How Cisco IT Built a Medianet to Handle Bandwidth-Intensive Traffic

By planning for bandwidth and QoS, Cisco IT is ready for more video traffic on the corporate network.

Cisco IT Case Study/Video/Medianet: This case study describes the decisions and activities of Cisco IT for supporting growing volumes of video traffic within the Cisco network, a leading-edge enterprise environment that is one of the largest and most complex in the world. Key decisions over the years about the network architecture, multicast support, quality of service standards, and bandwidth in individual WAN links have simplified the deployment of new video technologies such as Cisco TelePresence™. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

CHALLENGE

From video downloads on an Internet site to company broadcasts to live meetings, video traffic is increasing on many corporate networks. Cisco has long transported many varieties of video traffic, along with data and voice, across its converged IP network.

> "Because we designed a Medianet, we do not need to rearchitect the Cisco WAN when we deploy high-demand applications such as TelePresence."
>
> **Craig Huegen, IT Director and Chief Network Architect, Cisco**

In the mid-1990s, Cisco began broadcasting company meetings and executive announcements to global employees. These live IPTV broadcasts originated from studios at Cisco headquarters in San Jose, California, and were streamed across the Cisco IP WAN using multicast to Cisco offices worldwide. Cisco began to use more video for employee training, sending large video files from servers at Cisco headquarters over the WAN to local sites, where the files were stored on content servers for faster access by employees. Cisco transported these early video applications on its IP data network, which had a client/server architecture.

Cisco also transported most of its intersite voice traffic between private branch exchanges (PBXs) across the IP WAN by converting the analog voice signal into IP before transport. However, in the late 1990s, much of the voice traffic that did not travel between major Cisco sites was sent over the Public Switched Telephone Network (PSTN). In addition, Cisco used digital switched services over the PSTN to support ISDN videoconferencing and transported security camera video within campus LANs across separate, dedicated fiber paths.

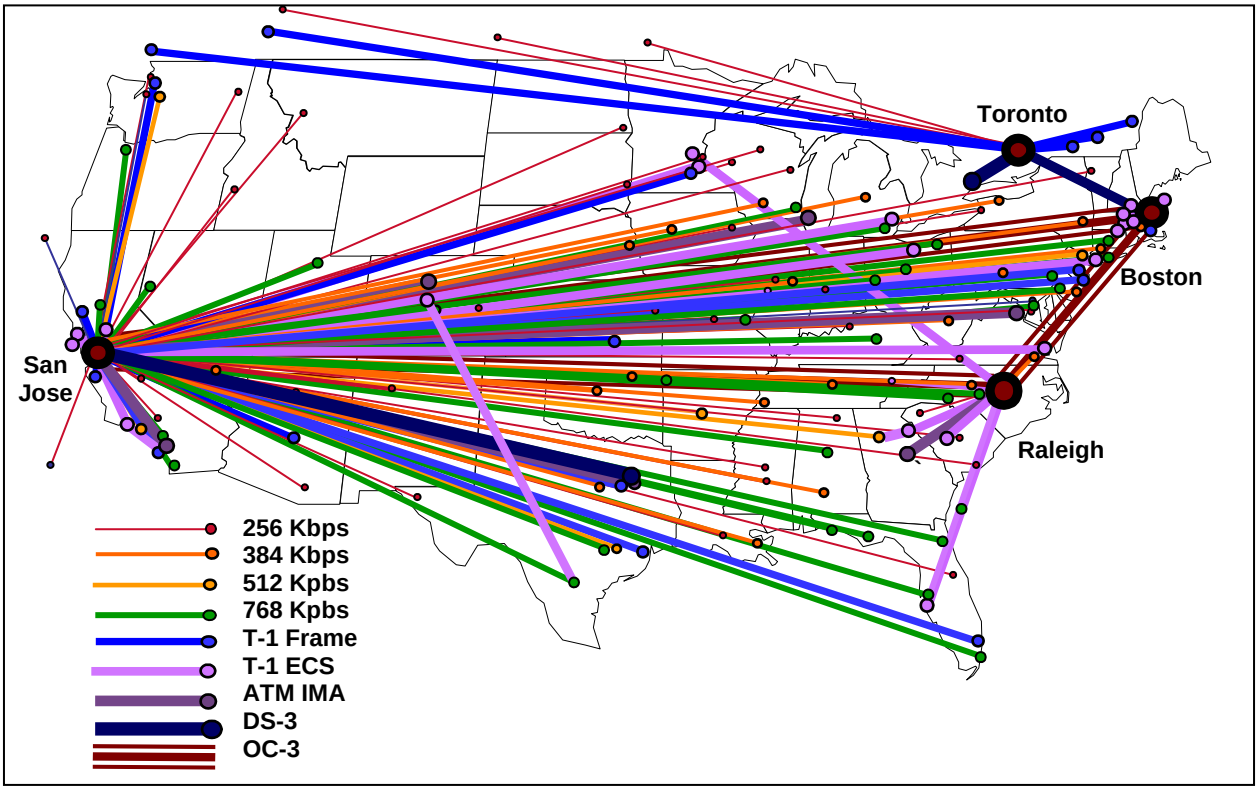
By 2001, the costs of supporting these separate networks were increasing as traffic volumes grew. Also, the potential of IP telephony and the collaborative potential of shared desktops and video conferencing encouraged Cisco IT to consider consolidating these separate networks. Clearly, the traditional client/server WAN architecture was no longer adequate to serve Cisco's communications needs.

