WIDE AREA NETWORKS

Free At Last: The Move To Dedicated IP-VPN Networks

Rick Malone

It's a buyer's market for dedicated IP-VPNs, as more enterprises come off long-term legacy network contracts.

For many enterprise network managers, coming off a long-term contract with an incumbent carrier is like being released from prison. The chains and shackles of high-priced legacy services are removed, vendors begin treating you like an important citizen again, and new opportunities abound.

What network managers find after their release is an increasingly proven and popular alternative for migrating their legacy data networks: dedicated IP-VPNs. These services, which rely on fixed broadband access connections like T1 and DSL, and MPLS backbones, have become the architecture of choice for most large enterprises that decide to trade in their frame relay ports and private lines. More than 8,000 U.S.-based enterprises use dedicated IP-VPN services now—and we expect installations to more than double by 2010.

Although quantifying the business drivers for switching to a dedicated IP-VPN requires more than a perfunctory analysis, most customers we have surveyed tell us that they view this migration as an investment in future-proofing their networks. IP-VPNs are perceived as more economical, more flexible and more scaleable than traditional frame relay, ATM and private line networks.

Based on our research, customers tell us they rank the benefits of switching to a dedicated IP-VPN in the following order of importance:

1. Reduced cost of network ownership
2. Secure data tunnels and routes
3. Increased mesh connectivity
4. Increased network reach
5. Investment protection
6. Path to VOIP convergence

Realizing these benefits depends on a number of factors, not the least of which is picking the right migration strategy and service provider. In addition, there are considerable challenges in matching moving targets—like new applications, user mobility, security, capacity, technology and interoperability—with the enterprise's human resources, budget and fixed operational resources. And there are other areas in which customers are finding that a lot has changed since their last round of contract negotiations.

Radical Changes

The remnants of the telecom bubble continue to haunt service providers as they struggle to find viable new market opportunities. What the carriers are seeing is the commoditization of their core markets—voice minutes and Internet access—as well as an erosion of profits due to competitive pricing pressures.

Consolidation, streamlining and self-preservation have in recent years taken precedence over innovation and servicing commercial customers. Consider the recent activities of the six largest providers of enterprise communications services in the U.S.: SBC acquired and merged with AT&T. Verizon acquired and merged with MCI. Sprint, having merged with Nextel, has shifted almost all its marketing energy to wireless products. And BellSouth is being teed up with a transition team for its pending merger with SBC/AT&T.

Today's carrier strategies and capital expenditures are weighted more heavily toward consumer wireless and residential triple play infrastructure than enterprise initiatives. The levels of investment are much higher for 3G/4G wireless and for fiber-based services (such as Verizon's FIOS) than for any commercial services.

However, there are still incentives to providing premium services to large enterprise customers. These top spenders yield longer-term revenue stability and, above all, profits.

Leading carriers are focused on delivering the services that enterprise customers want today and for the future, including VOIP, next generation wireless, Ethernet and IP-VPNs. Enterprise customers are focused on buying the latest technology that fits their needs at the most competitive prices. This is typically accomplished by bundling multiple services under one-off discount and contractual agreements of 3–7 years' duration.

Although service bundles and one-off multi-

Rick Malone is a principal of Vertical Systems Group, www.verticalsystems.com, specializing in telecom market dynamics and sizing for more than 20 years. Market statistics cited in this article are excerpted from the firm's on-line ENS research programs. Case studies are adapted from the firm's extensive database of enterprise networks.

year discounting have characterized enterprise carrier contracts for more than 15 years, today it’s a buyer’s market—another radical change.

Street prices, that is, the prices paid by the average discounted customer, for frame relay, ATM and business DSL have declined more than 40 percent during the last few years. Private line and DSL pricing has also fallen 20 to 30 percent as a result of competitive pressures and the availability of newer technologies.

Dedicated IP-VPN services are comparably or favorably priced compared to ATM, frame relay, private lines and DSL, but with the bonus functionality of being able to economically support and manage converged voice/data/video over secure data paths in a highly-meshed, scaleable, highly available, standards-based architecture.

