How Cisco IT Deploys Closed-Circuit TV Cameras over the Secure IP Network

Cisco migrates fiber traffic to IP network and network video recorders to data center.

Cisco IT Case Study / Security and VPN / CCTV on IP Network: This case study describes how Cisco Systems transitioned from using analog closed-circuit TV for surveillance to digital closed-circuit TV over IP. 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.

"Cisco Safety and Security—Investigations and operations personnel can access surveillance video of the past 30 days, from any facility worldwide, by pulling it from their own PC terminal. Access to archived video on demand accelerates evidence review and improves evidence control."

– Bill Jacobs, manager of Security Technology and Systems, Cisco Systems

BACKGROUND

At Cisco Systems®, the Safety and Security department manages internal security for more than 300 facilities worldwide. Based on the size and risk level of a facility, the department deploys security technologies such as physical intrusion detection and electronic security access control systems, including more than 6000 card readers and more than 2600 closed-circuit TV (CCTV) cameras for surveillance.

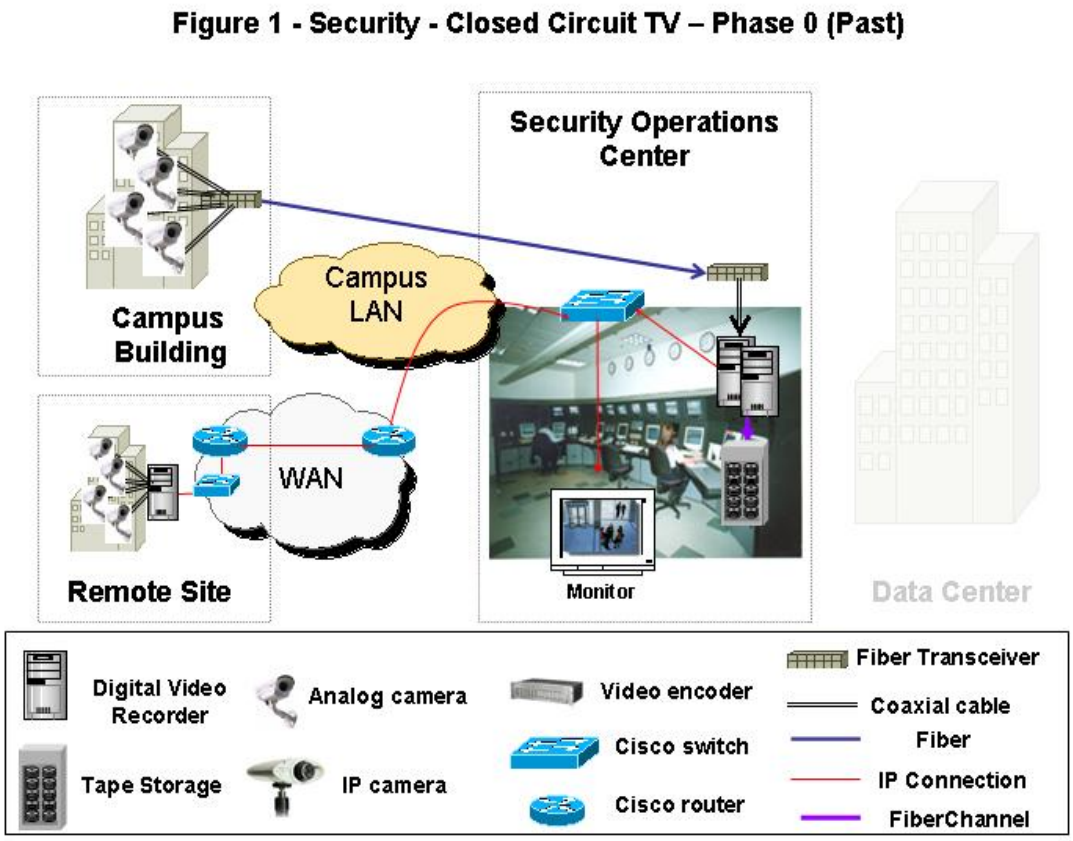
When Cisco® first began using CCTV for surveillance, analog cameras at building entrances and other high-security locations sent analog video signals over coaxial cable to video cassette recorders (VCRs) that recorded onto tape. Managing the tapes was labor intensive and prone to human error. Cameras were multiplexed in groups of eight or nine. They captured action at the rate of 1.88 frames per second, and each tape could hold only one day's worth of video. As a result, for every VCR in operation, Cisco needed to store 31 tapes—one for each day of the month. A month's worth of video from the current 2600 cameras would fill nearly 10,000 tapes. Security guards personally had to visit each building daily to verify that the recorders were operating (tape review) and then remove, label, and store the old tape, and insert a fresh one. Forgetting to press the record button meant a day of lost video—and the risk that Cisco would have no video evidence to investigate an incident. In addition, if a break-in or theft occurred, the facility had to send the physical tapes to the Safety and Security department at Cisco headquarters, resulting in investigative delays of up to several days.

