White Paper

Achieving Business Goals and Enhancing Customer Relationships with a Secure Guest Access Wi-Fi Network

This paper explains why wireless LANs are the best way to enable a guest network and describes how to enable guest networks without compromising internal security.

SUMMARY

Many enterprises are interested in providing access to the Internet for their partners, vendors, consultants, or other visitors while maintaining security of their own wireless and wired networks. Assisting visitors with access to IT resources while they are on the premises can have many benefits. For some enterprises, providing access to IT resources is a simple extension of hospitality to visitors—an assumed service, much like providing coffee. For other enterprises, providing guest access is crucial to business goals and improving the bottom line. Examples of some useful applications of guest access in different environments include:

- **Education and hospitality**— Making a research or conference center more attractive to prospective customers
- **Retail, healthcare, and government**—Allowing suppliers and vendors to automatically update inventory positions or place refill orders while on the premises in order to minimize stock shortages
- **Retail**—Increasing customer loyalty and/or spend per visit
- **Enterprise**—Enabling consultants to complete audits more efficiently

Whatever the business reason for guest access, it’s critical to maintain the security of your enterprise as you implement guest networks. Your implementation and security goals should include the following:

- Ensure that guests have access only to the Internet, not to internal resources.
- Create no additional burden for IT administrators to individually authorize users.
- Use existing infrastructure.
- Ensure that internal users and applications have priority over guest users.
- Monitor use of the network and prohibit services on a location or per-user basis, as required.

This paper discusses how you can quickly and securely install guest access networks using the Cisco® Unified Wireless Network.

THE CHALLENGES OF GUEST NETWORK IMPLEMENTATION THROUGH A WIRED NETWORK

Providing guest services over a wired network can pose significant challenges. For larger enterprises in particular, what seems like a simple request to provide Internet access can turn into a major drain of resources and time. To maintain internal corporate network security, guest traffic must be restricted to the appropriate subnet and VLAN. Reconfiguration of the access switches that serve conference rooms, offices, and cubicles where the network is needed can involve many IT staff hours. In addition, providing a wired network connection to some places within the enterprise may be very expensive or not feasible. Bringing wired access to auditoriums and large conference rooms is particularly challenging as the rooms have not typically been designed to bring Ethernet cabling to each seat.

WIRELESS LANS AND GUEST SERVICES: NATURAL PARTNERS

Wireless LANs provide a much simpler method of delivering guest services. The obvious benefit for larger open spaces such as auditoriums, board rooms, and conference rooms is that wireless networks do not require expensive and unsightly cabling runs to each seat. Mounting an access point provides ubiquitous access throughout the coverage area.

A second major benefit is the significant reduction in IT time and resources for network reconfiguration. The Cisco Unified Wireless Network architecture uses wireless LAN controllers to centralize configuration and management of the access points. With this architecture, VLAN and subnet configuration need to occur only at the access switch that the controller is connected to. The result is a dramatic reduction in time to reconfigure the network. Consider, for example, a large enterprise that requires 300 access points to cover all the areas where the guest network will be available. Using the Cisco Wireless Services Module (WiSM), which can manage 300 access points, only one module will need to be configured to route guest traffic to the appropriate subnet and VLAN.

SECURELY IMPLEMENTING A GUEST ACCESS NETWORK

One of the great benefits of wireless LANs is how easy it is for clients to connect. Most access points ship with default settings that allow anyone with a compatible Wi-Fi client to gain access to the network. This is a boon to administrators who do not have the resources to individually set up IP networking for each guest network user. However, this same ease of connectivity is not appropriate for the enterprise wireless LAN, where internal network resources must be protected and the privacy of over-the-air communications maintained. In the past, the only solution would have been a redundant infrastructure for the guest network.