Dedicated IP-VPN prices compare favorably with other options but offer more functionality

Dedicated IP-VPNs Defined

Dedicated IP-VPNs are available in two basic flavors: site-to-site and network-based (Table 1). Although definitions differ somewhat from vendor to vendor, here is how we define the terms:

■ **Dedicated Site-to-Site IP-VPNs** operate over the public Internet. The oldest and most widely deployed enterprise IP-VPNs use IP Security (IPSec) protocols for the secure exchange of packets at the IP layer. IPSec creates an encrypted virtual tunnel through the Internet, and it’s complicated compared to Secure Socket Layer (SSL), which also has become a popular method for easily setting up Web-accessed IP-VPN. SSL is simpler and less expensive, but it doesn’t afford the control that many large enterprises require.

Because these techniques use the public Internet and typically traverse a variety of shared network facilities, performance for enterprise applications can be unpredictable. Applications like email, file transfer and other non-response-time-critical applications can tolerate such uncertainty. Others—like transaction processing and voice—require lower, more predictable latency.

The primary access technologies used to connect enterprise locations to dedicated site-to-site IP-VPN services are DSL, T1/fractional T1 and cable modem services. Pricing for these services is modest, emulating the cost of vanilla business Internet access, and range from about $80/month for a low-performance DSL link with static addressing to about $700/month for a full T1. Host, and other hub sites, which typically require more bandwidth, are priced from about $1,000/month for a 10-Mbps Ethernet connection to $5,000/month for a T3 to $12,000/month for OC-3. All vary depending on location. Management fees are additional. At the end of last year, we counted almost 300,000 domestic enterprise sites using site-to-site IP-VPN technology.

■ **Network-Based IP-VPNs** are more robust offerings where the encryption, tunneling, routing and classes of service (COS) are managed within a specific carrier’s network, rather than across the public Internet. Most of today’s network-based IP-VPNs use Multiprotocol Label Switching (MPLS) as the core technology, enabling multiple classes of service and stronger SLAs. MPLS, which can be implemented by the carier in either a Layer-2 or a Layer-3 VPN, offers significantly better latency, jitter and packet loss than the public Internet, as well as greater meshing capability than frame relay. Service providers are rolling out MPLS-based services to most of the points-of-presence (POPs) that house frame relay and ATM switching equipment.

IP circuits—the majority (70 percent) supplied via T1—are the most widely used access technology for connecting to a domestic MPLS network. Direct IP access to MPLS services exceeds 90,000 U.S. sites. Ethernet access is growing worldwide, and several carriers plan to offer a range of bit-rates including mid-band speeds of 2 to 20 Mbps. Most network-based IP-VPN customers pay a premium of 12 to 18 percent to ensure reliable transmission, as end-to-end application performance is usually a requirement. In addition to dedicated access, some VPN providers may integrate off-net access (e.g., dial, Wi-Fi) via the public Internet for mobile or remote users. As mentioned above, good negotiators can make deals that bundle other services into their term and volume contracts.

The largest providers of legacy services (AT&T, Verizon Business, etc.) offer a smooth transition to dedicated IP-VPNs by using the frame relay or ATM access links as on-ramps to their MPLS services. A FR/IP upgrade (i.e., “IP-enabled frame relay) is often less disruptive for a customer than a full conversion to an IP-VPN, which likely would require different access lines and upgraded CPE routers. Moreover, some carriers use this migration technique as a customer retention strategy after the decision to move to MPLS has been made by the customer. More than 9 percent of the frame relay ports in service today support access to dedicated IP-VPN services in this mixed configuration.

A single enterprise may use multiple types of dedicated VPNs in a hybrid network environment to satisfy different traffic requirements within the enterprise. For example, a MPLS VPN might sup-

TABLE 1 Comparing Site-to-Site vs. Network-Based VPNs

	Site-to-Site VPNs	Network-Based VPNs
Management Responsibility	SP/user	SP
VPN Transport	Public Internet	Carrier IP/MPLS Network
SLAs	Limited	Strong
VPN Technology	IPsec	MPLS
VPN Functionality	Endpoint-based	Network-based
Primary Access Technologies	DSL, Cable, IP circuit, Ethernet	IP circuit, ATM/Frame, Ethernet
Access Reach	ISP Points of Presence	Carrier Points of Presence
Recurring Network Costs	Low - Medium	Medium

Source: Vertical Systems Group

port headquarters and large datacenters throughout the world, while a site-to-site VPN expands connectivity to branches or remote sales offices.

