PRODUCT BULLETIN NO. 3004

CISCO CENTRALIZED WIRELESS LAN SOFTWARE RELEASE 3.0

Cisco Systems® announces the availability of Cisco® Centralized Wireless LAN Software Release 3.0 for the Cisco Centralized WLAN Solution of the Cisco Integrated Wireless Network. This release contains new features, as well as support for the features delivered in Cisco Centralized Wireless LAN Software Release 2.2. This new software release provides support for the following new features: bridging on Cisco Aironet 1030 Series lightweight access points, guest tunneling, sniffer mode for access points, RADIUS server per wireless LAN, site-specific VLANs, a Cisco Wireless Control System (WCS) flash-based floor map editor, Web authentication enhancements, support for the Cisco 7920 Wireless IP Phone, and AP provisioning enhancements. It also introduces support for the Cisco Wireless Location Appliance and the Cisco 4400 Series Wireless LAN Controller.

NEW FEATURES

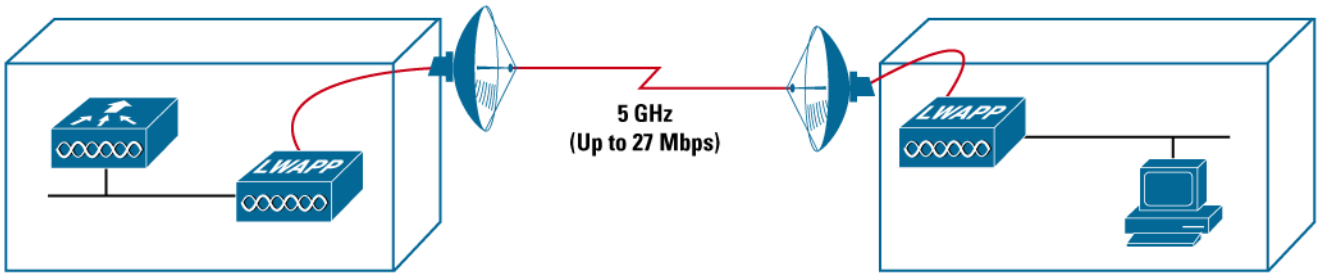
The following new features are included in Cisco Centralized Wireless LAN Software Release 3.0. These features are supported by Cisco Aironet 1000 Series lightweight access points, Cisco Wireless LAN Controllers, the Cisco 2700 Series Wireless Location Appliance, and the Cisco Wireless Control System (WCS) as noted for each feature listed below.

Bridging on Cisco Aironet 1030 Series Lightweight Access Points

This feature provides cost-effective, high bandwidth wireless bridging connectivity. Applications supported are point-to-point bridging, point-to-multipoint bridging, point-to-point wireless access with integrated wireless backhaul, and point-to-multipoint wireless access with integrated wireless backhaul.

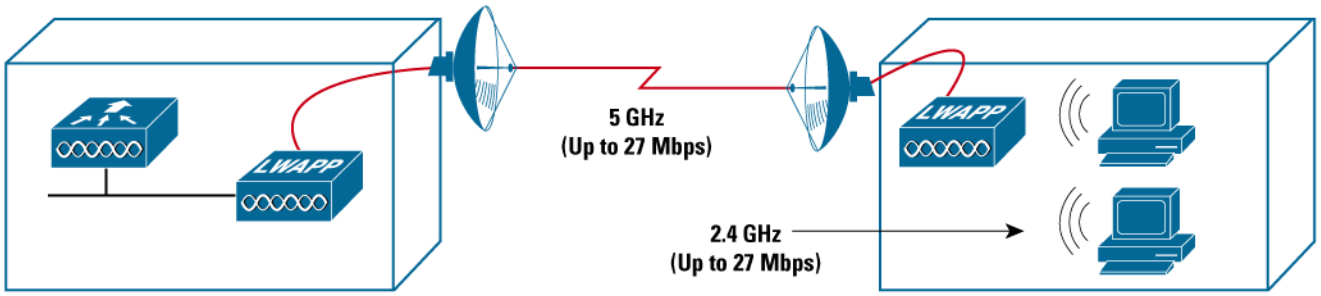
Point-to-point bridging—In this application, two access points (Cisco Aironet 1030) are connected via a wireless link. The Ethernet interface on each access point is plugged into the wired network (Figure 1).

