

Cisco Wireless LAN Controllers

Figure 1. Cisco 2000 Series and 4400 Series Wireless LAN Controllers



Cisco 2000 Series Wireless LAN Controller



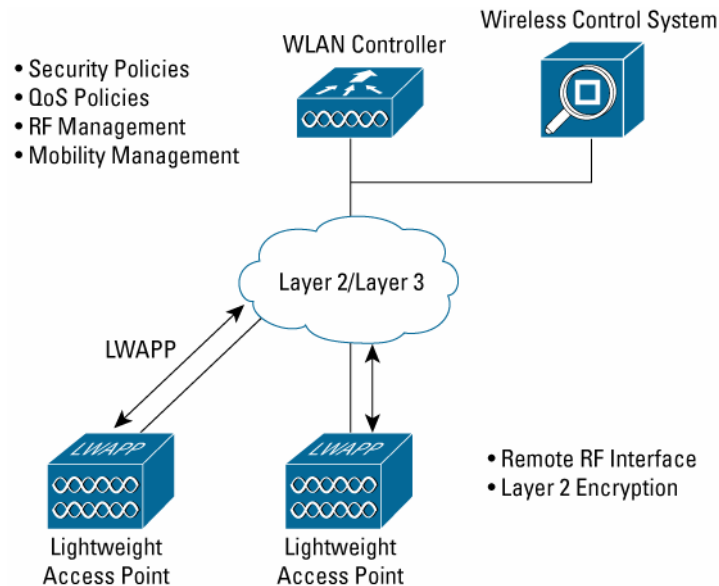
Cisco 4400 Series Wireless LAN Controller

PRODUCT OVERVIEW

Cisco[®] wireless LAN controllers are ideal for enterprise and service provider wireless LAN deployments and provide system-wide wireless LAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Cisco lightweight access points and Cisco Wireless Control System (WCS) Software to support business-critical wireless applications. From voice and data services to location tracking, WLAN controllers provide the control, scalability, and reliability that IT managers need to build secure, enterprise-scale wireless networks—from branch offices to outdoor campuses.

Cisco wireless LAN controllers smoothly integrate into existing enterprise and service provider networks. They communicate with Cisco lightweight access points over any Layer 2 (Ethernet) or Layer 3 (IP) infrastructure using the Lightweight Access Point Protocol (LWAPP) (Figure 2). This emerging IETF standard helps ensure that communication between access points and wireless LAN controllers remains secure, and it enables important wireless LAN configuration and management functions to be completely automated for cost-effective wireless LAN operations.

Figure 2. Centralized Wireless LAN



Cisco wireless LAN controllers enable enterprises to create and enforce policies for an end-to-end wireless LAN system that supports business critical applications. Multiple WLAN Controllers automatically discover each other and seamlessly coordinate WLAN services across themselves. In this way, Cisco wireless LAN controllers work together as a single, seamless system to deliver a scalable WLAN network with thousands of APs. From voice and data services to location tracking, Cisco wireless LAN controllers provide the control, scalability, and reliability that IT managers need to build secure, large-scale wireless networks.

Flexible Deployment Options

Cisco Systems offers several wireless LAN controllers that address different enterprise deployment scenarios. These include the Cisco 2000 Series and 4400 Series.

The Cisco 2000 Series delivers Cisco's award-winning wireless LAN services to small and medium-sized enterprise environments. It supports up to six lightweight access points, making it a cost-effective solution for smaller buildings. With integrated Dynamic Host Control Protocol (DHCP) services and zero-touch access point configuration, the Cisco 2000 Series is also ideal for environments with limited onsite IT support, such as branch offices within a distributed enterprise.

