Integrity of Information on the Move with the Cisco Secure Wireless Solution for the Campus

Today's Campus Network

Business in today's world requires a very different level of network sophistication than what was acceptable only a few years ago. Business networks must now support constant and immediate interaction, which has become a priority for employee productivity. As applications evolve from centralized to interactive, networks must support multidirectional traffic. This shift calls for a real-time network infrastructure and a reshaping of the network to become a strategic business platform.

The campus network needs to target not only availability and reliability, but also services, as business-critical network applications become increasingly interactive and traffic patterns become less predictable. To adapt to these new demands and align the network with business priorities, IT managers must make sure the campus network delivers business value on two fronts: user experience and operational excellence. The Campus Communications Fabric, a framework from Cisco® to enable the interactive campus and address the IT gaps that businesses experience, can help companies meet those objectives. Through six primary attributes—application intelligence, unified network services, integrated security, virtualization, nonstop communications, and operational manageability—the Cisco® Campus Communications Fabric provides an architecture in which products and features work together to deliver highly consistent services and policies, anywhere, any way, anytime users connect to the network.

In this paper, we focus on two attributes of the Campus Communications Fabric—unified network services and integrated security—and more specifically on secure wireless services.

Unified Network Services for Convergence and Mobility

In today's highly interactive business climate, network users must be able to access and use any application, regardless of their location (on or off campus) or their access device (personal digital assistants, laptops, mobile phones, and so on). Cisco unified network services combine and integrate the best of wireless and wired networking to deliver simple, highly secure, scalable campus access with a low total cost of ownership. With products such as the Wireless Services Module (WiSM) integrated into Cisco Catalyst® 6500 Series Switches and the Cisco 4400 Series Wireless LAN Controllers, which can be used with the full switching portfolio, Cisco can provide its services transparently to any client and simplify the integration of wireless into the wired network.

With the emergence of new wireless and unified communications services—such as voice over wireless data network, and ID and location services—unified network services become increasingly important. Unifying wired and wireless provides ease of use, high security, mobility, and redundancy for users of business-critical wireless LANs. Through unified network services, the Cisco Campus Communications Fabric improves productivity and accelerates innovation.

Integrated Security for Network Access, Resources, and Content

Many new interactive applications run in a serverless or server-assisted model in which the application traffic does not pass through the data center. The network is the first line of defense, and as such, it must contain scalable, distributed security tools and features required to protect and secure new traffic flow patterns. Enforcing security at the first point of network entry helps prevent malware from breaching firewalls, eluding intrusion detection and prevention systems, and spreading internally. For this reason, Cisco Catalyst 6500 Series switches provide integrated security capabilities via services modules for integrated intrusion detection and prevention, firewall services, and distributed denial-of-service attacks. Firewall and intrusion prevention services are also provided for the full switching portfolio via the Cisco ASA Series Adaptive Security Appliances. Such security features help address regulatory compliance by protecting corporate and customer assets.

Introduction to Wireless Security

The growth of wireless networking has blurred the traditional boundaries between trusted and untrusted networks and shifted security priorities from the network perimeter to information security. To maintain the integrity of corporate information and systems, enterprises must focus on securing mobile information and controlling the wireless environment to prevent unauthorized access.

Given the rapid growth of wireless adoption, IT organizations have to make wireless security a priority, especially for Wi-Fi based wireless LANs. Wireless LANs have three characteristics that make it critical to secure the network. First, wireless, by definition, transmits via the air and is not contained by physical boundaries. Therefore, existing perimeter security defenses, such as firewalls, can no longer effectively enforce policy controls beyond those boundaries. Second, the 802.11 protocol is well documented, widely understood, and easily available in the public domain. This pervasiveness increases the ease with which malicious attempts can be made to exploit it. Finally, Wi-Fi operates in the unlicensed frequencies of 2.4 GHz and 5 GHz, which are open for use by anyone. While the Federal Communications Commission mandates certain rules of engagement that prohibit aggressive or malicious use of the frequencies, it’s difficult to enforce such rules, which means that most unlawful use goes unpunished.

