How Cisco IT in Europe Migrated to MPLS VPN WAN

MPLS VPN WAN quadruples available bandwidth, increases agility during office moves, and lowers costs.

Cisco IT Case Study / Routing and Switching / MPLS VPN WAN Migration: This case study describes Cisco IT's internal use of MPLS VPN 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.

"Now there's no network infrastructure behind our offices, so we only need to concern ourselves with connectivity to the cloud, not with connections from other offices. Any moves, adds, and changes to the Cisco real estate infrastructure cost significantly less and take less time."

– Stef de Borchgrave, Worldwide Network Operations Manager

CHALLENGE

For years, Cisco Systems® in Europe, the Middle East, and Africa (EMEA) has relied on a hub-and-spoke network topology. The EMEA core network comprised Cisco® offices in London, Amsterdam, and Brussels in a full mesh configuration, interconnected using OC-3 lines. Nine hub sites and approximately 30 partner sites connected to the hub by ATM services in a dual-homed fashion. Approximately 85 satellite sites connected to a hub by ATM connections with ISDN backup.

As the Cisco network in EMEA grew, the limitations of the hub-and-spoke topology became apparent. "We were at maximum capacity on the majority of our links and needed capacity upgrades," says Stef de Borchgrave, Cisco worldwide network operations manager. Bringing down a hub site to replace an uninterruptible power supply or upgrade the hardware, for instance, brought down all of that hub's spoke sites, affecting business continuity. Quality was not adequate for voice over IP (VoIP), particularly when a call traversed the extra distance required by traveling through multiple hubs, which introduced extra latency. Another challenge of the hub-and-spoke topology was quality of service (QoS). "We knew that QoS would become increasingly important as we deployed more real-time, peer-to-peer applications—not only voice, but also video over IP and real-time collaboration," says de Borchgrave. "The philosophy of Cisco IT is to prepare our network for planned applications two years ahead of time."

Cisco IT identified two networking options to meet its business needs. One was a combination of ATM and clear channel E-1 leased lines. The other was Multiprotocol Label Switching (MPLS) technology. MPLS is a network-based Layer 3 VPN technology, typically offered by a service provider as a managed service. The MPLS mechanism forwards packets based on the packet labels, which contain the IP destination address QoS information, the source address, and other information. Labels ensure that traffic for each partner or organization remains separate, and that packets are treated with the appropriate QoS. This is sometimes described as "ships-in-the-night" transport because packets from different enterprises share the wire without any effect on the others, enabling secure transport across a shared medium.

The MPLS VPN emerged definitively as the best choice for Cisco. "MPLS provides any-to-any connectivity because traffic can reach its destination over the optimal path, which improves the quality of real-time, peer-to-peer applications such as voice and video," says de Borchgrave. In addition, because MPLS VPN is a managed service, Cisco could offload Layer 3 routing tasks to the service provider, a function that previously required five dedicated

WAN staffers. “If we have an outage, it’s the vendor that troubleshoots and fixes the problem, and we just need to follow up,” says de Borchgrave. The MPLS VPN also would simplify moves and the connection of new partner sites. “When an office moved with our old model, we had to connect it to a hub site,” de Borchgrave continues. “Today we simply tell our vendor to connect the new office to the cloud.” Ease of moving offices became especially critical at the end of 2002, when Cisco EMEA faced loss of its lease on the London core site, which terminated two trans-Atlantic backbone network circuits and more than 40 hub and satellite site circuits. IT needed a flexible networking solution that would facilitate the move to a new London location. MPLS VPN provides that flexibility because routing and site connectivity occurs in the MPLS cloud, so moving a single site requires no more than moving a pair of access circuits. Finally, the timing was right, because Cisco IOS® Software began including support for multicast VPNs (M-VPNs) in January 2003, and Cisco relies on multicast technology for multiple business functions, including e-Learning, content delivery using Cisco Application and Content Networking System (ACNS) software, and Cisco IP/TV® broadcasting. “We had to have a multicast VPN operational on Day One to continue using Cisco IP/TV ,” explains Den Sullivan, IT manager for solutions implementation in Cisco EMEA.