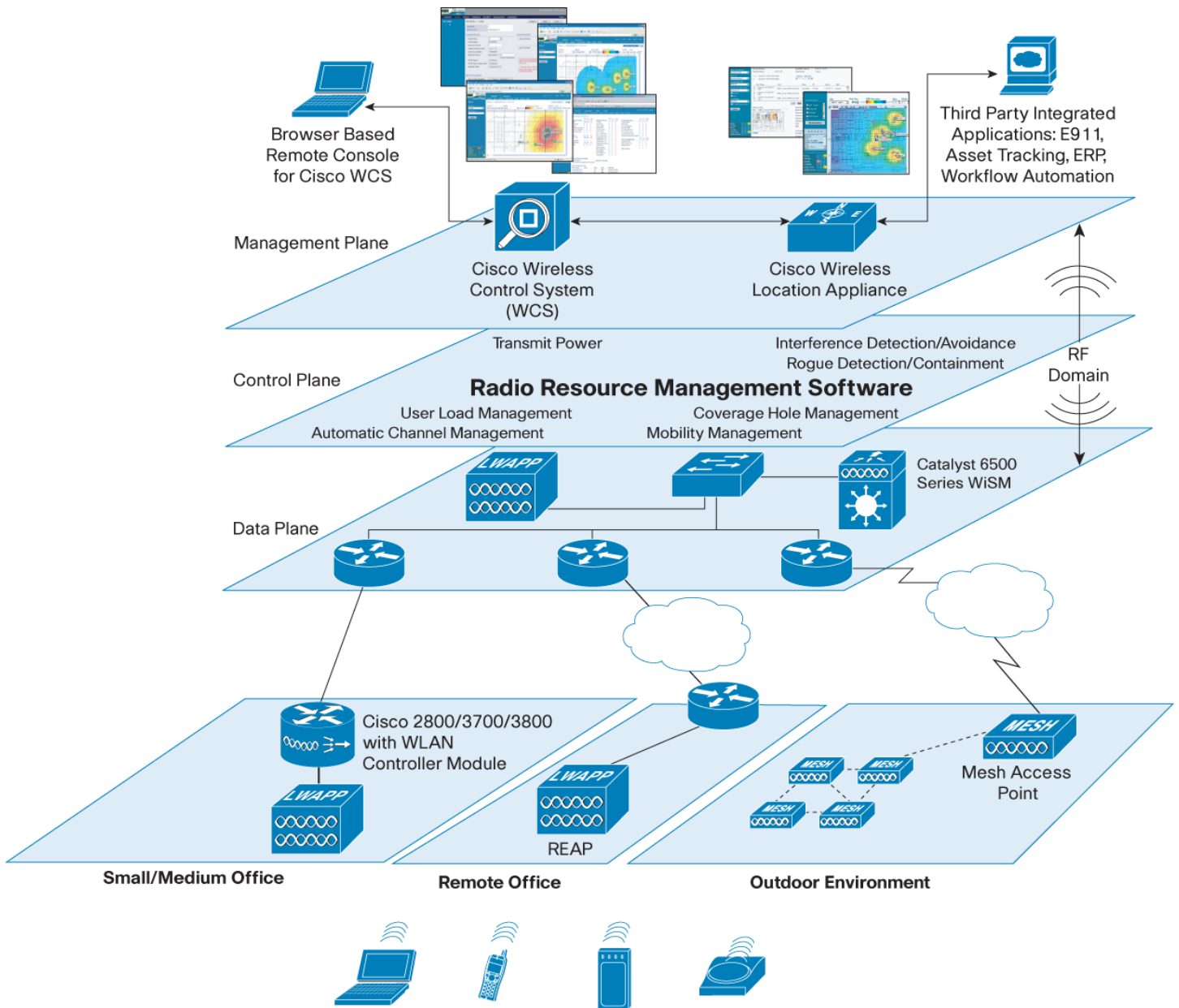
The Cisco 4400 Series Wireless LAN Controller is designed for medium to large size facilities and is available in two models—the 4402 with two Gigabit Ethernet ports comes in configurations that support 12, 25, and 50 access points, and the 4404 with four Gigabit Ethernet ports supports 100 access points. The 4402 provides one expansion slot and the 4404 provides two expansion slots that can be used to add VPN termination today, as well as enhanced functionality in the future. In addition, each 4400 WLAN Controller supports an optional redundant power supply to ensure maximum availability.

