



Cisco Manages the IP Telephony Environment for High Quality, High Availability, and Cost Savings

Cisco IT Best Practices / IP Telephony / IP Telephony Management: This case study describes Cisco IT's internal management of Cisco IP telephony technology 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

Companies worldwide increasingly are migrating to a Cisco Systems® IP Telephony environment. By the end of 2003, Cisco® had shipped more than 2.5 million IP phones; by 2006, the number has reached 8 million. Today, the Cisco IP Telephony environment uses a single network infrastructure for the transmission of data, voice, and video traffic to deliver high-quality IP voice and fully integrated communications. This enables enterprises to realize the business benefits of a converged network including increased productivity, business flexibility, and reduced operational costs.

For Cisco and other enterprises that deploy Cisco IP Telephony, the major concern is ensuring high-quality service along with high reliability of the combined voice and data network. Based on Cisco's own experience and success, enterprises can achieve the high levels of reliability required by a converged network, which is also highly scalable, easily managed, and cost effective.

Challenge

At a high level, the challenge for Cisco was in designing, implementing, and maintaining a highly available, reliable, and resilient converged voice and data network. Specific challenges included:

- Delivering voice quality and availability equal to or better than what users were accustomed to with legacy private branch exchange/time-division multiplexing (PBX/TDM) telephony
- Building redundancies into the network in addition to those found in traditional standalone voice and data networks
- Creating robust change management processes and standard practices
- Ensuring proper segmentation of voice and data packets on the same physical network as well as preventing data network security threats from affecting voice services
- Shifting from the traditional reactive mindset of monitoring PBX-based voice to a proactive mindset where problems are identified before they affect service
- Creating new, effective support models and procedures in this new converged environment



Solution

To address these challenges and ensure reliability, Cisco IT has focused on the areas of voice quality, availability, change management, security, monitoring, and support.

Voice Quality

Users are accustomed to hearing a dial tone and high-quality voice when they pick up the phone. They expect the same level of availability and quality in a converged environment. One of the first steps taken by Cisco IT was to perform a voice over IP audit to identify network readiness for voice. This included a review of the deployment of WAN and LAN quality of service (QoS) policies to ensure high-quality voice service end to end. It also included the deployment of auxiliary (AUX) VLANs (as illustrated in Figure 1) to logically segment voice and data to help support the voice-quality policy.

Figure 1 AUX VLANs

In a converged voice and data network, voice traffic must take precedence over other types of traffic that can tolerate latency. Cisco accomplishes that by trusting priority traffic, such as IP phone, video, interactive voice response, and IP Call Center traffic based on the voice VLAN. The Cisco standard practice is to rewrite other non-latency-sensitive data traffic to class of service = zero (best effort). Cisco also provides priority queuing at the WAN edge for both voice traffic and voice signaling traffic, to keep latency-sensitive voice packets from jamming behind large data packets in a mixed voice and data traffic jam.

Another critical step is to ensure consistent Call Admission Control (CAC) bandwidth parameters across the IP telephony infrastructure. Inadequate bandwidth allocation can affect every call on the segment—not just the last call to be established. Cisco IT ensures that bandwidth is allocated through an access control system, that QoS settings agree with the CAC parameters across the network, and that overflow traffic is routed over the public switched telephone network (PSTN).



Voice quality relies heavily on the bandwidth allocated to voice streams and to the analog-to-digital coder/decoder (codec) used to translate analog voice to a digital stream. Increasing bandwidth and deploying higher-bandwidth codecs to meet end-user expectations may be a consideration. Cisco IT tested several codecs, both in a lab environment and with a pilot group of users and steering committee. This ensured that it met the voice quality requirements of its end users. Cisco uses G.711 compression (supporting 64 kbps voice streams) locally in campus environments where bandwidth is plentiful. Across the WAN, where bandwidth is sometimes limited, Cisco uses G.729 compression (supporting 8 kbps voice streams). Despite the compression of G.729, its voice quality is measured as close to the toll quality of G.711 compressed voice.

