How Cisco IT Uses Analysis Module to Gather Information on Host, Network, and Application Traffic

Cisco Network Analysis Module provides full application layer visibility and proactive, real-time monitoring capabilities.

Cisco IT Case Study / Network Management / Network Analysis Module: This case study describes Cisco IT's internal deployment of the network analysis module (NAM) within the Cisco global network, 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.

BACKGROUND

As Cisco Systems® has expanded over the years, it experienced a symbiosis—as business grew, so did the demands placed on its network infrastructure. From 1990 through 2001, Cisco grew, on average, 160 percent annually. The number of Cisco sites that needed network connectivity grew rapidly, as well. Today there are 127 WAN sites in the United States, 25 in Americas International (11 in Canada, 14 in Latin America); 76 in Europe, the Middle East and Africa; and 50 in the Asia Pacific region. Demand drove new challenges, which in turn drove new solutions, based on three continuing factors:

- More employees
- Better and newer business applications
- A growing network infrastructure to support both

This growth in the number of sites and number of employees was fueled by the convergence of voice and video onto the data IP network and by the growing number of business applications used to support Cisco. The result was a continuously growing and dynamic network architecture, which became increasingly difficult to manage.

CHALLENGE

Large-scale enterprise networks bring several benefits to the enterprises they support, but they also create significant challenges for the teams that administer them—and Cisco was no exception. Communications problems between two different hosts, including network traffic problems or application malfunctions, are difficult to identify unless administrators can watch packet traffic between the two identified hosts as it moves across a particular network segment.

Trying to monitor network segments while looking at traffic or application performance is difficult. In the past Cisco administrators used Remote Monitoring (RMON)-based packet capture analysis software. Although that worked, it also created logistical problems, because it required installing a PC at the site of the problem traffic, which may be a building, a city, or a continent away. These approaches rarely offered the proactive monitoring abilities needed to intercept problems before they affected users.

Wilson Ng, network engineer for the Cisco Network Design and Engineering Group, describes the problems that administrators faced: "We tried a lot of tools. The biggest problem we faced was packet capture, but even with packet capture, there's a lot of information you still don't have, and a lot of inconvenience. If we wanted to do remote packet capture, we'd have to have someone hook up a laptop remotely—and sometimes that means another building or site,

sometimes hundreds of miles away. Getting monitoring started is hands-on work, but we've got centralized teams. With 160 sales offices, we needed something that would do the analysis remotely."

Network analysis continues to grow, and traditional methods of setting up packet capture using a laptop cannot scale to the requirement to capture simultaneous data from several data sources. For example, a multitiered application can have several components. A common multitiered application is the three-tier application, consisting of Web servers, application servers, and database servers. To perform detailed troubleshooting, data must be captured from all three components. "The traditional method would be to set up three laptops running packet capture software to monitor the network traffic from all three sets of servers: Web, application, and database," Ng says. "Setting up three laptops takes time, hardware, and other resource constraints. First, three laptops have to be available. After the laptops are configured, they have to be physically placed, and there is no easy way to manage the network analysis software remotely on the laptops. A distributed network analysis device is needed and must be able to perform more than one capture to solve the problem."

The Cisco team needed a solution that could provide more than packet capture. They needed to look at the application layer across the network, to manage performance and troubleshooting. They needed to integrate monitoring across the LANs and WAN, providing real-time and historical monitoring. Quality of service (QoS) has grown in importance, and with the emergence of voice over IP (VoIP), application-monitoring needs are more complex than ever. Monitoring VoIP, for example, demanded the ability to monitor voice quality, including jitter and dropped packets, for each phone call. As the network and its applications became more complex, so did its monitoring needs.

SOLUTION

The Cisco network analysis module (NAM) was the answer. The NAM is an integrated traffic monitoring service module that occupies a single slot in the chassis of the Cisco Catalyst® 6500 Series Switch. It gives Cisco network administrators full application layer visibility, providing this information to the network engineer using a browser from any point on the network. After it is installed, the NAM enables both real-time and historical application monitoring, including data and voice. With proactive monitoring capabilities, it is easy to capture and decode packets, analyze trends, isolate network problems, and find application response delays before they occur. New VoIP and QoS monitoring capabilities let administrators analyze IP telephony sessions and validate QoS policies. The twelve sample screens illustrated in Figure 2 show visual and easy network analysis for administrators—they include traffic analysis, port monitoring, application and VLAN monitoring, along with voice quality and packet capture and decoding.