Wireless LAN controllers are also available for the Cisco Catalyst 6500 and Integrated Services Routers. For more information on Cisco Catalyst 6500 (WiSM), visit <http://www.cisco.com/en/US/products/ps6526/index.html>. For more information on Integrated Service Routers (WLCM), visit http://www.cisco.com/en/US/products/hw/modules/ps2797/products_data_sheet0900aecd80364432.html.

Intelligent RF Management

All Cisco WLAN controllers come equipped with embedded software for adaptive real-time RF management. The Cisco WLAN system uses patent pending Radio Resource Management (RRM) algorithms that detect and adapt to changes in the air space in real-time. These adjustments create the optimal topology for wireless networking in much the same way that routing protocols compute the best possible topology for IP networks.

Figure 3. Network Wide RF Intelligence



Specific intelligent RF capabilities managed by Cisco wireless LAN controllers include:

- **Dynamic channel assignment**—802.11 channels are adjusted to optimize network coverage and performance based on changing RF conditions.
- **Interference detection and avoidance**—The system detects interference and recalibrates the network to avoid performance problems.
- **Load balancing**—The system provides automatic load balancing of users across multiple access points for optimum network performance, even under heavy load.
- **Coverage hole detection and correction**—Radio Resource Management (RMM) software detects coverage holes and attempts to correct them by adjusting the power output of access points.
- **Dynamic power control**—The system dynamically adjusts the power output of individual access points to accommodate changing network conditions, helping to ensure predictable wireless performance and availability

Airtight Security

Cisco wireless LAN controllers adhere to the strictest level of security standards, including:

- 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, and Wired Equivalent Privacy (WEP)
- 802.1X with multiple Extensible Authentication Protocol (EAP) types—Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS), EAP with Tunneled TLS (EAP-TTLS), EAP-FAST, EAP-SIM and Cisco LEAP
- VPN termination—optional module for the 4400 Series that provides IP Security (IPSec) VPN termination

The result is the industry's most comprehensive wireless LAN security solution.

In the Cisco wireless LAN architecture, access points act as air monitors, communicating real-time information about the wireless domain to wireless LAN controllers. All security threats are rapidly identified and presented to network administrators via Cisco WCS, where accurate analysis can take place and corrective action can be taken.

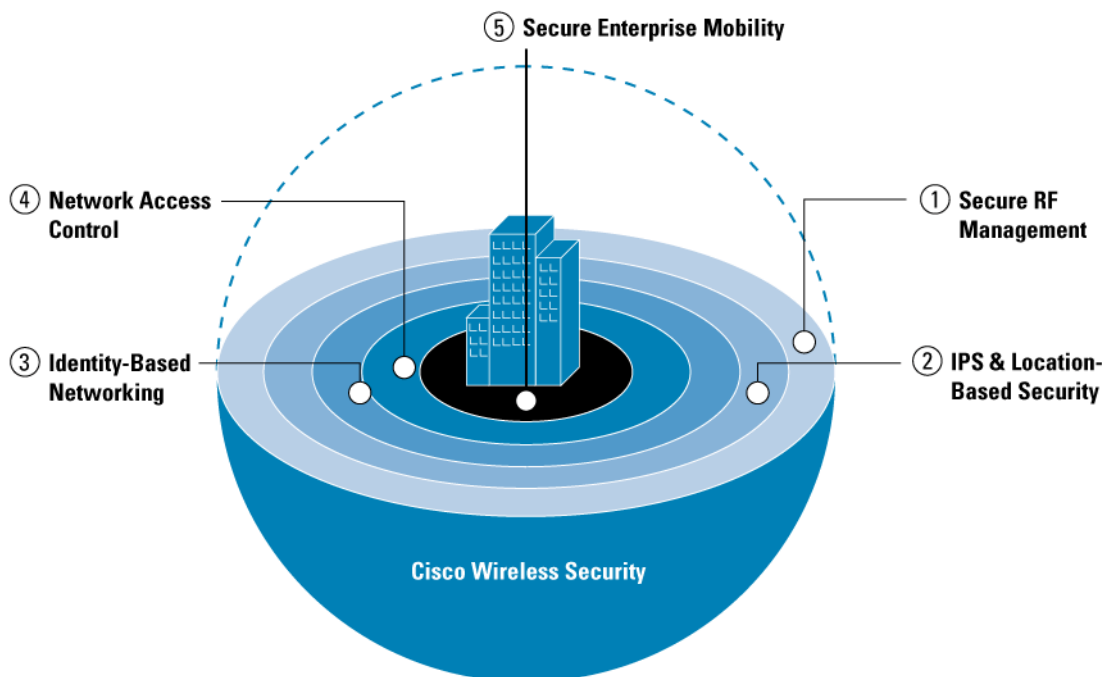
Cisco provides the only wireless LAN system that offers simultaneous wireless protection and wireless LAN service delivery. This helps to ensure complete wireless LAN protection, with no unnecessary overlay equipment costs or extra monitoring devices. The Cisco wireless LAN system can be deployed initially as a standalone wireless intrusion prevention system, and reconfigured later to add Wireless LAN data service. This allows network managers to create a “defense shield” around their RF domains, containing unauthorized wireless activity until they are ready to deploy wireless LAN services.

