Cisco Catalyst 6500 Series/Cisco 7600 Series Wireless Services Module

Product Overview

The Cisco® Catalyst 6500 Series/Cisco 7600 Series Wireless Services Module (WiSM) provides unparalleled security, mobility, redundancy, and ease of use for business-critical wireless LANs (WLANs). It delivers the most secure wireless system available by offering centralized security policies, wireless intrusion prevention system (IPS) capabilities, award-winning RF management, quality of service (QoS), and Layer 3 fast secure roaming for WLANs. As a key component of the Cisco Unified Wireless Network for the enterprise, and Cisco Service Provider Wi-Fi (SP Wi-Fi) for service providers, the Cisco WiSM provides the control, security, redundancy, and reliability that network managers and operators need to scale and manage their wireless networks easily. (Figure 1).

Figure 1. Cisco Wireless Services Module

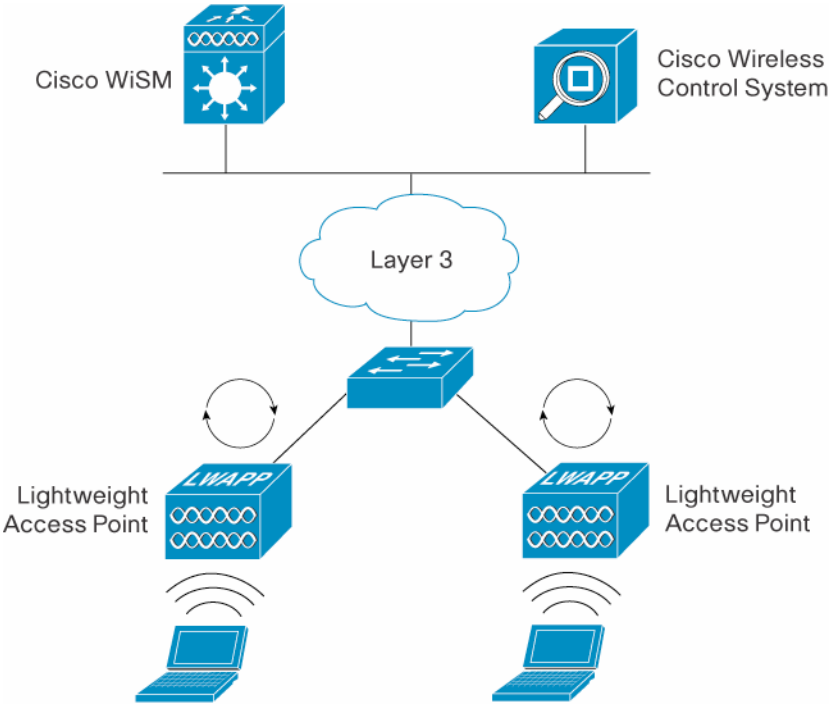
The Cisco WiSM is a member of the Cisco Wireless LAN Controller family. It works in conjunction with Cisco Aironet® access points, the Cisco Wireless Control System (WCS) and the Cisco Wireless Location Appliance to support mission-critical wireless data, voice, and video applications. It provides real-time communication between access points and other WLAN controllers to deliver a secure, end-to-end wireless solution.

The Cisco WiSM smoothly integrates into existing Cisco Catalyst® 6500 Series and Cisco 7600 Series networks. It communicates using the emerging Lightweight Access Point Protocol (LWAPP) standard to establish secure connectivity between access points and modules across Layer 3 networks. This protocol enables the automation of important WLAN configuration and management functions for cost-effective operations. With this integrated approach to large-scale wireless networking, customers can realize significant total cost of ownership benefits by streamlining support costs and reducing planned and unplanned network downtime.

Because the Cisco WiSM supports 802.11a/b/g and the IEEE 802.11n draft 2.0 standards, organizations can deploy the solution that best meets their individual requirements. Organizations can offer robust coverage with 802.11 a/b/g or deliver greater performance with five times the throughput and unprecedented reliability using 802.11n as part of an enterprise or service provider wireless solution.

The Cisco WiSM scales to deliver secure wireless access, with clustering capabilities of up to 7200 access points per roaming domain. It scales to 300 access points per module with support for 10,000+ wireless client devices. For even greater scalability, the Cisco WiSM can be deployed in conjunction with other Cisco wireless LAN controllers (Figure 2).

Figure 2. Wireless LAN with the Cisco WiSM



The Cisco WiSM enables enterprises and service providers to create and enforce policies that support business-critical applications and services. From voice and data services to location tracking, the Cisco WiSM provides the control, scalability, and reliability required to build secure 802.11 wireless networks.

