How Cisco IT Uses IP Multicasting Globally

Scalable IP Multicast technologies simplify network-based video broadcasts.

Cisco IT Case Study / Routing and Switching / Enterprise IP Multicast: This case study describes Cisco IT internal deployment of IP Multicast 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 real-world experience in this area to help support similar enterprise needs.

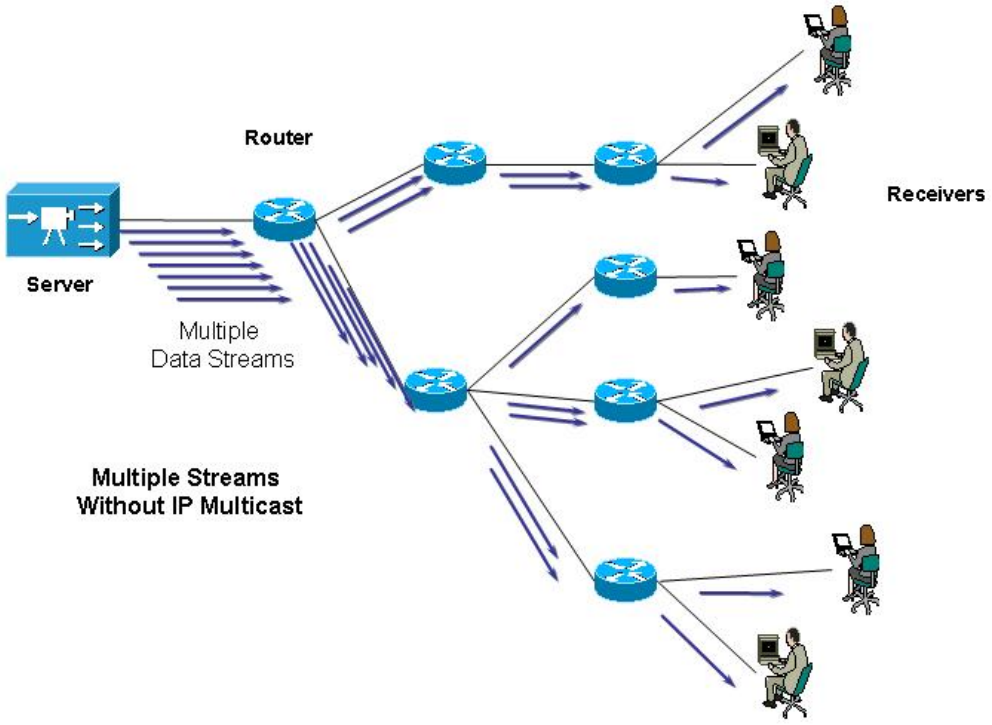
BACKGROUND

With a strong presence in North America; Europe, Middle East, and Africa (EMEA); and the Asia-Pacific region and supported by 35,000 employees worldwide, Cisco Systems® is a very large and growing enterprise. Consistent communications that reach everyone in a global corporation are a constant challenge. “One-to-many” communications, including training videos, corporate communications and meeting broadcasts, and Web content need to be uniform and available across the company.

CHALLENGE

In many ways, the solutions to bring consistent and available content were already in place. Cisco had brought to market Cisco IP/TV® technology, a powerful software application that delivers full-screen, full-motion video to desktop PCs, and deployed it internally in 1999.. Before that, Cisco groups would videotape meetings or training presentations and mail the tapes to remote sites for later viewing. Cisco IP/TV technology has made training and corporate communications available in real time over the Cisco global enterprise network to any Cisco location and over VPNs and the public Internet to remote-access sites like home offices. Cisco IP/TV central content-distribution points could deliver both real-time video and video on demand (VoD) to desktop clients. In 2002, Cisco IT deployed the Application and Content Networking System (ACNS) platform, which offered the Cisco enterprise a single, integrated caching and content-delivery platform for many network services. But all that data—video, graphics, and large-scale Web content—couldn’t scale when delivered simultaneously to thousands of Cisco employees in real time over enterprise networks. Cisco IP/TV technology streams MPEG video with audio streams at 100, 500, and 900 Kbps. Thousands of simultaneous point-to-point (unicast) video streams that size would overwhelm Cisco WAN circuits and would slow all traffic across the WAN (Figure 1). Cisco still uses unicast over VPNs for video streaming into home offices, but it is not the right solution for the one-to-many network broadcasts within the enterprise. Another option, using switched digital services from local carriers, would have been extremely costly. The Cisco IT team needed to implement a scalable and cost-effective transport solution within the corporate network that would allow applications such as a Cisco IP/TV solution, and eventually, Cisco ACNS, to deliver content.