Cisco addresses wireless LAN security by offering multiple layers of protection, including:

- **RF security**—Detect and avoid 802.11 interference and control unwanted RF propagation
- **Wireless LAN intrusion prevention and location**—The Cisco wireless LAN system not only detects rogue devices or potential wireless threats, but also locates these devices. This enables system administrators to quickly assess the threat level and take immediate action to mitigate threats as required.
- **Identity-based networking**—IT staff must support many different user access rights, device formats, and application requirements when securing wireless LANs. The Cisco wireless LAN system enables enterprises to deliver individualized security policies to wireless users or groups of users. These include:
 - Layer 2 security—802.1x (PEAP, TLS, TTLS, FAST, SIM, LEAP), WPA, 802.11i (WPA2)
 - Layer 3 security (and above)—IPSec, web authentication
 - VLAN assignments
 - Access control lists (ACLs)—IP restrictions, protocol types, port, and differentiated services code point (DSCP) value
 - QoS—multiple service levels, bandwidth contracts, traffic shaping and RF utilization
 - Authentication, Authorization, and Accounting (AAA)/RADIUS—User session policies and rights management
- **Network Admission Control (NAC)**—Enforce policies pertaining to client configuration and behavior, to ensure that only end-user devices with appropriate security utilities can gain access to the network.

- **Secure mobility**—Maintain the highest level of security in mobile environments. This includes VPNs that follow users as they move, eliminating the need to re-establish secure tunnels. In addition, Cisco has developed Proactive Key Caching (PKC), an extension to the 802.11i standard and precursor to the 802.11r standard that facilitates secure roaming with AES encryption and RADIUS authentication.
- **Guest tunneling**—Provides additional security for access to the corporate network by guest users. It ensures that guest users are unable to access the corporate network without first passing through the corporate firewall.
- **Secure backhaul**—Encrypts data traffic over wireless backhaul links for additional security.

Figure 4. Multiple Layers of Wireless LAN Protection



Real-Time Application Support

The Cisco wireless LAN system provides best-in-class performance to support real-time applications such as voice. Cisco wireless LAN controllers enable rapid handoff between access points and multiple controllers, providing smooth mobility with no interruption in service to the client. Intelligent queuing and contention management schemes provide effective resource management of the air space. In addition, Cisco wireless LAN controllers support PKC for real-time performance and mobility when using 802.11i security. Cisco also supports QoS capabilities that are Wi-Fi Multimedia (WMM)-compliant.

Mobility

Cisco wireless LAN controllers allow users to roam between and within indoor and outdoor environments, across access points, switches, and even across routed subnets. Security and QoS context information follows users wherever they roam, helping to ensure that mobility does not compromise performance, reliability, or privacy. Cisco wireless LAN controllers do not require any modifications to existing infrastructures or client devices to enable mobility (Mobile IP, for example). As a result, Cisco wireless LAN systems are easy to deploy, and cost-effective to own and operate.