Figure 1. Point-to-Point Bridging



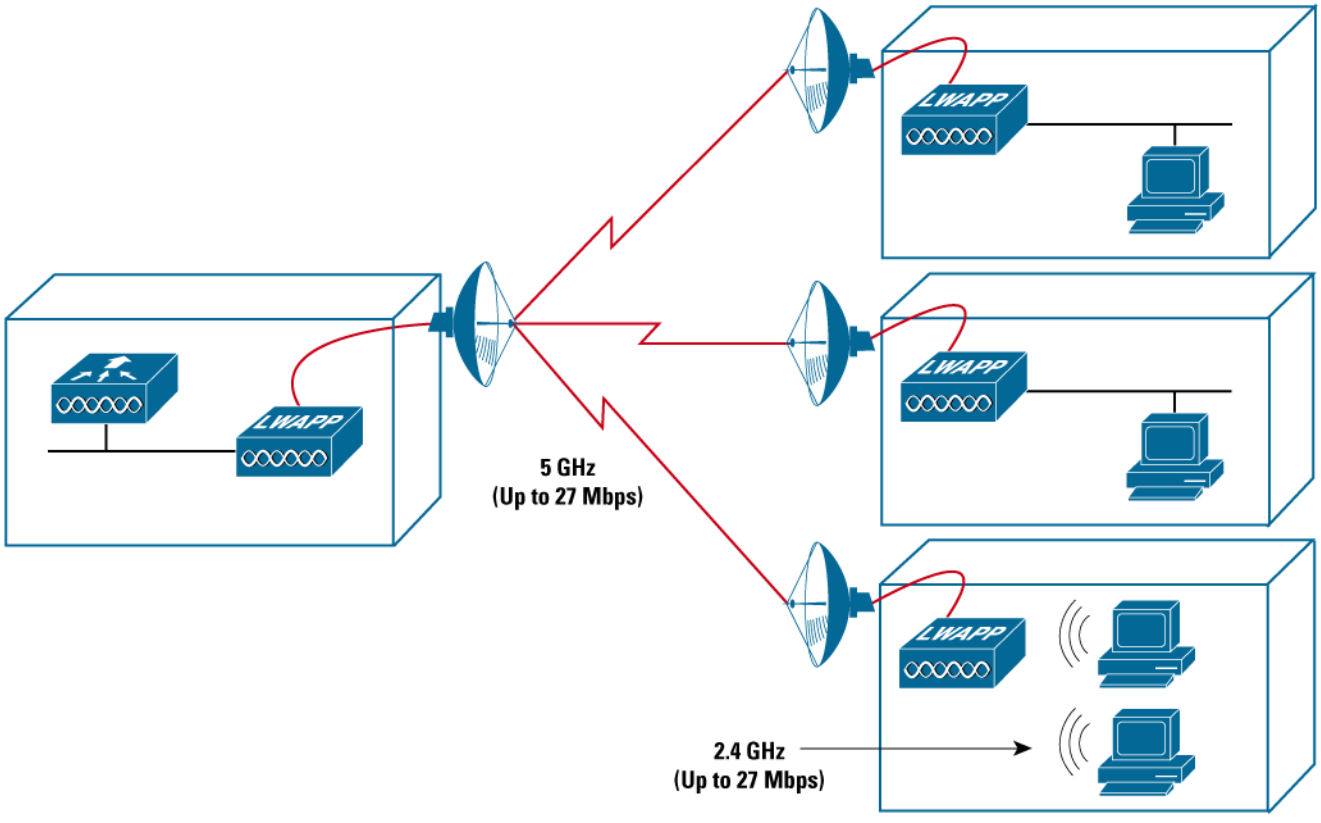
Point-to-point wireless access with integrated wireless backhaul—In this application, two bridging access points (Cisco Aironet 1030) are interconnected via a wireless link. One of the bridges is connected to a wired network that has a wireless LAN controller on it, while the remote access point offers service in one band, and uses the other band for backhaul (Figure 2).

Figure 2. Point-to-Point Wireless Access with Integrated Wireless Backhaul



Point-to-multipoint bridging with integrated wireless access backhaul and wired backhaul—In this application, multiple bridging access points (Cisco Aironet 1030) are interconnected via a wireless link. One of the bridges is connected to a wired network that has a wireless LAN controller on it. This access point is elected as the root of the point-to-multipoint tree (Figure 3).

