

How Cisco IT Deployed Guest Networking Services for Visitors

Secure wireless Internet access extended to guests at every Cisco location worldwide.

Cisco IT Case Study / Wireless LANs (WLANs) / Guest Wireless Hotspots: This case study describes how Cisco Systems used its existing WLAN to provide guest wireless hotspots for the benefit of visiting customers. The Cisco global network is a leading-edge enterprise environment that is one of the largest and most complex in the world. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

“Deployment was easy because we already had a wireless infrastructure. After we made the initial business decisions to deploy a Layer 2 hotspot solution, we simply installed the Cisco BBSM, configured a guest VLAN, opened the appropriate holes in the firewall, and created a legal banner for sign in. Then we were in business.”

– Tony Diep, Cisco IT Project Manager for Global Architecture and Design of Wireless Hotspots

CHALLENGE

When customers visit Cisco Systems®, the company strives to make their stay excellent in every respect—from executive or technical briefings, to proof of concept demonstrations, to convenience. Everyday conveniences are especially important when customers attend meetings that last several days at a Cisco® site in an Executive Briefing Center (EBC) or Technical Briefing Center (TBC), or attend training sessions or conferences. Most of these customers want to access e-mail, the Internet, or their own corporate networks using a VPN connection. “Our customer-facing areas, such as EBCs and TBCs, didn't provide wireless Internet access for our visiting clients, who frequently requested it,” says Sal Pearce,

technical project manager in the Europe, Middle East, and Africa (EMEA) with the Enterprise Technology Solutions team. Cisco decided to use its existing wireless infrastructure to provide Internet access to guests. The value of guest wireless hotspots also would extend to approved vendors and onsite Cisco contractors who need Internet access for several weeks to several months. Previously, vendors would be forced to use dial-up if they were on-site for prolonged periods of time..

Various groups within Cisco already provided Internet access for guests, either using DSL or wired hotspots, but these deployments were not standard, which increased the support burden. In addition, it was challenging to ensure that customers did not gain access to Cisco confidential resources. “A network is only as secure as its weakest link,” says Tony Diep, IT project manager for Global Architecture and Design of Wireless Hotspots. “Every enterprise needs a uniform IT-managed solution with unimpeachable security.”

Cisco established several criteria for its guest wireless hotspot solution, the foremost being security. The solution needs to restrict guest traffic to its own VLAN, segregating it from Cisco production traffic. Another aspect to security is the ability to know who is on the network and what they are doing, to identify and restrict harmful behavior and to protect the network. This requires end-to-end user authentication. Equally important is guest convenience. The solution had to be easy to use and not require heavy support from Cisco IT, lobby ambassadors, or receptionists. Finally, Cisco IT wanted the guest wireless hotspots to use the same Cisco Aironet® 350 and 1200 wireless access points already used for corporate voice and data traffic. Adding the guest VLANs on the same equipment reduces hardware costs

and minimizes radio frequency interference so that employees continue to experience excellent WLAN performance.

To protect the Cisco network, the Cisco Information Security (InfoSec) group stipulated that guest traffic is restricted to its own VLAN so that no guest traffic would pass through the Cisco network.

SOLUTION

Cisco IT developed a guest wireless hotspot solution that builds on the company's existing WLAN infrastructure, reducing the need to purchase infrastructure equipment. Theoretically, adapting the production wireless network for guest access was a simple matter of configuring the access points for an additional guest VLAN to supplement the existing corporate data and voice VLANs and adding a Cisco Building Broadband Service Manager (BBSM) server onto the existing LAN architecture. "Wireless guest hotspots are one of our more straightforward solutions," says Diep.

Cisco IT selected the Cisco BBSM—a "hotspot in a box," according to Diep—after also considering the Cisco Service Selection Gateway (SSG/Subscriber Edge Service Manager). The Cisco BBSM offers the lowest cost and greatest ease of deployment and configuration. Cisco BBSM runs on a Windows 2000 server platform, while Cisco SSG, designed for service providers, is a feature of Cisco IOS® Software and runs on Cisco routers and a UNIX server.

The BBSM provides authentication for each user. Guests at Cisco sites receive a guest user ID and password after signing in with a lobby ambassador or Cisco sponsor; the password expires after a preset duration. Because all guest wireless traffic is carried on a separate VLAN and directed by policy-based routing to the nearest BBSM, guest traffic will not have access to the internal Cisco network. The BBSM will also present users with a legal disclaimer when they first log in, advising them to take legal responsibility for their use of the service and limiting any legal liabilities that Cisco might incur by providing this service. In addition, the BBSM keeps accounting records of who is connected and when, so that if problem Internet activity is traced back to the Cisco guest hotspot, Cisco will be able to help law enforcement trace the activity to the responsible person.