Overview

Ng talks about the Cisco team approach: "Our interim solution was another vendor's distributed packet capture system. If you needed to capture something, you had to go where the problem was. But when we worked with the Cisco development team, we let them know that we wanted to get away from taking the actual packet capture box physically to the problem. One of us was always running around or calling people. The original idea was to distribute one device in each building; but now, because we can activate NAM remotely, we don't have to run around any more—but we get the same information with a lot less work." Ng says, "In addition to packet capture and analysis, we needed more information to understand real-time traffic. Remote Monitoring (RMON) data helped provide real-time traffic information, and the Cisco Catalyst 6500 Series exports limited RMON data—but not enough data. To get all the RMON data from the Cisco Catalyst 6500 Series—including backplane traffic—we needed the NAM. NAM gives us voice and data, along with switching statistics. It collects information 24 hours a day, seven days a week, on all ports. Competitive solutions would plug into a single port, or, if they saw passing data, they couldn't decipher what port it was coming in on."

With NAM modules deployed across the Cisco data center network, the Cisco team has an impressive view of network traffic and what goes on. The list of applications they can monitor is exceptional. Administrators can look at

customer relationship management applications like Siebel and Oracle, as well as front-end Web applications like Oracle Web Forms. As more applications have Web interfaces, NAM's capabilities are more crucial, because it allows administrators to look at enterprise Web communication and behavior. Cisco also uses NAM monitoring for IP telephony, checking the data layer for problems.

In the data center, NAM is essential when monitoring content switching. Ng describes Cisco IT moving toward content farms in the data centers and the advantages of NAM in that environment: "Traditionally, there's been a standalone Web server. From standalone server, Web servers were load balanced to scale Web applications. Next, you take specific content and use multiple servers, make a *farm* out of it. If you're looking for video, you go to a video farm, for example. In the next year, our content will be spread across content farms. We'll take the Web servers and break them down into more specific pieces. By then, our content will be distributed in a wide range, segregated by both data and content type. When you go to this kind of distributed architecture, the NAM can play a crucial role, because it can look at different applications between servers. Because the network plays a crucial role in this kind of distribution when you've got farms of machines, network analysis is more important. We need to understand how they connect and communicate, and NAM will let us."

In addition, the Cisco team also uses NAM for collecting RMON-1 and 2 port statistics remotely, without requiring a separate RMON probe. Similar to Simple Network Management Protocol (SNMP), RMON takes traps and reports on the data performance across the wire between devices from Layer 2 through Layer 7, enabling administrators to see all seven layers of data on the Layer 2 network where NAM is installed. Because NAM can look at all seven layers of traffic on the backplane of the device in which it is installed, NAM can see more than what is running on the wire: it can look at traffic on the wire between two devices to analyze performance, on the wire, between devices. NAM can also use NetFlow records to monitor applications, hosts, and application conversations for more visibility into the business of the network.