Integrity of Mobile Information

For IT organizations, protecting sensitive customer, partner, and financial information should be the primary focus of any wireless security strategy. The digitalization of information and the ubiquity of IP communications have improved productivity and business processes by facilitating immediate access to information. In an effort to control the availability and maintain the integrity of sensitive information, the government and certain industry bodies have defined regulations to help guide businesses on best practices for protecting sensitive data. The number and scope of regulations that affect any single business vary by company size and industry affiliation. But three major regulatory standards—the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry (PCI) Data Security Standard—affect a great number of businesses. Table 1 provides more information on these important standards.

Table 1. Regulatory Requirements

Regulatory	Requirements
Sarbanes-Oxley	All publicly traded companies must: • Maintain an adequate internal control structure and procedures for financial reporting • Assess the effectiveness of internal control structures
HIPAA	Requires maintenance of administrative, technical, and physical safeguards to: • Ensure the integrity and confidentiality of patient information • Protect against threats or hazards, and unauthorized uses or disclosures of patient information
PCI Data Security Standard	Any merchant (including electronic) using payment cards, must: • Build and maintain a secure network • Protect and encrypt cardholder data • Regularly monitor and test networks, including wireless networks

Although wireless security is not an explicit requirement in all three regulations, the implication is clear. Each standard proclaims the need to protect and control information, whether the information is financial data, sensitive patient records, or credit card transactions. The amount of data transmitted over wireless infrastructures will continue to increase and must be appropriately encrypted and controlled if we are to avoid unauthorized access. Further, the physical wireless environment must be monitored and secured to avoid the possibility of unauthorized access points that create “backdoor access” into corporate systems.

The Cost of a Security Breach

Regulatory compliance is important, and some regulations include a penalty component to enforce it. But the real impact of noncompliance to a business comes from the cost of a security breach, rather than from any enforcement measures. The immediate threat of fines may increase management’s awareness of the need for tighter security controls, but the less predictable cost drivers are far more compelling. According to analysis from the Gartner Group, the direct cost of a security breach of a single customer record ranges from $90 to $1,500.[1] Additional research published by Information Systems Security indicates that the impact of a public security breach on a company’s market capitalization can be significant. The study estimated that a drop in company share price attributed to a public security incident is 2.7 percent over one day, increasing to 4.7 percent over three days. [2]

The costs associated with a security breach of customer or financial data include:

- Regulatory fines
- Cost of third-party security audits
- Compensation to customers or partners
- Loss of customer confidence resulting in a decrease in future revenues
- Damage to the corporate brand
- Decrease in investor confidence
- Drop in market capitalization

[1] “Data Protection Is Less Costly Than Data Breaches,” Gartner Group, 16 September 2005.
[2] “The Financial Impact of IT Security Breaches: What Do Investors Think?” Information Systems Security, March/April 2003.

Limiting Exposure with the Cisco Secure Wireless Solution

Cisco helps companies meet their data security requirements through the Cisco Self-Defending Network. The Cisco Self-Defending Network is a long-term strategy to protect an organization's business processes by identifying, preventing, and adapting to threats from internal and external sources. This protection helps organizations take better advantage of the intelligence in their network resources, thus improving business processes and cutting costs.

Characteristics of Cisco Self-Defending Network security solutions include:

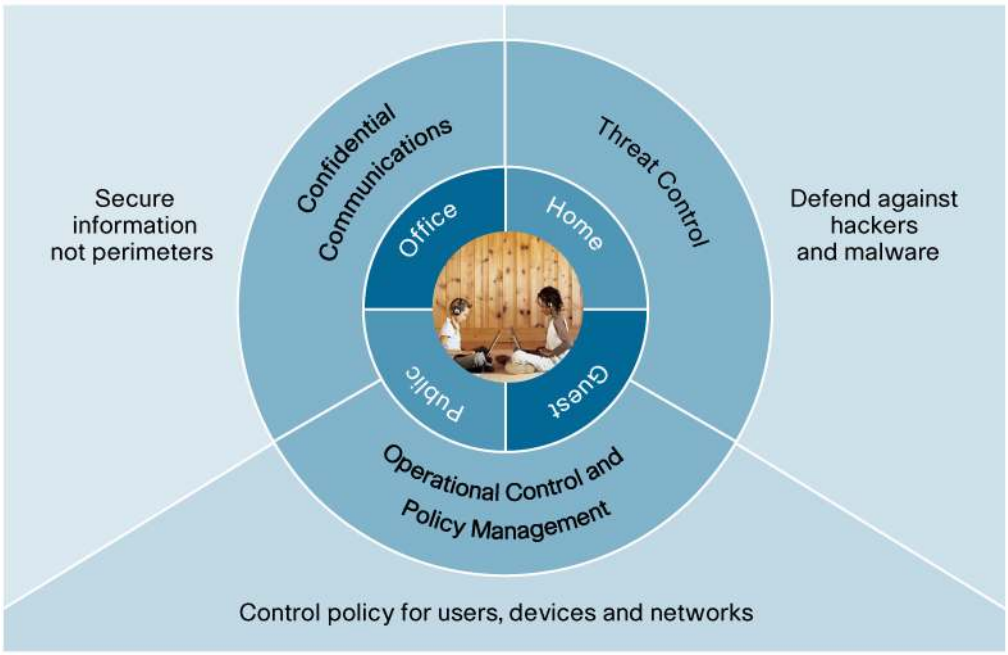
- The integration of security throughout all aspects of the network
- Collaborative processes between the various security and network elements
- The ability of the network to adapt to new threats as they arise

The self-defending methodology provides businesses with guidelines for creating a highly secure communications infrastructure and helping the business to achieve its compliance goals. To address wireless security requirements, Cisco recommends companies take an architectural approach to designing and building the wireless network.

The Cisco Secure Wireless Solution for the Campus is a scalable, comprehensive security framework that combines the Cisco Unified Wireless Network, its industry-leading portfolio of network security products that comprise the Cisco Self-Defending Network, and the Cisco Campus Communications Fabric blueprint for a real-time infrastructure that enables consistent services and policies anywhere, any way, anytime someone connects to the network. It enables confidential communications for information in transit, policy control for a variety of users and deployment scenarios, and a robust threat defense capability to protect information and systems from wireless threats (see Figure 1). It delivers a comprehensive architecture that integrates the inherent security capabilities of the Cisco Unified Wireless Network with relevant security solutions, including the Cisco NAC Appliance (Cisco Clean Access Appliance), Cisco ASA 5500 Series Adaptive Security Appliances or Catalyst 6500 Series Firewall Services Modules, Cisco ASA or Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Services Module with Cisco Intrusion Prevention System (IPS) software, Cisco Security Agent, and other components.

The Cisco Secure Wireless Solution for the Campus can be deployed using the Catalyst 3000 Series, Catalyst 4500 Series, or the Catalyst 6500 Series switches. A secure wireless architecture based on the Catalyst 6500 Series switch is highly scalable, capable of supporting up to 300 lightweight access points and more than 10,000 wireless clients per wireless services module. This architecture delivers improved operational manageability, with reduced footprint and physical cabling requirements, and helps ensure high availability through the redundancy and resiliency features of the Cisco Catalyst switch.