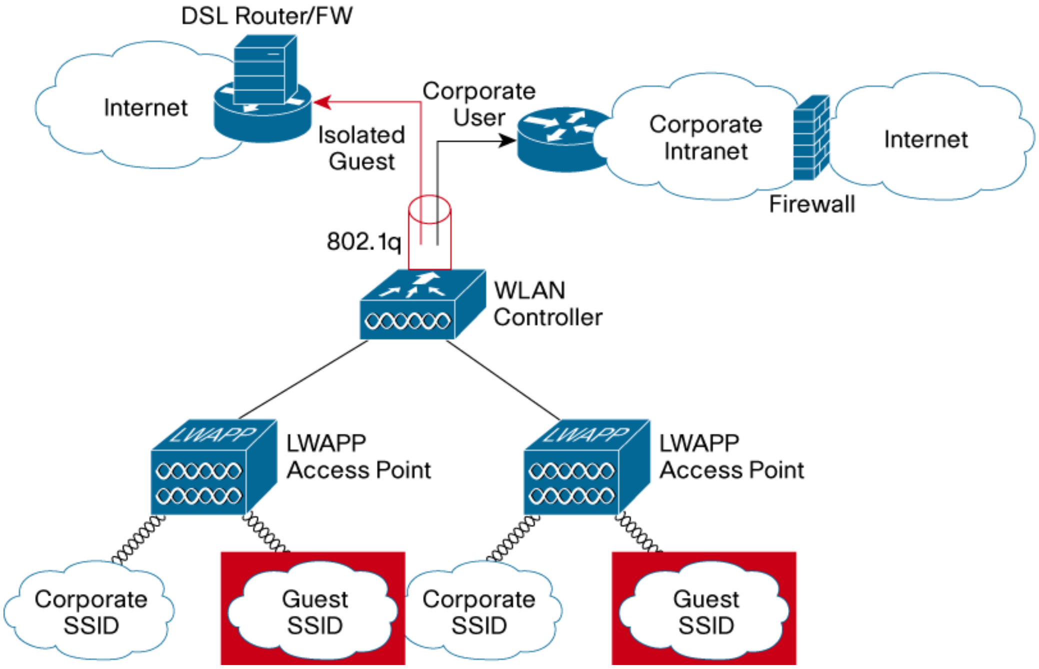
To allow multiple user groups to use the same infrastructure, the Cisco Unified Wireless Network enables up to 16 independent wireless LANs. Each wireless LAN is defined by a unique network name (Service Set Identifier or SSID), security, and quality of service (QoS) setting. Thus, the administrator can define separate SSIDS for different user groups. As an example, the SSID “guest” might be created for visitors who want wireless Internet access. Another SSID named “corp” could be set up for employees, while a third named “shipping” might be established for business-specific devices, such as bar code scanners.

Furthermore, each wireless LAN can be directed to a specific virtual LAN, ensuring that only the necessary resources are available to the users of that wireless LAN. Additionally, administrators can set the SSIDs to broadcast or not broadcast, at their discretion. This allows for an additional level of security. If the guest network SSID is the only one broadcast, unauthorized users may make fewer attempts to access the internal, private wireless LANs. To increase security, the Cisco Unified Wireless Network ensures that all clients gain access within a certain number of attempts as set by the administrator. Should a client fail to gain access within that limit, it is automatically excluded (blocked from access) until the administrator-set timer expires. Table 1 illustrates how multiple WLANs might be configured. Figure 1 shows an example topology using VLANs and 802.1q trunking to isolate guest network traffic.