Reliability

Cisco delivers the highest level of reliability for mission-critical wireless networks. In the event of an access point failure, the Cisco WiSM automatically adjusts power on adjacent access points to cover the area where the failed access point provided service. In the event of an individual Cisco WiSM failure, access points automatically find a backup Cisco WiSM on either a Cisco Catalyst 6500 Series Switch or a Cisco 7600 Series Router, or any other Cisco LWAPP-enabled platform. Multiple Cisco WiSMs can be configured to work together as a single system to deliver a scalable WLAN network with tens of thousands of client devices.

High Availability

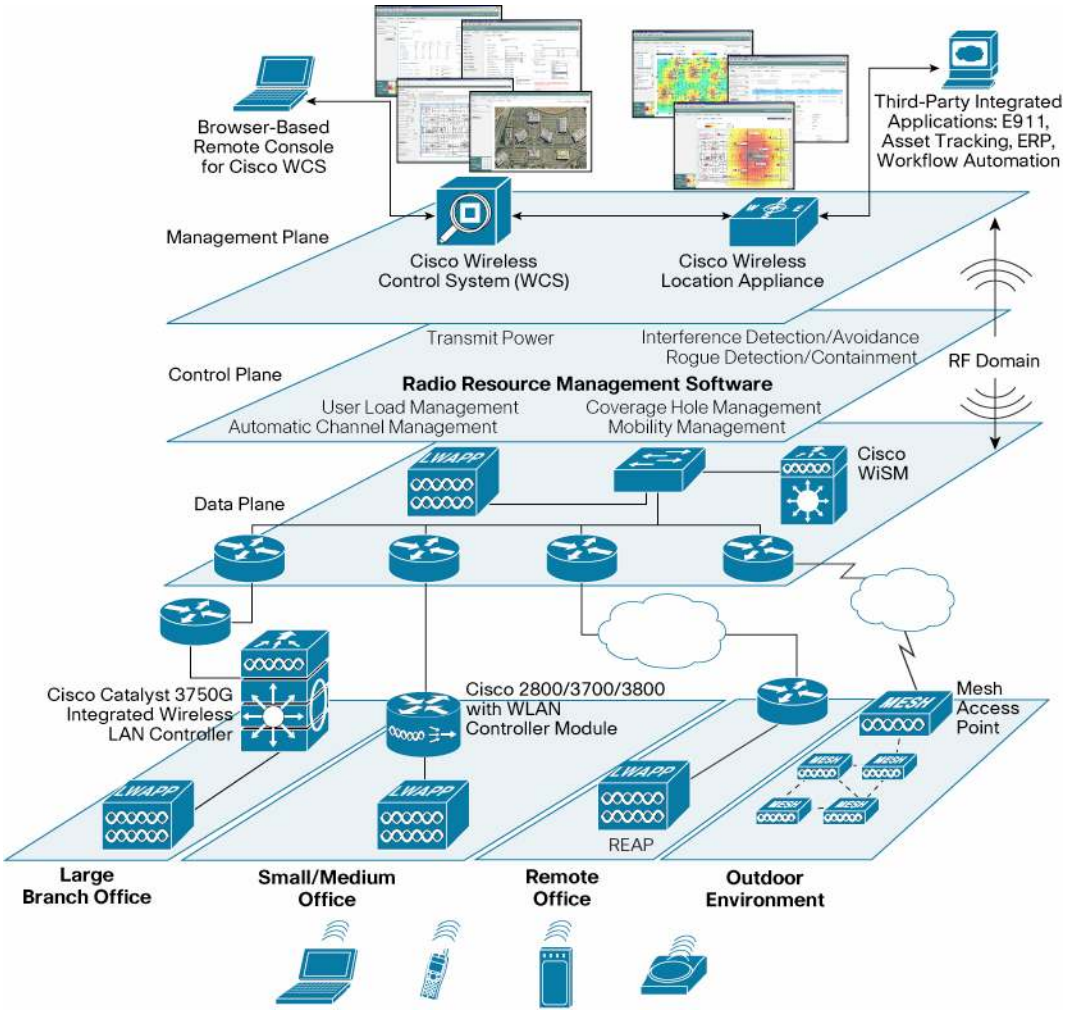
The Cisco WiSM provides multiple redundancy options and network resiliency with automated failover features, which maximizes network uptime for wireless traffic. The Cisco WiSM allows IT managers and network operators to minimize the impact of a potential wireless outage by clustering multiple Cisco WiSMs together. This reduces the failure domain size when the Cisco WiSM is deployed lower in the network hierarchy.