Reliability

Cisco delivers the highest level of reliability for mission-critical wireless networks. In the event of an access point failure, wireless LAN controllers automatically adjust power on adjacent access points to cover the area where the failed access point provided service. In the event of an individual controller failure, access points automatically find a backup wireless LAN controller to keep wireless service available. Cisco wireless LAN controllers can be deployed in an N+1 redundant topology, allowing enterprises to scale their wireless networks while knowing that they are protected from both hardware and software disruptions. Only the Cisco wireless LAN solution allows users to control wireless deployment costs without sacrificing reliability. The Cisco 4400 Series supports redundant power supplies ensuring system operation even if a power supply fails.

FEATURES AND BENEFITS

Table 1 lists the features and benefits of Cisco wireless LAN controllers.

Table 1. Features and Benefits of Cisco Wireless LAN Controllers

Feature	Benefits
Scalability	Scalable architecture provides business-critical wireless services for locations of all sizes
Integrated Radio Resource Management (RRM)	Create an intelligent RF control plane for self-configuration, self-healing, and self-optimization
Zero-Configuration Deployment	The system is deployed without modifying existing routing and switching infrastructures, and without configuring access points
Multilayered Security	Flexible security policies adapt to changing corporate security needs
Intrusion Detection, Location, and Containment	Integrated wireless intrusion protection preserves the integrity of wireless networks and sensitive corporate information
Mobility Management	Intersubnet roaming without special client software facilitates device management; no changes to core routing infrastructure makes roaming easy
Reliability	Automated recovery from lightweight access point and Wireless LAN controller failures maximizes the availability of the wireless network
Intuitive Management Interfaces	Better visibility and control of the air space reduces operational cost

SUMMARY

The Cisco Wireless LAN Controller is ideal for enterprise and service provider wireless LAN deployments. It simplifies deployment and operation of wireless networks, helping to ensure smooth performance, enhance security, and maximize network availability. The Cisco Wireless LAN Controller manages all of the Cisco lightweight access points within campus environments and branch locations, eliminating complexity and providing network administrators with visibility and control of their wireless LANs.

PRODUCT SPECIFICATIONS

Table 2 lists the product specification for Cisco 2000 Series and 4400 Series wireless LAN controllers.

Table 2. Product Specifications for Cisco 2000 Series and 4400 Series Wireless LAN Controllers

Item	Specification
Wireless	IEEE 802.11a, 802.11b, 802.11g, 802.11d, 802.11h
Wired/Switching	<p>2000 Series:</p> <ul style="list-style-type: none"> • IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, and IEEE 802.1Q VLAN tagging <p>4400 Series:</p> <ul style="list-style-type: none"> • IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, IEEE 802.1Q VLAN tagging, and IEEE 802.1D Spanning Tree Protocol
Data RFCs	<ul style="list-style-type: none"> • RFC 768 UDP • RFC 791 IP • RFC 792 ICMP • RFC 793 TCP • RFC 826 ARP • RFC 1122 Requirements for Internet Hosts • RFC 1519 CIDR • RFC 1542 BOOTP • RFC 2131 DHCP
Security Standards	<p>2000 Series:</p> <ul style="list-style-type: none"> • Wi-Fi Protected Access (WPA) • IEEE 802.11i (WPA2, RSN) • RFC 1321 MD5 Message-Digest Algorithm • RFC 2104 HMAC: Keyed Hashing for Message Authentication • RFC 2246 TLS Protocol Version 1.0 • RFC 3280 X.509 PKI Certificate and CRL Profile <p>4400 Series:</p> <ul style="list-style-type: none"> • WPA • IEEE 802.11i (WPA2, RSN) • RFC 1321 MD5 Message-Digest Algorithm • RFC 1851 The ESP Triple DES Transform • RFC 2104 HMAC: Keyed Hashing for Message Authentication • RFC 2246 TLS Protocol Version 1.0 • RFC 2401 Security Architecture for the Internet Protocol • RFC 2403 HMAC-MD5-96 within ESP and AH

