How Cisco Upgraded to Next-Generation Guest Networking

New architecture supports more than 350,000 sessions per year, with reliable and secure service and lower-than-ever support costs.

Cisco IT Case Study / Wireless LAN / Guest Networking: This case study describes why and how Cisco upgraded its original guest networking service to a next-generation architecture with greater reliability, enhanced capabilities, and lower administrative requirements. The project involved deploying new components, resolving IP address depletion issues, and educating Cisco® employees to reduce support calls. Cisco customers can draw on Cisco IT's real-world experience in this area to plan their own wired and wireless guest access programs.

Background

Since 2004, sponsored visitors to any of Cisco's 440 global offices have enjoyed wired and wireless Internet access. Any Cisco employee can sponsor a guest by visiting an internal web portal (hotspot.cisco.com) and entering the guest's name and the dates and times that access is allowed. The portal generates a unique guest access account that the sponsor provides to the guest. To connect to the guest network over Cisco's wired or pervasive indoor wireless network infrastructure, guests launch their browser as they ordinarily would. They are redirected to a sign-in page, where they enter their full name; agree to Cisco's acceptable use policy; and enter their unique access account. After being authenticated, guests have unrestricted access to the Internet, including web browsing, email, and VPN sessions to their remote offices.

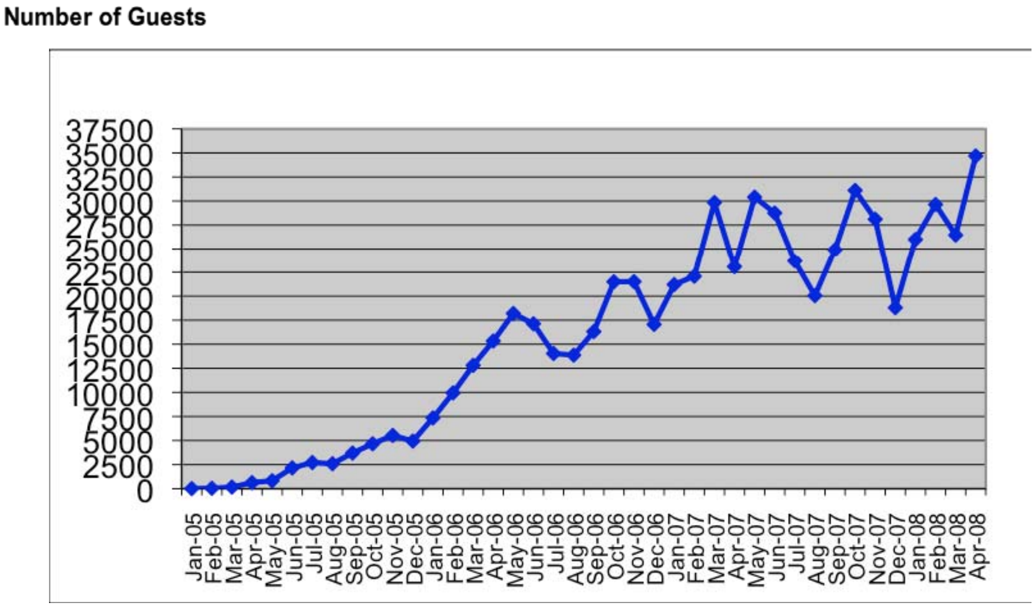
> "Guest access at Cisco was originally an amenity, a convenience for visitors who wanted to browse the web or check email. But adoption grew rapidly as Cisco staff began using the guest network for training classes, and customers who visited Cisco offices for executive briefings counted on reliable guest access to stay in touch with their companies. Guest access evolved into a business-critical tool. We needed an enterprise-class solution."
>
> **Oisin Mac Alasdair, Member of Technical Staff, Cisco**

The Cisco solution records the IP address provided to guests, access account details, and visitor name in compliance with Cisco IT legal department requirements. Traffic is not filtered, intercepted, recorded, or analyzed.

Challenge

Usage of the Cisco guest network quickly exceeded expectations, growing 150 percent year over year (Figure 1). The dips in usage occurred during companywide holidays.