Deployment

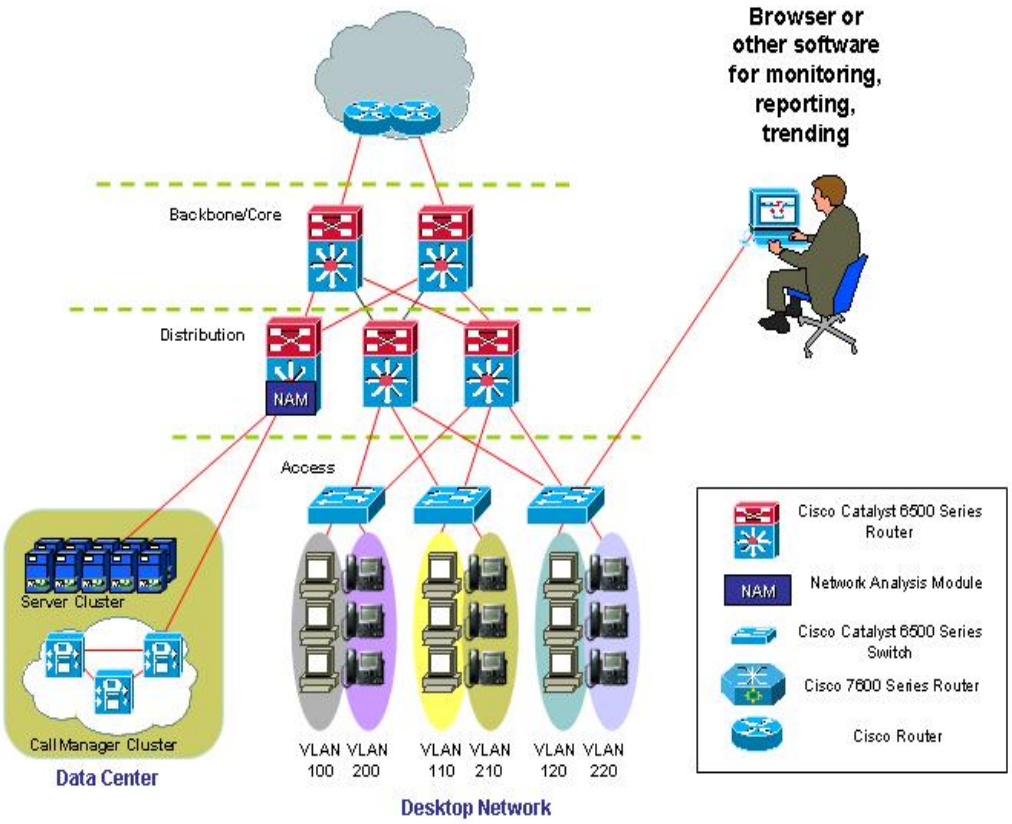
NAMs have been deployed across Cisco production data centers (see Figure 1). As part of a standardized IT infrastructure, NAM is installed in the spanning-tree root distribution switch, a Cisco Catalyst 6500 Series Switch, in each data center. With Layer 2 switch architecture, all traffic flows in and out of the root switch. As a result, the NAM can be strategically placed in the root switch. NAM can inspect and analyze traffic flowing through that root switch.

Securing the NAM required a little extra work. Mr. Ng explains, "Using the NAM in standalone, multilevel TACACS is required to provide the security to separate various users from performing packet captures. Application support groups and system administrators with TACACS accounts are allowed to view NAM monitors. However, packet captures will be done only by network engineers, because Switched Port Analyzer and Remote SPAN configuration will be required on the switches and routers."

To capture data from each individual NAM, the network engineer or administrator accesses the browser-accessed GUI on the NAM to set up data capture on the appropriate interfaces or VLANs. Each NAM can be accessed individually to capture packets, decode packets, and monitor the network, using an Internet browser; CiscoWorks can be used to view equipment configurations and layouts. Data from multiple NAMs can be collected, stored, and displayed by any of several front-end interface software packages. Cisco IT has initially chosen nGenius Real-Time Monitor as part of the CiscoWorks package solution, but other vendor products (including Concord, Infovista, and NetScout) work effectively.

The NAM blade uses a slot in the Cisco Catalyst 6500 or 7600 series chassis. Cisco IT may not be able to install the NAM blade in high-density oriented switches and plans an alternate solution by using the NAM as an external device with a separate Cisco Catalyst 6503 Switch chassis equipped with a Supervisor Engine 1 or 2 module. However, this solution is unable to collect RMON statistics from the switch. At this point, Cisco IT has not found it necessary to do this.

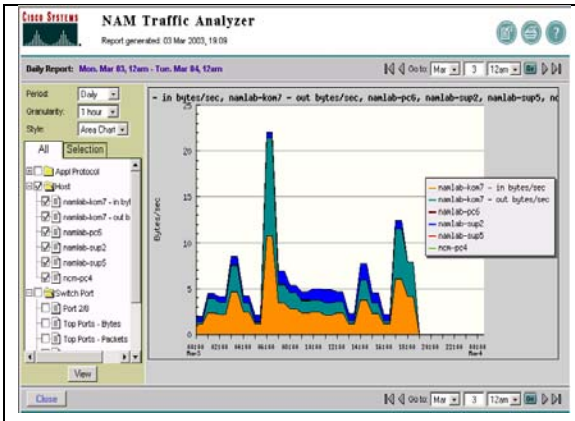
Figure 1. NAM in Cisco IT Currently Monitoring Data Center Networks



