Routing and Switching Case Study: How Cisco Uses VPN Solutions to Extend the WAN

WAN VPNs provide cost-effective remote site and disaster recovery connectivity.
.Cisco Systems® is a global organization with more than 250 company sites worldwide. It is essential that Cisco® IT provide and maintain adequate and reliable connectivity to every site, independent of size or location. Sites can range from large campuses like San Jose, California, and Research Triangle Park (RTP), North Carolina, with thousands of employees to small remote field offices such as Anchorage, Alaska, with eight employees. Cisco IT's goal is to provide high-performance, high-availability network connectivity as soon as it is needed at each site. The challenge is finding the right technical solution at the best price at each location. Internet VPN circuits for either primary or backup connectivity is the solution of choice for a small but increasing number of Cisco locations. This case study examines three areas where Cisco IT has selected Internet VPN connections to replace traditional WAN circuits:

- VPN connections as primary WAN links between Cisco offices
- VPN connections as disaster recovery for WAN links between global regions
- VPN connections as WAN links between Cisco offices and partner locations

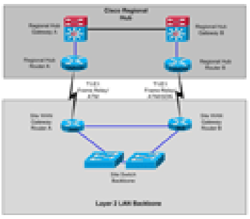

Figure 1. Typical Field Office WAN

Primary WAN links between Cisco offices: Connectivity to most smaller offices typically is provided through dual dedicated circuits (for instance, T1/E1, Frame Relay, or ATM) terminating on dual gateway routers at the nearest regional hub location, as illustrated in Figure 1. Regional hubs include San Jose and RTP in the United States; Amsterdam, The Netherlands; Sydney, Australia; Tokyo, Japan; and Hong Kong. Dual routers and dedicated circuits, on physically diverse paths when possible, provide redundancy. This design has proven to be reliable and cost effective where multiple carriers can provide point-to-point leased lines that combine high availability with a reasonable vendor pricing structure.

Cisco has used Internet VPN connections for more than two years to provide remote access for Cisco employees. In addition, Cisco IT in Europe, Middle East, and Africa (EMEA) migrated most of its WAN to a service-provider-based Multiprotocol Label Switching (MPLS) VPN network. Both case studies are available at http://www.cisco.com/web/about/ciscoitatwork/case_study.html.

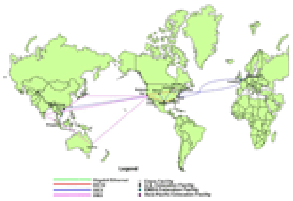

Figure 2. Cisco IT Cisco All Packet Network

Disaster recovery between global regions: In addition to providing adequate, reliable connectivity to remote sites, it is essential that Cisco IT ensures reliable connectivity between the large regional hubs. Cisco deployed the Cisco All Packet Network, a high-bandwidth core network that interconnects regional hubs with up to four layers of dedicated circuit redundancy (see Figure 2). For much of its history this circuit redundancy was considered enough to protect Cisco backbone connectivity from failure, but the price and performance of high-bandwidth Internet VPNs has caused Cisco IT to reconsider this approach.

Links between Cisco and partner locations: The Cisco extranet provides a secure, highly available connection to the Cisco intranet for companies that supply Cisco with manufacturing, software development, or call center functions, as well as financial, legal, fulfillment, marketing, and publications services. Approximately 30 percent of Cisco extranet partners provide manufacturing services and are fully integrated into the Cisco supply chain applications and processes. These connections are similar to Cisco WAN links, private line or Frame Relay in pairs for partners who require high availability, and private line or Frame Relay with ISDN backup for other sites. For extranet leased-line circuits, Cisco manages the entire circuit and the connecting equipment at the partner's site.

CHALLENGE

Cisco IT faced challenges in three areas of WAN connectivity: with primary WAN links between offices, with disaster recovery or backup links on the backbone WAN, and with partner Extranet links.

WAN links between Cisco offices: Providing primary and failover backup connectivity to small, geographically remote Cisco field offices through traditional dedicated circuits can be cost prohibitive and, in some situations, not an option because of the poor reliability or lack of existing carrier infrastructure. A single T1 circuit from the eight-person Anchorage office to the nearest regional hub (San Jose, for example) could cost US$8000 to $9000 per month, while a similar circuit from Costa Rica could cost $25,000. In Nairobi, Kenya, reliable dedicated circuits of any bandwidth are unavailable. What Cisco IT needed was a cost-effective and dependable alternative to dedicated circuits at remote sites such as these.