In 1999, the Cisco Security, Technology, and Systems (STS) department surmounted these difficulties when it transitioned from VCRs to a third-party digital video recorder (DVR) card running on a Microsoft Windows NT 4.0 server platform that Safety and Security supported without help from IT. An economic evaluation proved that a systemwide conversion from VCRs to DVRs would save worker resources (no one would be replacing tapes), and support faster and more efficient video retrieval during investigations. The analog camera continued to send an analog signal over coaxial cable, but rather than capturing the video on a VHS tape, Cisco captured it on a proprietary card in a server that converted the signal to digital and then stored the digitally-encoded video on a local hard disk (see Figure 1). Because the DVR software could be programmed to store only the video that included motion, Cisco could store data collected during an entire month on direct attached storage within the DVR server. To preserve LAN and WAN bandwidth, Cisco security operations personnel "pulled" the video over the network only if

they needed it for incident investigation.

This case study begins when Cisco transitioned from its original proprietary DVR solution to a network-centric application that Security Operations controls and IT supports from its existing server and network operations centers. The new IT-supported system reduces costs at the same time it improves the effectiveness of surveillance video.

Figure 1. Previous CCTV Solution (Phase 0)



CHALLENGE

After the Cisco Safety and Security department began storing digital surveillance video on DVRs, the system grew until the STS department found itself managing more than 330 servers at Cisco facilities worldwide. The department was overburdened by the need to keep so many servers online and up to date with the latest software patches. “One hardworking IT administrator can take care of 100 boxes, and we had three times that many,” says Ken Lang, STS video program manager. Adds Jacobs, “The major problem resulting from our transition to digital surveillance video was that servers with hard drives require a higher management skill set compared with VCRs. Traditional security investigators don’t understand patches, secure access, and data backups, and these are among the IT Infrastructure group’s core competencies.”

Another powerful incentive to find an IT-managed solution for CCTV over IP arrived in 2003 in the form of the Nimbda virus. “One morning, IT informed us that about a third of our servers were infected,” says Lang. “That was our wake-up call to abandon the “silo” support model, where we purchased and self-managed equipment, and instead to work closely with IT to deploy standard server equipment for CCTV.” By collaborating with IT, the Safety and Security department mitigated the risk of being unable to record or retrieve surveillance video due to a malfunction of the server hardware or software.

Working with Cisco IT, the Cisco Safety and Security department established the following criteria for its new CCTV over IP system:

- IT standards-compliance—The system would conform to IT standards for the server platform, operating system, and virus software. Because IT agrees to support standards-compliant platforms, the STS group would shrink its management responsibility to the application software and associated device peripherals, and it meant that the solution could no longer include non-IT-standard video cards in the servers. “We wanted the server and everything in it to belong to IT and everything associated with the security applications and the cameras to belong to Safety and Security,” explains Lang. “That meant that the encoding could no longer take place on a card inside the server chassis but would need to happen in a dedicated video encoder outside the server.”
- High video quality—The higher the video quality, the easier to identify faces. The target was four frames per second, as compared to two frames per second on the previous system, or 1.88 (multiplexed) on analog tapes.
- Enterprise-friendly topology—Previously, STS maintained a separate database for each remote DVR. By centralizing the CCTV video database into four regional database environments that would replicate back to an enterprise master, Cisco would simplify management and lower equipment costs.
- Network-friendly design—To ensure that the system would not saturate network bandwidth, STS met with the Cisco IT Transport group. Together, they determined that for remote sites with limited WAN bandwidth, the video-recording server would reside at the facility itself rather than at Cisco headquarters. Surveillance video would travel over the WAN only if security operations personnel explicitly retrieved it during or after a security incident, retaining their “on demand” philosophy.
- Integration with access control and intrusion detection section—The ability to integrate, or unify, the CCTV surveillance system with alarm systems would increase the effectiveness of security operations personnel and lower the expense of responding to false alarms. “Say a lobby ambassador feels threatened and presses a button to send an alarm to the operations center,” says Deon Chatterton, program manager for the STS group. “We might want that action to push the real-time surveillance video to security operations personnel, so that they can see the situation and take the appropriate response.” This unification capability would reduce the false alarm rate, which exceeds 90 percent in most organizations. In another instance, the security officer might determine that the source of a “door-forced alarm” was a gust of wind. Video verification over IP increases speed of response and accuracy of information (alarm) validation.
- Upgradability—Finally, Cisco wanted its new CCTV solution to accommodate new technologies as they matured, including IP video cameras and audio capture, video analysis, integrated facility management, and expert information engines, as well as network management technologies such as Simple Network Management Protocol.

