultants, but CiscoWorks WLSE helps IT managers to perform cost-effective site surveys in-house without being experts in RF propagation and measurement. The assisted site survey tool automatically determines optimal frequency selection, transmit power, and other settings, which the administrator can then apply. The coverage areas can be defined to cover only specified areas. CiscoWorks WLSE also provides an automated re-site survey that periodically assesses the performance of the network with respect to baseline site-survey settings. When radio settings in the network are no longer optimal, CiscoWorks WLSE generates a notification allowing the administrator to quickly apply newer, more optimal radio settings.

Operations

CiscoWorks WLSE automates a wide range of repetitive, time-consuming tasks, simplifying the management of Cisco Aironet access points and bridges to enhance productivity for network administrators.

- *Centralized firmware updates* – Access point and bridge firmware may be updated in mass. Updates may be assigned to a specific device or to groups. Tasks may be scheduled or executed on demand.
- *Mass configuration changes* – Configuring a group with hundreds of devices requires no more effort than configuring a single device. Configuration tasks may be scheduled or executed on demand. CiscoWorks WLSE supports all the configuration settings available on Cisco Aironet access points, including Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) security settings. Configuration updates are done using Secure Shell (SSH) Protocol. Specific RF settings such as channel and power, as recommended by the CiscoWorks WLSE Site Survey Wizard, can also be applied to devices based on a schedule.
- *Dynamic grouping* – The Device Groups feature makes administering the WLAN more effective and intuitive. Devices may be organized into hierarchical groups defined by the administrator. Groups may span multiple subnets.
- *Automated discovery* – CiscoWorks WLSE automatically discovers Cisco Aironet access points, bridges, and switches connected to access points using Cisco Discovery Protocol. Discovery may be scheduled or run on demand.
- *Configuration archive* – The CiscoWorks WLSE is able to store the last four configuration versions for each managed access point, allowing configuration tasks to be undone.
- *VLAN configuration* – VLANs on access points may be configured and monitored, allowing differentiation of LAN policies and services, such as security and quality of service, for different users on enterprise and public-access VLANs.

- *Multiple Basic Service Set Identifier (MBSSID) support* – CiscoWorks WLSE supports the configuration of multiple broadcast Service Set Identifiers (SSIDs). It supports up to eight broadcast SSIDs per access point radio.
- *Customizable thresholds* – Administrators may define different faults and performance thresholds for specific sites and groups accompanied by specific actions and fault priorities. A centralized fault screen simplifies quick resolution of problems. Various WLAN health indicators such as network load, RF usage, errors, and client associations can be monitored.
- *Fault status* – CiscoWorks WLSE provides a centralized tree view of all access points and device groups. Color coding and group icons indicate fault status. Faults may be filtered and sorted by priority to facilitate viewing and resolving problems.
- *Fault notification* – Fault notification and forwarding are implemented with syslog messages, SNMP traps, and e-mail.
- *Switch monitoring* – Switches connected to access points are monitored for availability and the utilization of ports, CPU, and memory.

Security and WLAN Intrusion Detection

Organizations need to protect their RF environment and data networks from unauthorized access. Unauthorized (rogue) access points installed by employees or intruders create security breaches that put the entire network at risk. WLAN IDS quickly detects, locates, and automatically shuts down rogue access points. CiscoWorks WLSE provides effective rogue access-point switch-port tracing by monitoring and using the clients that are associated to rogue access points, thus providing a means to contain the rogue access point by shutting down the switch port connected to the rogue access point. Rogue access points can be filtered by Received Signal Strength Indicator (RSSI) threshold to avoid triggering alarms for access points that might be in a neighboring network. CiscoWorks WLSE will also periodically monitor for changes in the status of rogue access points that are marked “Friendly” to alert the administrator in case its location and RSSI values change.

CiscoWorks WLSE detects unauthorized WLANs, and locates and identifies which wireless clients are participating in the network. It also detects clients spoofing authorized MAC addresses and generates notifications. CiscoWorks WLSE monitors per-channel excess wireless management frames such as excess association, disassociation, probe requests, responses, and authentication and deauthentication frames that may signal WLAN attacks such as denial-of-service and “man-in-the-middle” attacks. EAP over LAN (EAPOL) flood-message monitoring provides a means to detect excess authentication requests by an intruder.