Item	Specification
	<ul style="list-style-type: none"> • RFC 2404 HMAC-SHA-1-96 within ESP and AH • RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV • RFC 2406 IPSec • RFC 2407 Interpretation for ISAKMP • RFC 2408 ISAKMP • RFC 2409 IKE • RFC 2451 ESP CBC-Mode Cipher Algorithms • RFC 3280 Internet X.509 PKI Certificate and CRL Profile • RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec • RFC 3686 Using AES Counter Mode with IPSec ESP
Encryption	<p>2000 Series:</p> <ul style="list-style-type: none"> • WEP and TKIP-MIC: RC4 40, 104 and 128 bits (both static and shared keys) • Secure Sockets Layer (SSL) and TLS: RC4 128-bit and RSA 1024- and 2048-bit • AES: CCM, CCMP <p>4400 Series:</p> <ul style="list-style-type: none"> • WEP and TKIP-MIC: RC4 40, 104 and 128 bits (both static and shared keys) • SSL and TLS: RC4 128-bit and RSA 1024- and 2048-bit • AES: CCM, CCMP • IPSec: DES-CBC, 3DES, AES-CBC
AAA	<ul style="list-style-type: none"> • IEEE 802.1X • RFC 2548 Microsoft Vendor-Specific RADIUS Attributes • RFC 2716 PPP EAP-TLS • RFC 2865 RADIUS Authentication • RFC 2866 RADIUS Accounting • RFC 2867 RADIUS Tunnel Accounting • RFC 2869 RADIUS Extensions • RFC 3576 Dynamic Authorization Extensions to RADIUS • RFC 3579 RADIUS Support for EAP • RFC 3580 IEEE 802.1X RADIUS Guidelines • RFC 3748 Extensible Authentication Protocol • Web-based authentication

Item	Specification
Management	<ul style="list-style-type: none"> • SNMP v1, v2c, v3 • RFC 854 Telnet • RFC 1155 Management Information for TCP/IP-Based Internets • RFC 1156 MIB • RFC 1157 SNMP • RFC 1213 SNMP MIB II • RFC 1350 TFTP • RFC 1643 Ethernet MIB • RFC 2030 SNTP • RFC 2616 HTTP • RFC 2665 Ethernet-Like Interface types MIB • RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions • RFC 2819 RMON MIB • RFC 2863 Interfaces Group MIB • RFC 3164 Syslog • RFC 3414 User-Based Security Model (USM) for SNMPv3 • RFC 3418 MIB for SNMP • RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs • Cisco private MIBs
Management Interfaces	<ul style="list-style-type: none"> • Web-based: HTTP/HTTPS • Command-line interface: Telnet, SSH, serial port
Interfaces and Indicators	<p>2000 Series:</p> <ul style="list-style-type: none"> • Console port: RS-232 (DB-9 male, DTE interface) • Network: Four 10/100 Mbps Ethernet (RJ-45) <ul style="list-style-type: none"> – LED indicators: link, activity • Other indicators: Power <p>4400 Series:</p> <ul style="list-style-type: none"> • Uplink: 2 (4402) or 4 (4404) 1000Base-X transceiver slots <ul style="list-style-type: none"> – LED indicators: link, activity • Service Port: 10/100 Mbps Ethernet (RJ45) <ul style="list-style-type: none"> – LED indicators: link, activity • Utility Port: 10/100/1000 Mbps Ethernet (RJ45) <ul style="list-style-type: none"> – LED indicators: link, activity • Expansion Slots: 1 (4402) or 2 (4404) • Console Port: RS232 (DB-9 male, DTE interface) • Other Indicators: Status, Alarm, Power Supply 1, Power Supply 2