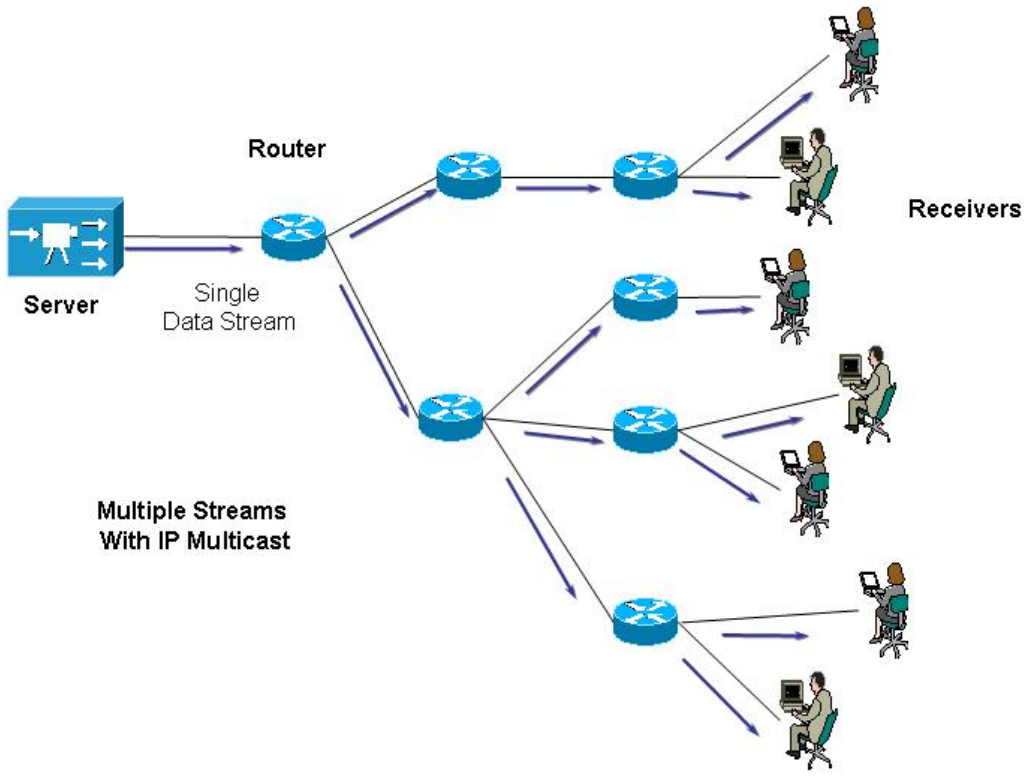
Figure 1. Multiple Streams Without IP Multicast



SOLUTION

It was obvious that Cisco had growing business needs for one-to-many communications: more and more training, quarterly meetings, and CEO talks needed to reach more and more people. The right solution, using the Cisco global enterprise network, had to be scalable and support hundreds or thousands of users simultaneously. That solution was IP Multicast—a network technology that enables multiple receivers to get identical copies of the same data stream at the same time, without putting more than one copy of the stream on any single network link (Figure 2). Each router in an IP Multicast group receives the data stream and makes a single copy to send to each downstream link that eventually connects to a broadcast receiver. Because multicast enables one-to-many transport, IP Multicast technologies based on Cisco IOS® Software were ideal to enable one-to-many content delivery and video applications. Mike Anderson, a network engineer involved in the IP Multicast deployment, talked about the advantages of IP Multicast: “The great thing about applications that can use IP Multicast, such as Cisco IP/TV technology and Cisco ACNS, is this: IP Multicast delivers a more scalable solution. It delivers a single thread of communication, a single source of communication or multimedia content and from that same source, you can build distribution trees for the stream of information—going to a remote office, many people—10, 100, or 1000 people can all get content from that same single source, enabling scalable content delivery across the network.”