Figure 1. By 2008 Cisco Visitors Conducted an Average of 27,000 Sessions Monthly



In addition, guest access had become a highly visible service. “Guest access at Cisco was originally an amenity, a convenience for visitors who wanted to browse the web or check email,” says Oisin Mac Alasdair, a member of Cisco’s technical staff who is responsible for Cisco’s internal security architecture and roadmap. “But adoption grew rapidly as Cisco staff began using the guest network for training classes, and customers who visited Cisco offices for executive briefing counted on reliable guest access to stay in touch with their companies. Guest access evolved into a business-critical tool. We needed an enterprise-class solution.”

An improved enterprise-class solution would accommodate rapidly growing volume and also enable Cisco IT to meet increasingly stringent service-level agreements (SLAs) for wireless guest access. Service outages were originally Priority 4 events, with a two-day SLA. They have more recently become Priority 2 events with a four-hour SLA at Cisco Executive Briefing Centers (EBCs) and Customer Briefing Centers (CBCs). “The underlying infrastructure did not support such a high SLA,” says Mac Alasdair. “Although the proportion of cases to the number of guest sessions was very small, even one case is too many because it affects Cisco customers.”

To begin planning a Next-Generation Guest Networking (NGGN) solution, Cisco IT first analyzed the nature of the cases opened during a two-month study period in 2008. During that time, 159 cases were opened for 60,000 guest networking sessions. The three most common types of cases included:

- **Usage questions (65 percent).** Cisco employees called with questions ranging from whether Cisco even had a guest network to how they could create a guest access account. Even the simplest call to the Global Technical Response Center (GTRC) cost Cisco IT US$15.
- **IP address depletion (16 percent).** As the service grew in popularity and more guests connected simultaneously, some visitors were unable to obtain IP addresses. The problem was made worse because certain devices and operating systems automatically acquired an IP address, even if the user did not plan to access the guest network. In downtown Cisco offices, people in nearby buildings would sometimes acquire Cisco guest networking IP addresses in error.
- **Solution components (8 percent).** The original access control platform, the Cisco Broadband Services Manager (BBSM), was not deployed in a redundant fashion and had also reached end of life. Lack of redundancy resulted in occasional outages, dissuading some Cisco trainers from using the guest network.

Instead, they used time-consuming workarounds such as setting up a wired LAN to tunnel into the lab, which required opening a case. “We wanted a new guest architecture with fewer single points of failure,” says Mac Alasdair.

Solution

Cisco IT embarked on a project to make guest networking more reliable, scalable, and convenient. In Phase 1 of the next-generation guest networking deployment, Cisco IT would eliminate the single points of failure that were responsible for most of the service outages: the access control platform (previously Cisco BBSM) and the provisioning portal, which Cisco had developed internally. In Phase 2, Cisco IT would further increase scalability and reliability by eliminating other single points of failure and adding new features.

Solution Components

For provisioning, Cisco IT replaced the internally developed portal with the Cisco Network Access Control (NAC) Guest Server. For access control, Cisco IT replaced Cisco BBSM with Cisco NAC Server and Cisco NAC Manager. “The Cisco NAC products meet our requirements for an enterprise-class solution,” says Mac Alasdair. “In addition, Cisco NAC Server was one of the few products at the time that supported wired as well as wireless guest access, and the Cisco NAC Guest Server offered Multilanguage support and a PDA Portal.”

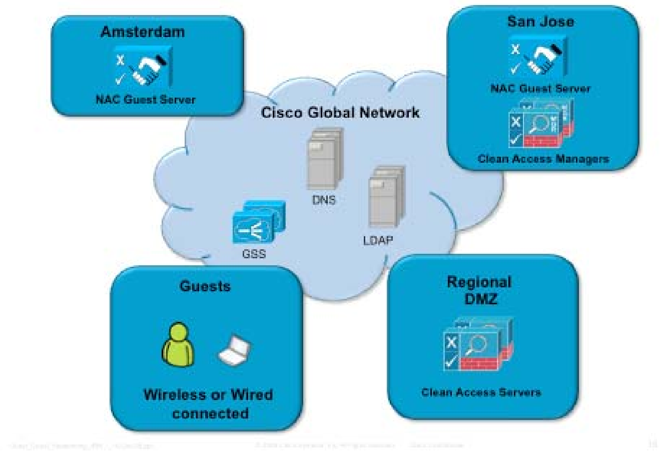
Table 1 shows the solution components used for management, traffic segmentation, and guest access control during different phases of the guest networking project.