Street prices for network-based IP-VPNs are at or near prices for frame relay

VPN Players

Dedicated IP-VPN suppliers include local and interexchange carriers in the U.S., ISPs, cable MSOs, global carriers, virtual network operators, plus domestic carriers in countries throughout the world. Big customer bases in frame and ATM equate to big opportunities in the IP-VPN market.

Not surprisingly, the top three U.S. vendors of dedicated IP-VPNs are also the share leaders in the domestic frame relay and ATM markets: AT&T, Verizon Business (i.e., MCI) and Sprint accounted for two thirds of the dedicated U.S. IP-VPN market in 2005.

Other key providers of dedicated IP-VPNs in the U.S. are BellSouth, Qwest, Level 3, Alltel and others. Specialized vendors like Masergy, Broadwing, Energis, New Edge, Savvis and Virtela also offer IP-VPNs. For global networks, enterprises turn to Equant, BT Infonet, Global Crossing, Cable and Wireless, Vanco, COLT and others, in addition to U.S. providers with global reach.

Decision Triggers

VPN decision triggers—that is, factors that make a company convert to a dedicated IP-VPN—include management, security, application performance requirements and pricing. As any manager knows, the key to successful administration of network resources is the ability to incrementally migrate without busting the network or the budget.

Central to the migration decision are the pricing dynamics of dedicated VPN services as compared to legacy services. Monthly recurring charges for dedicated IP-VPN connections are priced by port and speed, while frame relay and ATM use a pricing model which includes a fixed charge for the port based on speed plus a charge for each of the permanent virtual circuits (PVCs) that runs through each port.

In frame and ATM networks, the more meshed connectivity a particular site requires, the higher the total charge for the port. Based on the domestic networks in our research base, T1 frame relay ports in service last year averaged $1,140 per month for the embedded base, with approximately 20 percent of that number attributable to PVC circuit charges. However, carriers will price a frame relay T1 port for a new or renegotiated customer at less than $1,000 per month. Street prices for network-based IP-VPN connections are at or near traditional frame relay services. Site-to-site T1 VPN connections average about 30 percent lower than frame relay. Higher-speed connections like T3 and OC-3 are required at hub and datacenter sites. Many of today's OC-3 connections are priced where T3 connections were five years ago.

So how do customers negotiate contracts that won't again land them in chains and shackles? Considering the historical truisms that the requirements for each enterprise network are unique, and that strong negotiators make the best deals, perhaps we can get some clues from recent customers who were coming off lengthy fixed price contracts for legacy services.

The following two cases, drawn from our research base, illustrate the VPN choices, decisions and available solutions that enterprises are facing today (note: identifying details have been changed). Cost reduction is a factor in both cases, but only one of these customers realized net savings. As for vendor selection, the incumbent frame/ATM supplier was replaced in the first case and a new provider was added to the mix in the second case.

Case 1—Nationwide MPLS

This national financial institution, headquartered in the Southwest, offers corporate banking, retail banking and wealth management services. It has grown through several acquisitions, and expects to acquire more banks and financial institutions. The company operates 500 branches scattered throughout a 10-state region, a dozen major hub sites, a dozen redundant datacenters and 1,000 automatic teller machines. Key application initiatives include a new banking platform, distributed leasing and cash management, as well as upgrading the voice systems to IP-telephony. The company has a history of aggressively trying and adopting many technologies in their early stages, including IP call centers and an integrated IP Web/voice contact center.

For eight years, this company used frame relay to its branches at full and fractional T1. The hub sites were connected via ATM and SONET with multiple T3 and OC-3 links. The automatic teller machines used a separate network of 9.6-kbps leased lines. Port and PVC management had become expensive and cumbersome for the staff to manage. Specifically, the number of PVCs in the network and per node had expanded beyond the frame service's scale, and the port capacities on the related network equipment had reached their max. This led to some ongoing reliability problems and inefficient use of resources. Because many links and ports were maxed out, an inordinate amount of engineering resources had to be devoted to bring a new or changed location onto the frame net.