In 2001, the original hub-and-spoke design of the Cisco WAN across North America had grown in size but was no longer adequate to support voice, video, or other collaborative, peer-to-peer services because the design was optimized for client/server applications. All Cisco data traffic from PCs and other clients in North and South America needed transport to and from Cisco's San Jose data center, so the network was designed with the shortest possible path from more than 100 locations to the one hub site (Figure 1).

The average site-to-hub-and-back circuit length for any traffic across the WAN was 1800 miles. This was an excellent design for client/server applications but a poor design for the new peer-to-peer applications such as voice and video,

where an IP data connection would be needed between any two or more people in any location. With the previous WAN architecture, all peer-to-peer connections had to travel through San Jose, which increased the delay for voice and video traffic to unacceptable levels.

Figure 1. US/Canada Cisco WAN in 2001: A Client-Server Architecture Based on SONET with Servers in San Jose and Clients at Branch Offices.



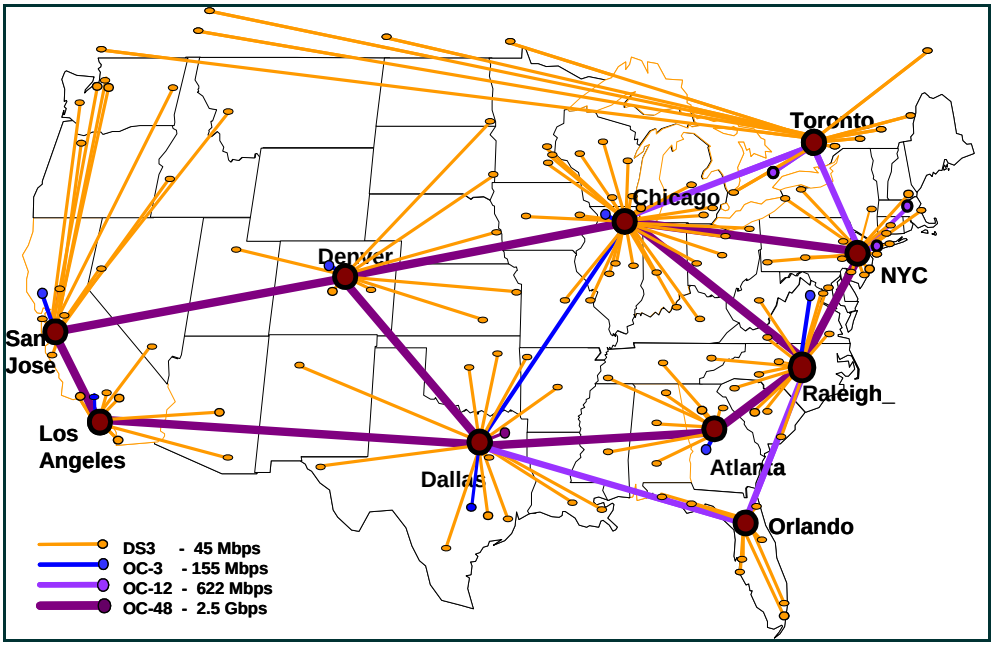
Cisco network managers needed a new architecture to converge voice, video, and data onto a single IP network. The new architecture would also benefit video and unified communications, because voice and video traffic have many of the same characteristics and network requirements: low-latency paths, sufficient bandwidth, multicast support for large streaming broadcasts, and quality of service (QoS) protection for all voice and video traffic to avoid delayed or dropped packets.

SOLUTION

The new WAN architecture in North America, built in 2002, met Cisco IT requirements (Figure 2). This peer-to-peer network architecture is similar to that of a small service provider network with a SONET-based ring backbone and access links that connect each Cisco location to the nearest hub site. The backbone architecture follows underlying fiber paths and helps maintain low latency.