RESULTS

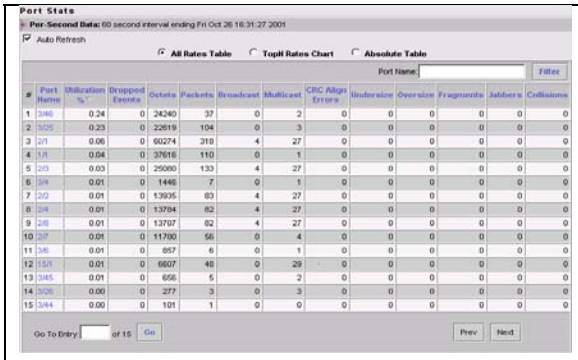
Although Cisco IT has not yet quantified the results of using NAM, Ng describes the results: “So far, it’s been interesting. After we installed the NAM module, there were far fewer problems in the request for packet captures recently. Using NAM, our administrators had more visibility into the backplane, giving them information that wasn’t normally available. That additional information allowed them to make more changes. Looking at the backplane, I learned a lot about several applications. For example, at peak times, our enterprise resource planning traffic can burst up to 70 percent capacity. Before NAM, I expected the number to be high, but I never knew what it was. I do now. It’s one more tool to help resolve issues.”

Figure 2. Examples of NAM Reports

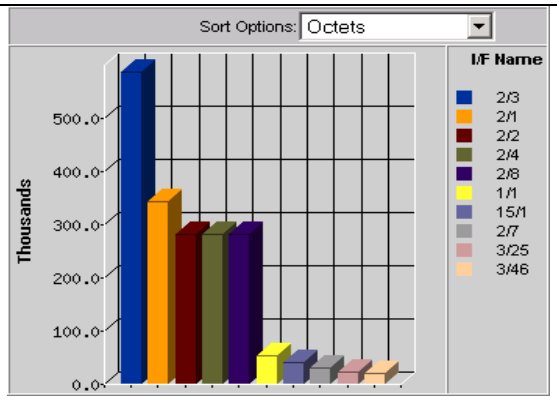


2.A - Historical Traffic Analysis

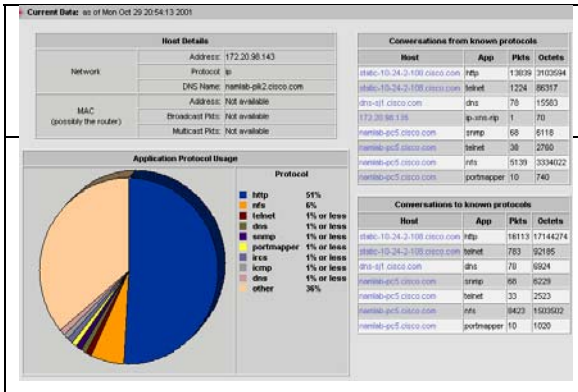
2.B - Traffic Analysis – Applications, Hosts, Protocols, Server Response Times

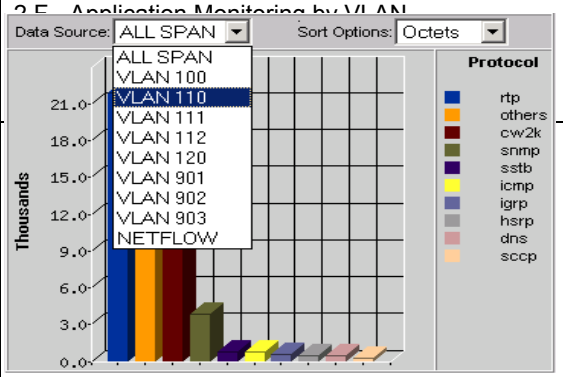


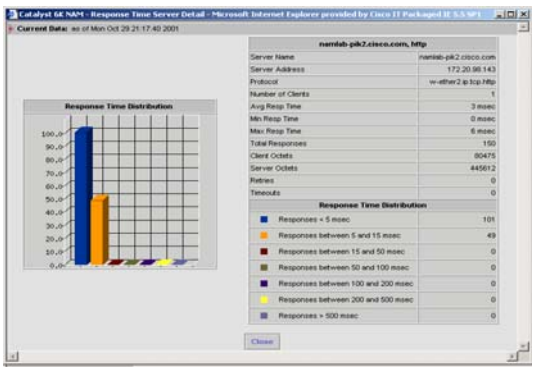
2.C - Port statistics – Utilization, Packets, Bytes, errors