Figure 2. Multiple Streams with IP Multicast



Cisco IOS IP Multicast in the Cisco Network

IP Multicast as defined in RFC1112, the standard for IP Multicast across networks and the Internet, supports one-to-many content needs by delivering application-source traffic to multiple users without burdening the source or the network, using a minimum amount of network bandwidth. At the point where paths diverge, Cisco routers replace IP Multicast packets in the network, resulting in the most efficient delivery of data to multiple receivers.

Even low-bandwidth applications can benefit from IP Multicast when there are thousands of receivers. High-bandwidth applications, such as MPEG video, may need a large portion of the available network bandwidth for a single stream. In these applications, IP Multicast is the only way to efficiently send the same content to more than one receiver simultaneously, because it makes sure that only one copy of the data stream is sent across any one network link. It relies on each router in the stream to intelligently copy the data stream whenever it needs to deliver it to multiple receivers.

Cisco IT supported Any Source Multicast (ASM), a “many-to-many” IP multicast technology, on the corporate network for more than four years. With ASM, a receiver joins a multicast group but has no ability to specify a single source for multicast traffic. Multiple sources can exist and all data from them will be received. If there is only one source (which is usually the case), ASM must go through several steps to determine that single source, and the best path to that source. In 2003 Cisco IT upgraded the network to support Single Source Multicast (SSM), a more efficient one-to-many technology. SSM enables the selection of a single source for IP Multicast data from the very beginning. This prevents traffic from other sources for the same group from being forwarded to the host, and also greatly simplifies the setup of an IP Multicast session. This upgrade resulted in changes both to the host signaling and to the IP Multicast routing in the network.

Host Signaling

IP Multicast operates by having each receiver join an IP Multicast "group" for that particular data stream. Each group has its own multicast IP address from a pool of IP addresses specifically saved for IP Multicast. Each receiver, usually the PC of a person requesting the data, uses the Internet Group Management Protocol (IGMP) to join the group. IGMP establishes host memberships in particular IP Multicast groups on a single network. It dynamically registers individual hosts in an IP Multicast group on a particular LAN. IGMP alerts all the routers and switches along the path which receivers are part of any IP Multicast group. Implementing IP Multicast requires that all the routers and switches in the network path support IGMP. Hosts that will be delivering IP Multicast content also identify their IP Multicast group memberships by sending IGMP messages to their local IP Multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which IP Multicast groups are active or inactive on a particular subnet.

The mechanisms of the protocol allow a host to inform its local router, using host membership reports, that it wants to receive messages addressed to a specific IP Multicast group.

All hosts wishing to receive ASM traffic must support IGMP Version 2 in the host stack and the application layer. IGMP Version 3 optimizes support for SSM, and is a requirement to deploying SSM on the network.

Multicast Routing

IP Multicast also requires a mechanism to transport content from the source to the end user efficiently over the enterprise network. The goal of multicast routing protocol is to enable the flow of IP Multicast traffic from the central source server to end users located at the edge of the network using the shortest and best possible path. After the routers and switches are aware of where the receivers are, they use Protocol Independent Multicast (PIM) to determine the shortest and best path from the sender to each receiver while avoiding any loops in the path.

PIM identifies the best possible path using the concept of network "branches" and "leaves." The network of paths connecting the IP Multicast source to all the IP Multicast receivers is seen as a tree. Each router subnet with a receiver is a "leaf" on the IP Multicast distribution tree. Routers can have multiple receivers on a single leaf, and can also have multiple leaves on different interfaces. When routers receive IP Multicast packets from upstream, they send a copy of each IP Multicast packet on each interface that has a leaf on it. Whenever a new receiver joins the IP Multicast group, a new leaf is added to the tree, and a new branch is built between that leaf and the IP Multicast source at the base of the tree. When a receiver leaves the IP Multicast group, if it is the only receiver in that leaf, the branch that it is on is pruned from the tree and the router stops sending IP Multicast packets out that interface.

PIM is protocol-independent and can use whichever unicast routing protocols are used to populate the unicast routing table, including Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) Protocol, Border Gateway Protocol (BGP), and static routes. Cisco IT uses EIGRP within the Cisco network. PIM uses this EIGRP unicast routing information to perform the IP Multicast forwarding function.