Availability

An important success factor in assuring reliability of a converged voice and data network is using proven available technologies to bring the reliability of the network infrastructure up to the levels required in the new converged design. Every level of the infrastructure must be considered, from the Cisco CallManagers and voice gateways to the desktop network switches and routers and WAN routers.

Cisco CallManagers

The first Cisco CallManagers were deployed at Cisco in late 1999 to support a small initial group of IT professionals at the San Jose and Research Triangle Park (RTP) campuses. The subsequent expansion to nearly 150 sites throughout North and South America used a decentralized call-processing environment with clusters of 2 to 10 Cisco CallManagers per location. To greatly simplify management and maintain resilience, Cisco migrated to a more centralized environment with Cisco CallManager clusters located in regional hubs, minimizing the number of clusters.

Each cluster typically consists of five Cisco CallManagers, with two servers supporting call processing and two servers providing backup call processing in case of failures on the first two. A final server acts as the local Trivial File Transfer Protocol (TFTP) server and publisher, transferring files for phone software, ring tones, and music on hold. If one Cisco CallManager in a pair should fail, the other Cisco CallManager pair supports the entire load. (For more details on centralized versus decentralized Cisco CallManagers, see “Lessons Learned” at the end of this document.)

Where practical, Cisco increased reliability by physically separating cluster members. For example, Cisco CallManagers are placed in separate data centers at separate buildings in the Cisco RTP campus. Therefore, the loss of Cisco CallManagers in one data center has no effect on the voice service across the entire campus.

High availability and resilience is secured further by deploying Cisco CallManager clusters in Class-A data centers protected by multicircuit uninterruptible power supply and backup generator power systems. Cisco also ensures two-hour runtime in all the wiring closets to power phones, continuing the policy adopted from legacy PBX systems. Continuous phone service is critical to business continuity. In December 2002, the Cisco RTP campus was without power for three days because of ice storms, but it never lost phone service. This enabled Cisco Technical Assistance Center personnel at RTP that support Cisco customers to continue handling calls remotely from their homes using VPN connections.

Class-A data centers additionally provide standard heating, ventilating, and air conditioning and fire suppression features as well as robust physical access security that prevent unauthorized access to Cisco CallManagers and other network infrastructure.



Voice Gateways

Providing diverse routing for voice gateways is essential to assuring reliability in a converged voice and data network. From the beginning, Cisco has designed its voice gateways with multiple circuits: One for connection to the local exchange carrier (LEC) and one for connection to the inter-exchange carrier (IXC). If the long distance circuit fails, the LEC can provide long distance service. For larger Cisco sites, Cisco provides connections to two LECs and one IXC.

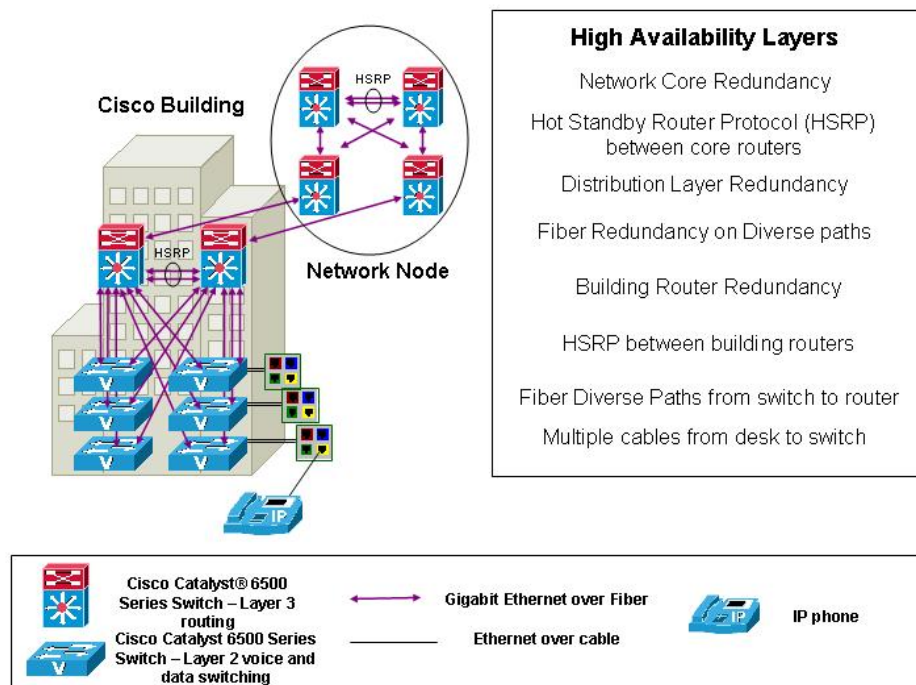
Additionally, Cisco provides separate voice gateways with multiple paths out of each cluster. For example, at the San Jose and the RTP sites two network operations centers (NOCs) have circuit connections evenly split between them. Even if a complete failure occurred in one NOC, inbound and outbound phone service is unaffected at that site.