Table 1. Cisco Next-Generation Guest Networking Components

Component	Function	Original Guest Network Solution	NGGN Phase 1 Solution (Current)	NGGN Phase 2 Solution (Planned)
Provisioning Portal	Enables enterprise users to sponsor visitors and create a unique access code for guests	Internally developed web application	Cisco NAC Guest Server	Cisco NAC Guest Server
Traffic Segmentation	Helps ensure that guest traffic is securely segmented from the Cisco corporate wired and wireless networks	Generic routing encapsulation (GRE) tunnels and policy-based routing	GRE tunnels and policy-based routing	Ethernet over IP (EoIP) using Cisco Unified WLAN Controllers
Access Control and Policy Enforcement	Provides a welcome screen and validates guest identity, enforcing Cisco policy	Dual Cisco BBSM	Dual Cisco NAC Servers	Dual Cisco NAC Servers and Cisco NAC Manager

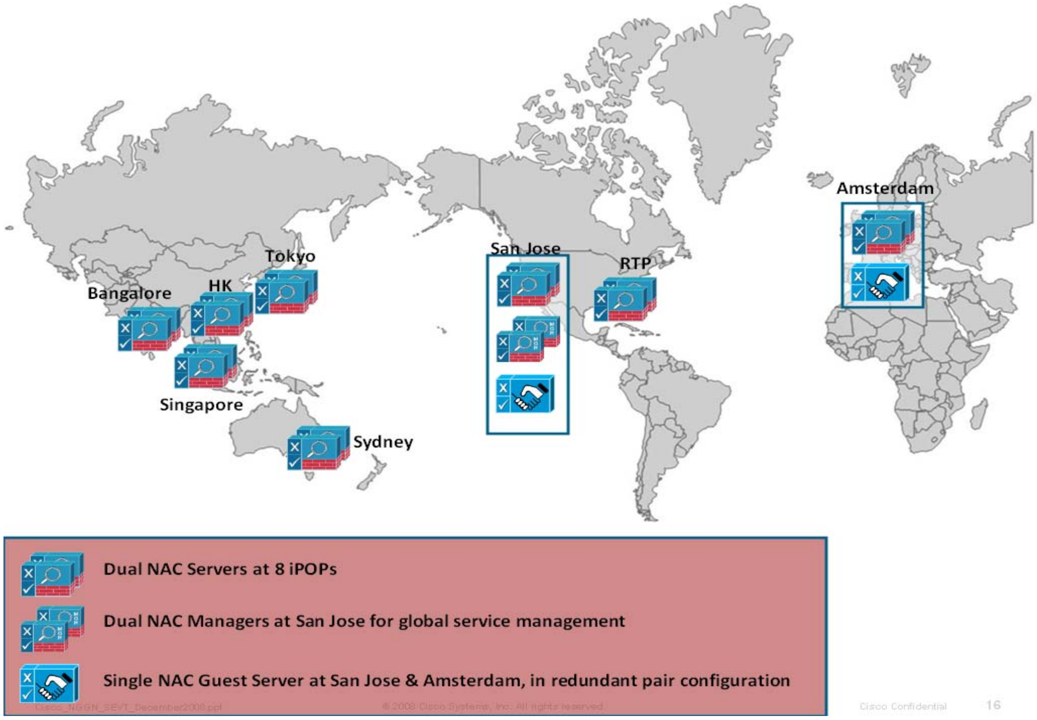
Cisco IT installed two Cisco NAC Guest Servers, one in San Jose, California, and the other in Amsterdam, to serve all Cisco global offices (Figure 2). The Cisco NAC Guest Servers operate in active-active mode. If one fails, the other automatically takes over its load so that Cisco employees can always sign up their guests for network access. Automatic failover is accomplished using the Cisco Application Control Engine (ACE) Global Site Selector Appliance.

Figure 2. Cisco Next-Generation Guest Networking Deployment



For access control and policy enforcement (Figure 3), Cisco IT installed redundant Cisco NAC Servers in each of Cisco's eight global points of presence (POPs). The redundant configuration eliminated a single point of failure present in the previous architecture.