Table 1. Configuring Multiple WLANs

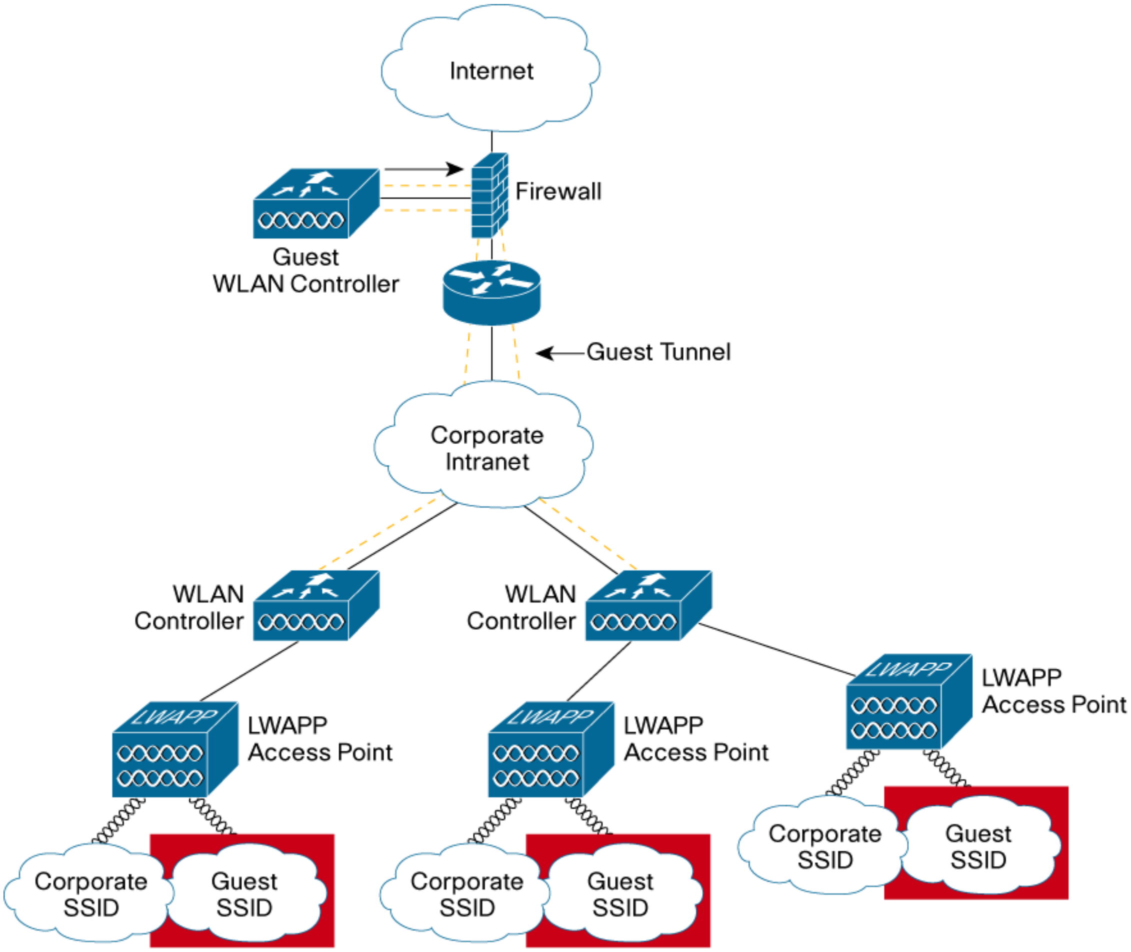
Network Name (SSID)	Purpose	Broadcast SSID?	VLAN Port	Security
corp	Internal, private network for employees	No	20	WPA2
shipping	Internal, private network specifically for bar code scanners	No	30	WEP
guest	Public network for enterprise visitors desiring access to Internet	Yes	40	Web authentication, open

Figure 1. An example of how the Cisco Unified Wireless Network can provide secure guest services on the same wireless LAN infrastructure that employees use through the use of a separate SSID and 802.1q trunking.



For some enterprises, guest traffic isolation via a VLAN does not provide a sufficient level of security. In this case, the Cisco Unified Wireless Network can create a Layer 2 tunnel to direct all guest traffic outside the unsecured network area to a controller dedicated to guest services. As Figure 2 shows, even remote and branch office guest users can be tunneled to a “guest” wireless LAN controller, which then applies the appropriate policies before Internet access is granted. Corporate wireless use policies are managed by the wireless LAN controller(s) internal to the enterprise.

Figure 2. An example topology where guest traffic is directed outside the unsecured network area via a Layer 2 tunnel using the Cisco Unified Wireless Network.



PROACTIVELY ENSURING SECURITY COMPLIANCE WITH CISCO NAC

Endpoint visibility and control is needed to help ensure that all wired and wireless devices attempting to access a network meet corporate security policies. Infected or vulnerable endpoints, whether they are internal corporate devices or guest users, need to be automatically detected, scanned, and if necessary, isolated and cleaned.

Network Admission Control (NAC) is a set of technologies and solutions built on an industry initiative led by Cisco Systems®. NAC uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from emerging security threats such as viruses, worms, and spyware. Customers using NAC can allow network access only to compliant and trusted endpoint devices and can restrict the access of noncompliant devices. NAC is an important part of the Cisco Self-Defending Network, a strategy to dramatically improve the network's ability to automatically identify, prevent, and adapt to security threats.