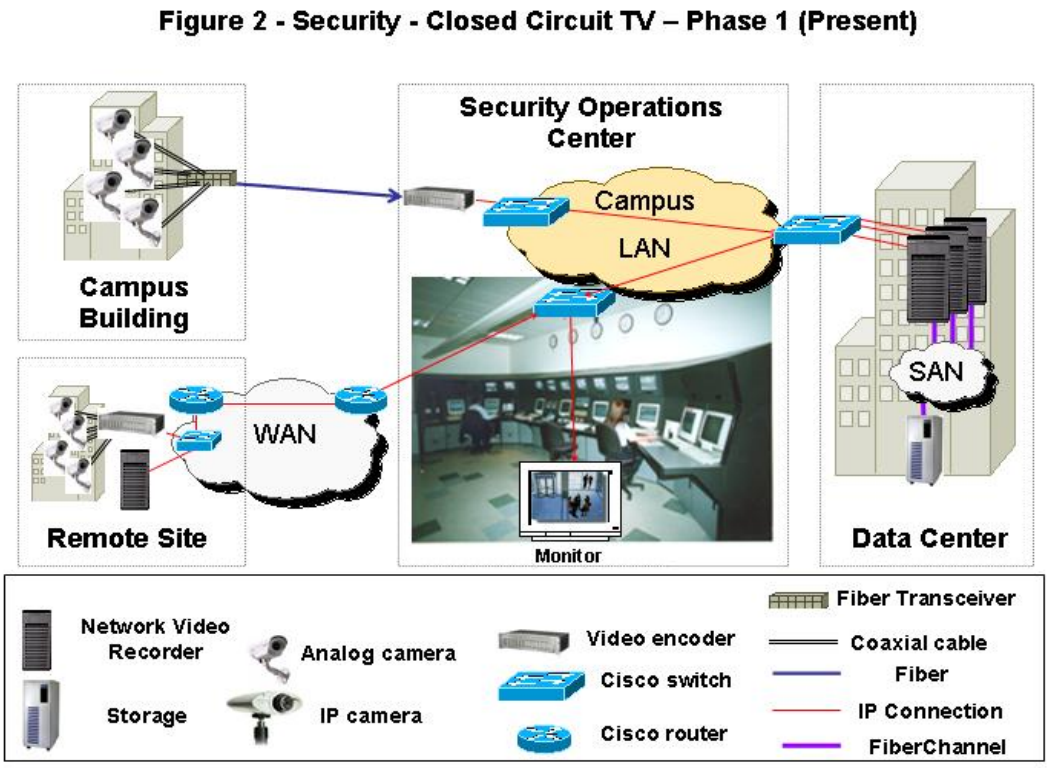
SOLUTION

After evaluating nine video management software technologies against the selection criteria, Cisco chose a digital video system that provides a software-only solution that runs on standards-based servers—Network Video Recorders (NVR). Today, many different and mutually exclusive video protocols exist, and most equipment supports only one or two of these protocols, which makes it difficult to integrate new cameras and network video recording servers into an existing security environment. Compatibility with existing security systems helped drive the Cisco STS group’s selection of these NVRs. “Encoding standards still vary, and our new NVR solution integrates well with our current Intrusion Detection alarm system, fire alarm software, access control badge readers, and visitor management database for badges,” says Chatterton. “In fact, we can pull up video data and compare it on screen to badge pictures and data with a single user interface.”

Cisco selected a global service delivery organization as the implementation arm for the new solution and deployed

the solution in eight pilot locations worldwide. These include a mix of campus environments and remote locations—San Jose, California; Research Triangle Park, North Carolina; Pleasanton, California; Bedfont Lakes, United Kingdom; Amsterdam, Netherlands; Warsaw, Poland; Tokyo, Japan; and Sydney, Australia.