Figure 3. Redundant NAC Servers for Policy Enforcement


Amsterdam
San Jose
RTP
Tokyo
HK
Bangalore
Singapore
Sydney
Dual NAC Servers at 8 iPOPs
Dual NAC Managers at San Jose for global service management
Single NAC Guest Server at San Jose & Amsterdam, in redundant pair configuration
Cisco_NGGN_SEVT_December2008.ppt
© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Confidential
16

Transition Process

Cisco IT conducted a one-month pilot of the next-generation guest networking architecture at four U.S. sites, validating the design, product capabilities, and migration model. No issues arose during the pilots, so Cisco IT began the global deployment.

To minimize risk, Cisco IT migrated to the (NGGN) next-generation guest networking solution a few offices at a time rather than within all 440 global offices simultaneously. Cisco IT automated the migration process for all the global sites by using Cisco management products and scripting tools. “Automation reduced the deployment effort by more than 90 percent,” says Mac Alasdair.

During the transition, some Cisco offices would still be using the old service while others were using Cisco NAC Guest Server. Cisco IT needed a simple way to inform employees which website they should visit to sponsor guests. The team decided to:

- Continue using the hotspot.cisco.com provisioning portal for sites that still had the old architecture
- Set up a temporary URL for sites that were migrated to the next-generation architecture. Employees in these sites received emails notifying them of the temporary URL one week before the upgrade, 24 hours before, and again the afternoon of the upgrade.
- Resume using hotspot.cisco.com when all sites were migrated to the new architecture

IP Address Management

To help ensure that IP addresses are available for all guests who need them, Cisco IT took the following steps:

- **Globally deployed Cisco Secure Services Client (SSC) to Cisco employees and configured it to prevent simultaneous wired and wireless connections.** “This measure will significantly reduce the number of Cisco employees who unintentionally acquire an IP address for the guest network,” says Mac Alasdair.
- **Disabled Service Set Identifier (SSID) broadcast for the Cisco guest network in most locations:** When Cisco first began offering guest access, the IT group decided to broadcast the guestnet SSID, which is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. The choice was made for guests’ convenience, so that they would not need to configure their wireless client to associate to the Cisco guestnet SSID. The unintended consequence was that laptops belonging to visitors, employees, and even people in nearby buildings acquired an IP address, even if the owner had no intention of using the guest network. Now Cisco IT has disabled SSID broadcast in most locations, retaining it only in sites where visitor convenience is paramount, such as EBCs and CBCs.
- **Increased the IP addresses** assigned to the guest network by 50 percent.

Employee Education

Most support calls related to guest networking are from employees with questions about how to use the service. Cisco distributes ongoing educational materials starting before the upgrade. Communications include:

- Newsletter articles sent by email and published on internal websites
- Broadcasts on digital signage in cafeterias and other common areas within Cisco
- Online discussion forums
- Handouts, posters, and tri-fold brochures placed in lobbies
- Inclusion of smart tags in articles published on Cisco’s intranet so that employees who search for guest access topics can more easily find resources