PIM has three different modes: sparse mode, dense mode, and sparse-dense mode. PIM sparse mode, used mostly for WANs, assumes that very few of the receivers connected to the WAN want to join the IP Multicast group, and so waits until a receiver specifically joins the group. PIM dense mode, used mostly for LANs and in older multicast applications, assumes that all receivers want to join the IP Multicast group, and so floods the network with IP Multicast session setup packets, and prunes back those network subnets that fail to respond or respond with no interest in joining the IP Multicast group. PIM sparse-dense mode (used in Cisco today) allows the network to determine which IP Multicast groups should use sparse mode and which should use dense mode. PIM sparse mode and sparse-dense mode require the use of a rendezvous point, which is a common router in the network that acts as a broker, enabling sources to register with this router and shared trees to be built from the receivers to the rendezvous point. When Cisco employees ask the sender to connect them to the IP Multicast data stream, the network forwards their requests to the rendezvous point, where they join that particular IP Multicast group.

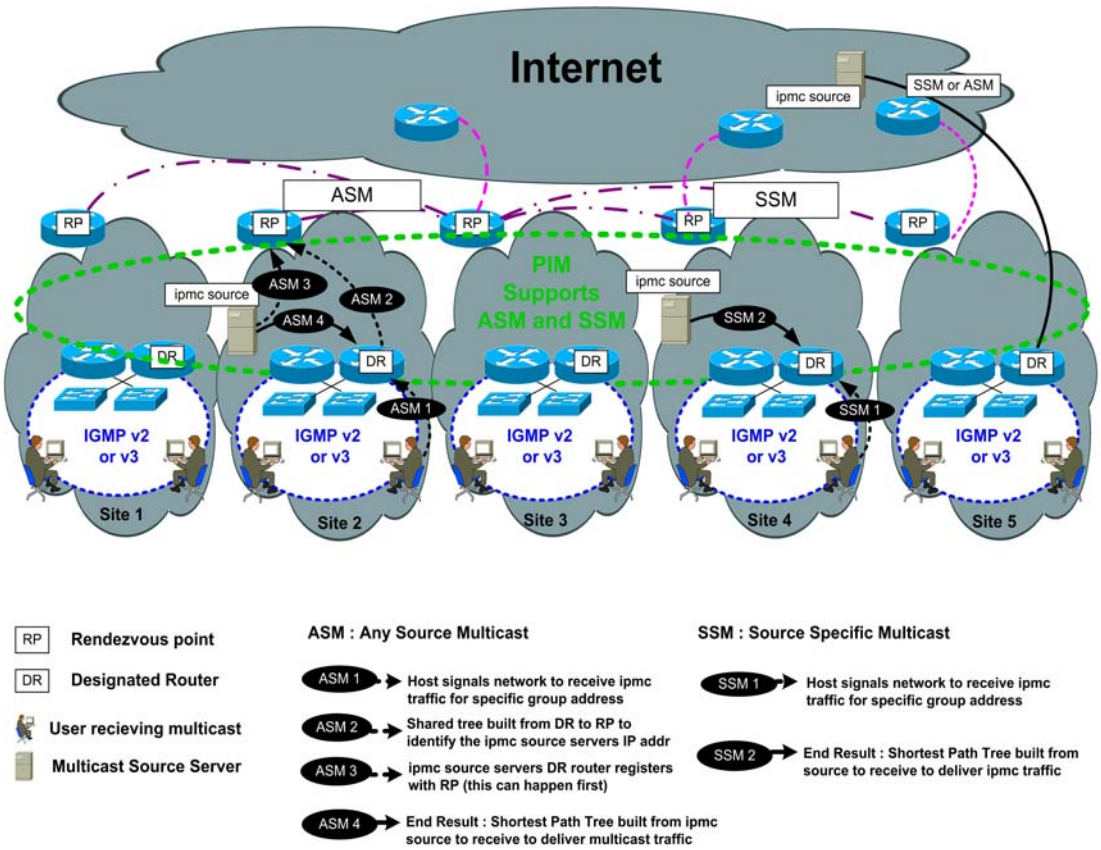
The IP Multicast packets sent to the rendezvous point from the source to register for a particular IP Multicast group are forwarded down the shared tree toward the receivers in that group. The edge routers learn about a particular source when they receive data packets on the shared tree from that source through the rendezvous point. The edge router nearest to the receiver then sends PIM join messages toward that source. Each router along the reverse path compares the unicast routing metric of the rendezvous-point address to the metric of the source address. If the metric for the source address is better, it will forward a PIM join message toward the source. If the metric for the rendezvous point is the same or better, then the PIM join message will be sent in the same direction as the rendezvous point.