The Cisco WiSM supports N+1 and 1:1 redundancy topologies, allowing organizations to scale their wireless networks and protect them from both hardware and software disruptions. N+1 redundancy supports single module failure redundancy for cost-effective WLAN deployments. 1:1 redundancy supports full redundancy of each active Cisco WiSM in the network. One of the main benefits of the Cisco WLAN solution is that it allows users to control wireless deployment costs without sacrificing reliability.

Intelligent RF Management

The Cisco WiSM comes equipped with embedded software for adaptive real-time RF management. The Cisco WLAN solution uses Cisco's 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. Cisco RRM creates an intelligent RF control plane for self-configuration, self-healing, and self-optimization of the WLAN (Figure 3).

Figure 3. End-to-End RF Intelligence



Specific intelligent RF capabilities managed by the Cisco WiSM 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 a heavy load.
- **Coverage hole detection and correction:** RRM 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.

Robust Security

The Cisco WiSM adheres 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, including Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS), EAP with Tunneled TLS (EAP-TTLS), and Cisco LEAP

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

In Cisco's WLAN solution, access points act as air monitors, communicating real-time information about the wireless domain to Cisco wireless LAN controllers. All security threats are rapidly identified and presented to network administrators via Cisco WCS, where accurate analysis takes 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. This solution can be deployed initially as a standalone wireless IPS, 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.

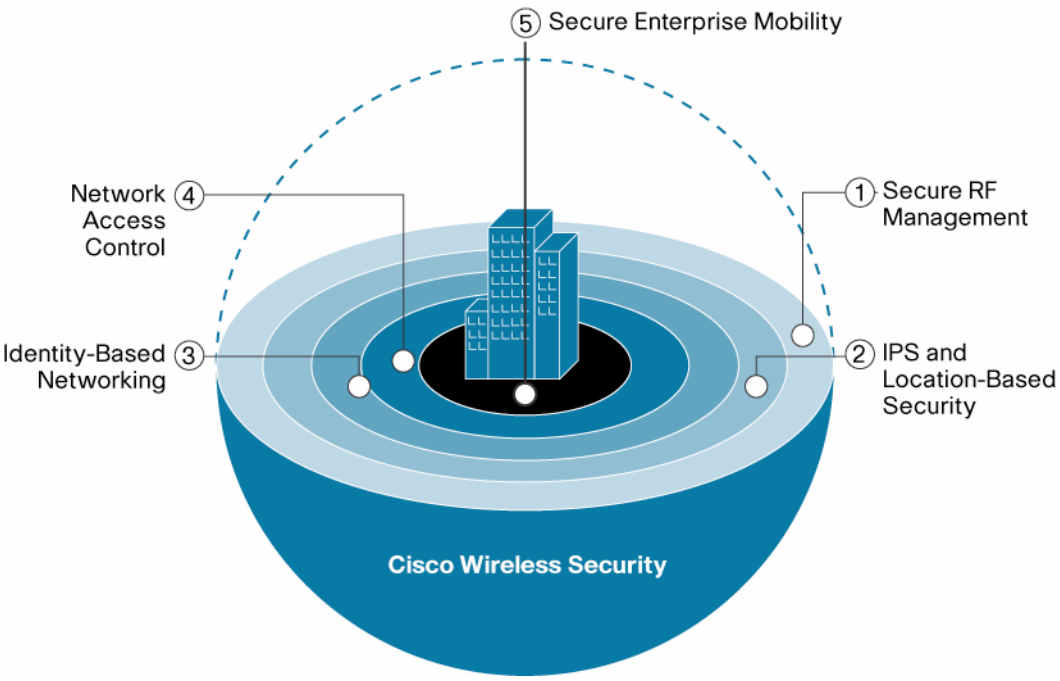
Cisco addresses wireless LAN security by offering multiple layers of protection (Figure 4), including:

- **RF security:** Detect and avoid 802.11 interference and control unwanted RF propagation.
- **Wireless LAN intrusion protection and location:** The solution not only detects rogue devices or potential wireless threats, but also locates these devices. This helps administrators to quickly assess the threat level and take immediate action to mitigate threats as required.
- **Identity-based networking:** Network managers must support many different user access rights, device formats, and application requirements when securing wireless LANs. The Cisco WLAN solution enables organizations to deliver individualized security policies to wireless users or groups of users. These include:
  - **Layer 2 security:** 802.1X (PEAP, LEAP, EAP-TTLS), WPA, 802.11i (WPA2), and Layer 2 Tunneling Protocol (L2TP)
  - **Layer 3 security (and above):** IP Security (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 authentication:** User session policies and rights management.