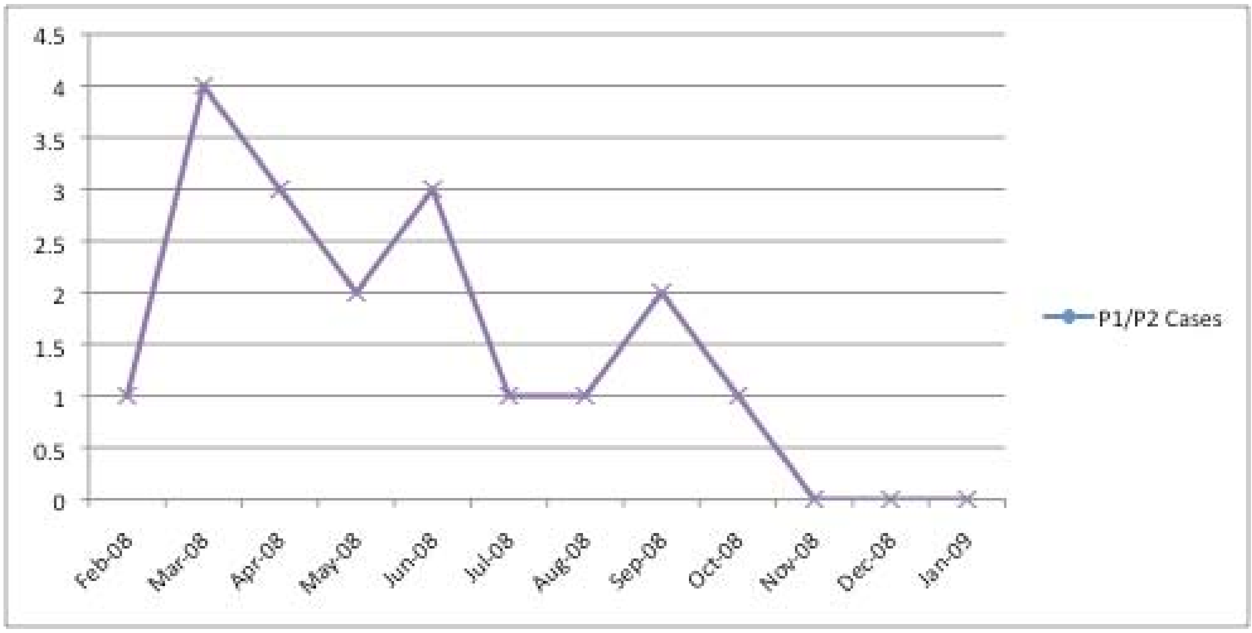
Results

The next-generation wireless guest access solution has met Cisco IT goals for reliability, scalability, lower support requirements, and increased user satisfaction.

Improved Reliability

The redundant Cisco NAC appliances provide the required reliability for a mission-critical service. “Previously, we opened a couple of cases related to solution components each week, and resolution ranged from a simple service reboot to involving the TAC [Technical Assistance Center],” according to Mark Sullivan, global lead design engineer at Cisco. “Since deploying the new architecture, we have not opened any Priority 2 cases for guest access.” Figure 4 shows the number of monthly Priority 1 and Priority 2 cases related to guest access.

Figure 4. No Priority 1 or Priority 2 Cases Have Been Opened Since the NGGN Architecture Was Fully Deployed



Increased Scalability

The new guest access solution is managing an average of more than 7000 authenticated connections weekly, with a cumulative connection time of 18,000 hours. During the first four weeks of the service, more than 9000 Cisco employees, almost 20 percent of Cisco’s workforce, sponsored a guest at least once.