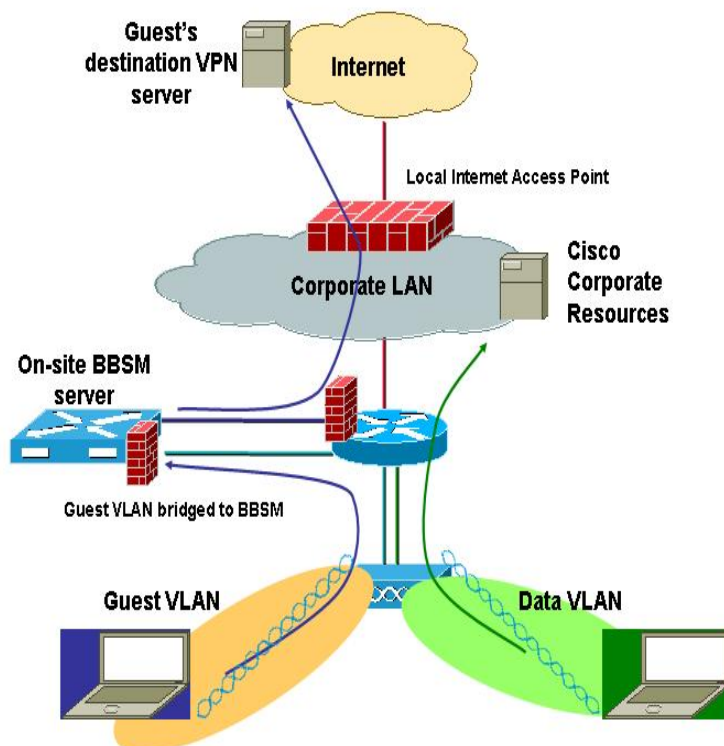
Cisco IT embarked on a two-phase approach to providing guest wireless hotspots. In Phase 1 the company used the Layer 2 functionality in the Cisco BBSM, which requires one server for each hotspot. At the same time, to prepare for introducing guest wireless hotspots in every Cisco office worldwide, Cisco IT worked with the Cisco's Network Management Technology Group business unit to add Layer 3 functionality in Phase 2, so that a single Cisco BBSM server could support multiple geographically dispersed hotspots.

Phase 1: Layer 2 BBSM Hotspots

In Phase 1, completed in September 2003, Cisco IT deployed guest wireless hotspots in three EBCs in the San Jose headquarters, as well as in London and Amsterdam. The Cisco BBSM servers reside in the same subnet as the Hotspot it services.

Each Cisco BBSM server has two interfaces: One to a switch that connects to Cisco Aironet 350 or 1200 wireless access points, and another to the Internet (see Figure 1) using a connection in the Internet demilitarized zone (DMZ). The IP address of the interface to the access point is the default gateway for all guest traffic; therefore, all guest Internet traffic is routed immediately to the Cisco BBSM and completely bypasses the corporate LAN. Wireless corporate traffic, in contrast, bypasses the Cisco BBSM entirely because it is on a separate VLAN and has its own Service Set Identifier (SSID).

In the Layer 2 model, the Cisco BBSM acts as an IP address allocation server (using Dynamic Host Configuration Protocol) and domain name server, as well as the default gateway for the hotspot.

Figure 1. Cisco Guest Wireless Hotspot Deployment: Layer 2 Design.