High Availability Switches

To further ensure reliability in the converged voice and data network, Cisco has equipped its core, distribution, and access switches with high-availability features. Within each switch, redundant power supplies connect to different power circuits in the data center, and redundant line cards and redundant supervisory modules run high availability.

The desktop network for both IP phones and PCs at Cisco locations also is built for reliability through redundant physical paths (see figure 2). Each Layer 2 switch has two separate paths back to distinct Layer 3 gateways, and the network is designed so that each Layer 2 domain cannot be segmented due to a single failure. In addition, each Layer 3 gateway also is provisioned with two distinct paths back to the redundant network core.

Figure 2 High Availability Desktop Network Design



Routers

Cisco applies the same engineering standards followed in data-only router environments to its converged voice and data environment with redundant core and distribution routers throughout the network.



WANs

At the WAN level, Cisco has built redundancy into its WAN routes through Hot Standby Routing Protocol (HSRP) by creating primary and secondary data and voice paths. HSRP provides nonstop path redundancy for the IP by sharing protocol and MAC addresses between redundant gateways. Figure 2 illustrates HSRP deployment within a converged voice and data network.

Centralized Call Processing

Cisco IT worked to keep costs down and manageability high by reducing the number of Cisco CallManagers in the network. With more than 250 sites globally, Cisco IT initially deployed a Cisco CallManager cluster at every site. They have nearly completed a migration to consolidating call processing into fewer than 20 Cisco CallManager clusters supporting all 250+ sites, which saves both equipment and support costs and speeds up deployment of new software.

All this was made possible by supporting Survivable Remote Site Telephony (SRST) features in the local site router. If the WAN link fails between any site and the centralized Cisco CallManager cluster, the local router takes over routine call processing and makes sure that calls are routed properly.

Disaster Recovery Plan

Migrating to a converged voice and data network has a major impact on disaster recovery plans, with a different set of options to be considered from the legacy TDM environment.

In developing a disaster recovery plan, Cisco evaluated its unique business requirements, based on a cost-benefit analysis, to ensure that it had the proper plan in place.

Change Management

Change is constant, and without a rigorous process for managing change in a converged voice and data environment, high reliability is unlikely. Cisco has adopted several procedures and policies to ensure a sound change management process.

Change management meetings should be held regularly and frequently (daily, weekly, or biweekly, depending on level of activity) to review all changes that could affect client services. The Cisco IT team meets daily on a conference call at 8:00 a.m. Pacific Time, Monday through Friday, except for holidays observed by Cisco offices worldwide. These meetings are attended by a variety of principally operational IT staff.

The convergence of voice and data necessitates the integration of voice and data teams into a single change management review board. The Cisco change management review board oversees all change management requests companywide.