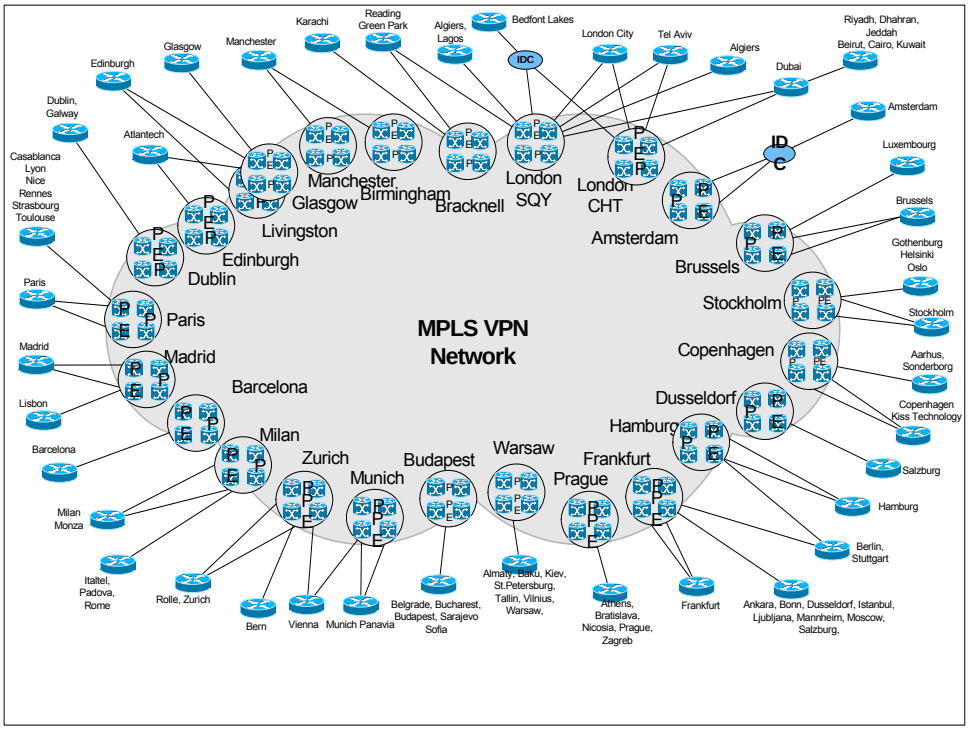
The backbone was first built with OC-12 fiber connectivity, which offers four times more bandwidth than the OC-3 circuits previously available in the WAN. Since initial deployment, Cisco has increased the backbone speed to OC-48.

Figure 2. US/Canada Cisco WAN in 2008: Peer-to-Peer Architecture Based on SONET (data endpoints can be added at any Cisco location).



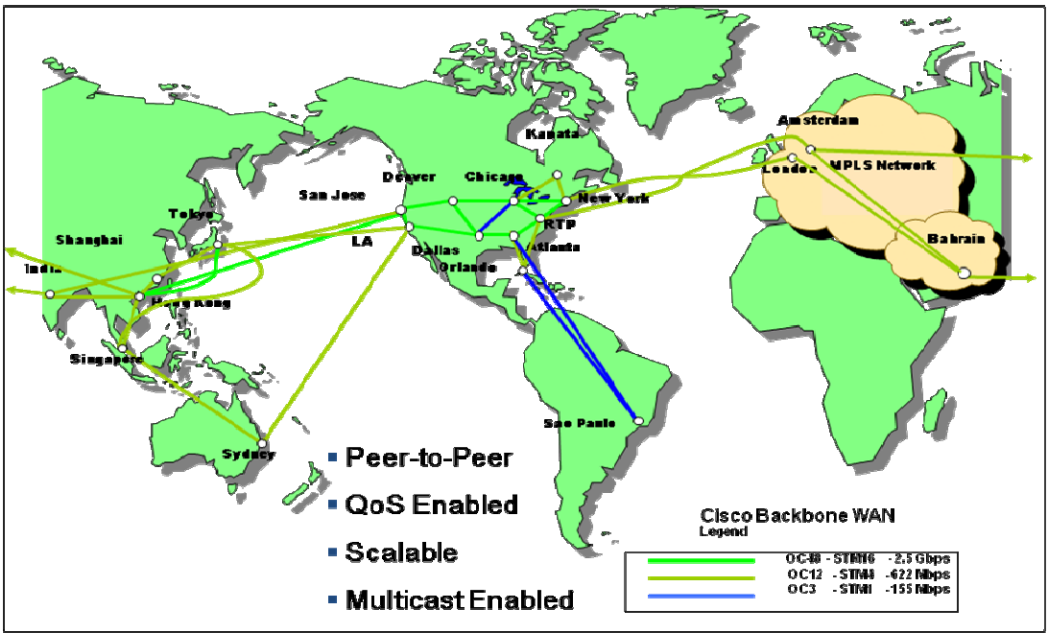
In Cisco's European and Middle Eastern regions, a Multiprotocol Label Switching (MPLS) VPN supports the new peer-to-peer network (Figure 3). This service is supplied by a Tier 1 service provider and runs on the provider's larger backbone network, taking low-latency paths that are made possible by the service provider's size and guaranteed by contractual service level agreements (SLAs). Cisco offices connect to the nearest hub sites on the MPLS VPN.

Figure 3. Europe Cisco WAN in 2008: Peer-to-Peer Architecture Based on MPLS VPN.



For both the US/Canada and European networks, connectivity to most smaller Cisco offices is typically provided through dual dedicated circuits that terminate on dual gateway routers at the nearest regional hub location. Globally, a high-bandwidth core network interconnects Cisco's regional hubs in the Americas, Asia, Europe, and the Middle East (Figure 4).

Figure 4. Cisco Global Backbone Network in 2009



Dual routers and dedicated circuits, on physically diverse paths when possible, provide redundancy throughout the Cisco network. In some instances, VPN connections have been added to the WAN to provide backup in case of cable failures.