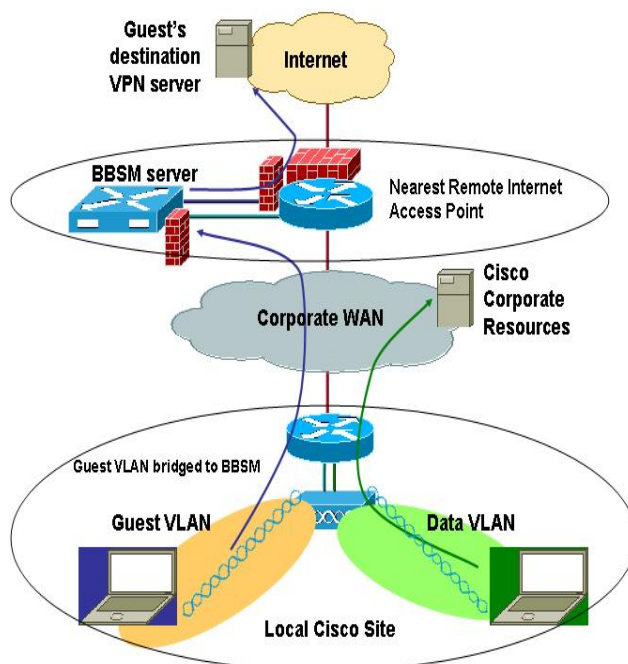
Phase 2: Layer 3 BBSM Hotspots

Cisco IT still is in the process of deploying the second phase of wireless hotspots, making use of the Layer 3 BBSM capabilities. The architecture is similar to the Phase 1 architecture, but now a head-end router is needed for the Generic Routing Encapsulation (GRE) tunnels with the BBSM server. The BBSM servers will be deployed in key Internet access sites on Cisco IT Internet POPs. Guest users don't need access to the Cisco intranet, so the best design is to place the BBSMs and Head-End Tunnel router closest to the Internet," says Diep. "Consolidating our hotspot infrastructure with the existing network infrastructure simplifies management and reduces unnecessary traffic across the WAN." Hotspot users in any one of the 250+ Cisco sites worldwide will log on to the wireless guest VLAN at the local site and be tunneled over the WAN (using the same default quality of service markings given to most data traffic) to the BBSM server located at the nearest Internet access point. There the BBSM server will display a SSL encrypted web page with the required legal disclaimer and authenticate the user using the user ID and password they were given when they signed in. Since guest traffic is on a separate VLAN, Quality of Service (QOS) can also be defined if required.

Cisco IT's cost to provide the service at all 250+ sites is relatively small, because the service uses existing network equipment and bandwidth. This assumes that the WAN circuit bandwidth from each site to the Internet access point will not need to be increased, because the number of guests working from any Cisco site probably will remain a small percentage of that site's population. Public routable Internet IP addresses will be provided to guests (rather than private addresses, to minimize potential VPN client issues), from an address block currently assigned to Cisco for Internet connectivity. The only new equipment required is a pair of BBSM servers (one active and one on standby, for redundancy), and a Cisco 7206VXR Router to terminate all the guest generic routing encapsulation (GRE) tunnels, at each of the eight Internet access points within the global Cisco network. (Note: A separate router is only needed if separation is needed from the DMZ router for any reason. Cisco IT dedicates a router here to maintain clear separation of responsibility between the Hotspot service and the Internet access service, supported by separate groups within IT.) Because hotspots for a few specific areas are considered high priority, IT added an additional

Cisco 7206 Router as a redundant device in the design (see figure 2).

Figure 2. Cisco Guest Wireless Hotspot Deployment: Layer 3 Design.



Security Considerations

“Layering on guest access to an existing WLAN is relatively easy,” says Diep. “The challenge is getting it right regarding security.” Therefore, Cisco IT worked closely with Cisco InfoSec to plan the deployment. “We had to reassure InfoSec that the business need was legitimate, and they asked us to harden the server and router according to the InfoSec Security Guideline for DMZ Devices¹. The chief directive was that nobody would be able to hack into the Cisco BBSM, because it resides on the DMZ at the Internet access point.” In addition, because Cisco InfoSec required that guest traffic not travel on the corporate switch fabric, Cisco IT used GRE tunnels from the Cisco distribution router to the BBSM-connected router to ensure no hop-off points for guest traffic within the Cisco internal network.

The most secure way to deploy guest wireless access is to purchase additional circuits that are physically disconnected from the corporate network—“air gap,” as Diep describes it. Additional circuits can be expensive and increase the support burden. “A close second is Cisco BBSM or SSG hotspot solutions,” says Diep. “The combination of the BBSM, a strong firewall, and policy based routing, gave us peace of mind in terms of security.”

Next, Cisco IT configured the firewall to prevent guest traffic from traveling to the Cisco intranet. Cisco opted for the “accept all, deny some” method, as opposed to the “deny all, permit some” method. The former permits all traffic with the exception of known security vulnerabilities—for instance, ports 135 and 4444, exploited by the Blaster and Nachi worms, respectively. The alternative, “deny all, permit some,” would create additional support overhead because IT would be called upon repeatedly to reconfigure the firewall for different visitor requirements, such as unique TCP port identifiers for their client VPNs. Inbound and outbound access control lists (ACLs) on the Cisco 7200 Series Router, to which the Cisco BBSM external interface is connected, prevent guests from accessing the Cisco internal network.