SOLUTION

Service Provider Selection

Cisco issued a request for proposal and selected a primary and secondary service provider. “We were the first enterprise in the world to use an M-VPN MPLS network in production and worked with the first service provider to offer M-VPN services in an MPLS cloud,” says Sullivan.

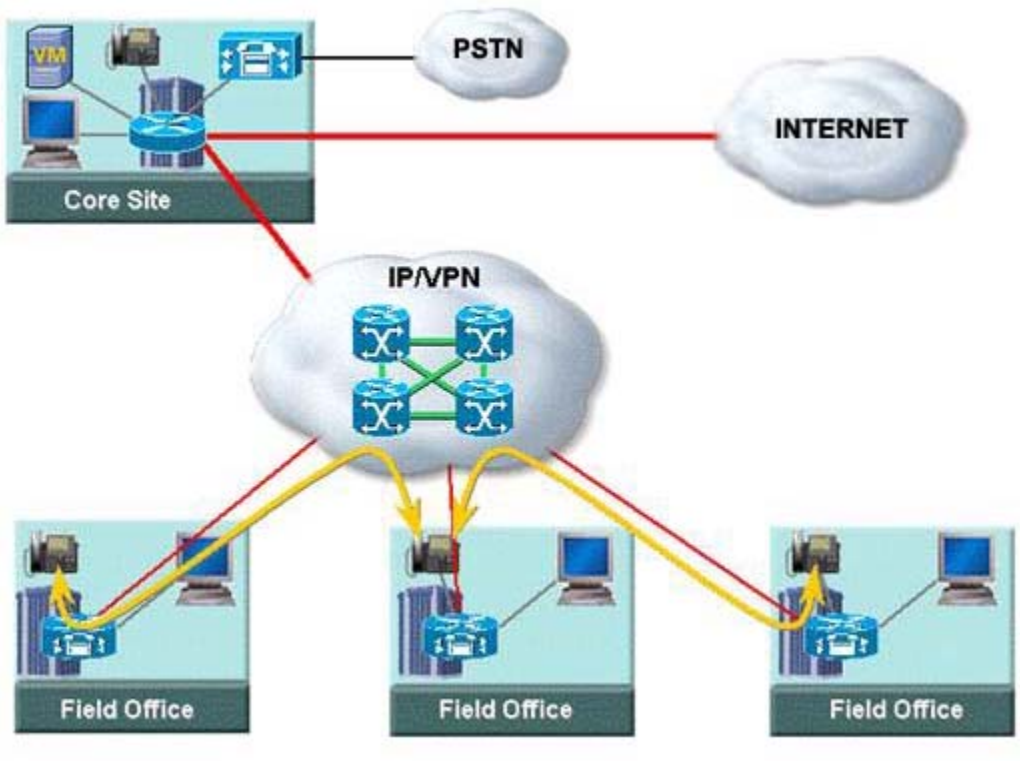
Cisco selected its service providers based on the following criteria:

- **Service-level agreements (SLAs)**—“SLAs weren’t terribly important for our previous network because it carried mostly non-real-time traffic,” says de Borchgrave. “But for our M-VPN network, which would be carrying voice and video traffic, SLAs were the number-one requirement.” Cisco requested SLAs for availability, latency, RTD (Round Trip Delay), and delay variance or “jitter.” The latter is important for voice and video. Cisco also wanted the service provider to provide a Website where Cisco IT could view SLA statistics, as well as implementation schedules and operational information such as availability and major network outages.
- **Solution transparency**—Cisco wanted to maintain the same QoS, connectivity to the provider edge, and multicast capabilities it already enjoyed. QoS transparency was particularly important. Cisco uses Enhanced Interior Gateway Routing Protocol (EIGRP) on its core network and needed the service provider to map its own QoS to the EIGRP QoS. “The service provider was very flexible in accommodating our QoS settings,” says de Borchgrave. “Our traffic comes into the cloud labeled with five classes of service and reaches its destination with the original class of service. The manipulation the service provider does in the cloud to achieve this is completely transparent to us.”
- **Geographical reach**—Cisco IT sought a service provider that could support MPLS VPN connections to the greatest number of the company’s 95 sites in EMEA, especially the largest, which are in Western Europe. MPLS VPN was new in late 2002, and no single provider could connect all Cisco IT EMEA sites into its MPLS service cloud. Therefore, Cisco identified two service providers who together offered good coverage in Western Europe and decided to migrate as much of its network as possible, including all our large Western European sites, to MPLS.
- **Pricing**—“Although important, pricing was not the key selection criterion for Cisco,” says de Borchgrave. “We made sure the price was competitive, but we’re actually more concerned with performance and availability.” The lower pricing of MPLS VPN service in Europe allowed Cisco IT EMEA to quadruple its network bandwidth for approximately the same price paid previously.