Figure 3. Point-to-Multipoint Bridging with Integrated Wireless Access Backhaul and Wired Backhaul



Notes on Bridging

- The access point that has a connection via a wire line network to a Cisco Wireless LAN Controller is the root bridge. If more than one access point is able to connect via a wire line network to a Cisco Wireless LAN Controller, one is automatically elected as the root bridge.
- When the remote access points come up, they will automatically connect to the root access point. The connected link uses a shared secret to generate a key that provides Advanced Encryption Standard (AES) encryption for the air link.
- Once the remote bridge connects to the root bridge, it is held in a “pending” state until an administrator enters a new secret. The access point will then be able to pass data traffic.
- All traffic must travel through the root bridge and the wireless LAN controller before being sent out to a remote location.

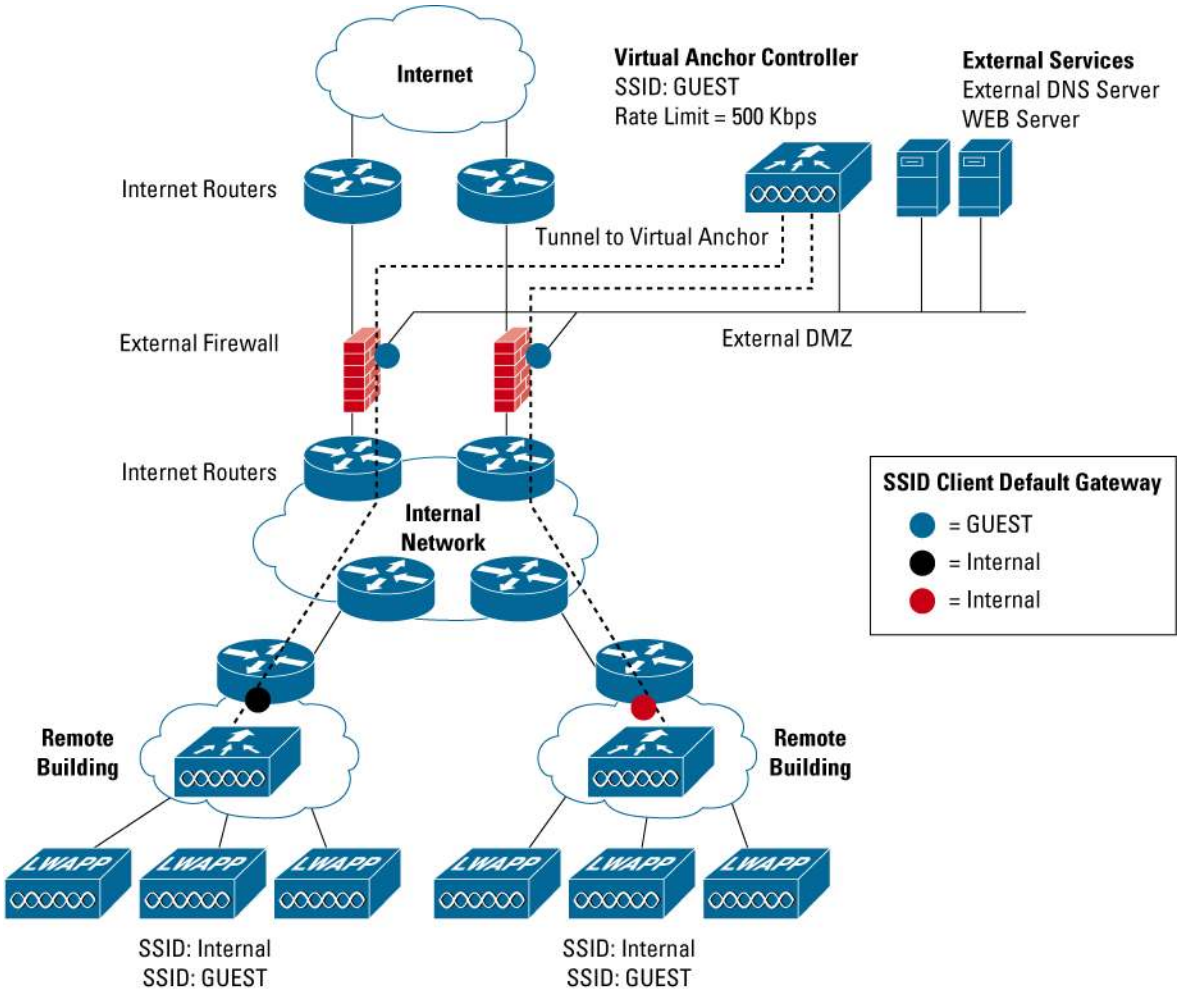
Wireless LAN Controllers supported: Cisco 2000, 4100, and 4400 Series