Next came two policy decisions: whether to turn on Wireless Encryption Protocol (WEP) in the Cisco Aironet 350 or 1200 access points, and whether to broadcast the “guestnet” SSID. Cisco opted not to turn on WEP, which encrypts

¹ www.cisco.com/application/pdf/en/us/guest/products/ps533/c1244/cdcont0900aecd80093fe0.pdf

traffic between the laptop and the access point. The reasons: Guest convenience and avoiding support requirements. “If we supported WEP, guests would need to configure their wireless client to support WEP and enter a 26-character encryption key,” says Diep. “We instruct guests to use VPN to encrypt their data.”

Cisco IT decided to broadcast the guestnet SSID, which is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Here, too, guest convenience influenced the decision. If Cisco had not broadcast the SSID, guests would need to hardcode their wireless client to associate to the SSID. “SSIDs should not be considered a layer of security because it’s very easy to use a network sniffer to identify a SSID,” Diep adds. “We depend on the access codes, our firewalls, and VPN to provide security. Down the line, we plan to implement Publicly Secure Packet Forwarding (PSPF) to further protect our users.” PSPF is a feature on Cisco access points that prevents interclient communication.

User Experience

To control who can use the guest network and gain audit capabilities, Cisco assigns unique guest access codes that are valid for access during specified times. For the Layer 2 deployment, an administrative assistant at Cisco acts as the access code manager, logging into the Cisco BBSM interface with limited access to enter the guest’s name and the hours that the Cisco sponsor has requested for access—for example, Monday through Friday from 8:00 a.m. to 5:00 p.m. for one week. The Cisco BBSM generates an access code that can be printed and handed to customers during their visit. As part Phase 2’s deployment, Cisco plans to allow the sponsors to generate the access codes, eliminating an administrative layer. Sponsors will use an internal Web page that securely sends access code data to the BBSM. The new feature also will allow batch access code requests and provide several administrative tools. The centralized access code generation Web page is also critical for a Layer 3 deployment so that one can generate access codes to different locations without having to log in to different BBSMs.

To use the guest wireless hotspot, guests launch their browser, as they would ordinarily do. As long as they request a Web page that is not on the Cisco internal site, they are redirected to a sign-in page, where they enter their full name for tracking purposes, and agree to an acceptable use policy. Next, guests are prompted to enter their unique access code. After authentication with the BBSM, guests are connected to the Internet without access to the Cisco internal network. Transmissions are unencrypted unless the guest is using a VPN client. Cisco IT logs Internet usage using Cisco NetFlow technology and can retrieve that data if needed for legal reasons.

Guests enjoy nearly complete unrestricted access to the Internet, including Web browsing, e-mail, and VPN sessions to their remote offices. Cisco IT decided to block peer-to-peer connections and some known Trojan ports are not allowed. The solution records session details so that Cisco IT can associate the IP address provided to guests with their access code and visitor name, if needed by the Cisco IT legal department or law enforcement agencies. Traffic is not intercepted, recorded, or analyzed.

Session Description

When a guest enters a URL, traffic flows from the guest’s wireless PC to the Cisco Aironet access point, out the site’s WAN router and over the WAN, to the BBSM-connected router in the Internet DMZ and to the BBSM server.

The BBSM looks up both the IP and MAC addresses of the PC sending packets into the internal BBSM network interface card (NIC) to determine if this PC already has been authenticated. If so, the traffic matches a predefined filter and flows to the external BBSM NIC. If not, the BBSM redirects the PC to the URL displaying the Cisco legal banner. After the guests have agreed to the conditions on the legal banner, the BBSM redirects them to the authentication page to enter their eight-digit alphanumeric access code. Next, the BBSM looks up the access code to determine if it is valid. If so, the BBSM forwards the guest’s request to www.cisco.com, ensuring that traffic flows through the guest network from the external NIC of the BBSM server in the following manner:

“Traffic from the PC to the Cisco 2600 Router (Cisco 6500 is used for the desktop router) that acts as the BBSM desktop router is all Layer 2,” says Patrick Gilbreath, Cisco IT network engineer. “This protects the Cisco intranet

because guest traffic on the guest VLAN cannot travel anywhere else except to the BBSM desktop router.”

After guest traffic is received on the desktop router, it is redirected by a route-map that sets the next hop for all traffic using an ACL and sets the next hop to the GRE tunnel interface connecting the BBSM desktop router to the BBSM DMZ router. This tunnel is created on both routers with a static route pointing to the production network because guest networks are not advertised in the dynamic routing protocol. “All other routes on both the BBSM desktop router and BBSM DMZ router are static,” says Gilbreath. By using static routes we are able to have strict control on what traffic flows through the network. Traffic then crosses the GRE tunnel through the corporate network to the DMZ. It hits another route-map that matches the guest network using an ACL and sets the next hop to the IP address of the internal NIC of the BBSM. At this point, all guest traffic is ready to be filtered by the BBSM to the external NIC for Internet-bound traffic or redirected for authentication. Return traffic follows the same path as outbound traffic.