Topology

The MPLS VPN is a fully meshed topology (see Figure 1). “In our MPLS VPN design, we can allow every site to have a direct route to every other site, a capability called ‘full mesh,’” says Steve Pickavance, Cisco IT EMEA network architect.

Figure 1. MPLS VPN Topology



Customer Premises Equipment

Most MPLS VPN service providers offer their customers the choice of managing the customer premises equipment in-house or out tasking. “We chose to take responsibility for all routers: both the outward-facing edge toward the cloud and the inward-facing edge toward Cisco,” says Sullivan.

Each satellite site has two routers: a pair of Cisco 3700 Series multiservice access routers for field sales offices or a pair of Cisco 7200 Series routers for larger engineering sites. Each is connected to the MPLS cloud by two parallel access trunks, which are physically diverse when possible. Depending on need and availability, the connections can be fractional E-1, nxE-1, DS-3, or E-3. Most hub sites use a pair of Cisco 7200 Series routers, connecting to the cloud using nxDS-3 or nxE3. Core sites use pairs of Cisco 7600 Series routers and connect to the cloud using dual Synchronous Transfer Mode (STM)-1 (155 Mbps) or STM-4 (620 Mbps) lines.

Migration Process

With its previous hub-and-spoke model, every packet—inbound, outbound, or interenterprise—touched one of the three core sites: London, Amsterdam, or Brussels. Therefore, Cisco IT needed to migrate this core network to MPLS before it migrated to other sites. Because the London core site was moving to another location, it had to be done quickly. “If we missed the deadline to turn off the old network, we’d incur an accounting charge of millions of dollars against sales profits,” says Sullivan. In fact, the deadline for moving was so close that Cisco IT considered carefully whether to move the current infrastructure to the new site or to migrate to MPLS at the same time as the move. “Moving the existing infrastructure entailed moving two trans-Atlantic links, approximately 30 corporate network links,

and approximately 15 partner site links," says Sullivan. The cost was estimated at US$2 million. "Given the cost and the fact that moving the two trans-Atlantic links alone would take 12 weeks, we decided to migrate to MPLS."

The kickoff meeting with the primary service provider occurred at the end of October 2002, and the Cisco London office had to be decommissioned by February 29, 2003. Within four months, the service provider needed to build a full MPLS cloud that connected the three core sites, while keeping the remaining VPN infrastructure intact. All three offices had to be changed at the same time.

IP Addressing

Cisco had to update its IP addressing plan to reflect changes in hub points and homing of certain sites, although the logical hierarchy remained unaffected by the migration to MPLS VPN. Each office was given address blocks consistent with its usage requirements. Cisco IT EMEA had earlier undergone a rigorous address summarization exercise, and each location's address blocks were relatively simple.

The Cut-Over Process

By mid-February 2003, the service provider had built out the MPLS cloud. Cisco IT, with the assistance of the service provider, began the cutover process at 8 p.m. on Thursday, February 14, 2003. The network had to be fully operational by 5 a.m. Saturday to accommodate employees and customers in Saudi Arabia and the Cisco Technical Assistance Center (TAC).

"During this brief window, we had to rip down the core triangle and connect each site to the new network," says Sullivan. The week preceding the cutover, Cisco IT installed new routers in the three main sites. The service provider delivered the cabling infrastructure from the Cisco offices to the nearest node in the cloud.

With the infrastructure in place, Cisco IT began testing the six core links end-to-end. First, Cisco IT deactivated one of the old links between London and another core site by issuing a router command. At this point, production traffic continued to flow over the old leased-line network, not the MPLS cloud. "When we cut the second link, that site had no option but to use MPLS," says Sullivan. Then Cisco cut the third link. "If something had gone wrong, we could have reestablished the link in approximately 10 seconds," says Sullivan. "In fact, we kept the old equipment in place for a month, just for insurance, though it didn't turn out to be necessary. The amazing fact that this worked on Day One is attributable the very thorough design and analysis." (See Lessons Learned.)