Figure 2. Present CCTV over IP solution (Phase 1)



Surveillance video is captured, stored, and retrieved at the pilot sites, as shown in Figure 2:

Analog cameras capture video, sending it to video encoders over coaxial cable. Each video encoder accepts video from four cameras.

The video encoder converts the analog signal to a video signal for transmission over the IP network and sends it to the new NVR in one of three data centers for processing according to the rules that Cisco has established. For instance, Cisco STS can program the software to record only in the event of motion and to issue alarms in the case of other events such as abrupt motion or motion that occurs between certain hours.

In remote locations, data is stored locally on direct attached storage within the NVR server hard drive. In campus locations, with its greater camera volume, data is stored on low-cost Clarion storage area network (SAN) frames in data centers. When the storage capacity of the system is exceeded, each new day's video overwrites the oldest stored video files, which are at least 30 days old.

Cisco security operations personnel can access surveillance video from at least the past 30 days from any facility by pulling it from their own terminals. "Access to archived video on demand accelerates evidence review and improves evidence control," says Jacobs. "It also reduces the investigation manpower we need, because we don't need to send investigators to other facilities as often as before. It allows us to centralize our function and perform global investigations over the WAN."

With the previous system, the surveillance cameras had to be within 1000 feet of the recording device over coaxial cable; longer distances required fiber connections. Now that encoding occurs in a separate device, the NVR server

can be located anywhere on the network. At San Jose headquarters, for example, Cisco centralized servers in two data centers to simplify management. Physically separating the encoding device from the server has another advantage, as well: The server no longer needs to devote compute cycles to managing video cards and compression. In fact, after the transition, each server can manage 32 cameras compared to the 8 to 16 it managed previously, reducing server hardware requirements from more than 330 to 172, or almost 50 percent.

Protecting LAN and WAN Bandwidth

Before deploying the CCTV over IP solution companywide, Cisco IT Transport estimated the LAN and WAN traffic that CCTV over IP would generate to be sure that the solution would not consume more bandwidth than was available. “Throughout the project, we were very careful to protect data center LAN links from too much traffic,” says Keith Brumbaugh, Cisco IT WAN engineer. At San Jose headquarters, for example, Cisco decided to send traffic from various cameras to two different data centers, to prevent any single LAN segment from taking too big a hit. “In fact, CCTV over IP has manageable impact on the LAN,” Brumbaugh says. In no cases does surveillance video stream over the WAN unless a security operations staff member explicitly requests a live or stored image; for example, during incidence response. “Storing video on local servers is what protects the WAN,” says Brumbaugh.

The Safety and Security group deploys the CCTV over IP solution differently for the campus LAN environments, which have data centers, and the remote locations, which do not. In the campus environment, cameras remain where they were previously and video encoders are installed in the same location as the previous DVR servers. The new NVR servers themselves have been centralized in the campus data centers. On the San Jose campus, for example, all 700 cameras in various buildings report to two data centers. “By using the Cisco LAN backbone and offloading the video encoding, we reduced the number of servers needed in San Jose from 53 to 23,” adds Chatterton. In smaller Cisco offices, the cameras, encoder, and NVR connect to a Cisco switch so that normal surveillance video traffic remains behind the switch.

Security

An added advantage of moving the DVR servers into the Cisco production IT data centers is that they receive corporate enterprise-level security and management. A dedicated support team monitors and manages the servers 24 hours a day, year round. The IT hosting team consists of experienced systems administrators whose core expertise is the care of Windows servers like the DVRs. The data center supports physical security and two levels of power backup (uninterruptible power supply and generator backup). Data is stored in a fully Redundant Array of Independent Disk (RAID 5) arrays, and additional data backup (using Veritas NetBackup) is being planned. In addition, this data can be backed up in an alternate disaster recovery data center across the country.

Within the storage area network, storage is secured using array-level Logical Unit Number masking and SAN zoning. Access to the Cisco Multicast Distributed Switching SAN switches, like all Cisco hosts and switches, is password protected.

Within the data center network, access is limited by access control lists (ACLs) and by stateful firewall ACLs at the gateway routers. In addition, the security video hosts are isolated on a separate subnet. A number of potential attacks are mitigated by port security and traffic restrictions throughout the data center.