- **Cisco Network Admission Control (NAC):** Enforce policies pertaining to client configuration and behavior, to help ensure that only end-user devices with appropriate security utilities can gain access to the network.
- **Secure Mobility:** Maintains the highest level of security in mobile environments with Cisco Proactive Key Caching (PKC), an extension to the 802.11i standard and precursor to the 802.11r standard that facilitates secure roaming with Advanced Encryption Standard (AES) encryption and RADIUS authentication.
- **Guest tunneling:** Provides additional security for access to a corporate network by guest users. It helps ensure that guest users are able to access a corporate network only by passing through a corporate firewall.

Figure 4. Multiple Layers of Wireless LAN Protection



Real-Time Application Support

The Cisco Unified Wireless Network provides best-in-class performance to support real-time applications such as voice. Cisco WiSM enables rapid handoff between access points and multiple modules and/or controllers, providing smooth mobility with no interruption in service to the client. Intelligent queuing and contention management schemes provide effective resource management in the air space. The Cisco WiSM also supports QoS capabilities that are Wi-Fi Multimedia (WMM)-compliant and closely mirror the emerging IEEE 802.11e standard. Full compliance with the finished standard will be achieved via a software upgrade when the final standard is ratified.

Mobility

The Cisco WiSM allows users to roam between access points and across bridged and routed subnets without requiring changes to the underlying infrastructure. Security and QoS context information follows users wherever they roam, helping to ensure that mobility does not compromise performance, reliability, or privacy. The Cisco WiSM does not require any modifications to existing infrastructures or client devices to enable mobility (mobile IP, for example).

Simplified Deployment and Management

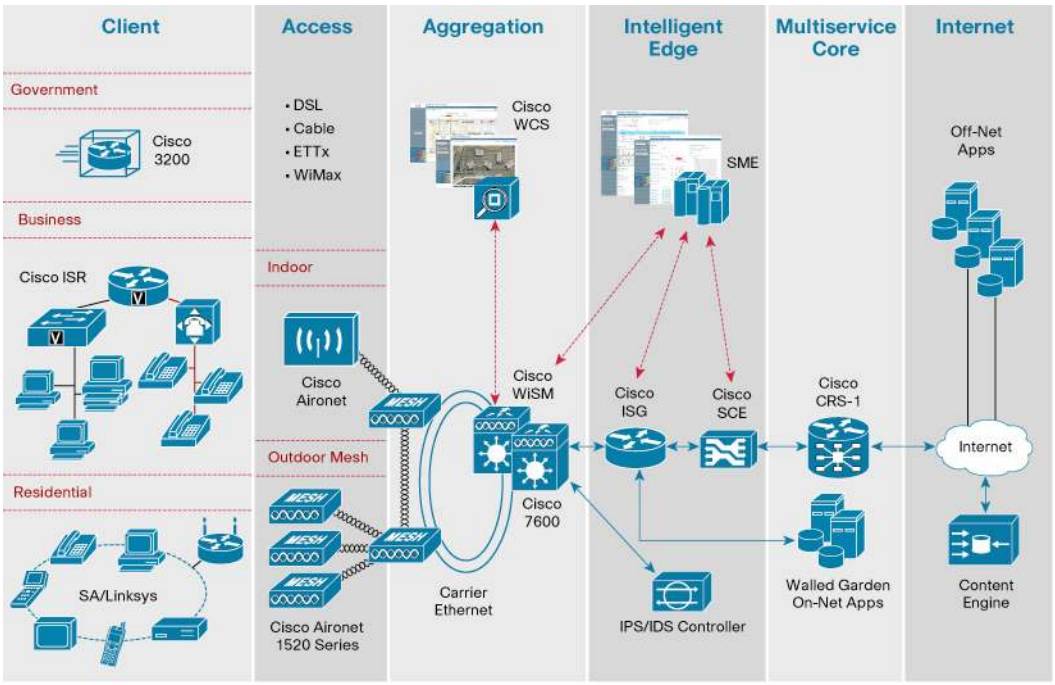
The Cisco WiSM is easy to deploy and cost-effective to own and operate. It provides maximum flexibility to deploy anywhere in the network—from access, to distribution, to the core—based upon customer business requirements. It supports zero-touch deployments that do not require manual or preconfiguration of the access points. It also supports template-based configuration management. These intuitive templates enable the quick application of systemwide security configurations, QoS policies, mobility groups, back-end services, and other important configurations via the easy-to-use, award-winning Cisco WLAN user interface.

The Cisco WiSM supports several embedded troubleshooting tools. When deployed with Cisco WCS, it supports enhanced monitoring and troubleshooting features, including intuitive heat map displays, alarm filtering, event correlation, and granular reporting tools.