Support

“Determining the support level for this new service is tricky because, traditionally, internal production wireless LANs are classified as a Priority 4 (P4), with two days’ resolution,” says Diep. “But to a Cisco account manager sitting next to a client, an outage almost would be considered a P2, which directly affects revenue and merits a four-hour resolution.” Given these circumstances, Cisco IT needed to provide adequate support to ensure minimal outages, without devoting more resources than warranted for a service that does not directly affect the business. “Ultimately, we came up with a two-level prioritization for hotspots. For Executive Briefing Center hotspots, we classified them as a P2 (four-hour resolution) and classified all other hotspots as P3, which means one-day resolution,” says Diep. Because of liability issues, Cisco IT will not configure an external client’s laptop. Instead, Cisco IT ensures that the service is operational, and guests learn to access the network from their sponsor or with on-line help.

Cisco IT uses its existing support structure for communication of outages. Cisco Global Technical Response Center (GTRC) fields all internal support calls and routes them to the appropriate support group. For the EBC, the GTRC contacts the on-call engineer if there is an outage and routes outages at other locations to the appropriate support group.

Cisco has many groups within IT, including Networking, Hosting, and Client Desktop. The BBSM is a unique device to support in the IT organization because it is a Windows server, is used for networking, does end-user authentication, and traverses the production LAN to access the DMZ. To simplify support, IT decided that the Network team would own the service from end to end because other devices used in the service also are networking devices. The Network team would work with different groups within IT if there were any problems (for instance, Hosting if there was a problem related to Windows or the server) and the Cisco Technical Assistance Center if there were any BBSM specific issues.

RESULTS

Cisco customers in the United States and EMEA enthusiastically have accepted guest wireless hotspots. “It’s a big hit,” says Pearce. “Our customers tell us they are impressed with the service—especially the ease of access and speed. They appreciate that they can keep on top of e-mail and other critical issues that arise during their visit. We’re making their visit as productive as possible.” In fact, several customers have requested an executive or technical briefing on the solution and have decided to deploy the Cisco BBSM and guest wireless networks at their own companies.

“I’ve been getting requests for Hotspots almost every day since the internal announcement was made of our plans,” says Diep. “The team is excited to get the Hotspots out there for everyone to use.”

NEXT STEPS

Now that Cisco has validated the success with guest wireless hotspots in a limited number of locations, the company is beginning to implement the solution to all Cisco offices worldwide. After finishing up wireless Hotspot deployments,

Cisco IT also intends to use Layer 3 BBSM technology to help secure its wired Ethernet LAN segments in specific areas. Wired ethernet ports in unsecured areas in a Cisco office is a potential security hazard since an accidental connection to the switch could mean direct access into Cisco. "Because the BBSM technology can be applied wirelessly or on the wire, it's a great tool for us to grant access to specific users while denying access to others," says Diep.

LESSONS LEARNED

Cisco compiled a list of recommended practices and lessons learned during its deployment, to ease the way for Cisco customers who deploy their own guest wireless hotspots. A sampling of compiled recommended practices follows:

- "Develop clear guidelines for customers to set up the laptop and use the service," says Pearce. Cisco, for example, produced instruction booklets that are provided in lobbies and meeting rooms with guest wireless access.
- Be prepared to coordinate with multiple groups in the company. Cisco IT coordinated with the legal, marketing, and security groups. "A major part of my role was to facilitate all the players talking to each other," says Diep. The Cisco BBSM, a network access control device that runs on a Windows 2000 server, straddled the responsibilities of both the Transport/Networking team and Hosting team. Ultimately, the Hosting team agreed to support the server hardware, and the Networking group supported everything else.
- Determine IP Address allocation strategy early in planning. Network Address Translation (NAT) address can be use but there may be limitations to some VPN clients. Routable address are not always in abundance.

"We don't just say to customers who purchase the Cisco BBSM, 'This is how you configure one box,'" says Pearce. "We also concern ourselves with the business processes surrounding the box. For instance, we had to understand how to support it, meet and greet our customers, and educate them about the service. We're keen to share lessons learned and best practices. Customers can avoid pitfalls by using the rich knowledge base we've accumulated through our own deployment."

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.



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.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0705R)