Disaster recovery between global regions: Although regional hubs have been designed with multiple layers of dedicated circuit redundancy, certain Cisco All Packet Network WAN links connecting major Cisco locations are particularly critical. Cisco IT needed cost-effective disaster recovery capabilities for its most critical WAN links.

Links between Cisco and partner locations: Partners are sensitive to the additional costs of traditional WAN links and look for cost-effective alternatives. In addition, some partner sites needed to be connected quickly to Cisco or were moving locations and needed to be reconnected to Cisco as quickly as possible, and the lead times for traditional circuits were too long. Like Cisco, many partners already had large Internet access connections and wanted to use this resource.

SOLUTION

Three Solutions

To meet the challenges, Cisco IT deployed the following:

"Internet VPN is ideal where dedicated WAN connectivity is cost-prohibitive, or as a final disaster recovery mechanism between major sites, or to use common infrastructure between Cisco partners, and where Cisco maintains a presence at partner sites."

Craig Huegen
Cisco IT network architect

- WAN VPNs to provide primary or backup WAN connectivity or both to small remote sites where it makes business sense
- A WAN VPN for disaster recovery connectivity on one of the most critical WAN links
- A WAN VPN for extranet connectivity to partner sites (in progress)

WAN links between Cisco offices: Unlike a traditional WAN link that requires a dedicated point-to-point circuit, a WAN VPN utilizes a local connection to the nearest Internet service provider (ISP) point of presence (POP). From there, the public Internet infrastructure carries the VPN connection to the other end point. Such site-to-site encrypted WAN VPNs offer the same benefits as a dedicated WAN, ensuring private communications from one trusted site to another, providing multiprotocol support, high reliability, and extensive scalability. In addition, site-to-site encrypted WAN VPNs are cost effective, secure, and allow for greater administrative flexibility than legacy private WANs.

Cisco IT uses IP Security (IPSec) to provide data encryption over the WAN VPNs. However, IPSec does not support IP Multicast over the VPN. IP Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients or sites (see the multicast case study at www.cisco.com/go/ciscoitatwork). Applications that take advantage of multicast include videoconferencing, corporate communications, and distance learning. Multicast technology is deployed widely throughout Cisco in nearly every office worldwide. When Cisco CEO John Chambers announces quarterly results in a company meeting, Cisco IP/TV® (which streams live or pre-recorded video, audio and slides to Cisco internal audiences worldwide) is broadcast over the WAN infrastructure using multicast technology. To allow multicast broadcasts to WAN VPN sites, Cisco IT uses generic routing encapsulation (GRE) tunneling technology. This Cisco IOS® Software-based GRE over IPSec VPN design was chosen for maximum configuration flexibility that closely mimics traditional private lines, Frame Relay, or ATM services.

Several different WAN VPN configurations can be deployed, depending upon the redundancy requirements and the cost of dedicated circuits. Configurations include primary connectivity with backup, primary connectivity without backup, and backup connectivity where a dedicated circuit exists for primary connectivity.

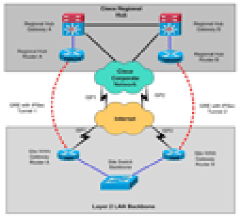

Figure 3. Remote Office with Dual WAN VPNs

Primary Remote Site WAN VPN

Cisco IT deployed WAN VPNs to provide primary connectivity to several remote field locations. Two standard configurations have been defined. Where the cost of providing dedicated circuits cannot be justified but high availability is critical, dual remote VPN routers and dual IPSec, GRE, or VPN tunnels provide the best high-availability solution. This configuration offers primary connectivity, plus full redundancy through the backup router and dual Internet connections and tunnels, as shown in Figure 3. The two tunnels terminate in separate routers at the closest headend hub location. Each remote router is required to establish a GRE tunnel over an IPSec peer connection with the corresponding headend router. Should one of the headend routers fail, traffic is rerouted over the alternate gateway. One tunnel is normally active, while the other serves as a backup. This configuration is preferred because there may be significant differences in end-to-end latency between the two connections if both were actively passing traffic. Cisco IT has not, as yet, deployed a WAN VPN with this configuration.