It is essential to develop a change management policy that defines the actions that require a change management request to eliminate ambiguity in determining when a change order should or should not be opened. IT management also must enforce those policies and adjust them as necessary. Cisco has created a detailed process for change management requests and it continually evaluates it, revising policies as needed, such as modifying lead times for disseminating change management requests.

Notification of all appropriate personnel is critical when making a change request. Cisco created an e-mail alias that enables personnel to review all change requests affecting the voice network worldwide. Network team members can populate the logged e-mail alias with “who, what, when, where, and why” information about their planned change, and anyone who implements changes must subscribe to the alias to help prevent change conflicts. This e-mail alias includes all IT personnel who interact with the voice and data network. One exception is Cisco CallManager configuration changes that do not require an approved change management request, such as local call routing changes, in which case an alias that includes only voice support personnel is used.

Due to the real-time nature of voice traffic, interruptions must be avoided during normal, as well as extended, working hours. Cisco has adopted a policy that no changes affecting voice services can be performed before 9:00 p.m. local time, unless authorized by the local site.



Standardization can simplify the change management process in any network. Cisco has established standard configurations globally for its LANs, WAN, and change management procedures.

Security

IT managers are familiar with security issues and solutions for data networks, but adding voice to data is unfamiliar for most. Cisco has taken a proactive stance to secure its converged voice networks. All Cisco CallManagers run antivirus software, which is automatically updated when the support team releases new data (DAT) files. Cisco CallManager operating system patches are tested by Cisco and immediately deployed by IT staff.¹ IT staff generates compliance reports daily to identify hosts that have failed to download the latest DAT file. After attempting to determine the reason for noncompliance, network engineers manually execute updates, bringing devices into compliance.

Cisco runs Cisco Security Agent, a threat protection software client, on Cisco CallManagers. This software analyzes the behavior of all software on the server in real time, identifying and preventing malicious behavior before it can occur. It does not block viruses; it simply prevents them from performing malicious activity on a server or spreading to other servers, protecting these servers from viruses that are not yet known. Cisco Security Agent also logs suspected attacks for review by IT staff.

To provide tight control on network access from the outside, Cisco implements standard Internet access controls such as firewalls, demilitarized zones, and intrusion detection systems. Cisco additionally deploys strong authentication mechanisms for reliability, availability, and serviceability/VPN users such as one-time passwords using SofToken software or hardware token cards.

Providing tight control on network devices internally depends on a well-managed PC environment, because PCs often are the first source of worm or virus contamination in a network. Cisco internal business conduct guidelines require the use of a standard OS and application set for antivirus protection. Cisco also makes extensive use of automated desktop management software to allow for responsive remediation of the machines. Being able to automatically address the majority of desktops creates a more manageable problem set. In addition, the broad geographical reach of the desktop technician team provides an ability to “touch” machines in most places when necessary without having to involve the PC user. Of course, Cisco users are technically proficient, and when a virus outbreak occurs, they are concerned and helpful in the remediation process.

Tight control is important in lab environments, as well, to keep problems with lab equipment or router configurations from overflowing into the corporate production network. Cisco uses RFC1918 space for all labs, and labs must use a proxy server to access the Internet. Virus filtering is provided at the edge using a Cisco Application and Content Networking System infrastructure, while access control lists limit traffic that can be sourced from a lab. Furthermore, all routing to labs is static and, as with all PCs enterprisewide, antivirus software is installed on all lab PCs.

Monitoring

Monitoring a converged network creates unique challenges for IT professionals whose experience has been monitoring voice and data separately. Cisco IT successfully has developed tools and procedures to effectively monitor the converged network.

Monitoring procedures were created by identifying devices to be measured, establishing event thresholds, and creating standardized monitoring policies for all network resources: Hosts, routers, switches, wireless access points, content engines, applications, and more. Cisco IT continually measures availability on these devices and ensures that problems get immediate responses. Within five minutes when established thresholds have been reached, e-mail and pager notifications are sent. Cisco IT tunes the current monitoring environment by adjusting settings, such as threshold levels or time-of-day notification, as needed. Cisco IT staff reviews the Cisco CallManager monitoring tool on an ongoing basis (by policy typically once an hour), and responds immediately to all alarms.