Although the company was under a five-year term agreement with a major service provider, they used a mix of vendors for certain parts of the network that were added through several mergers. As the bulk of their WAN services came off contract, they were faced with how to improve network reliability, manage moves, adds and changes efficiently, integrate the new locations acquired through the mergers, and accommodate the new applications and connectivity requirements.

Looking to the future, the company wanted its new network environment to be able to support IP-telephony and video convergence and service oriented architecture (SOA) management. Above all, the new network was required to meet the bank's security standards.

Case 1 Solution

This company narrowed its options down to the following four choices:

1. Keep the current FR/ATM network
2. Move to a FR/IP architecture
3. Convert to a dedicated site-to-site VPN
4. Implement an MPLS-based VPN

Options 1 and 2, proposed by the incumbent carrier, were dismissed as too expensive and cumbersome for the increased meshing of the new applications. Also, frame relay was viewed as limited in port and PVC scalability because of the previously discussed configuration constraints. The site-to-site VPN alternative, option 3, was best in terms of network reach and was most cost effective, yet lacking in robust traffic management features, especially multi-carrier QOS. This solution also lacked strong enough SLAs.

So the choice was Option 4. The company selected a new vendor to implement an enterprise-wide dedicated MPLS-based VPN to replace the frame relay/ATM network. The new network was deployed over an 18-month period to each branch, hub and datacenter. Network-wide, the new environment is providing 40 percent more bandwidth for a total cost 20 percent below the previous configuration. The new seven-year term agreement has price adjustment options every two years.

Now the branches are connected using T1 IP circuits and the hubs are connected using OC-3 and OC-12, instead of the multiple lower-rate interfaces to which the frame/ATM network was limited. The new environment improves performance by providing five classes of service with strong SLAs. It accommodates the company's move to distribute applications to the branches; the gradual rollout of VOIP at the branches; implementation of a new branch-based video application; easy network assimilation of acquired sites; redundant connections to backup sites; and compliance with new federal regulations like Sarbanes-Oxley, etc.

The customer has also experienced less down time because routing and traffic management are done by the network of carrier grade routers, instead of through manually-configured PVCs over a network of legacy switches.

Case 2: Global Site-to-Site

This U.S.-based global retail and wholesale chain sells an inventory of more than 20,000 products to consumers and small commercial customers through specialized retail stores. Established in the 1930s in the Midwest, the company has grown to 1,500 company owned stores, 1,000 franchised locations and 100 distribution centers.

While most operations are based in the U.S., the company has opened 30 stores in the UK and 20 in Germany. The stores must report sales figures throughout the day to corporate headquarters, stocking levels to the distribution centers, and do stock checks with the distribution centers and other stores at the point of sale. Purchasing and ordering for the distribution centers is centralized at corporate headquarters, and a service bureau manages the in-house EDI system.

The company operates with limited IT staff and is not considered an early adopter of new technology. While it has recently implemented supply chain management software, it continues to operate a batch inventory process using old IBM protocols from many locations.

The company currently runs a two-tiered network that connects all essential aspects of the retail operation from point-of-sale and inventory control to financial reporting and accounting. The upper tier consists of T3 frame relay and ATM links interconnecting the distribution centers with headquarters. The lower tier consists of PSTN (dial-up) and ISDN services used by the stores to send sales and inventory data to corporate and the distribution centers.

In order to increase competitiveness and better manage inventory, the company sought to improve the scope and responsiveness of the store systems. One goal was more timely reporting of sales and accounting information to headquarters. Another was to improve the customer point-of-sale experience with speedier inventory checks, automated ordering and credit processing. The traffic flow is generally hierarchical, but would require meshing in the future as store-to-store communications is implemented.

Other goals in migrating this network to a new environment also included bringing every store up to a dedicated broadband connection, minimal disruption to the current backbone data applications, and providing autonomy to the franchised sites, including the selection of service providers, billing functions and management.

A single vendor had most of the business under a three-year term agreement, including the frame/ATM backbone, the company owned stores and some of the franchises. The international locations used a combination of frame relay and ISDN from different providers.

Case 2 Solution

This company considered three choices:

1. Convert to a network-based IP-VPN for all sites, collapsing both tiers into one network.

2. Move to a frame relay/IP architecture for distribution centers (the upper tier) and a new dedicated site-to-site VPN for the stores (the lower tier).