Both the Cisco NAC Appliance (formerly Cisco Clean Access) and the Cisco NAC Framework provide security threat protection for WLANs. These solutions enforce device security policy compliance when WLAN clients attempt to access the network. These solutions quarantine noncompliant WLAN clients and provide remediation services to ensure compliance. Both solutions are fully interoperable with the Cisco Unified Wireless Network. Figure 3 illustrates the NAC Appliance architecture for the Cisco Unified Wireless Network. Figure 4 illustrates the NAC Framework architecture.

Figure 3. NAC Appliance Architecture for Cisco Unified Wireless Network

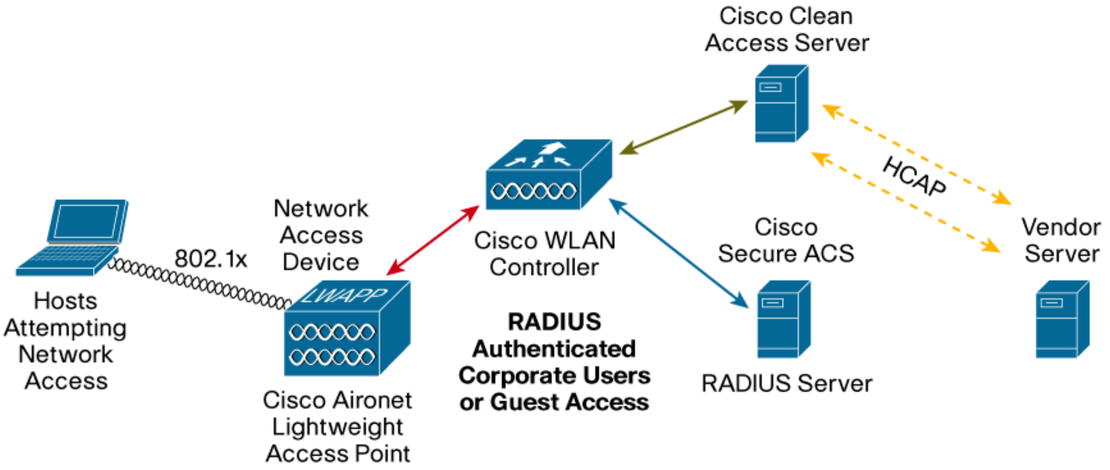
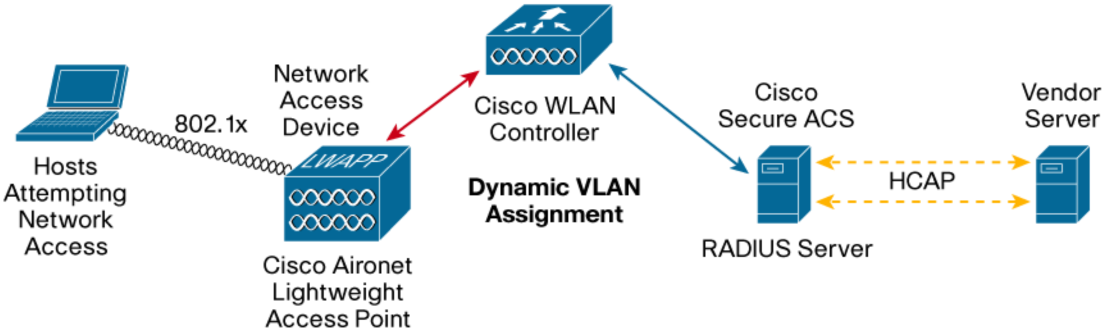

Cisco Clean Access Server
HCAP
Vendor Server
Network Access Device
802.1x
Cisco WLAN Controller
Cisco Secure ACS
Hosts Attempting Network Access
LWAPP
RADIUS Authenticated Corporate Users or Guest Access
RADIUS Server
Cisco Aironet Lightweight Access Point