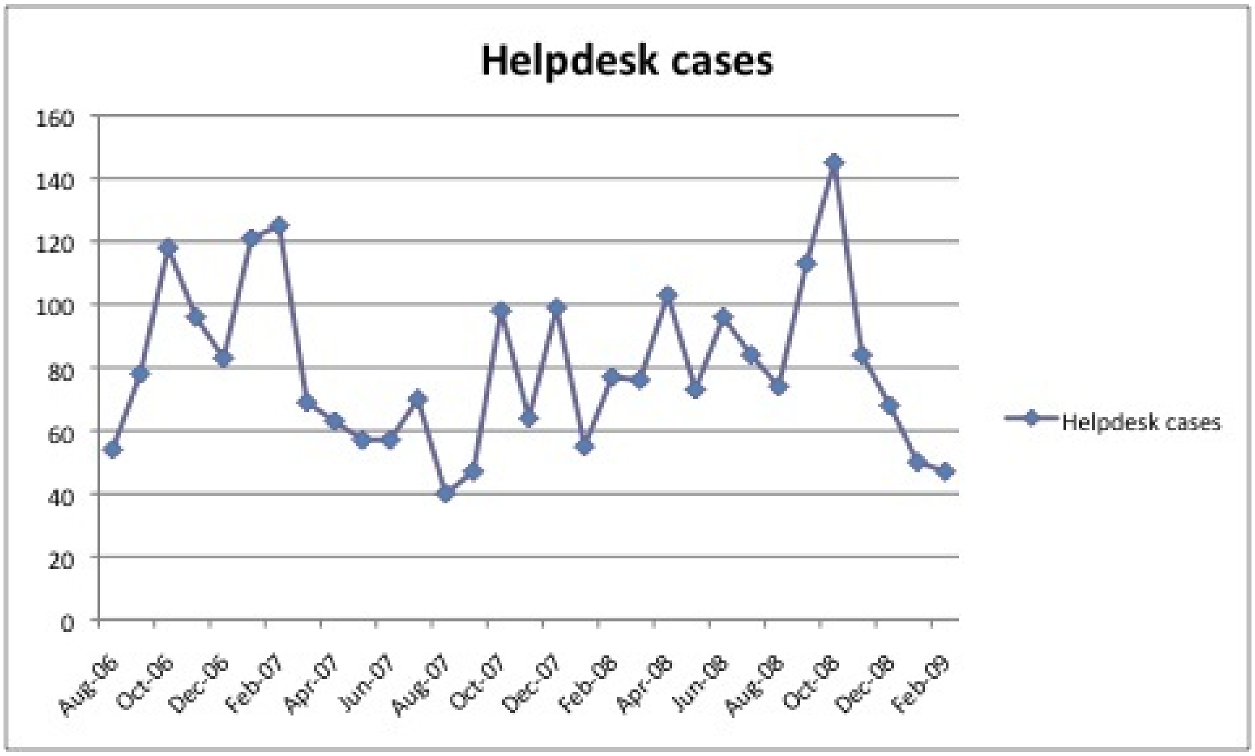
Reduced IT Support Costs

In Cisco’s fiscal year 2007 (12 months ending July 28, 2007), Cisco IT handled 991 support cases related to guest networking, or one case for every 221 sessions. Support costs were US$174,000 annually: $160,000 for one full-time employee responsible for Tier 2/3 support plus $15 per case paid to the GTRC.

“If current trends for the new architecture continue, Cisco IT will see support costs decrease by approximately 15 to 20 percent,” says Mac Alasdair. “In the 12 months before we deployed the next-generation guest network, we handled an average of 89 cases a month,” he says. “Now we’re handling an average of 49 cases, a 46 percent reduction.”

Figure 5 shows the decrease in total helpdesk cases.

Figure 5. Decrease in Guest Networking Helpdesk Cases



Improved User Satisfaction

“Cisco employees have provided positive feedback about the intuitive provisioning interface in the Cisco NAC Guest Server,” says Sergey Shitov, a network engineer in Cisco IT. “They can use it without assistance, which makes it a scalable and popular solution.”

Next Steps

Having remedied the major causes of guest networking services outages by replacing the old provisioning and access control components with Cisco NAC solutions, Cisco IT plans to embark on Phase 2 of the next-generation guest networking deployment:

- **Improve resilience.** “We are investigating methods of introducing reliable path separation between the remote office and the network edge ,” Shitov says. The plan is to use Cisco Network Registrar for Dynamic Host Control Protocol (DHCP).
- **Improve scalability and manageability.** Cisco plans to use Cisco Wireless LAN Controllers for traffic segmentation.
- **Improve integration with Cisco’s Enterprise Management (EMAN) platform, which is internally developed and based on web services.** Cisco IT uses EMAN for monitoring network and host availability, reporting and alerting, and more. “EMAN is an important tool for all Cisco IT engineers, and full integration will further reduce support costs and overhead of the guest access solution,” says Mac Alasdair.
- **Introduce new Cisco NAC Guest Server capabilities**, including:
  - Support for portals in Arabic, Chinese, Japanese, and Korean

  - Delivering guest's credentials to their smartphones with Short Message Service (SMS), which can be faster and more convenient than email in some cases. SMS is particularly popular in Europe and Asia.
  - Providing a guest portal that is optimized for smartphones and PDAs

Lessons Learned

Cisco IT shares the following lessons learned for other organizations that are introducing or upgrading their guest access solution:

- Do not underestimate the popularity of the service when making design decisions: "Design the guest network with the expectation that everyone will use it, even internal staff," says Shitov.
- Recognize that customer-facing services need to be high priority: "We initially conceived the guest access solution as a best-effort program," says Shitov. "But the field saw it as an essential service. Any outage or service disruption is highly visible."
- Plan for growth, especially when defining IP address pool sizes. "Our original DHCP pools had not been increased in four years," says Mac Alasdair. "This exacerbated the problems with IP address depletion and caused us some challenges initially."
- Integrate the service with your enterprise or network management tools. "We prefer to not monitor individual services in isolation from the others," says Sullivan. "It's critical that any service, especially a visible and popular service like guest networking, is properly integrated into standard reporting and alerting tools."

For More Information

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.
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.**