Defining QoS for a Medianet

After implementing the new WAN architectures in the Americas and Europe, the Cisco network initially provided the low-latency paths and sufficient new capacity to support basic video communications. IP multicast support was continued, but the new network did not provide the levels of QoS needed for appropriate support of voice and video traffic.

The earlier WAN supported some levels of QoS for PBX-to-PBX voice traffic between major hub sites, as well as for some backup data. However, this QoS was applied within the affected few network nodes using access control lists in network routers. Because of this approach, the QoS mechanisms could not securely and accurately classify traffic from more than 70,000, IP phones, more than 1200 H.323 video conferencing units, and more than 240 TelePresence sites deployed within Cisco, as well as streaming and surveillance video traffic.

As real-time, interactive media applications such as voice over IP (VoIP) and IP video conferencing (IPVC) increased, Cisco IT needed to create a more rigorous QoS scheme for traffic classification that would be applied at the network edge. With the addition of TelePresence, with its significantly higher bandwidth requirements, special network treatment was necessary to protect TelePresence traffic and avoid interference with other video traffic. This QoS capability, and its ability to change as new media are added, is vital for creating a medianet.

QoS mechanisms define traffic identification, policing, queuing, shaping, and congestion avoidance to help deliver voice and video with appropriate performance levels. Understanding the distinctive characteristics of voice and video

traffic is critical because both applications are sensitive to packet loss, latency, and jitter (variable latency).

Without proper QoS policies, the perceived quality of voice or video drops whenever other application traffic creates delays for latency-sensitive voice or video content. Voice traffic consists of small packets that, without proper QoS handling, can be lost behind large data packets, causing voice quality problems. Video traffic is even more sensitive to packet loss, because the human eye can detect problems with video much more quickly than the human ear can detect problems with audio.

"By 2003, we needed to consolidate QoS across the LAN and WAN, because managing the access control lists on the edge routers was becoming such a big task. There was also a lot of inconsistency in QoS definitions among different sites, meaning packets could be marked in one way from site A but interpreted differently at site B," says Tom Wojciaczyk, a Cisco IT network engineer.

QoS is critical for interactive media such as voice and video conferencing. Voice packets are usually small, and risk getting delayed and dropped if they are trapped behind larger data or video packets. To avoid this risk, Cisco uses low-latency queuing (LLQ), which puts voice packets at the top of the queue when they arrive at each network hop.

Cisco IT also uses QoS to protect other video streams from the high bandwidth demands of TelePresence. By creating one QoS class for TelePresence and another QoS class for all other video, the Cisco network delivers appropriate service levels for applications such as room-based IP video conferencing and personal conferencing with Cisco Unified Video Advantage (Cisco UVA).

All other media described in this case study are considered noninteractive. These media, such as streaming IPTV and video-on-demand (VoD) downloads, closed-circuit TV (CCTV) surveillance camera traffic, and WebEx® and MeetingPlace® desktop sharing, are handled in the same QoS class as normal IP traffic. Moderate amounts of latency or jitter are handled by the router buffers and the application, so quality remains high without special handling.

Table 1 shows the classes of service defined for the Cisco network (as of mid-2008), covering all voice, video, and data traffic. Cisco IT configures routers with LLQ to prioritize sending real-time voice traffic from a local WAN interface, Class-Based Weighted Fair Queuing (CBWFQ) to provide a minimum bandwidth guarantee, and Flow-Based Weighted Fair Queuing (FBWFQ) to handle low-priority, "best-effort" traffic.

Table 1. Classes of Service Defined for the Cisco Network

QoS Class	Description	IPP*	DSCP**	Queuing Technique	Sample Applications
6	Network control/routing traffic	6 & 7	48-63	CBWFQ	
5	Voice bearer traffic	5	46	LLQ	IP voice from hardware phones or Cisco IP Personal Communicator software phones
4	High-priority video	4	32-39	CBWFQ	TelePresence
3	Signaling/high-priority data	3	24-31	CBWFQ	
2	Medium-priority video	2	16-23	CBWFQ	IP video, Cisco Unified Video Advantage
1	Batch/scavenger traffic	1	8-15	CBWFQ	
0	Default/best effort	0	0	FBWFQ	Shared desktop, noninteractive video such as CCTV surveillance cameras, IPTV, VoD downloads

*IPP = IP Precedence (or Type of Service) bits, the leading three bits of the Differentiated Service Code Point (DSCP), which summarize QoS classes. IPP bits are helpful when transporting QoS information across vendor network services, such as MPLS, that have limited service classes.

**DSCP = Differentiated Service Code Point, 6 bits (including the 3 IPP bits) used by Cisco at the trusted edge to mark different data streams and to control packet handling (which affects service quality during congestion) at each network hop.