Carrier-Class Outdoor Wireless Mesh

The Cisco WiSM is a key component of Cisco Service Provider Wi-Fi (SP Wi-Fi)—the outdoor wireless mesh architecture for service providers. Cisco SP Wi-Fi combines a superior wireless access network with a fully integrated and intelligent back-end network for an end-to-end architecture that securely and dynamically controls subscriber access and applications across outdoor wireless mesh networks. With Cisco SP Wi-Fi, providers can offer outdoor wireless broadband services to current and new business and government customers, all while making use of their existing Carrier Ethernet investment. This converged IP Next Generation Network platform translates into new revenue streams, reduced operating expenses, improved communication and efficiency for business customers, and better service and safety for communities.

Figure 5. Cisco WiSM -- A Key Component of Cisco SP Wi-Fi



Features and Benefits

Table 1 lists the features and benefits of the Cisco WiSM.

Table 1. Features and Benefits of the Cisco WiSM

Feature	Benefits
Integration with the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router	Embedded system delivers centralized security policies, IPS, RF management, QoS, and Layer 3 fast secure roaming for WLANs.
Scalability	Scalable architecture provides business-critical wireless services for deployments of all sizes.
Reliability	Automated recovery from failures of Cisco Aironet access points, Cisco WiSM, and Cisco Catalyst 6500 Series/Cisco 7600 Series to maximize the availability of the wireless network.
Integrated RRM	Integrated radio resource management (RRM) creates an intelligent RF control plane for self-configuration, self-healing, and self-optimization.
Zero-configuration deployment	The Cisco WiSM is deployed without the need to manually configure access points or modify existing network infrastructures.
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	Users can roam between access points and across bridged and routed subnets without requiring changes to the underlying infrastructure.
Intuitive management interfaces	Better visibility and control of the air space reduces operational costs.

Summary

The Cisco WiSM is ideal for large scale wireless LAN deployments. It eliminates the complexity of wireless networks, helping to ensure smooth performance, enhanced security, and maximized network availability. The Cisco WiSM works in conjunction with Cisco WCS and the Cisco Wireless Location Appliance to support mission-critical, wireless data, voice, and video applications. It delivers centralized security policies, IPS, RF management, QoS, and Layer 3 fast secure roaming for enterprise WLANs. As a key component of enterprise and service provider wireless solutions, the Cisco WiSM provides network administrators with the visibility and control they need to effectively manage and scale their indoor and outdoor wireless networks.

Product Specifications

Table 2 lists the product specifications for the Cisco WiSM.

Table 2. Product Specifications for the Cisco WiSM.

Item	Specification
Wireless	IEEE 802.11a, 802.11b, 802.11g, 802.11d, 802.11h, 802.11n
Wired/Switching	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	• 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	• NAC • 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 • 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 2661 L2TP • 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	• 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

Item	Specification
AAA	• 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
Management	• Simple Network Management Protocol (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	• Web-based: HTTP/HTTPS • Command-line interface: Telnet, Secure Shell (SSH), serial port
Interfaces and Indicators	• Console port: RS-232 (DB-9 male, DTE interface) • Status LED: Normal sequence, fault during initialization, environmental monitoring • Disk LED
Physical and Environmental	• Dimensions (W x D x H): 1.6 x 15.3 x 16.3 in. (4.1 x 38.9 x 41.4 cm) • Weight: 11 lbs (5 kg) • Temperature: • Operating: 32 to 104°F (0 to 40°C) • Storage: –40 to 167°F (–40 to 75°C) • Humidity: • Operating humidity: 10 to 95 percent, noncondensing • Storage humidity: Up to 95 percent • Power • 164 watts • 6.07 Amps at 42V
Regulatory Compliance	• CE Mark • Safety: • UL 60950-1:2003 • EN 60950:2000 • EMI and susceptibility (Class A): • U.S.: FCC Part 15.107 and 15.109 • Canada: ICES-003 • Japan: VCCI • Europe: EN 55022, EN 55024

Ordering Information

Table 3 provides ordering information for the Cisco WiSM. To place an order, visit the Cisco Ordering Website: http://www.cisco.com/en/US/ordering/index.shtml.

Table 3. Ordering Information for the Cisco WiSM.

Part Number	Product Name	Software Release
WS-SVC-WISM-1-K9	Cisco Wireless Services Module with support for up to 300 Cisco Aironet access points	SWISMK9-32 or later

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative 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 the Cisco WiSM, contact your local account representative or visit: http://www.cisco.com/go/wism

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

For more information about Cisco SP Wi-Fi, visit: http://www.cisco.com/go/spwifi

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Printed in USA C78-354044-07 07/11