Figure 1. The Security Framework of the Cisco Secure Wireless Solution



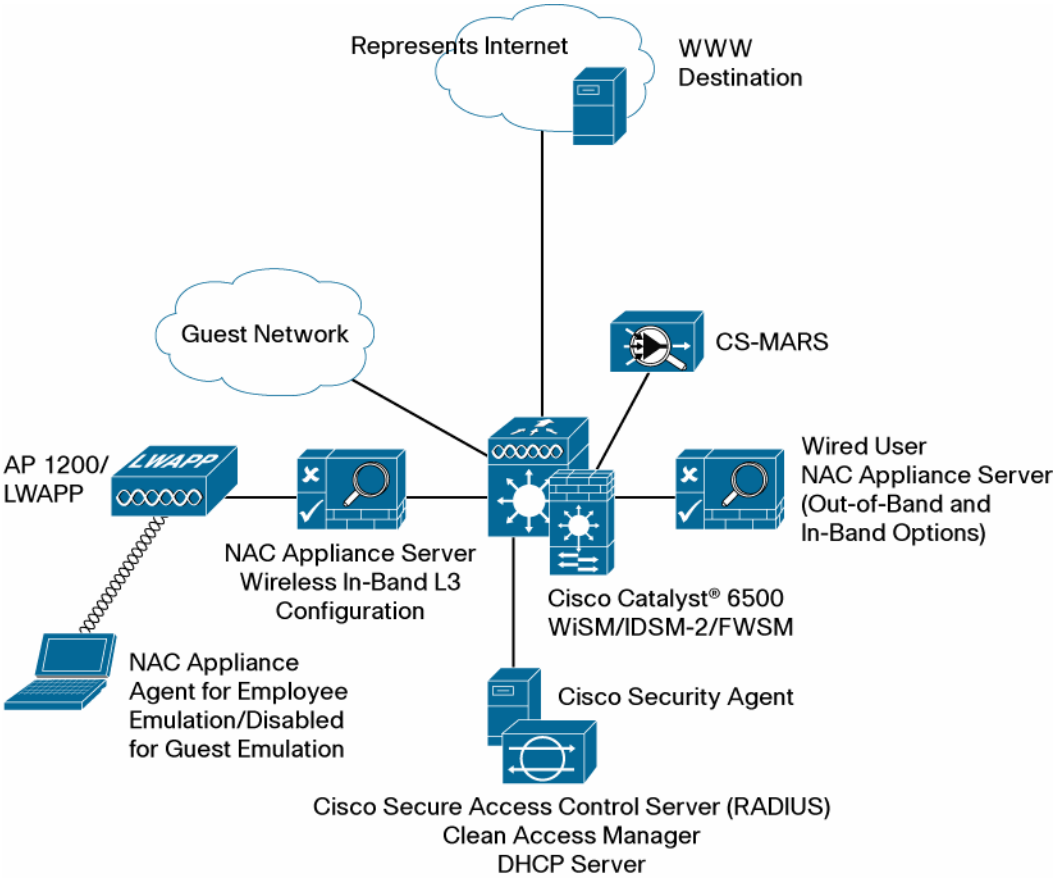
The Components of the Cisco Secure Wireless Solution

The Cisco Secure Wireless Solution is an end-to-end architecture that integrates important security and wireless solutions to deliver standards-based, industry-leading network protection (see Figure 2). The architecture combines both wired and wireless security services to present a unified suite of security capabilities that not only deliver a more robust threat defense but also lower the total cost of implementing and maintaining a highly secure wireless network.

Critical features of the Cisco Secure Wireless Solution include:

- Unified wired and wireless network intrusion prevention system/intrusion detection system (IPS/IDS)
- Client validation, posture assessment, and remediation
- Wireless single sign-on and 802.1X integration
- Granular control for secure guest access
- Host intrusion prevention
- Rogue detection via automatic RF monitoring
- Wireless security management

Figure 2. Campus Communications Fabric Integrated Secure Wireless Example Architecture



Unified Wired and Wireless Intrusion Prevention

Featured Products
• Cisco Advanced Inspection and Prevention Security Services Module or Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Services Module • Cisco ASA 5500 Firewall or Cisco Catalyst 6500 Series Firewall Services Module • Cisco Wireless LAN Controller, Cisco Catalyst 6500 Series Wireless Services Module, or Cisco Catalyst 3750G Integrated Wireless LAN Controller

The Cisco Secure Wireless Solution integrates wired and wireless intrusion detection and prevention to mitigate the threat from hackers and malicious code. The network inspects traffic flows from the IP layer up to the application layer (Layer 3 to Layer 7) and monitors for potentially harmful signatures or suspicious application behavior. In the event that it detects a signature, the wired IPS solution will alert the wireless LAN controller that the signature is originating from the wireless network. The wireless LAN controller will then issue a client shun request to the identified client and physically block its association with the access point. This integration of wired and wireless solutions offers zero-day alerting and response to potential viruses, malware, and suspect signatures.

Client Posture Assessment and Remediation

Featured Products

- Cisco NAC Appliance (Cisco Clean Access Appliance)
- Cisco 4400 Wireless LAN Controller, Cisco Catalyst 6500 Series Wireless Services Module, or Cisco Catalyst 3750G Integrated Wireless LAN Controller

The Cisco Secure Wireless Solution can validate the identity of the user and device and enforce granular policies to help ensure that the user or device is supporting the latest antivirus and spyware protection software. In the event that a client is not up-to-date, the solution will quarantine the client, isolating it from the rest of the network, until such time as the user (or administrator) can resolve the problem. This tight integration between the Cisco NAC Appliance and the Cisco Unified Wireless Network helps ensure that the wireless client adheres to the latest security policies and does not infect the network with malware obtained from external networks.