Access points supported: Cisco Aironet 1030 Series lightweight access points

Guest Tunneling

Guest tunneling provides additional security for guest-user access to the corporate wireless network, helping to ensure that guest users are unable to access the corporate network without first passing through the corporate firewall. Instead of extending the DMZ VLAN to each wireless LAN controller on the network, a wireless LAN controller can now be placed in the DMZ. When a user associates with a service set identifier (SSID) that is designated as the guest SSID, the user’s traffic is tunneled to the wireless LAN controller that is located on the DMZ outside of the corporate firewall (Figure 4).

Figure 4. Guest Tunneling



In guest tunneling scenarios:

- The user's IP address is administered from the DMZ.
- All user traffic is transported over an Ethernet over IP (EoIP) tunnel between the regular wireless LAN controller and the virtual anchor wireless LAN controller, which acts as an anchor as the client moves around the network.
- Mobility is supported as a client device roams between wireless LAN controllers.
- Each virtual anchor controller can support 40 tunnels from various "inside" controllers. These tunnels are established from each controller for each SSID utilizing a virtual anchor, meaning that many wireless clients can ride the tunnel.
- For a customer with many remote sites, it is now possible to forward different types of guest traffic from different sites to different DMZ controllers, or to the same DMZ controller with different wireless LANs. Any user getting placed on the DMZ can use the AAA-override feature to apply RADIUS Vendor Specific Attributes (VSAs) on a per-session basis.

This feature will initially only be available on Cisco 4100 and 4400 Series Wireless LAN Controllers. It is not currently available on the Cisco 2000 Series Wireless LAN Controller.

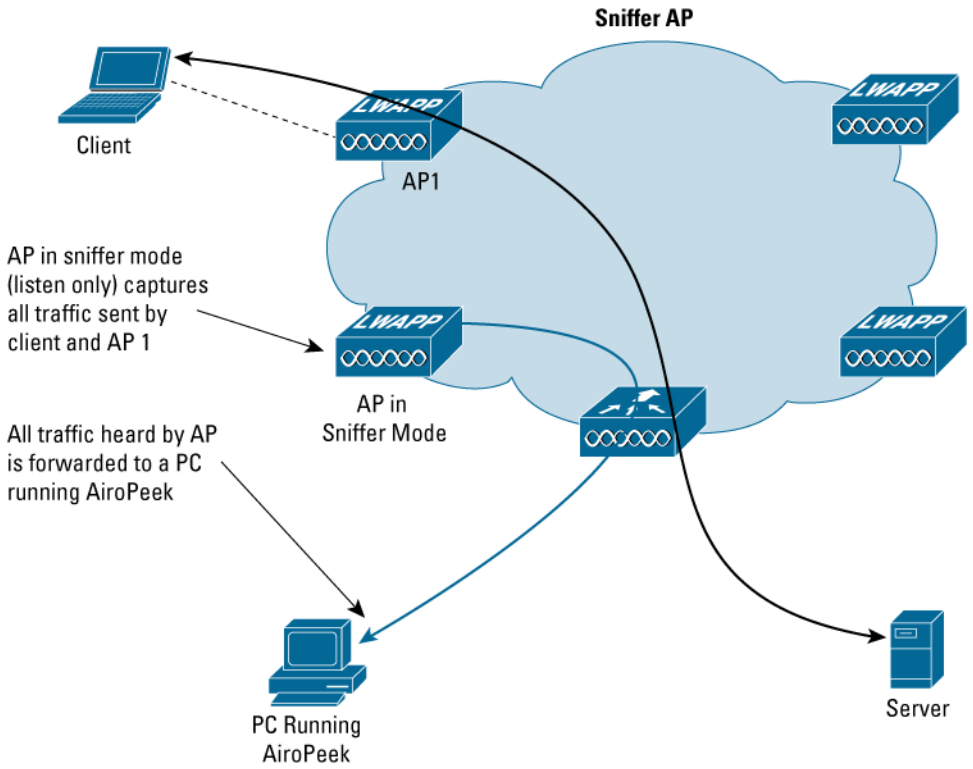
Wireless LAN Controllers supported: Cisco 4100 and 4400 Series