Item	Specification
Physical and Environmental	<p>2000 Series:</p> <ul style="list-style-type: none"> • Dimensions (W x D x H): 9.5 x 6.0 x 1.6 in. (241 x 152 x 41 mm) • Weight: 2.45 lb (1.11 kg) • Temperature: <ul style="list-style-type: none"> – Operating: 32 to 104°F (0 to 40°C) – Storage: –13 to 158°F (–25 to 70°C) • Humidity: <ul style="list-style-type: none"> – Operating humidity: 10 to 95 percent, noncondensing – Storage humidity: Up to 95 percent • Power adapter: <ul style="list-style-type: none"> – Input power: 100 to 240 VAC; 50/60 Hz – Output power: +5V @ 3A; +12V @ 1A; 27W – Heat Dissipation: 92 BTU/hour <p>4400 Series:</p> <ul style="list-style-type: none"> • Dimensions (WxDxH): 17.45 x 15.75 x 1.75 in. (443 x 400 x 44.5 mm) • Weight: 15.3 lbs (6.95 kg) with 2 power supplies • Temperature: <ul style="list-style-type: none"> – Operating: 32 to 104°F (0 to 40°C) – Storage: –13 to 158°F (–25 to 70°C) • Humidity: <ul style="list-style-type: none"> – Operating humidity: 10 95%, non-condensing – Storage humidity: up to 95% • Input power: 100 240 VAC; 50/60 Hz; 0.43 A at 110 VAC, 0.23 A at 220 VAC; 50W. Redundant power option available. • Heat Dissipation: 171 BTU/hour
Regulatory Compliance	<p>2000 Series:</p> <ul style="list-style-type: none"> • CE Mark • Safety: <ul style="list-style-type: none"> – UL 60950-1:2003 – EN 60950:2000 • EMI and susceptibility (Class B): <ul style="list-style-type: none"> – U.S.: FCC Part 15.107 and 15.109 – Canada: ICES-003 – Japan: VCCI – Europe: EN 55022, EN 55024 <p>4400 Series:</p>

Item	Specification
	<ul style="list-style-type: none"> • CE Mark • Safety: <ul style="list-style-type: none"> – UL 60950-1:2003 – EN 60950:2000 • EMI and susceptibility (Class A): <ul style="list-style-type: none"> – U.S.: FCC Part 15.107 and 15.109 – Canada: ICES-003 – Japan: VCCI – Europe: EN 55022, EN 55024
Warranty	One year

ORDERING INFORMATION

Table 3 provides ordering information for the Cisco 2000 Series and 4400 Series. To place an order, visit the Cisco Ordering Website: <http://www.cisco.com/en/US/ordering/index.shtml>

Table 3. Ordering Information for Cisco 2000 Series and 4400 Series Wireless LAN Controllers

Part Number	Product Name
AIR-WLC2006-K9	Cisco 2000 Series Wireless LAN Controller for up to six Cisco lightweight access points
AIR-WLC4402-12-K9	4400 Series WLAN Controller for up to 12 Cisco lightweight APs
AIR-WLC4402-25-K9	4400 Series WLAN Controller for up to 25 Cisco lightweight APs
AIR-WLC4402-50-K9	4400 Series WLAN Controller for up to 50 Cisco lightweight APs
AIR-WLC4404-100-K9	4400 Series WLAN Controller for up to 100 Cisco lightweight APs
AIR-PWR-4400-AC=	4400 Series WLAN Controller AC Power Supply (redundant)
AIR-VPN-4400-K9=	4400 Series WLAN Controller VPN Termination Module

SERVICE AND SUPPORT

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, visit [Cisco Technical Support Services](#) or [Cisco Advanced Services](#).

FOR MORE INFORMATION

For more information about Cisco wireless LAN controllers, contact your local account representative or visit: <http://www.cisco.com/en/US/products/ps6366/index.html>

For more information about the Cisco Unified Wireless Network framework, visit: <http://www.cisco.com/go/unifiedwireless>



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

Copyright © 2006 Cisco Systems, Inc. All rights reserved. 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, 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, 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, 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. (0601R)