In other remote sites where uninterrupted availability is not as critical, facilities available from providers are limited, or the cost of Internet connections are high, a single remote VPN router and single ISP connection can be cost-effectively deployed. To retain some measure of redundancy, the single remote router connects to two headend routers at the regional hub using two IPSec or GRE tunnels, as shown in Figure 4. A failure of one of the headend routers at the hub location would cause traffic to be routed over the second tunnel, and the remote office would continue to function. This configuration also allows Cisco IT to "bring down" one of the headend routers for maintenance without affecting service to the remote site. A single Internet connection and remote router do not provide redundant connectivity to the remote office, however, if the local ISP connection or router fails.

Instances where this dual remote router and dual tunnel configuration has been deployed include Anchorage, Alaska, and Honolulu, Hawaii. As explained earlier, the cost of a dedicated Frame Relay circuit between Anchorage and San Jose, the closest hub site, would be about $8000 to $9000. These sites benefit from dedicated service at a lower cost.

Cisco IT also has been supporting this type of WAN VPN configuration for nearly five years at two offices allocated to Cisco sales people on the Microsoft campus in Redmond, Washington. Cisco IT uses Microsoft's infrastructure to connect to the Internet.

At the Cisco site in Costa Rica, the cost of a dedicated circuit back to San Jose, California, could be $25,000. Although the Internet connectivity available creates high latency levels, the WAN VPN is capable of supporting reliable service, even for voice. In Nairobi, a WAN VPN link over satellite connection is used, which also creates high latency. Bandwidth is limited to 512 Kbps but it provides essential network connectivity.

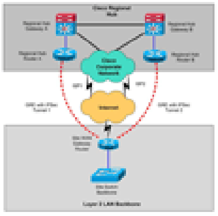

Figure 4. Remote Office with Single WAN VPN, Dual Headend

Backup Remote Site WAN VPN

Many locations, particularly larger sites, are able to justify the expense of dedicated circuits (leased line, Frame Relay, or ATM) for primary connectivity. These sites can be vulnerable to outages of with single circuits, but deploying additional expensive dedicated circuits for redundancy may not easily be cost justified. Alternatively, an ISDN dial-on-demand service for backup purposes also may be costly to establish and maintain. In these instances, a WAN VPN can be used in addition to a remote site's current primary connectivity to provide the site with a reliable and cost-effective backup WAN solution, as shown in Figure 5. When a WAN is implemented as a backup solution to a primary leased-line circuit, it is not necessary to establish dual tunnels to the headend routers at the hub location because an outage of the VPN connection will not result in isolation of the remote office.

Cisco IT has used extensive WAN VPNs extensively for backup in Latin America in locations such as Mexico City, Buenos Aires, Rio de Janeiro, Sao Paulo, Santiago, and Bogotá. These sites rely on primary connectivity through E1 (2.048 Mbps) or bundled E1s where additional capacity is required. A separate remote router supports the VPN.

Disaster recovery between global regions: Cisco IT continually evaluates the Cisco All Packet Network for networkwide reliability and fault tolerance. WAN links connecting major Cisco locations have been designed with redundancies to help ensure failsafe operations. In catastrophic situations, however, additional measures may be justified to protect these links. The same WAN VPN technology deployed for connectivity to smaller remote sites also can be utilized to provide disaster recovery capabilities for WAN links between regional hub sites.

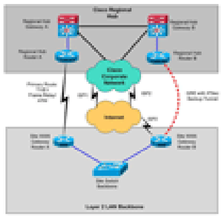

Figure 5. Remote Office with Single Backup WAN VPN

A WAN VPN is unlikely to be an appropriate disaster recovery solution for all major Cisco locations because of the cost of high-bandwidth VPN connections and other factors. The business case for WAN VPN disaster recovery can vary considerably. The expense incurred to mitigate the risk of a complete WAN failure must be evaluated on a site-by-site basis. Among the business factors that should be considered when evaluating a site for WAN VPN disaster recovery are the diversity of existing primary and backup facilities, the impact of a catastrophic WAN failure, and the cost to implement or upgrade an ISP POP to accommodate the needed bandwidth.