Access points supported: Cisco Aironet 1010 and 1020 Series lightweight access points

Sniffer Mode for Access Points

This feature provides Wildpackets® AiroPeek sniffer capability at a remote site without having to deploy a laptop with the AiroPeek software. This provides for flexible deployment of monitoring capabilities in any enterprise environment. With the sniffer mode feature, any access point can be placed into promiscuous mode and can capture all 802.11 transmissions it receives. These packets, including information on timing and signal strength, are forwarded to a remote PC running AiroPeek. The AiroPeek software analyzes the packets it receives to provide the same information as it does when capturing packets using a wireless card (Figure 5).

Figure 5. Sniffer Mode for Access Point



Wireless LAN Controllers supported: Cisco 2000, 4100, and 4400 Series

Access points supported: Cisco Aironet 1010 and 1020 Series lightweight access points

RADIUS Server per Wireless LAN

This feature allows administrators to specify up to three RADIUS servers on a per-wireless LAN basis. If a RADIUS server is configured for a specific wireless LAN (SSID), it overrides the default RADIUS servers. The default RADIUS servers are used if no RADIUS servers are configured for the wireless LAN. This allows for flexible deployments, where a single wireless LAN infrastructure can support multiple classes of users by providing separation of authentication on a per wireless LAN (SSID) basis.

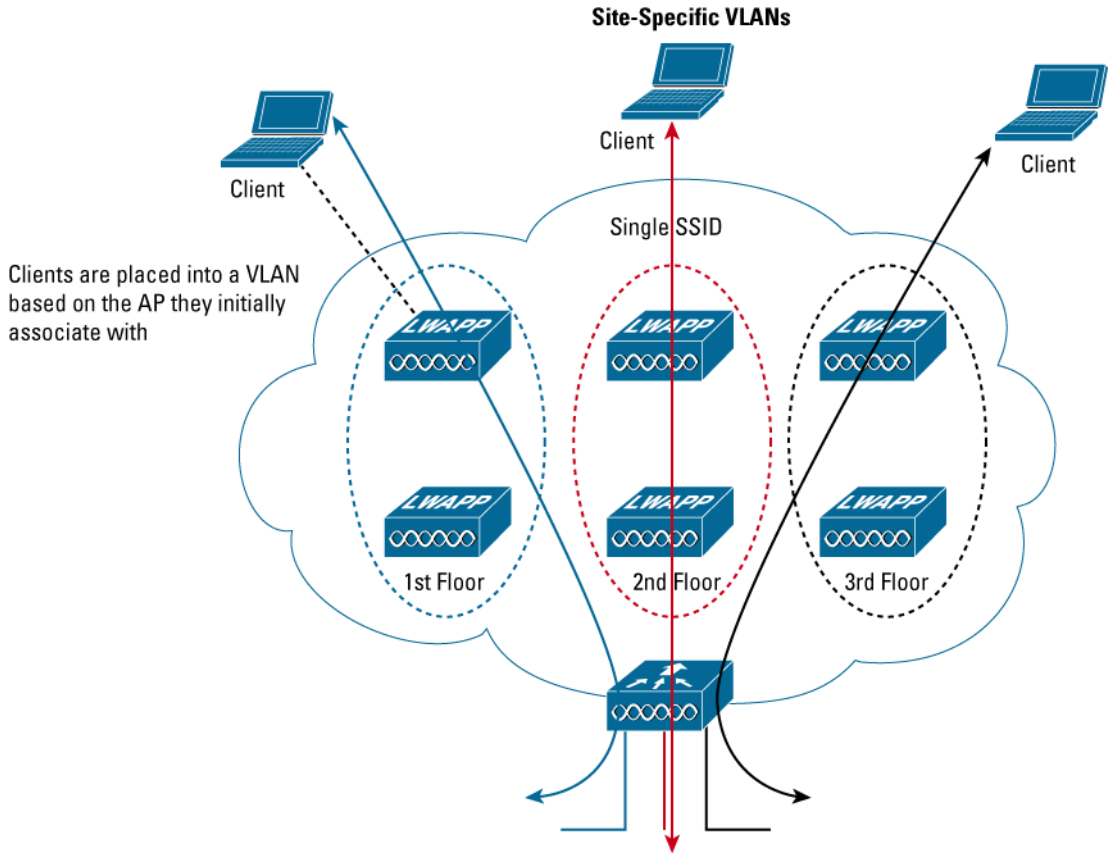
Wireless LAN Controllers supported: Cisco 2000, 4100, and 4400 Series