Although QoS parameters determine the priority of different traffic types on the WAN, bandwidth allocations determine the maximum amount of bandwidth reserved for different traffic types during times of serious WAN congestion. For example, voice traffic might be allowed up to 10 percent of all bandwidth on the majority of WAN links, while video (a much larger consumer of WAN bandwidth) is allocated as much as 55 percent. Table 2 lists the bandwidth policies defined for each circuit type in the Cisco network WAN backbone. For more information on Cisco IT deployment of QoS, see the Cisco IT case study "QoS for Voice and Video" at http://www.cisco.com/web/about/ciscoitatwork/network_systems/qos_for_ip_voice_and_video.html.

Table 2. Bandwidth Allocation Percentages for Circuits in the Cisco Global WAN

Traffic Type (%)/Circuit Type	DS3	OC3	OC12	OC48	OC192
Control	1	1	1	1	1
Voice	10	10	10	5	5
High-bandwidth video	30	30	40	30	30
Signaling/high-priority data	2	2	2	2	2
Low-bandwidth video	25	15	12	17	15
Scavenger	1	1	1	1	1
Default	31	41	34	44	46
Total	100	100	100	100	100

WAN Requirements for a Medianet

Although video and voice traffic has grown quickly, these traffic types still account for only a small percentage of the total traffic on the Cisco WAN. TelePresence, with its larger bandwidth requirements, represents more than 8 percent of WAN traffic, a portion that is rising as more TelePresence systems are installed in more company sites (Table 3).

Table 3. Sample Monthly Voice and Video Traffic Volumes on the Cisco Global Network (April 2008)

Traffic Type	Volume	Percent of Total Traffic
TelePresence	328 TB	8.5%
VoIP	168 TB	4.4%
Other video	3 TB	.1%

Note: Other media traffic is not tracked separately from other IP data streams.

In addition to providing adequate bandwidth, the IP WAN must meet four design criteria to be considered a medianet:

- Minimize latency, no matter what transport technology is used (Cisco IT uses SONET and MPLS VPN).
- Provide the bandwidth needed to carry all offered traffic and allow scalability to meet all future traffic needs.
- Support multicast for one-way streaming media, such as IPTV and IP telephony "music on hold," to reduce the load on the WAN and the originating servers.

- Support a well-planned set of QoS policies deployed in the same manner across all LAN and WAN links to protect latency-sensitive voice and video traffic.

Whether voice or video, a recorded stream or a real-time interaction, each media application also has its own network requirements. Table 4 compares the network requirements of media applications used by Cisco; each application is discussed in more detail following the table.

Table 4. of WAN Requirements for Video Applications Used at Cisco

	Streaming and Noninteractive Media				Interactive Media				
	Video Surveillance Security Cameras	IPTV	Video on Demand	Cisco WebEx and Cisco MeetingPlace	ISDN Video (H.320)	IP Telephony	IP Video (H.323)	Cisco Unified Video Advantage	Cisco TelePresence
Business use	Real-time and stored security video	One-way streaming for company meetings, training	One-to-many downloads for training and meetings	Voice and video conferencing with desktop sharing	Cisco-to-customer video connections	Internal and external voice connections	Cisco-to-Cisco video connections	Video telephony calls within Cisco	Internal and external virtual meetings
Type of transmission	Multipoint to Point, Security system only	Point to Multipoint, IPTV Only	Point to Multipoint, VoD Only	Point to Multipoint	H.320 to H.323 gateways used for Point to Point	Point to Point or Point to Multipoint	Point to Point or Point to Multipoint	Point to Point (with either Cisco Unified Video Advantage or H.323)	Point to Point or Point to Multipoint
Endpoints (June 2008)	2400 cameras, 4 Security Operations Centers	4 studios to 70,000 PCs	4 studios to 70,000 PCs	70,000 PCs within Cisco	1200 endpoints configured; average 850 active	75,000 IP Phones	1200 endpoints configured; average 850 active	30,000 web cameras	350+ Cisco TelePresence units at 240+ sites (and growing rapidly)
Bandwidth required per endpoint	1-4 Mbps	128Kbps – 1.5Mbps	128Kbps – 1.5Mbps	Varies	384 Kbps	70-80 Kbps	384 Kbps + 20% overhead	384 Kbps + 20% overhead	Cisco TelePresence 3000: average 15 Mbps Cisco TelePresence 1000: average 5 Mbps
Quality of Service (QoS)	Default Data CBWFQ	Yes – Low-Bandwidth Video CBWFQ	Default Data CBWFQ	Default Data CBWFQ	N/A	Yes – Voice LLQ	Yes – Low-Bandwidth Video CBWFQ	Yes – Low-Bandwidth Video CBWFQ	Yes – High-Bandwidth Video CBWFQ
Multicast	No	Yes	No	No	No	No	No	No	No
Underlying network	IP LAN and WAN	IP LAN and WAN	IP LAN and WAN	IP LAN and WAN	ISDN over PSTN	IP LAN and WAN	IP LAN and WAN	IP LAN and WAN	IP LAN and WAN

Deployment Considerations for Specific Video Solutions

Different video technologies have different requirements for amounts of WAN bandwidth, QoS handling, and other network services.

Streaming Media

Streaming media communicates information from one location, one-way, to another site. This information can support a wide range of functions. At Cisco it supports building and personnel security, corporate communications, or training. Each of these functions uses the global reach of the Cisco corporate IP WAN (and in some cases the connected Internet) to bring information to people regardless of location, creating more options for where and how Cisco employees work.