3. Install a dedicated site-to-site IP-VPN at the stores only (the lower tier), keeping the upper-tier distribution center network unchanged.

These two cases illustrate the complexity and flexibility of today's VPNs

Thousands of legacy data network contracts will be expiring in the next two years

Option 1, which involved rolling out MPLS to each of the company's 2,600 sites, was not feasible due to network reach and cost. MPLS was not available at all store locations worldwide, even from the largest providers, and would need to be backhauled from some stores. Also, the cost of such a robust change in network functionality greatly exceeded budgetary limits, and the project was beyond the staff's current technical expertise.

The second option included migrating the distribution centers gradually to a Layer-2 MPLS VPN through the use of FR/IP connections and installing a new dedicated site-to-site VPN at the stores. While a good solution for the store network tier, this option failed when the company encountered version compatibility problems operating their older protocols (SNA SDLC, BSC, etc.) at the distribution centers over the FR/IP link and MPLS backbone during their tests.

Because the roadmap to extinction of those old protocols is still a couple of years out, and because there was no additional cost savings with an MPLS-based solution (compared to a re-negotiated frame/ATM contract), the company dropped the idea of moving the upper tier and the distribution centers to a VPN.

Only Option 3, a dedicated site-to-site IP-VPN at each store, fit this enterprise's needs best. The company contracted with a single service provider, not its incumbent frame relay vendor, to roll out an IPSec VPN to each company-owned store. The agreement included providing dedicated Internet access using low-cost DSL or cable modems, installing or upgrading the store's LAN to support multiple simultaneous users over the VPN, and managing security, authentication and firewalls. The result is that each store has full-time, dedicated VPN connectivity to headquarters, distribution and other stores.

The frame network for the distribution centers, the upper tier, remained essentially unchanged, although pricing and terms were renegotiated and improved substantially with the incumbent vendor. For example, at headquarters, several T3 ATM links were replaced by OC-3 links, each for approximately the same monthly recurring charge as a single T3 under the old contract.

The franchised stores, with autonomous control of their own store and telco budgets, were added to the VPN after obtaining their own Internet connections from their local providers.

The new network environment leaves intact the upper-tier network of the 100 distribution centers, while providing broadband communications to each of the 1,500 company-owned store locations and 1,000 franchised locations with economical local access. The European stores can now be managed seamlessly with the U.S. stores; financial reporting and inventory control are being done in near-real time; point-of-sale inventory checks are available instantaneously at multiple stations within each store; a new merchandizing system which broadcasts to all stores daily is in place; and some stores are converting to VOIP key sets.

The major expense for this project was in implementing long-overdue LANs and customer edge routers at each store. Yet the company estimates that converting 1,500 company-owned stores from dial-up or ISDN to a dedicated site-to-site IP-VPN, along with renegotiating new contract terms for the existing frame relay distribution center backbone, have increased monthly recurring network costs by only 20 percent overall.

Parole On The Horizon For Thousands

More than 30,000 U.S. companies currently use frame relay, ATM or private line services for domestic and/or global networking. An estimated 25 percent of this base has contracts expiring within the next two years.

Migrating the legacy data net this time around is not just about swapping out technology to reduce costs. It's about scalability, reach, security, application convergence and enabling enterprise evolution. Contrary to the axiom that users will opt for incremental change over wholesale change, many will consider their newfound contractual freedom as an opportunity to try something new, re-evaluate their vendor relationships and future-proof their networks□

Companies Mentioned In This Article

Alltel (www.alltel.com)
AT&T (www.att.com)
BellSouth (www.bellsouth.com)
Broadwing (www.broadwing.com)
BT Infonet (www.btinfonet.com)
Cable and Wireless (www.cw.com)
COLT (www.colt.net)
Energis (www.energis.co.uk)
Equant (www.equant.com)
Global Crossing
(www.globalcroassing.com)
Level 3 (www.level3.com)
Masergy (www.masergy.com)
New Edge (www.newedgenetworks.com)
Qwest (www.qwest.com)
Savvis (www.savvis.net)
Sprint (www.sprint.com)
Vanco (www.vanco.com)
Verizon (ww.verizon.com)
Virtela (www.virtela.net)