CiscoWorks WLSE provides a WLAN IDS dashboard that acts as a launch pad for all WLAN IDS features. The dashboard provides a summary of all WLAN IDS alarms. In addition, it displays WLAN IDS reports pertaining to rogue access points, unauthorized networks, and unregistered clients, which can be exported using comma-separated value (CSV), PDF, and XML formats. These reports provide detailed information including the estimated location of the WLAN IDS fault, which access point detected it, its channel, and its basic service set identifier (BSSID). Administrators can select and enable specific WLAN IDS events they are interested in through a WLAN IDS profile. These WLAN IDS profiles can be customized per location to provide greater flexibility and control. Notifications can be sent through e-mail, syslog, or SNMP trap messages.

WLAN IDS protection can be tailored to suit individual needs:

- *Integrated WLAN IDS* – Standard Cisco Aironet access points are deployed with the radio (IEEE 802.11a, b, or g) placed in multifunction mode to service client devices and to provide WLAN intrusion monitoring. Intrusion detection information is gathered from the access points that scan the RF environment. Optionally, Cisco client cards and Cisco compatible client devices provide additional information about the RF environment. Rogue access-point detection, unauthorized WLAN detection, and excess management-frame detection are supported using the integrated WLAN IDS.
- *Dedicated WLAN IDS* – A dedicated access-point-only WLAN is deployed with the access-point radio (802.11a, b, or g) placed in radio scan mode to support WLAN intrusion monitoring. Access points configured for dedicated IDS do not support clients. This solution provides continuous monitoring of the RF environment. Active-but-unassociated client device monitoring is supported to minimize the risk

of clients associating to rogue access points and to protect the network from malicious intruders probing the RF environment for weaknesses.

Other security features of CiscoWorks WLSE include:

- *Security policy monitoring* – All access points on the network are monitored for consistent application of security policies. Alerts are generated for violations and can be delivered by e-mail, syslog, or SNMP trap notifications. Several policies including SSIDs, security schemes (Open, EAP), encryption, and telnet and HTTP settings can be monitored for enforcement.
- *Monitoring of IEEE 802.1X server availability* – IEEE 802.1X Extensible Authentication Protocol (EAP) servers, including Cisco Secure access control servers (ACSs), are monitored for response time. Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), Protected EAP (PEAP), and generic RADIUS authentication types are supported.
- *Secure user interface* – CiscoWorks WLSE provides a secure HTML-based user interface that may be accessed anywhere, even through firewalls. In addition to the Web-based GUI, a command-line interface (CLI) like that in Cisco IOS® Software provides direct console, Telnet, or SSH access for basic configuration and troubleshooting. CiscoWorks WLSE communicates with access points using HTTP Secure Sockets Layer (SSL) sessions for management.
- *Role-based access model* – CiscoWorks WLSE has a flexible, role-based user access model. For example, help-desk personnel can be limited to viewing reports and faults. Several common authentication modules are supported, including TACACS+, RADIUS, and Microsoft NT Domain authentication.

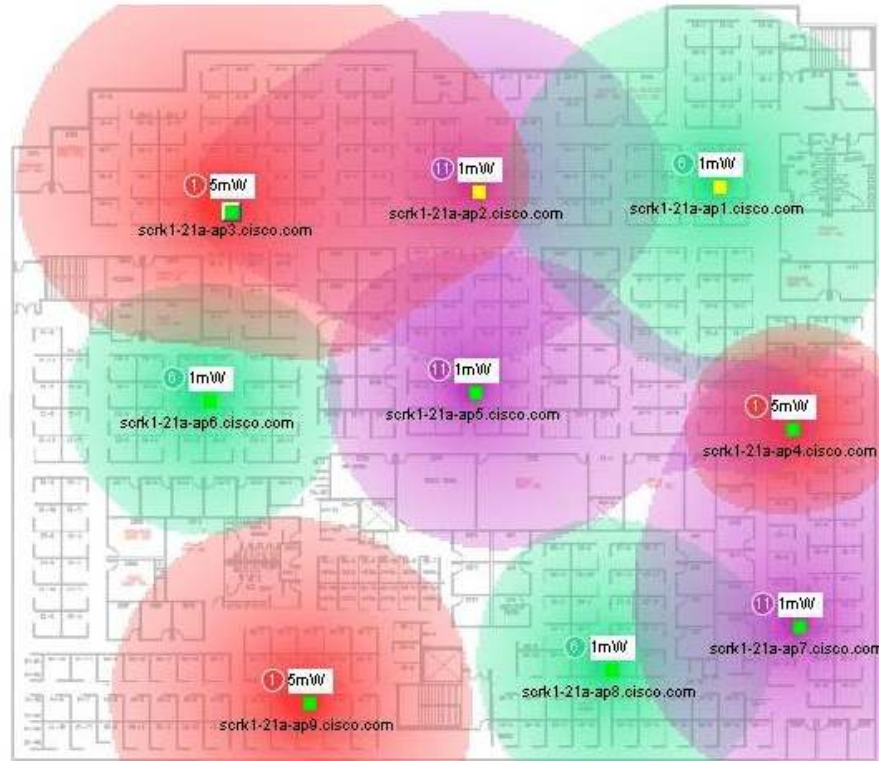
Performance Optimization and High Availability