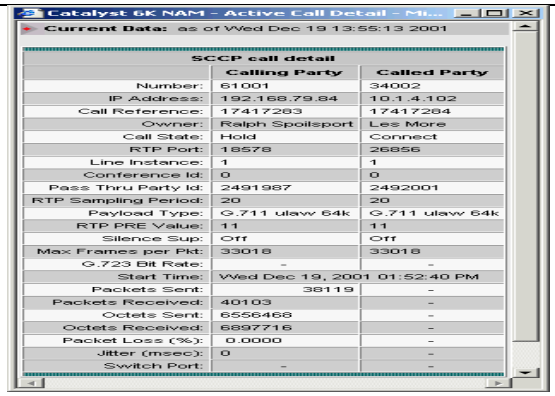
2.D - Traffic throughput per Port - graphic



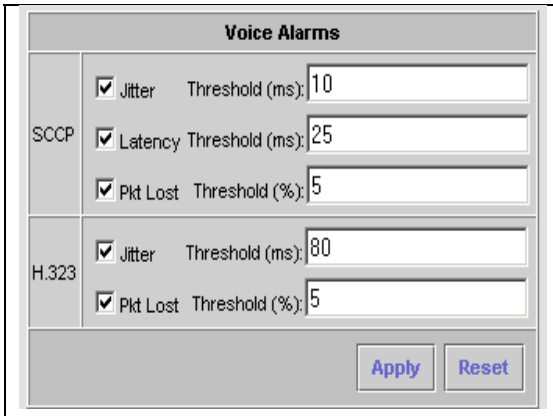




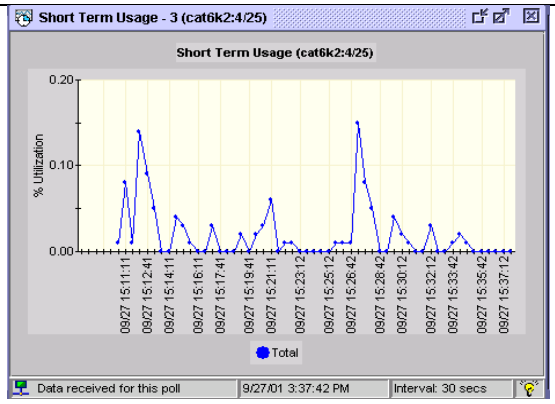
2.G - Application and Server Response Time