¹Cisco makes these tested updates available to all Cisco CallManager customers; see “Cisco Customer Contact Software Policy for use of Third-Party Software and Security Updates” at http://www.cisco.com/application/pdf/en/us/guest/products/ps3651/c1037/ccmigration_09186a0080207fb9.pdf.



Network resource uptime is monitored continually for availability through ping tests. Cisco employs an internally developed Simple Network Management Protocol monitoring system for this task, but other applications, such as HP Openview, can perform the same function. Device components also are monitored, including memory utilization, CPU utilization, interface utilization, interface errors, power supplies, disk drives, and network interface cards. Cisco CallManager events and components also are monitored, including calls in progress, registered phones, active and inactive phones, and active and inactive gateways.

Trunk availability must be measured in the converged Cisco IP network, just as it was in the traditional PBX environment. Cisco IT regularly monitors voice gateway utilization and trunk availability to allow proper bandwidth provisioning on LANs, metropolitan-area networks, and WANs and to facilitate capacity planning across IP and PSTN trunks.

Users expect a dial tone when they pick up the phone. Cisco IT periodically runs application checks on Cisco CallManagers to monitor dial tone availability and ensure that TFTP service is available for IP telephone downloads.

Configuration backups are an important element of reliability. Configuration backups for Cisco CallManagers, voice gateways, and LAN/WAN devices are monitored through automated daily reports that verify configuration compliance. Cisco uses a Router Audit Tool from www.cisecurity.org to enforce its standard configurations. In addition, Cisco IT manually audits all connectivity, topology, network maps, and configurations at least once every six months to ensure accuracy. Also, regular “rogue IP phone registration” reports are run to query local SRST routers about rogue IP phones that may have registered with them, bypassing the required internal Cisco CallManager processes.

Redundant paths are another important element of high availability. Cisco runs a Perl script weekly to verify that each Layer 2 switch has two separate paths back to distinct routers and that each Layer 3 router has two separate paths back to the core.

Support

Supporting a converged voice and data network poses unique challenges. Cisco IT took several actions to ensure effective support.

Case management, the process of responding to customer calls, logging them, and resolving system- or network-related problems, requires a high level of cross-technology expertise and procedural structure. Cisco IT provides an escalation path for support teams consisting of subject matter experts in voice, LAN, and WAN, and additionally enforces escalations through proper channels.

The successful introduction of new features or implementation of upgrades demands adequate training of users who will be affected by these changes. Prior to any implementation, Cisco IT forms a steering committee, which includes clients, to discuss upgrades and new features. Specific training plans are created for each implementation that can include Web pages, quick guides distributed to clients, online tutorials, etc.

Because of the inherent complexities of a converged voice and data network, comprehensive documentation—and the ability to access it—is essential. Cisco IT develops implementation and support documentation, which is stored in an easy-to-access online location. Q&A documents describing common problems and solutions also are developed and provided to the Tier-1 support team.

Cisco CallManagers, like any server, require OS patches and upgrades to be performed occasionally. To efficiently execute these changes, Cisco uses remote administration tools such as Virtual Network Computing (VNC) and Remote Insight Board (RIB), which eliminate the need for onsite technical resources. VNC is a software-based tool, while RIB is hardware based and connects to Cisco CallManagers through a separate and independent connection. Because some patches cannot be completed through Microsoft Terminal Services, (for instance, the Cisco CallManager recognizes that the connection is remote and will not allow the download), local console access, like that provided by the RIB, is necessary.

Cisco CallManager application patches and upgrades also must be performed periodically. To prevent service interruptions during upgrades, Cisco IT support staff has adopted the following policies. First, the support staff utilizes the change management process for all updates, which helps keep changes in short time windows and at a time when it affects the fewest people, usually during off-peak hours. Second, support staff preserves the current software image by powering down Cisco CallManager and removing the redundant drive prior to a major application



upgrade. This allows staff to revert back to the original image by reinserting the backup drive, if a problem occurs with the primary drive during the upgrade procedure.