Physical Security Monitoring

The first form of video used in Cisco was CCTV cameras for surveillance and physical security at its facilities worldwide. The video streams from more than 2600 building security cameras are sent to recorders within each site (in the building or at a data center on the campus LAN). Security personnel at centralized security operations centers can access the stored or real-time surveillance video for any location over the Cisco WAN and, when needed, send it in real-time to local police and fire officials.

Accessing security camera information remotely has reduced the number of false alarms by 90 percent and allowed Cisco to centralize its security functions and perform global security investigations over the WAN. Using the IP WAN for transport has eliminated the need to dedicate dark fiber in the campus metropolitan-area network (MAN) to security applications, which freed scarce fiber resources for other traffic.

Before deploying the CCTV-over-IP solution companywide, Cisco IT estimated the amount of LAN and WAN traffic that the surveillance video streams would generate in order to reduce the traffic's impact on the data center LAN links for video storage and the WAN when video streams are retrieved. For more information about this deployment, see the Cisco IT Case Study CCTV on IP Network at http://www.cisco.com/web/about/ciscoitatwork/security/cctv_on_ip_network.html.

Cisco IPTV

Cisco began using IPTV in 1997 to broadcast corporate meetings and training events from centralized studios to employees worldwide. Using IPTV added to the need for more efficient global video content distribution. It was immediately apparent that the local video servers, as well as the WAN links near the video server studios, would not be able to support the enormous number (sometimes tens of thousands) of unicast streams necessary to allow all Cisco employees to see the same live event at the same time.

Cisco broadcasts the same IPTV content at varying bit rates (typically 100, 500, and 700 Kbps). These streams are controlled via established "scopes" that help ensure only streams of an appropriate bit rate for a site's WAN bandwidth are delivered to that site. Support for multicast does not require new WAN equipment; instead it is activated within Cisco IOS® software.

As of 2008, Cisco supports 40-50 IPTV events every month, which are multicast across the LAN and WAN to avoid overloading the origin server and WAN links. For more information about this deployment, see the Cisco IT case study "Video for Companywide Broadcasts" at http://www.cisco.com/web/about/ciscoitatwork/unified_comm/ip_video_for_companywide_broadcasts.html.

Video on Demand

Employees can view recordings of previously streamed company meetings by downloading large video files across the WAN. Over time, this service was used to record and send training videos to Cisco employees, a solution that has almost entirely replaced expensive live training courses and associated travel costs.

By 2008, approximately 85,000 video files were downloaded every month across the WAN (about 60,000 internally, 20,000 externally, and 5000 as flash video downloads from blogs). These video files are sent in the same way as any other large IP file, without multicast or QoS. Although these file transfers can be handled without special equipment on the network, significant amounts of WAN bandwidth are saved by caching content in or near local Cisco offices worldwide. For details about how the Cisco network distributes broadcast and recorded video, see the Cisco IT case study “Enterprise Content Networking System” at http://www.cisco.com/web/about/ciscoitatwork/data_center/enterprise_content_networking_system.html.

Interactive Media

Cisco employees need to communicate in real time to solve problems and work collaboratively. Although the WAN can easily carry email and instant messaging, other forms of real-time collaboration require more network capabilities and bandwidth.

IP (H.323) and ISDN (H.320) Video Conferencing

Cisco uses more than 1200 H.323 video-conferencing systems that are installed in company buildings worldwide. This deployment is supported by a distributed environment of gateways and gatekeepers that are located in global regions, plus a single multipoint control unit (MCU) to support multipoint conferencing.

MCUs are required to support multipoint video-conferencing sessions. The MCU and meeting rooms are reserved by Cisco employees through a Microsoft Outlook calendar application.

When these video-conferencing systems are used between Cisco locations, the traffic remains in the original H.323 IP streams. Gateways, which translate H.323 IP video streams to H.320 ISDN, are needed when Cisco employees connect to external customer locations. These calls are translated by globally installed H.320 gateways, then sent over the PSTN. Cisco IT uses WAN routers (with the appropriate Cisco IOS feature activated) as gatekeepers to support the video-conferencing dial plan and route video calls between different video zones on the network.

H.323 video streams use a default bandwidth setting of 384 Kbps and QoS enabled on all WAN connections. Total bandwidth required on the WAN for H.323 video connections is 384 Kbps plus about 20 percent for transport protocol overhead, or about 470 Kbps per call. Cisco IT is considering doubling the size of the some of these video streams in the future to provide greater video resolution, which will help to improve employee satisfaction when this service is interconnected with Cisco TelePresence.

Several Cisco TelePresence multipoint switches support multipoint TelePresence conferences from major hub locations on the Cisco WAN. “When placing the TelePresence multipoint switches or MCUs, it is vital to remember the total bandwidth usage, latency within WAN links, and geography,” says Keith Brumbaugh, a member of the technical staff in the Cisco network implementation group. “For example, it may be more effective to place an MCU in a distant location where higher capacity WAN links are available to maintain high video quality.” Cisco IT’s MCU for IP video conferencing is connected to the backbone WAN by a pair of OC-48 (622 Mbps) links, which can support all IP video traffic offered.