Multicast Across the Cisco Network

Figure 3 shows how IP Multicast delivers data from one source to many interested recipients on the Cisco network, using either ASM or SSM. In ASM mode, the host first signals the network to receive IP Multicast traffic for a specific group address (ASM 1). Then a shared tree is built from the designated router to the rendezvous point to identify the IP Multicast source server's IP address (ASM 2). The IP Multicast source server's designated router registers with the rendezvous point (ASM 3), and then a shortest-path tree is built from the receiving designated router to the IP Multicast source to deliver IP Multicast traffic to the receiver. This setup process is quite complex and can cause some problems.

SSM is much simpler. First (SSM 1) the host signals the network to receive IP Multicast traffic for specific source and group addresses. The end result (SSM 2) is that a shortest-path tree is built from the receiver-designated router to the IP Multicast source to deliver IP Multicast traffic to the receiver.

Figure 3. IP Multicast Across the Cisco Network



Advantages of SSM

SSM enables a receiving client, when it has learned about a particular IP Multicast source through a directory service, to then receive content directly from the source, rather than receiving it using a shared rendezvous point. In an SSM-enabled IP Multicast network, the receiver will connect to the sending application (for example, will request information about a Cisco IP/TV broadcast that the user wants to join), and learn the IP address of the application server over HTTP. The receiver application then can signal the nearest router that it wants to join that particular source and can ask for it by its unique IP address. This SSM enhancement avoids all the initial ASM process of determining the IP Multicast source using a rendezvous point, and avoids the complex process of building a path to the source, because the IP network router already knows the best path.

SSM also resolves some other problems with the earlier ASM technology. In traditional ASM, if two applications with different sources and receivers use the same IP Multicast group address, receivers of both applications will receive traffic from the senders of both the applications. Even though the receivers can filter out the unwanted traffic, this situation will still generate a lot of unwanted network traffic. It can also cause IP Multicast address collisions. In addition, because ASM can allow multiple senders in an IP Multicast group, there is a potential network security issue as unintended senders could join the group and send unwanted packets to receivers.

Deployment

The Cisco IT team started its implementation of ASM in the United States in the late 1990s. The first phase of implementation was in North America, followed a year later by deployment in Europe, and two years after that, deployment was completed in the Asia-Pacific region.

Mr. Anderson addressed the question of planning IP Multicast for Cisco: “To implement IP Multicast for Cisco, we needed to enable it across the entire global Cisco IT enterprise network. This required a single global strategy for IP Multicast configuration on the network to ensure the reliable delivery of IP Multicast traffic. We needed to take a global approach, because we needed to scope IP Multicast traffic the right way.”

Predicting optimal delivery included understanding that some Cisco sites are connected to the WAN with smaller-bandwidth links, and that IP Multicast doesn’t negotiate a connection based upon the bandwidth of the available circuits. The source sends the content at a preconfigured bit rate regardless of the circuit bandwidth. For example, sending out a 900-kbps MPEG-1 video stream of IP Multicast traffic could cause problems if it were delivered over a single 1500-kbps T1 WAN link. To solve the problem, the IT team assigned specific bit rates to ranges of IP Multicast addresses. The team used the address ranges to build standard boundary access control lists (ACLs) that could be applied to WAN links of specific bandwidth to ensure that IP Multicast traffic with high bit rates wouldn’t flow across low-bandwidth WAN links. These administrative scopes were also used to determine the group address that should be allocated to someone responsible for an application or server sending IP Multicast traffic. For example a Cisco IP/TV server sending a 900-kbps MPEG-1 video stream would get a group address in a different administrative scope from an IP Multicast music-on-hold server sending a G.711 64-kbps audio stream.

The Cisco IT team planned a phased deployment. At the time, IP Multicast was in its early stages, and in the beginning, the complexity of IP Multicast made it challenging to support and challenging to make it work transparently. The biggest challenge came from traversing technology—IP Multicast needed to be delivered transparently across the variety of router and switch platforms already installed in the Cisco IT global network. Today, a more mature IP Multicast, combined with a greater standardization on hardware platforms, Cisco IOS Software versions/releases, and overall network topology work together to deliver more stable IP Multicast applications and data.