On a converged network, changes to voice can affect data, and conversely. As part of the change management process for data equipment that could affect voice, Cisco support staff reviews effects on the telephony infrastructure from other device upgrades such as LANs, WANs, voice gateways, and phones.

Various levels of IT support staff must have the ability to make changes to Cisco CallManagers. Without some restrictions, however, administrators with read/write access to Cisco CallManager configuration could change any or all of the database and directory elements that are accessible through Cisco CallManager Administration and Cisco CallManager Serviceability. Support staff inadvertently could disable the entire system with a few mouse clicks by accidentally modifying the data to which they do not need access.

Cisco multilevel administration access provides multiple levels of security to Cisco CallManager Administration. Cisco CallManager Administration functions comprise functional groups. Each functional group can have different access levels, such as no access, read-only access, or full access, to different user groups. One support team, for example, can perform only adds, moves, and changes, while another can add and remove gateways or change routing patterns. Multilevel administration access also provides audit logs of user logins and access and modifications to Cisco CallManager configuration data.

Cisco IT has identified two other success factors for the support of converged voice and data networks. During deployment and throughout the operational phase, a project manager and a project champion at the senior management level are important. Like any project that affects many network parts, and many parts of the internal IT organization, migrating a legacy voice network to a Cisco converged IP network is an ongoing effort. A project manager is critical to ensuring that the various efforts are integrated into a coherent team. Management “buy-in” also must be obtained in the beginning and maintained throughout the project, as the new teams determine the best methods and the best organizational structure to build and support the Cisco SONA environment.

Equally important in this mixed voice and data traffic environment is an IT team with strong cross-functional skills to address all the issues that arise. It is important to identify those people in the IT voice organizations who are interested in learning data technology and to identify those people in the IT data organizations who are interested in learning voice applications; these people make up future core IT Cisco IP telephony teams.

Results

Currently, Cisco deployment of Cisco IP Telephony supports about 55,000 employees and contractors at approximately 300 sites globally. Cisco IT target for voice availability is 99.999 percent.

Lessons Learned

Cisco IT led the movement to converge voice and data and, in doing so, learned through first-hand experience what worked and what needed to be changed. Following are some of the lessons learned in the deployment of Cisco IP telephony environment.

Centralized versus Decentralized Call Processing Model

Cisco initially deployed a decentralized call processing model where small Cisco CallManager clusters at each site supported local users. Today, Cisco IT is migrating to a centralized model where fewer total clusters support multiple sites, which requires less support, is easier to manage, and has a lower total cost of ownership (TCO). This is illustrated in the following example, which mirrors Cisco IT Americas deployment. In a decentralized configuration with two Cisco CallManager clusters at 150+ sites, IT staff must support 300 Cisco CallManagers and 150 clusters. In a centralized configuration, five hub sites are deployed with five Cisco CallManagers per cluster—a total of 25 Cisco CallManagers. This results in an immediate 12-to-1 reduction in capital investment—25 servers versus 300. Ongoing support costs also diminish. For example, applying patches to 25 servers requires less labor than updating 300.



A centralized model can reduce TCO and it also can require a wider breadth of knowledge by support staff. For example, in a fallback scenario where connectivity to Cisco CallManagers fails, call processing takes place on a router. Support staff familiar with the Cisco CallManager information format now must have knowledge of the command-line interface on a router. In addition, a centralized environment requires a robust WAN to support geographically diverse Cisco CallManagers in each cluster.