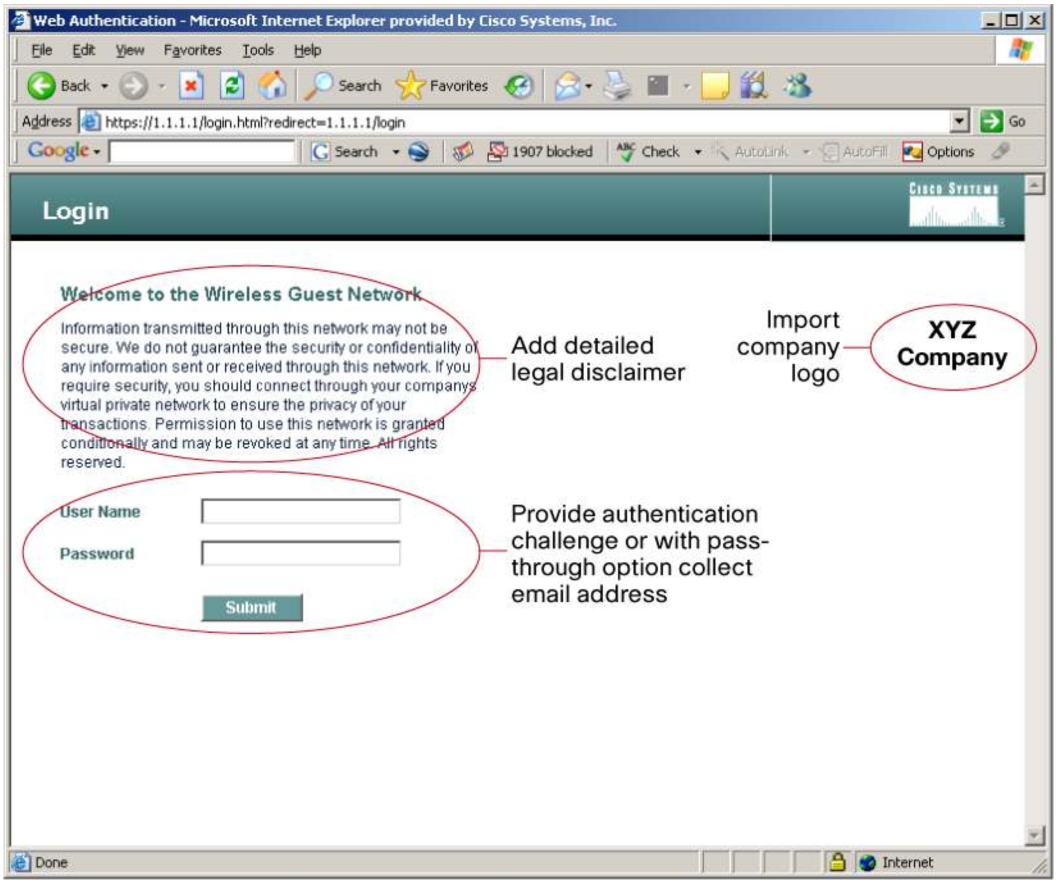
Figure 4. NAC Framework Architecture for Cisco Unified Wireless Network



MANAGING ACCESS TO THE GUEST ACCESS NETWORK

The ability to manage access to the guest network is important to many enterprises for the sake of transparency and also for legal reasons. To monitor use, a captive portal capability can be built into the Cisco Unified Wireless Network. The captive portal redirects the user’s browser window to a specified address when the user first tries to access the Internet. This specific address may then contain additional information for the guest. For enterprises that need a higher level of visibility into guest network use, usernames and passwords can be required. When users launch a browser, they may be requested to provide login information if the IT organization wishes to track each individual. In addition, terms and conditions may be presented to grant Internet access. Figure 5 illustrates a sample authorization login webpage for a guest network that includes an authentication challenge and terms and conditions of use.

Figure 5. Web Login Page Presented to Guest Network Users Before Internet Access


Web Authentication - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back
Search
Favorites
Address https://1.1.1.1/login.html?redirect=1.1.1.1/login
Go
Google
Search
1907 blocked
Check
AutoLink
AutoFill
Options
Login
Cisco Systems
Done
Internet

Welcome to the Wireless Guest Network

Information transmitted through this network may not be secure. We do not guarantee the security or confidentiality of any information sent or received through this network. If you require security, you should connect through your companys virtual private network to ensure the privacy of your transactions. Permission to use this network is granted conditionally and may be revoked at any time. All rights reserved.