RESULTS

Reduced Operations Overhead

By outtasking MPLS VPN services, Cisco IT has unburdened itself of the following responsibilities:

- Troubleshooting and solving trouble tickets
- Maintaining Layer 3 routing tables
- Configuring the core WAN router for new technologies, such as multicast. "In the past, we were responsible for configuring every core device to handle new technology," says de Borchgrave. "Now we just make sure the office infrastructure has the capability and leave everything inside the cloud to the service provider."

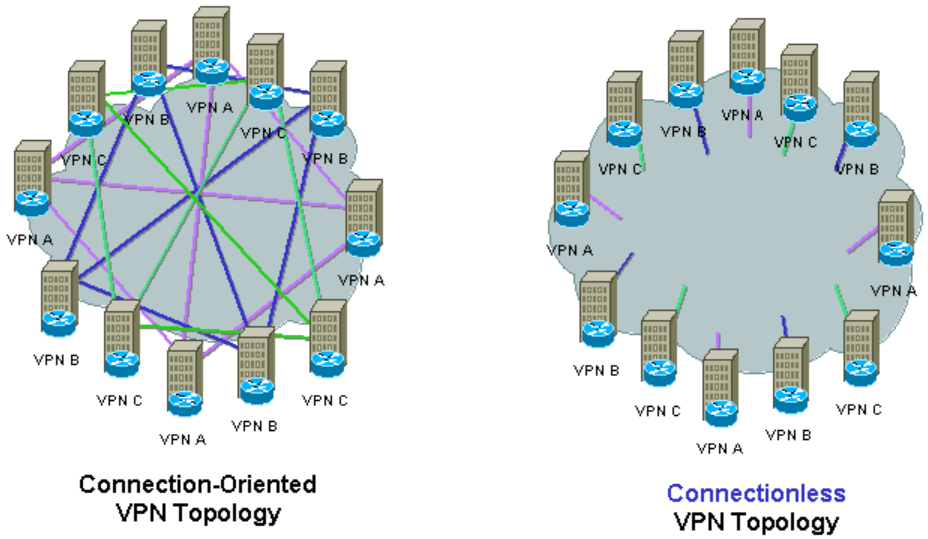
IT now has more time for more strategic activities. "Eliminating the need to configure individual site-to-site connections, traffic paths, and bandwidth considerations between any two customer edges frees up the engineering efforts of the enterprise operations team to focus on core engineering activities," says Pickavance. Adds de Borchgrave, "No longer do we need five dedicated WAN staff people. Instead, VPN support is part of the day-to-day network support job."

Scalability

In traditional Layer 2 networks, any-to-any connectivity requires an expensive full mesh (see Figure 2). Pickavance

explains, “Full-mesh networking in a network with a large number of endpoints is always expensive, as it requires (n2-n)/2 point-to-point connections, where n is equal to the number of sites. The 90 sites in EMEA would require more than 4000 point-to-point connections. In the Layer 3 MPLS VPN model, each site needs only one connection to the VPN, which can scale to include hundreds or thousands of sites. Not only does this eliminate the need to manage thousands of mesh connections, it radically simplifies the management of moves, adds, and changes.”

Figure 2. Connectionless MPLS VPN Facilitates Scalability



Streamlined Acquisitions and Moves

In the past, moving offices and integrating newly-acquired companies into the Cisco network required a significant effort. Every satellite office that moved had to be reconnected to a hub site—and if a hub site moved, all links into that hub site also had to be moved. If Cisco moved its Brussels office, for example, it also had to move the links from all Eastern European offices. “Now there’s no network infrastructure behind our offices, so we only need to concern ourselves with connectivity to the cloud, not with connections from other offices,” says de Borchgrave. “Any moves, adds, and changes to the Cisco real estate infrastructure cost significantly less and take less time.”

Greater Flexibility in Connecting Partner Sites

With its previous hub-and-spoke network topology, Cisco had to connect all extranet partner sites to one of the two core sites with firewalls—Amsterdam or London—no matter where in EMEA the partner is located. (Firewalls ensure that partners can access only those network resources for which they are authorized.) This meant leasing international E-1 lines for each partner location.