Access points supported: Cisco Aironet 1010, 1020, and 1030 Series lightweight access points

Site-Specific VLANs

This feature allows the system to place users into different VLANs dynamically, based on the access points they initially associate with, instead of all users from a wireless LAN being placed into a single VLAN or using RADIUS to assign users to the VLAN. This feature spreads users into different VLANs based on where they connect to the wireless network, better distributing the client load across backend physical interfaces (Figure 6).

Figure 6. Site-Specific VLANs



Wireless LAN Controllers supported: Cisco 2000, 4100, and 4400 Series

Access points supported: Cisco Aironet 1010 and 1020 Series lightweight access points

Web Authentication Enhancements

Web authentication enhancements extend the total number of characters on Web authorization customization to 500 characters. The user can also use a “submit” button instead of a full user name / password challenge. A third enhancement allows Wi-Fi Protected Access/Pre-Shared Key (WPA/PSK) and WPA2/PSK to work with Web authentication. These enhancements provide more flexibility in deploying wireless networks with Web authentication.

Wireless LAN Controllers supported: Cisco 2000, 4100, and 4400 Series

Access points supported: Cisco Aironet 1010 and 1020 Series lightweight access points

Cisco WCS Integrated Floor Map Editor

With this feature, Cisco WCS allows users to add walls to imported drawing images using an integrated flash drawing tool. Adding walls to drawings improves the accuracy of the RF prediction algorithms used for radio resource management and RF fingerprinting, which in turn improves the automated optimization of the wireless network and location accuracy. This additional information is also utilized by the Cisco Wireless Location Appliance.

Cisco 7920 Wireless IP Phone Support

With the 3.0 release, the Cisco 7920 Wireless IP Phone is now supported by the Centralized WLAN Solution. The new feature added in the 3.0 release that enables 7920 support is the QoS Basis Service Set (QBSS) Information Element (IE). The QBSS IE is a beacon and probe information element (IE) that enables the AP to communicate its channel utilization to wireless devices. Because APs with high channel utilization might not be able to handle real-time traffic effectively, clients such as the 7920 use the QBSS value to determine if they should associate with another AP. This enables the 7920 to make better roaming decisions and improves overall voice quality.

Wireless LAN Controllers supported: Cisco 2006, 4100 and 4400 Series

Access Points supported: Cisco Aironet 1010, 1020 and 1030 Series lightweight access points

AP Provisioning Enhancements

A new provisioning mechanism has been added for the lightweight APs. After successfully obtaining an IP address and DNS information via DHCP, the AP will resolve the well known name CISCO-LWAPP_CONTROLLER to determine the IP addresses of WLAN controllers to which it can join. This new method is in addition to the existing methods used by the AP to join a controller, including local subnet broadcast, DHCP Option 43, Over the Air Provisioning, and local caching.

Wireless LAN Controllers supported: Cisco 2006, 4100 and 4400 Series

Access Points supported: Cisco Aironet 1010, 1020 and 1030 Series lightweight access points

Support for New Cisco Wireless Products

This software release provides support for the Cisco 2700 Series Wireless Location Appliance and the Cisco 4400 Series Wireless LAN Controller.

DOWNLOAD THE NEW SOFTWARE FOR THIS RELEASE

Download the software from the Cisco Wireless Software Display Tables (Cisco.com login required).

RELATED INFORMATION

For more information about Cisco wireless LAN products, visit: http://www.cisco.com/go/securewireless

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

For more information about wireless security, visit: http://www.cisco.com/go/aironet/security

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

205414.Q_ETMG_LS_10.05

Printed in the USA