Wireless Single Sign-On

Featured Products

- Cisco NAC Appliance (Cisco Clean Access Appliance)
- Cisco 4400 Wireless LAN Controller, Cisco Catalyst 6500 Series Wireless Services Module, or Cisco Catalyst 3750G Integrated Wireless LAN Controller
- Cisco Secure Services Client
- Cisco Secure Access Control Server

The solution also takes advantage of the 802.1X authentication capabilities of the Cisco Secure Services Client to simplify the wireless user experience by allowing single sign-on to the wireless network domain as well as to the NAC appliance (for posture assessment). This feature streamlines the user experience and serves to consolidate accounting and administration while improving password management. The combination of 802.1X authentication and posture assessment helps secure the connection and protects the network from malware while being noninvasive to the user.

Secure Guest Access

Featured Products

- Cisco 4400 Wireless LAN Controller, Cisco Catalyst 6500 Series Wireless Services Module, or Cisco Catalyst 3750G Integrated Wireless LAN Controller
- Cisco ASA 5500 Series Firewall or Cisco Catalyst 6500 Series Firewall Services Module
- Cisco NAC Appliance (optional)

Businesses are experiencing increasing demand to provide network connectivity to a variety of nonemployees, including but not limited to visitors, contractors, consultants, and partners. Wireless is an optimum guest access medium given the ubiquity of Wi-Fi in laptop computers. The Cisco Secure Wireless Solution offers two levels of guest access. The baseline guest capability uses a secure tunnel from the controller within the network to a guest controller in the unsecured network area to direct guest traffic directly outside of the enterprise network. The guest controller also offers a customizable Web interface for user login and liability clauses and has a lobby ambassador feature to support variable login permissions on a per-user basis. For more advanced guest services, including the ability to define role-based access and conduct client posture assessment and remediation, the Cisco Secure Wireless Solution incorporates the Cisco NAC Appliance to supplement the inherent capabilities of Cisco wireless LAN controllers. Using Cisco ASA 5500 Series firewall products, the solution can add granular network traffic policies and enforcement for unparalleled content control.

Endpoint Wireless Use Controls

Featured Products
• Cisco Security Agent

A mobile client often connects to both trusted and untrusted networks. While IT focuses primarily on protecting the internal network from exposure to attacks brought in by these mobile clients, the client itself must also be protected. The Cisco Secure Wireless Solution incorporates wireless-acceptable use capabilities to enforce client connection policies to better protect the corporate device while connecting outside of the trusted network. The Cisco Security Agent also provides day-zero attack protection and has the ability to enforce specific wireless policies, including the following:

- Disabling the wireless network interface card when connected to the wired network
- Disabling of wireless ad hoc connections
- Enforcement of Service Set Identifier association policies
- Enablement of VPN during network connections that are not trusted

Rogue Detection and Containment

Featured Products
• Cisco Unified Wireless Network • Cisco Wireless Location Appliance

A critical component of any wireless security strategy is the use of RF monitoring capabilities to gain visibility into the wireless environment in order to prevent unauthorized use. Because so many employees are attracted to the freedom of wireless connectivity and the low cost of consumer-grade access points, rogue access points have become a common problem for many businesses. Most companies take an aggressive approach toward building a secure transport for wireless connections, and they generally base their approach on the Wi-Fi Protected Access (WPA) and WPA2 industry standards. Few companies, however, fully understand the need for comprehensive RF monitoring. Companies need RF monitoring to gain visibility into the wireless environment and to help ensure that rogue access points or malicious activity from external (or internal) parties are not creating backdoor access to their network, leaving their corporate systems exposed.

The Cisco Secure Wireless Solution integrates RF monitoring directly into the access points and offers continual, 24-hour-a-day monitoring to identify, locate, and contain unauthorized wireless activity. This capability is an essential part of any business compliance initiative to protect sensitive information.