With the MPLS VPN, Cisco can connect partners anywhere in the cloud. Each partner’s traffic is tagged with a unique identifier. The service provider creates a tunnel within the cloud that leads to the firewall, and all partner tunnels remain separate from each other. “MPLS VPN technology is a secure way to connect to the cloud, travel through the cloud to the firewall, and then be routed internally to the destination,” says de Borchgrave. The MPLS VPN solution also makes it easier to treat geographically separated employees of the same partner as belonging to the same company. With its previous topology, Cisco had to connect them physically to the same core site; now they are connected logically.

Cost Savings

The any-to-any connectivity of MPLS VPN technology cuts costs: Cisco pays approximately the same amount for four times its previous bandwidth. An important factor in the cost savings is toll bypass arising from VoIP. Whereas the old topology enabled toll bypass for interoffice traffic only, the new MPLS VPN creates savings for international calls, as well. “The more sites connected to the cloud, the more creative you can be in dealing with voice traffic,” says de Borchgrave. “Where it’s legal, we route all traffic with a Cisco destination in a different country over the network, which eliminates tolls. In countries where this is not permitted, or when the destination is outside Cisco, we route calls to a central location, where they can hop off to the public switched telephone network (PSTN). We receive large discounts because of the volume.” This benefit is particularly important for Cisco EMEA, because the cost for international traffic in Europe is three to four times higher than it is in the United States.

Increased Security and Availability

By consolidating its services in IDCs in the service provider cloud, Cisco has increased the security and availability of its network services. “Services are closer to the cloud,” says de Borchgrave. “And they’re in an area that’s highly secure and available because that’s the service provider’s core competency.” In the future, Cisco has the option to extend this security and availability to other servers that it plans to colocate in the Central Office, such as Cisco Unity™, centralized Cisco CallManager, file and print servers, and others.

LESSONS LEARNED

De Borchgrave emphasizes that SLAs are crucial for any network carrying real-time, peer-to-peer applications. Cisco stipulated that the service provider deliver SLAs for availability, latency, RTD, and delay variance.

According to Sullivan, preparation and planning were critical to the company’s smooth migration from Layer 2 technologies to an MPLS VPN. For instance, Cisco had a fall-back scenario in the event that cutting the first link to the other two core offices in the London site had unexpected consequences. “We couldn’t have kept old links live without suffering serious accounting charges,” he said. “So we asked the service provider to provide a second point-to-point network for the new office, to replicate the old one. Ultimately we didn’t need it, but this fall-back plan averted even the potential for catastrophe.”

Sullivan adds that for migration to MPLS VPN, like any IT project, sticking to good program management practices reaps benefits. “Know your individuals and capabilities,” he says.

NEXT STEPS

In its long-term plans, Cisco EMEA will transition more of its network operations to IDCs, an approach sometimes called telco hotelling. When this occurs, the service provider can provision VoIP as a regular connection to the PSTN. “Today, when an office moves it’s very easy to move the network connection, simply by asking the provider to connect the new site to the cloud,” says de Borchgrave. “But attaining new voice connectivity is still a hassle because you need connectivity from the office to the PSTN, and phone numbers change. We are influencing service providers to deliver PSTN voice as a VoIP packet. When that happens, we’ll be able to connect any service provider to the cloud, and inbound and outbound voice will reach the office over IP. This will greatly reduce the complexity of provisioning voice when an office moves. But before this service is feasible, service providers will need to provide more redundancy.”

Advantages of IDCs include:

- No need for onsite personnel
- Hardened site closet
- Reduced access line costs
- More flexibility in moving offices

- Greater flexibility and scaling, because changes made to a regional hub apply to all connected offices

Cisco also is seeking to extend its MPLS VPN to additional locations worldwide. “Growth is much simpler now because we are no longer responsible for building or maintaining the infrastructure,” says Sullivan. “Simply by plugging into the service provider cloud we can communicate with any other Cisco or partner office, in any part of EMEA, that’s also plugged into the cloud. As a result, Cisco IT can focus more on productivity solutions than on the infrastructure that delivers them.”

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.**