Cisco IT identified the transatlantic WAN links connecting the United States and Europe as vital communication routes. Two OC-3 (155 Mbps) circuits provide redundant, diverse routes between New York and London and between RTP and Amsterdam. Each circuit has sufficient bandwidth to handle the total traffic load between the United States and Europe if a circuit fails. In the unlikely event that both circuits fail, EMEA would be isolated from the rest of the network. The potential impact of this event convinced Cisco IT that a WAN VPN disaster recovery solution was justified. Furthermore, the cost to implement a WAN VPN would be minimal because the existing Internet connections in both Amsterdam and RTP were large enough (STM-3 and OC-3, respectively) to provide sufficient bandwidth for the disaster recovery VPN connection. A WAN VPN was deployed between these sites in late 2003. Figure 6 illustrates how a WAN VPN might be configured for disaster recovery between Boxborough, New York, and RTP.

Links Between Cisco and Partner Locations

VPN technology significantly reduces the costs of extranet connectivity because it eliminates monthly circuit costs. The ratio of requests for VPN connectivity compared to leased-line connectivity is presently 5 to1; however, Cisco IT must work with each partner to determine the best price and performance tradeoffs for their location. Major benefits of VPN extranet connectivity are:

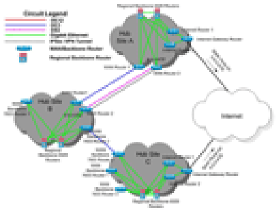

Figure 6. Disaster Recovery Using WAN VPNs

- Eliminating the cost for WAN circuits used for "traditional" extranet connectivity
- Eliminating hardware costs for internal clients and reducing inventory management for the Internet Services Group (ISG)
- Accelerating implementation
- Facilitating short-term extranet connectivity or fast location moves
- Supporting partner telecommuters with user-based VPNs

To set up a site-to-site VPN, Cisco IT Internet Services Group deploys a Cisco 7206VXR Router at the Cisco POP. At the partner site, the tunnel terminates either at a VPN device that the partner manages (using the interconnect model, described in the next section), or at a Cisco VPN router that the Cisco ISG manages (using the extranet remote LAN model, described in the next section). The partner's business needs determine which configuration model is best.

Cisco IT has approximately 50 extranet customers using VPN connectivity; most are in the United States and some are in Latin America and Japan.

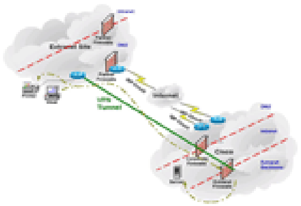

Figure 7. Remote LAN Model for Site-Based VPN Extranets

Extranet Remote LAN Model

A remote LAN is an extension of the Cisco network at a partner site. A managed Cisco router at the partner site terminates the transport connectivity from Cisco and connects to one or more managed switches at the partner location (see Figure 7). The Cisco business client typically provides the PCs and printers connected to the remote LAN. This extranet solution is common for manufacturing, global product services (GPS), and Auto-Test partners. "Manufacturing partners generally need to print files from servers at the Cisco site, which they couldn't do if the printers were on their own network as opposed to the Cisco network," says Julie Nordquist, Cisco IT project manager. Similarly, GPS and Auto-Test partners need to set up their own routers on the Cisco remote network in order to test. The remote LAN topology isolates the client's subnetwork so that it cannot inadvertently send test data over the production network. Cisco IT provides and manages the VPN router located at the approximately 20 partner sites, most of them in the United States. However, there is no additional circuit to lease and bill for, because the VPN connection uses the Internet access circuit already in place at Cisco and at the partner location.

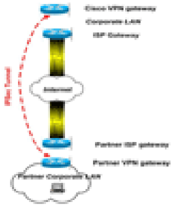

Figure 8. Interconnect Model for Site-Based VPN Extranets

Extranet Interconnect Model

With the interconnect model, partners connect using their corporate LAN, which interconnects with the Cisco LAN (see Figure 8). Firewalls at each side protect each company's respective resources. Because Cisco does not allow or advertise partner internal networks into the Cisco network, Cisco translates the partner IP addresses into Cisco addresses using Network Address Translation. This is another layer of protection to prevent access into Cisco by any device on the partner network. In contrast, the remote LAN models are limited to desktops that are physically connected to the remote LAN. Some sites incorporate both topologies, depending on the requirements of the connection. This flexibility is helpful, for example, if a manufacturing partner's buyers want to access buying information from their desks instead of walking to the product-build area in the warehouse. In this model the partner provides the VPN router and owns and manages all equipment on the site. Cisco is responsible only for supporting the equipment at the Cisco location and for troubleshooting the connection between the two sites when needed. More than 30 partner companies currently use Interconnect VPN. Most of these companies are in the United States and some are in Japan and other parts of Asia, in Latin America, or in Europe