For more information on multipoint video conferencing within Cisco, see the Cisco IT case study “IP Video Conferencing for Business Continuity” at http://www.cisco.com/web/about/ciscoitatwork/unified_comm/ip_videoconferencing_for_business_continuity.html.

Desktop Video Conferencing

Cisco Unified Video Advantage (Cisco UVA) provides video telephony functionality to Cisco 7900 Series Unified IP phones through a USB camera connected to a PC. With Cisco UVA, users make and receive point-to-point video calls, hearing the audio through a phone while the video stream is displayed on the PC. Employees find Cisco UVA very useful for unscheduled video conferencing, because this application does not require reserving a MCU or video conference room. They also use these cameras to create low-cost videos for blogs and other internal

communications.

No new network equipment was added to support Cisco UVA. Instead, Cisco IT upgraded the Cisco Unified Communications Manager to support the service and updated the H.323 gatekeepers to support interaction with IP video-conferencing equipment. Like the H.323 video streams, Cisco UVA calls require 384 Kbps, plus about 20 percent extra bandwidth for transport protocol overhead (about 470 Kbps per call)

Although nearly 30,000 Cisco UVA cameras were initially deployed to users in 50 major Cisco offices worldwide, this application has not added a significant traffic demand on the Cisco network. For a description of this implementation, see the Cisco IT case study "Cisco Unified Video Advantage" at http://www.cisco.com/web/about/ciscoitatwork/unified_comm/cisco_unified_video_advantage.html.

Cisco TelePresence

Cisco's internal deployment of Cisco TelePresence systems represents the largest demand for WAN bandwidth among all video applications. Although the rearchitecture of the Cisco network to support voice also served well for previous video traffic, TelePresence requires bandwidth upgrades and QoS refinements to deliver a high-quality user experience.

PRODUCT LIST

Routing and Switching
- Cisco 3845 Integrated Services Router

TelePresence
- Cisco TelePresence 3000 and TelePresence 1000 endpoints

Content Networking
- Cisco ACNS

Streaming On-Demand/Live
- Cisco Digital Media System
- Cisco IPTV

Interactive Desktop Video
- Cisco Unified MeetingPlace
- Cisco Unified Video Advantage
- Cisco WebEx

Video Surveillance
- Cisco Video Surveillance Manager
- Cisco Video Surveillance IP Camera

Video transmission is bursty, even by data standards, and very sensitive to dropped packets. Packet sizes and rates vary with the amount of motion in the video image, a factor that is amplified in a TelePresence session. When transmitting, Cisco TelePresence requires between 5 to 15-Mbps bandwidth into each meeting room, depending on the number of sites, plasma screens, and pixels per screen. For best performance, Cisco TelePresence requires one-way latency end to end of no more than 150 ms. Jitter cannot exceed 10 ms, and the target for packet loss is 0.05 percent.

Cisco chose to implement 1080p (ultra high-definition) resolution in all sites, and the initial tests indicated that local circuit bandwidth of 8–10 Mbps would be necessary. In some locations, upgrades to WAN circuit bandwidth were required, typically from a DS-3 to an OC-3 circuit or from multiple T1 circuits to a DS-3 or E3 circuit. To deliver the target performance levels for TelePresence sessions, Cisco IT also refined QoS policies to prioritize the bandwidth allocations to TelePresence traffic (Table 2).

Along with the WAN circuit upgrade, most local Cisco offices received Cisco 3845 Integrated Services Routers (ISRs) to handle the expected increase in network traffic of all types. For a discussion of Cisco IT practices for upgrading equipment on the Cisco network, see the Cisco IT case study "Network Infrastructure Program" at http://www.cisco.com/web/about/ciscoitatwork/network_systems/network_infrastructure_upgrade_program.html.

"Because we designed a medianet, we don't need to rearchitect the Cisco WAN when we deploy high-demand applications such as TelePresence," says Craig Huegen, Cisco IT director and chief network architect.

For details about Cisco's internal TelePresence deployment, see the Cisco IT case study "TelePresence Virtual Meetings" at http://www.cisco.com/web/about/ciscoitatwork/telepresence/telepresence_virtual_meetings.html.

RESULTS

The current Cisco network supports low-latency paths between sites with bandwidth sufficient for a variety of latency-sensitive voice and video applications. The network also offers multicast to support streaming one-way video for IPTV and robust QoS for supporting interactive media.

Cisco has realized many benefits from its evolution to a medianet, including simplicity, scalability, and the ability to

adapt to new traffic types and network technologies.

Easier deployment of new video technologies. The single, converged IP network transports all voice, video, and data traffic. This architecture simplified Cisco's deployment of new video technologies, including IP video conferencing, CCTV for physical security, collaboration tools such as Cisco MeetingPlace and Cisco WebEx, and Cisco Unified Video Advantage. Additionally, deploying Cisco TelePresence did not require a change in the overall network architecture, because Cisco had created a peer-to-peer and scalable WAN with QoS standards.