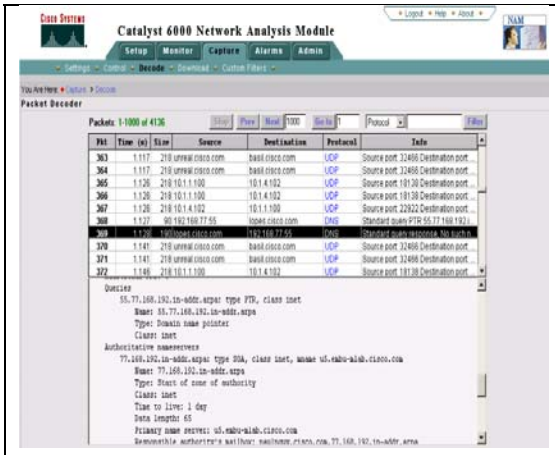
2.H - Voice Call Detail and Quality



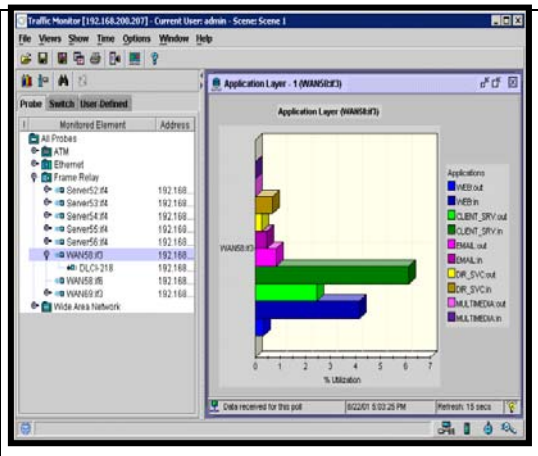
2.I - Alarm Thresholds



2.J - Switch Port Utilization



2.K - Packet Capture and Decode

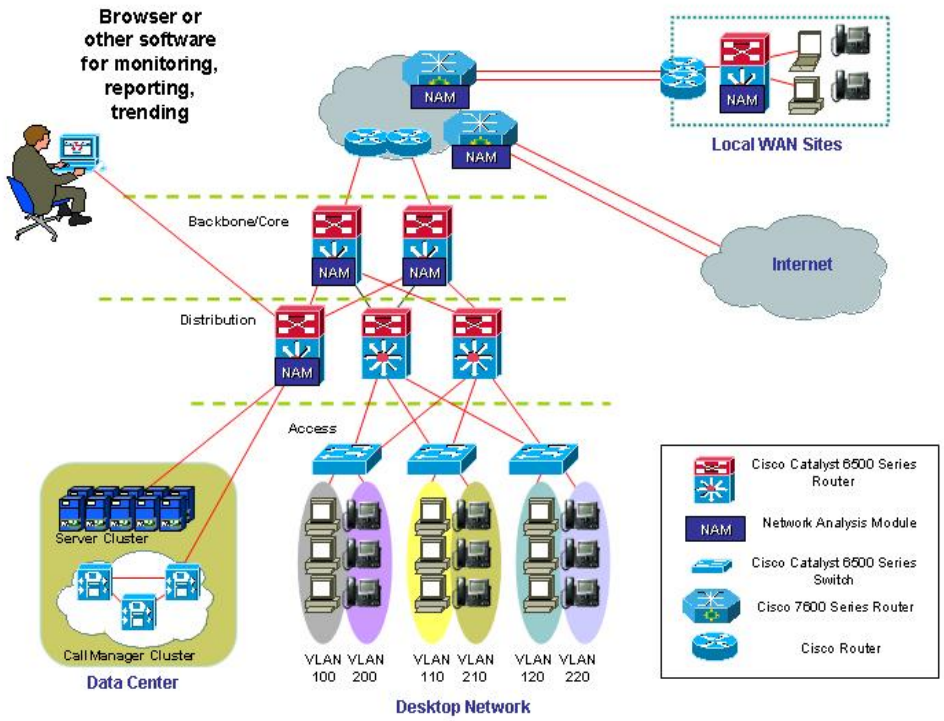


2.L - Application traffic per Interface

NEXT STEPS

Cisco IT is working to develop a comprehensive, next-generation picture of what the network is doing and how it will be managed. NAM is an important player in the new architecture. Beyond the data centers, IT plans to install NAMs in both Internet (Cisco CCO and Cisco.com) environments and in the core backbone, because the NAM was designed to work in both Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers (see Figure 3). It performs the same functions in those environments, as well. NAM is in the planning stages for worldwide adoption, in both the Asia-Pacific region and Europe.

Figure 3. Proposed Future NAM Architecture: Monitoring Data Centers, Internet Access and selected WAN links



Cisco IT uses other tools to use NetFlow information in detail, such as Arbor PeakFlow and NetQoS Reporter Analyzer. “Although the NAM uses NetFlow data and can do NetFlow analysis,” says Ng, “for a complete network analysis picture right now, I believe we need to use SNMP, NetFlow detail, RMON, and packet capturing and analysis. We also need NAM data to help troubleshoot VoIP traffic.”

Ng discusses planning to use NAM: “Cisco is also coming out with more network analysis technologies. Some of these technologies will either be integrated or used with Cisco IOS® Software. As more of the technologies mature, I think we will need to find network management software that will be able to analyze data from various sources to form a complete view of traffic across the network. You have to look at all the players—devices, applications, servers, and server farms. Are they doing what they’re supposed to be doing? NAM enables much better capacity planning—there are a lot of things that you can figure out from the information that the NAM delivers. As more things come onto the network, you need more and better analysis and analytical tools. NAM is key.”

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.**