Interference detection and location is critical to maintaining a reliable WLAN. RF measurements sent to CiscoWorks WLSE include measurements for both 802.11 and non-802.11 interference. If the interference exceeds an administrator-defined threshold, a fault is generated so that the administrator can quickly locate and suppress the source of the interference.

- *Air/RF scanning and monitoring* – Cisco Aironet access points are multifunctional, with built-in RF scanning and measurement capabilities. CiscoWorks WLSE analyzes these RF measurements, provides notification if performance degrades, and displays air/RF coverage (Figure 2). It also analyzes RF measurements from Cisco Aironet and Cisco compatible client devices. Client air scanning and monitoring provide 10 to 20 times more RF measurement data than access-point RF measurements alone. Because WLAN clients can freely move about all areas of a building, the addition of client scanning and monitoring extends RF monitoring into areas most likely to contain rogue access points while allowing for more accurate detection.

Figure 2

Assisted Site Survey, Access-Point Scan Mode



- *Interference detection* – CiscoWorks WLSE catalogs the physical location of all managed access points and creates a site map of the WLAN installation. This allows the wireless-aware network to detect points of interfering RF energy that affect network performance. The source of this energy could be a rogue access point or a device that operates in the same frequency range, such as a cordless telephone or leaky microwave oven. Interference detection and location is critical to maintaining a reliable WLAN. Administrators can define thresholds to generate fault notifications when detected interference levels are exceeded.
- *Self-healing WLANs* – CiscoWorks WLSE can detect and compensate for an access point that has failed by automatically increasing the power and cell coverage of surrounding access points. The self-healing process provides contiguous coverage to maximize the available coverage of the WLAN and minimize client impact.
- *Automated re-site surveys* – CiscoWorks WLSE automatically reassesses radio throughput and performance to provide notification if performance falls below administrator-defined thresholds. New optimal settings can be found by running the site survey wizard, and can then be applied to the network.
- *Support for 802.11h/Dynamic Frequency Selection* – When Cisco Aironet 802.11a access points detect radar transmission on the same channel, they change the frequency to not interfere with the radar frequency. CiscoWorks WLSE will be notified of this and update its RF data model and Location Manager GUI coverage display to reflect the changes.
- *Warm standby redundancy* – CiscoWorks WLSE supports redundancy through a primary and backup mechanism. If the primary WLSE fails, the backup WLSE automatically takes over. Data such as performance data, fault messages, and radio scans between the primary and backup WLSE is synchronized on a user-defined interval to minimize the loss of collected data when a backup WLSE takes over. A notification is generated during the switchover.

Reporting, Trending, Planning, and Troubleshooting

Real-time client tracking is a powerful tool for troubleshooting client network-access issues. Using only a client name, username (supported for Cisco LEAP and PEAP), or MAC address, it is easy to determine which access point a client is associated to in real time. In addition, the previous 10 associations for the client and associated access points can be accessed to aid in troubleshooting.

CiscoWorks WLSE provides several reports to monitor the health of the network. Information about network usage, client association and usage, historical and current client-usage statistics, Cisco Aironet access point Ethernet and radio interfaces status, and error details are displayed in both graphical and tabular form. Reports may be generated both at the individual device level and the group level. All reports may be scheduled, delivered by e-mail, or exported in CSV, XML, and PDF formats.

CiscoWorks WLSE also provides comprehensive coverage display overlaid on floor maps to provide visibility into the RF environment. The CiscoWorks WLSE Location Manager tool can display a graphical view of radio coverage by data rate and signal strength. CiscoWorks WLSE also supports RF management for directional antennas. Details about device settings, including channel and power, can be overlaid on the coverage display.