Wireless Security Management

Featured Products
• Cisco Wireless Control System (WCS) • Cisco Security Monitoring, Analysis, and Response System (MARS)

As with any security solution, intuitive management tools are a prerequisite to maintaining a secure network. The Cisco Secure Wireless Solution uses the Cisco Wireless Control System (WCS) for wireless LAN planning, configuration, and management. Cisco WCS provides a foundation that allows IT managers to design, control, and monitor enterprise wireless networks from a central location, simplifying operations and reducing total cost of ownership. WCS will alert network managers to security threats and provide a graphical view of the network, including the location and threat level of rogue access points. In combination with WCS, the Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) recognizes and correlates real network attacks and provides actionable guidelines on how to stop them. Combined, these management capabilities provide the most comprehensive and intuitive management framework of any wireless security architecture available today.

In addition to the features already outlined, the Cisco Secure Wireless Solution incorporates industry-leading features for enhanced security. Cisco has led the industry in the development of management frame protection (MFP), a technology that increases the level of encryption for data in transit by encrypting the management frames of the 802.11 packet. When deployed in combination between the client and the infrastructure, MFP drastically reduces the threat of protocol-based attacks, including man-in-the-middle attacks.

As the number of client devices accessing the network dramatically increases, Cisco recognizes the importance of client management and security. Through the Cisco Compatible Extensions program, Cisco is able to bring security features such as MFP to companies by working with Wi-Fi silicon manufacturers to uniformly embed specific features into devices. The support for specific security features improves the overall network security and ensures simple, secure connectivity between client and infrastructure. In parallel, Cisco continues to work with the standards bodies to bring the same security features to market in an open, standards-based way.

Integrated Services and Support

To remain competitive in business, companies today need to be able to quickly address unexpected changes, opportunities, or threats that come their way. Cisco Services and Cisco Specialized Partners with expertise in Wireless LAN and Security can help your organization address today's regulatory requirements.

Our security and WLAN experts use proven Cisco tools and best practices, and can help you build an end-to-end secure WLAN infrastructure, creating a highly secure and flexible solution that addresses business challenges like PCI compliance, security, and risk management.

The Cisco Secure Wireless Solution can be deployed using an appliance model or a model based on switch-integrated service modules. Customers who choose the integrated Secure Wireless Solution with the Catalyst 6500 Series gain the additional advantage of leveraging their investment in their switching fabric for their secure wireless services.

Summary

Wireless networking is changing the way IT approaches network security. The characteristics of wireless and the experience of user mobility mean information moves more freely, unconstrained by physical boundaries. The widespread adoption of wireless technology also means businesses are relying more heavily on the digitalization of information for improved productivity and now face increasing regulatory requirements to protect the integrity of this information. Providing adequate control and security for all information, but especially customer and financial data, is at the heart of many regulatory requirements, including Sarbanes-Oxley, HIPAA, and PCI.

Cisco is delivering the Cisco Secure Wireless Solution as the preferred architecture for helping to ensure the integrity of information and IT systems. Cisco is the industry leader in providing technology solutions that combine wireless security protocols such as WPA and WPA2 with best-in-class security solutions such as the Cisco NAC Appliance, Cisco ASA firewalls, and Cisco Security Agent. The result is a security solution that not only helps to ensure the protection of financial, customer, patient, and credit card data, but also allows IT to support business regulatory compliance initiatives with confidence.

For more information, visit:

- Cisco Wireless Security Solutions: http://www.cisco.com/go/wirelesssecurity
- Cisco Unified Wireless Network: http://www.cisco.com/go/unifiedwireless
- Cisco Campus Communications Fabric: http://www.cisco.com/go/ccf
- Integrated Services Modules for Cisco Catalyst 6500 Series Switches: http://www.cisco.com/en/US/products/hw/switches/ps708/products_announcement0900aecd804b5665.html
- 3750G Cisco Catalyst Integrated Wireless LAN Controller: http://www.cisco.com/en/US/products/ps6957/index.html
- Cisco 4400 Wireless LAN Controllers: http://www.cisco.com/en/US/products/ps6366/index.html
- Cisco 5500 Series ASA: http://www.cisco.com/en/US/products/ps6120/index.html
- Cisco NAC Appliance: http://www.cisco.com/en/US/products/ps6128/index.html

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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 C11-424694-01 12/07