Mr. Anderson talked about large-scale deployment and automation: “Because of the size of the network, a great deal of the network configuration is automated. Automated configuration involves custom scripts or using our network management tool. The global Cisco IT network has thousands of routers; implementing new technologies manually

incurs costs from having engineers execute repetitive configuration commands on hundreds of routers, one by one. The IT team used *autoconfig*, a tool that maintains consistency across all the routers. The team used automated Perl scripts to configure IP Multicast commands at the interface level. Because the interface numbers change from router to router (each router is very specific), Perl automation was a great help. For example, we just completed a global implementation of SSM. We created Perl scripts to deploy the SSM and IGMP Cisco IOS Software configuration commands that the regional network engineers needed to execute. We also created a script that tracked the adoption rate of SSM globally so that each region knew its exact status. With these tracking mechanisms in place, it was easy to declare the project 100-percent complete. The entire project took about three months, but most of that time was devoted to coordination and management. Manual migration would have taken longer; automation shrank what could have been a much larger deployment window."

In July 2003 the Cisco IT team completed upgrades on 1035 routers worldwide to support SSM and IGMPv3 on the global enterprise network. Cisco IT had been supporting ASM for Cisco IP/TV delivery for more than three years; but SSM brings additional stability to the existing IP Multicast infrastructure. SSM, while a very new feature of Cisco IOS Software, greatly simplifies the process of setting up an IP Multicast stream between the origin and the user's PC. The network had to be upgraded to support IGMPv3, along with SSM, at all the user-connected edge routers, to allow the user's workstation to contact the network and provide it with the information it needs to set up the SSM distribution tree. Today the minimum software release required is Cisco IOS Software Release 12.1(8B)E14 for Cisco Catalyst® 6000 Series switches and Cisco Catalyst 7600 Series routers in the LANs and WAN, and Cisco IOS Software Release 12.2(13)T5 for the Cisco 3600 and 3700 Series multiservice platforms and Cisco 7200 Series routers in the WAN.

RESULTS

Cisco uses IP Multicast-enabled Cisco IP/TV technology to send corporate communications, including companywide meetings, training, and global team meetings. With dedicated video studios in San Jose, London, and Sydney, Cisco produces global and region-specific content for live Cisco IP/TV broadcasts or VoD presentations. This approach to communications saves travel time, resources, and still delivers consistent messages—from product training to business information—to all the Cisco employees who need to know.

IP Multicast also enables rapid one-to-many broadcasts of multimedia content from any content source on the public Internet. Cisco ACNS uses IP Multicast to allow content to be stored and forwarded—pushing popular content to the LANs at the network edge and letting users make many requests for the same content locally, thereby avoiding network congestion.

IP Multicast also provides Cisco with a fast and cost-effective way to scale these communications as the company grows.

NEXT STEPS

With the advent of unified networking, data and voice networks and networking capabilities have merged, and the power of IP Multicast can help save bandwidth through IP telephony applications. IP Multicast will support a new generation of telephony applications, including multicast Music on Hold and Info Cast.

Today, all Cisco IP phones rely on unicast technologies to provide music for callers who are on hold or being transferred. The IT team is testing the IP Multicast Music on Hold feature for future deployment. It relies on IP Multicast to provide a single stream of on-hold music for waiting callers. In a large campus environment with IP telephony, something as simple as the bandwidth consumed by hundreds of threads of music for waiting callers can affect the overall efficiency of the network. The IP Multicast Music on Hold feature is a great way to use IP Multicast to do more with the available network bandwidth.

Another possible future application to take advantage of IP Multicast in the Cisco network will be Info Cast. In

enterprises where IP phones are deployed throughout entire buildings, campuses, or sites, those IP phones can display one-to-many messages. Info Cast is a feature that uses IP phone message screens to receive IP Multicast-based one-to-many messages—very much like one-way instant messages such as reminders or emergency notifications.

CONTACTS

For more information about IP Multicast or other Cisco production deployments in the LAN or WAN, start a conversation with the IT experts in the Cisco@Work Campus, WAN, and Metro forum at:

http://iforums.cisco.com/iforum/servlet/SCom?page=scom&folderID=caw&CommCmd=MB?cmd=display_messages&mode=new&location=.ee77358.

For more information about IP Multicast as a technology, please visit:

http://www.cisco.com/warp/public/732/Tech/multicast/index.shtml.

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.**