Dial Plan

Rarely is the dial plan given adequate attention in the IP telephony implementation planning stage. Migrating to a centralized call processing environment can have a major effect on the dialing plan. In a decentralized environment, each location typically has a four-digit dial plan. It is common for multiple sites, therefore, to have similar direct inward dialing (DID) numbers. Converging these sites into a single Cisco CallManager and dial plan creates duplicate DID numbers. Cisco resolved this issue by expanding internal directory numbers to 8 + seven digits (for example, users dial a prefix number “8” to get on the network, followed by the seven-digit number, such as 8-555-0111). Other organizations with fewer DID numbers may find a dialing plans with fewer digits adequate (for instance, a five-digit dialing plan).

Broad Range of Skill Sets

When migrating to IP telephony, the implementation team should include staff with expertise in both legacy telephony as well as network and server technologies. In this way, team members can learn from each other.

QoS Policy

Voice quality perhaps is the foremost statistic in measuring the performance of a converged voice and data network. By not having a comprehensive QoS policy in place prior to initial deployment, Cisco experienced some voice quality issues between sites. A standardized policy throughout the network is essential for avoiding voice-quality issues.

Next Steps

The IP telephony deployment at Cisco continues to evolve and expand through new processes and procedures and through the introduction of new applications that simplify operations and increase productivity for both IT staff and end users. Following are a few of these.

Video

Cisco IT plans to add integrated telephony and video capabilities to the converged network. The existing network supporting H.323 video endpoints in conference rooms will be integrated into the Cisco SONA network, eliminating parallel video and voice dial plans. Cisco has introduced a videophone and camera that work with the PC, which will extend videoconferencing beyond the conference room to virtually any Cisco employee with a network-attached PC and videoconferencing equipment. This upgrade will require Cisco IT to modify QoS to support video and adjust bandwidth accordingly.

Disaster Recovery Planning

Cisco IT continually seeks to improve its disaster recovery plan. Among the efforts under way is ongoing implementation of clustering across the WAN to ensure continuation of operation even in the event of a complete failure of a major data center. Another effort, dependent upon future technology, is the deployment of IP/PSTN gateway connectivity, allowing Cisco CallManagers to route inbound and outbound calls in the event of a disaster.

Traffic Convergence

Cisco IT converges voice (both on-net and off-net) and data traffic over the WAN where it is economically feasible, saving long distance voice costs by using the Cisco IP WAN backbone. Traffic is converged, for example, in South America and to other continents outside the USA. It is



not economical at this point, however, to route all voice traffic over the WAN within the USA, such as between small branch locations with very low traffic volume. Cisco IT continues to evaluate converging traffic to provide the most economical solution.

Although Cisco considers its network converged, traffic currently is segregated over local Primary Rate Interface (PRI) trunks, long distance PRI trunks, and even external basic telephone service lines for emergency dialing. In the future, one “fat” IP pipe will be used to hand off inbound and outbound data, voice, and video traffic to service providers. These IP pipes are presently available only in a limited number of venues.

New Telephony Applications

Cisco IP voice technology has enabled Cisco IT to implement new applications to increase productivity. Until recently, for example, users calling the Global Technical Response Center had to “walk” through a recorded multilevel touchtone menu to reach a service representative to request a password reset. The new application bypasses the cumbersome menu by allowing the user to press a “Password Reset” menu option on their IP phone, immediately connecting them to the service representative.

In another productivity-boosting application, desktop technicians previously had to return to their offices after completing each repair case to input actions taken on the visit into the Alliance case management application because they did not carry laptop PCs with them. Cisco IT integrated the Alliance application into the Cisco IP phone system, building XML application hooks into Alliance so that people can use their phones to access the application. Now desktop technicians not only input case status information from any IP phone, but query cases as well.

Cisco is still learning how IP Communications is providing new opportunities for business improvement—from consolidating diverse IP call centers to a single platform, to turning a phone into a video phone and Web browser. Cisco as a company is learning that turning voice into a data application builds far greater opportunities than savings on phone network costs.



For additional Cisco IT case studies on a variety of business solutions,
go to Cisco IT @ Work

www.cisco.com/go/ciscoitatwork

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.



Corporate 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: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe



Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Printed in the USA