RESULTS

Migrating to CCTV over IP has yielded the following benefits for Cisco:

- Lowered storage requirements by 60 percent, representing US$500,000 in savings. The new system reduces storage volume requirements because it has the intelligence to store video only if motion is detected.
- Reduced the number of servers by 40 percent, representing $200,000 in savings. Servers support nearly double the number of cameras they did previously because they no longer need to devote compute cycles to video encoding.

- Improved video quality. At four frames per second, the ability to recognize faces is vastly improved over the previous system's two frames per second.
- Gained ability to unify the CCTV system with other security systems, such as alarm detection and access control systems.
- Reduced false alarms in areas covered by video surveillance cameras by an anticipated 90 percent, by giving security personnel the ability to view the associated video in real time.
- Mitigated risk by expediting maintenance and repair. "When a proprietary box broke, we had to dispatch local security integrator technicians, who often were unfamiliar with our site requirements, to come on site and work with in-house video system technicians," says Chatterton. "Remediation might take five days or longer. Now we have a two-hour response and 24-hour turnaround for repair."
- Trimmed the time required to investigate security incidents. Security Operations Center and other authorized safety and security personnel can view stored or real-time CCTV video from any camera around the world, responding more quickly and appropriately to incidents. Investigation is further accelerated because investigators can retrieve more video at one time. "Our old software limited the amount of video we could pull on-demand to one hour's worth," says Lang. "With our new NVR system, we're limited only by processing power, so we can easily pull 24 hours' worth of video at a time." To speed investigations further, the software allows Cisco Security Operations to highlight only the changes to a particular area of the video footage, such as a desktop.
- Reduced maintenance costs by 20 percent because Cisco IT has economies of scale and spends less time monitoring and maintaining servers.
- Increased security. "Now that we're standards-based, the system is much more secure," says Chatterton. "Network protection and virus definitions are implemented as soon as available instead of when we get to it." Cisco IT has contracted through a global service provider to deploy remote security-related updates. The system has paid for itself more than once by enabling the Safety and Security department to apprehend people who had stolen equipment and then recover the stolen property.

NEXT STEPS

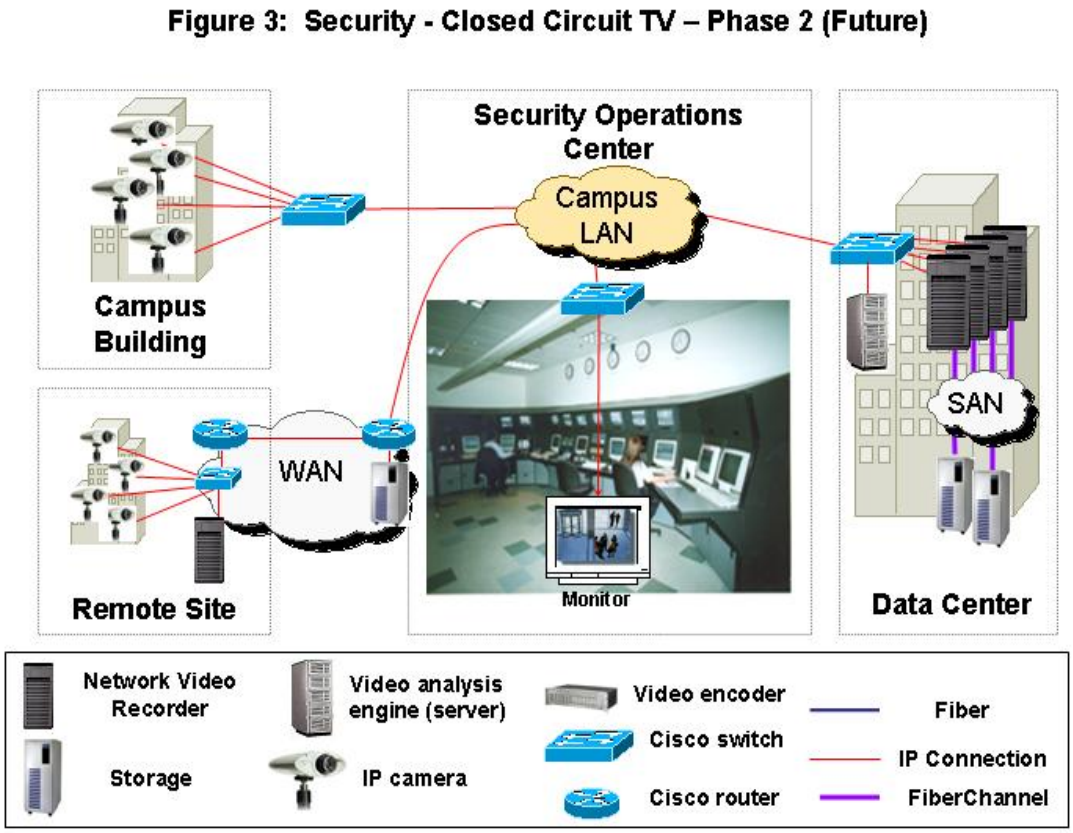
The STS group is monitoring the evolution of IP cameras to replace the existing analog cameras. When this occurs, traffic will be sent directly from the IP camera to the data center, eliminating the need for standalone encoders and freeing fiber for Safety and Security to use for other purposes, if needed (see Figure 3). A major condition for migrating to digital cameras is the development of a format with lower bandwidth consumption. In a small sales office with a T1 line, two cameras presently generate 600 Kbps— more than a third of available bandwidth—making it impractical to transmit video over the WAN unless a security incident occurs. If a new format emerges with lower bandwidth consumption, for example, 30 Kbps per camera, then transmitting video from remote offices will become feasible. In the meantime, STS is investigating more flexible and capable video encoders to allow them to use a variety of legacy and newer cameras. Another possible solution that STS is considering is using storage equipment in WAN hub sites to support collection and storage of more remote site data without requiring it to be stored locally or transmitted across the WAN and burdening WAN links..