User Name

Password

Submit

Add detailed legal disclaimer

Import company logo

XYZ Company

Provide authentication challenge or with pass-through option collect email address

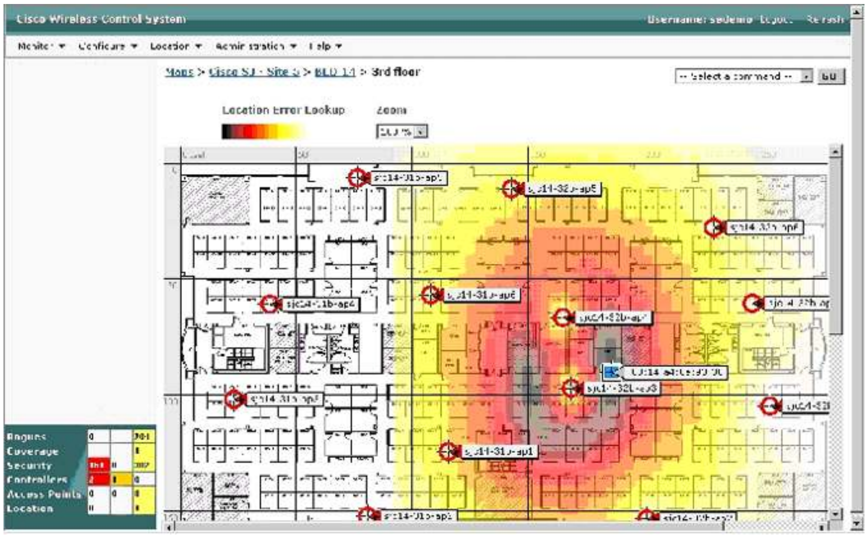
MONITORING USE OF THE GUEST ACCESS NETWORK

You can monitor guest network use through the Cisco Wireless Control System (WCS). The Cisco WCS provides a rich selection of client statistics that you can use to monitor guest network usage. In addition to displaying a summary of all clients, the Cisco WCS can present:

- Client use by time
- Client use by access point
- Client type by protocol and authentication
- Top five access points by client use

You can use the Cisco WCS to look up clients and their current location (Figure 6).

Figure 6. Real-Time Client Location Display on the Cisco Wireless Control System


Cisco Wireless Control System
Username: sedemo Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Maps > Cisco SJ - Site 5 > BLD 14 > 3rd floor
-- Select a command -- GO
Location Error Lookup
Zoom
sjc14-31b-ap1
sjc14-32b-ap5
sjc14-31b-ap4
sjc14-31b-ap6
sjc14-32b-ap7
sjc14-32b-ap3
sjc14-31b-ap1
sjc14-31b-ap2
Rogues
Coverage
Security
Controllers
Access Points
Location

PRIORITIZING ACCESS TO THE WIRELESS LAN

Guest use of the wireless LAN can be prioritized below that of other enterprise users. The Cisco Unified Wireless Network offers individual quality of service (QoS) prioritization for each wireless LAN. Four levels are available: platinum (voice), gold (video), silver (best-effort), and bronze (background). As an example, voice over wireless LAN applications can be prioritized at the platinum level, enterprise data traffic at the silver level, and guest network traffic at the bronze level. This ensures that critical enterprise applications and users have a higher QoS when the network is more heavily used.

CONCLUSION

Guest networks can used for many purposes—from enhancing an enterprise's bottom line to providing hospitality to visitors. In all cases, the enterprise will want to ensure that the guest network does not compromise enterprise security nor cause a drain on IT resources. The Cisco Unified Wireless Network makes it easy to accomplish these goals. Multiple wireless LANs on each access point, each with their own security and QoS setting, enable the enterprise to use a single WLAN infrastructure to meet internal, private wireless needs as well as to provide an open guest network. To manage the access that you provide users of the guest network, you have a range of options, from allowing guest users to simply connect to the open network, to using a captive portal to redirect them to an authorization login page. [[edit ok?]] The Cisco WCS allows detailed monitoring of client network use, including precise location tracking. Finally, QoS settings allow you to prioritize enterprise applications and users over guest network users to ensure that your internal business goals are achieved.

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

Printed in the USA