Integration

When network faults are detected or user-defined performance thresholds are exceeded, CiscoWorks WLSE can generate notifications through SNMP trap and syslog messages. Integration with third-party network management systems is provided through these event messages. As part of the CiscoWorks network management product line, CiscoWorks WLSE integrates with the CiscoWorks LAN Management Solution (LMS) and other CiscoWorks applications to increase the efficiency of managing a converged wired and wireless network. Device inventory and credentials, for example, can be imported or exported between CiscoWorks WLSE and CiscoWorks LMS's Resource Manager Essentials (RME) tool, an application that provides broad network management for a wide range of Cisco devices. If desired, device discovery may be turned off to allow automatic inventory synchronization with CiscoWorks RME. CiscoWorks WLSE uses the same default user roles as CiscoWorks LMS, but it allows customization. CiscoWorks WLSE can be launched from the CiscoWorks LMS desktop.

CiscoWorks WLSE also provides an XML API for exporting data and for third-party integration. Devices in the network, detected faults and alarms, reports, and information collected from the network using SNMP can be exported to other external systems for customization.

CiscoWorks WLSE itself is a manageable device which supports SNMP MIB-II. CPU and memory utilization of CiscoWorks WLSE can be monitored using SNMP.

Features and Benefits

Table 1 summarizes the features and benefits of CiscoWorks WLSE.

Table 1. Features and Benefits

Feature	Benefit
WLAN IDS with rogue access-point detection, switch-port shutdown, client MAC spoofing, and WLAN attack detection	Eliminates security threats posed by malicious intruders and by employee-installed unauthorized access points
Automated Cisco Aironet access point deployment using the CiscoWorks WLSE deployment wizard	Allows for rapid deployment and expansion of the WLAN
Interference detection	Notifies administrators quickly about conditions that may affect network performance
Self-healing adjusts cell coverage area to compensate for disabled or failed access points	Increases WLAN availability and optimizes WLAN performance
Assisted site survey tool	Assisted site surveys performed by IT personnel reduce the costs, skills, and time required to make optimal radio settings for best network performance

Feature	Benefit
Automated re-site surveys	Maintains peak WLAN performance and reliable WLAN coverage by periodically reassessing the performance of optimal settings in the network
Automated configuration and bulk firmware updates	Simplifies daily operations and management
Access point and bridge security-policy misconfiguration detection and alerts	Enhances security by monitoring consistency throughout the network
Proactive fault and performance monitoring	Increases WLAN availability
Access-point-group usage reports	Fast troubleshooting improves user satisfaction
XML data export	Facilitates integration with third-party applications

Supported Cisco Devices

For up-to-date device support information, please visit:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

Technical Specifications

Table 2 outlines the technical specifications for CiscoWorks WLSE.

Table 2. Technical Specifications

	CPU	Intel Pentium IV processor, 3.2 GHz
Core Logic	Front side bus	800 MHz
Drives	Hard drives	One 80-GB SATA hard drive
	CD-ROM drive	Slim type, low-profile IDE CD-ROM drive
	Disk drive	One 3.5-inch, 1.44-MB disk drive
Ports	Serial	One 9-pin connector
	USB	One USB connector in front and two in rear
	RJ-45	Two RJ-45 connectors for connection to two 10/100/1000 Ethernet controllers
Power	AC power supply wattage	280W
	AC power supply voltage	100–127V at 47–63 Hz; 200–240V at 47–63 Hz
	System battery	CR2032 3V lithium coin cell
Physical	Rack mountable	1 rack unit
	Height	1.68 in.
	Width	16.8 in.
	Depth	21.5 in.
	Weight	28.6 lb (13 kg) maximum
Environmental	Operating temperature	50 to 95°F (10 to 35°C)
	Storage temperature	–40 to 149°F (–40 to 65°C)



Supported Web Browsers

CiscoWorks WLSE is accessible through the following browsers:

- Mozilla 1.6
- Microsoft Internet Explorer 6.0 with Service Pack 1

Ordering Information

To place an order, contact your Cisco Systems® sales representative. For more information, go to <http://www.cisco.com/go/wlse> and <http://www.cisco.com/go/integratedwireless>.

**Corporate Headquarters**

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

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Aironet, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks or 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) KW/LW9278 09/05