Scalability to serve growing traffic demands. The Cisco network has been able to accommodate growing volumes of video traffic through simple adjustments of QoS and bandwidth where needed.

Simpler bandwidth management. Standard QoS classifications across the network make it easier for Cisco network managers to see the unique impact and behavior of video traffic. By using standard QoS policy, capacity planning based on NetFlow data, and QoS classification maps, updating all routers in the Cisco network with new QoS policies can be automated.

Network positioned for the future. The simplicity and flexibility of the Cisco network will make it easier to support future video applications without significant changes in the basic network topology and features.

LESSONS LEARNED

From many years of experience in supporting networked video services, Cisco IT personnel have gained several key lessons.

A low-latency, peer-to-peer network design is essential. "Knowing the mileage of our fiber paths to calculate latency has been important for helping our network architecture accommodate growing levels of video traffic," says Brumbaugh. He notes that evaluating the buffer capacity in the routers and switches at local offices is also important for determining whether the network can adequately handle the bursty nature of video traffic.

Huegen adds, "If you are using an MPLS network or other service-provider managed link, it is important to make sure that when the committed rate is lower than the physical rate of the circuit, the service provider is offering adequate traffic policing in order to verify that data is not lost during video traffic bursts."

> "Defining QoS end to end for voice traffic really set us up well for adding video traffic to the network."
>
> **Tom Wojciaczyk, Cisco IT Network Engineer**

Define end-to-end QoS. Creating an end-to-end QoS architecture makes the network more stable and simpler to troubleshoot and manage. "Defining QoS end to end for voice traffic really set us up well for adding video traffic to the network. Proper classification means the traffic marking is preserved end-to-end and routers at different sites handle packets in the same manner. The standards also allow us to automate QoS configuration changes through our network management system," says Wojciaczyk.

Be proactive about WAN capacity management. As the popularity of TelePresence and other video traffic continues to increase, Cisco's network managers will regularly monitor bandwidth utilization and available capacity at all sites. "Because of the long lead times for provisioning circuits, especially in the WAN backbone, you need to be proactive about predicting demand and increasing WAN capacity before it is fully needed," says Jon Woolwine, a Cisco IT architect. "Adequate capacity across the network is essential to delivering the video quality levels that users expect."

Consider link redundancy and diversity. Cisco typically deploys fully redundant WAN circuits for each local office. However, in some locations this redundancy may be too expensive or may not provide the desired level of diversity because of limited path availability. Instead, it may be more cost-effective to use a lower-capacity circuit for the backup link and accept a lower level of network performance or service availability when that backup link is in use. This design is appropriate for locations where it is acceptable to lose high-bandwidth video services during occasional circuit outages.

Plan for differences in local regulatory issues. In some countries, video calls are covered by the same regulations as voice calls, and are not allowed to be transported on the corporate WAN. These regulations may prompt network managers to make different choices about the location for installing gateways and other equipment, as well as how voice and video calls are routed across the corporate and public networks.

Encryption can be implemented selectively. Although it may seem important to encrypt all video transmissions, doing so adds a significant bandwidth overhead of up to 25 percent in the packet size. Because this overhead would be very costly to support on all WAN circuits, Cisco IT has configured video applications to use encryption only in selected locations.

NEXT STEPS

Cisco IT staff anticipate continued growth of video traffic, especially for TelePresence, on the company's network. To meet this demand, Cisco IT plans to increase the amount of network bandwidth allocated for TelePresence traffic to as much as 50 percent of available capacity on some circuits. This change will:

- Support more TelePresence codecs and displays in large offices
- Support more multipoint TelePresence sessions
- Allow interconnection of TelePresence with H.323 video-conferencing systems and other cameras and displays
- Prepare for the anticipated use of Cisco TelePresence 500 systems in employee offices and homes

Cisco IT staff will continue to plan for expected growth in video traffic on the network and new video technologies. For example, Cisco IT is investigating support for higher-definition video for video conferencing, VoDs, and IPTV. Digital-media signage is being deployed in many company locations, and enterprise TV services are being tested in pilot projects. Cisco IT is working to integrate TelePresence, IP video conference, and Cisco Unified Video Advantage endpoints for collaborative video sessions.

Integrating these different video media will greatly increase their use, and managing these new media services will require new tools, including:

- Improved ability to monitor media streams and service-quality levels through network modules that allow for deep-packet inspection of media streams.
- Improved admission control, upgrading from simple mechanisms to protect voice-from-voice and video-from-video traffic to more complex policy preemption mechanisms to help ensure that end-to-end resources are available before permitting new video or other media sessions on the network.

Cisco IT is also considering plans to:

- Secure video streams by leveraging network virtualization, which will restrict access to some video streams through Virtual Routing/Forwarding (VRF) technology within the LAN and WAN.
- Design for nonstop communications by using the Performance Routing (PfR) feature in Cisco ISR routers and Stateful Switchover (SSO) support in the Cisco ASR 1000 aggregation services routers.

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.