Another promising technology advancement that the STS group is actively pursuing is video analysis engines that monitor the surveillance video for violations of Cisco business rules—for instance, an individual walking the wrong way in a one-way area, standing in front of a lobby desk for more than a certain number of seconds, or leaving an unattended package. They could track and respond to people "tailgating" into buildings; that is, people entering the building directly behind employees who have correctly used their badges to unlock the door. "With this capability, surveillance video becomes a tool for prevention and early detection rather than simply reaction to incidents," says Chatterton.

Other departments in Cisco have begun inquiring about using surveillance video for their own uses. The Cisco

Workplace Resource Department, for instance, is interested in using the video to determine the number of people who enter and exit a building each day. This information would be helpful to determine how many people remain in the building if evacuation is required. In addition, they could gather information about the number of visitors entering a building. Cameras located within the building can be used to determine where people go and how long they stay in different areas of the building, which is becoming more important as Cisco Workplace Resources is investigating different workspace configurations to improve employee work process and efficiency.

Figure 3. Proposed CCTV over IP solution. IP Cameras Replace Analog Cameras, Eliminating the Need for Separate Encoding Devices (Phase 2)



Cisco plans to unify the video and alarm systems so that when specified alarms occur, the associated video will immediately be available to security operations personnel, providing them with more information with which to plan a response.

LESSONS LEARNED

The chief lessons learned from the transition to digital CCTV pertain to making the best use of Cisco IT resources. “Physical security and IT security are converging,” says Chatterton, “and the two groups need to work more closely than before. When we managed the servers ourselves, a hardware or software problem was a serious issue for the department. Now we just generate a case and IT uses their technical resources and expertise to resolve the issue. We had to shift our culture to let IT do the work and run through its own processes.” Chatterton also notes that for a successful partnership, IT has to fully understand and agree with the project goals.

Another lesson learned is that training is essential. “As the use of technology for physical security increases,

computer-literacy will become increasingly important," says Lang. "Systems are no better than the competent people who run them. We need to do a good job of training investigative staff to manipulate and understand CCTV over IP." Chatterton and Lang have held training classes for Cisco staff across the United States, Europe, Middle East, and Africa, the Asia-Pacific region, and Japan.

Finally, Jacobs notes that the key to a successful CCTV over IP deployment is preplanning. "Make certain that you totally understand your own group's responsibilities and IT's responsibilities," he says. "And make sure that management understands the costs and implementation effort needed to get the project going." At Cisco, for example, IT agreed at the outset to provide the funding for the hardware, but acquiring the funds for installation, maintenance, and monitoring required negotiating. "For a global deployment like ours, it's helpful to work with someone who has authority to approve the project worldwide so that you don't have to negotiate separately with someone in each theater," says Chatterton.

All parties agree that the culture change required to partner with IT yielded dividends. "The increased reliability, increased accuracy, and reduced manpower requirements of a digital CCTV solution with IT management completely offset the costs," says Jacobs.

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.**