Carrier Managed VPN Services

*by: Michael S. Podsedly*

Copyright 2003, Faulkner Information Services. All Rights Reserved.

Docid: 00016988

Publication Date: 0305

Publication Type: TUTORIAL

**Preview**

Carrier managed virtual private networks (VPNs) allow businesses to focus on their operations while leaving the installation, maintenance, and management of their networks to their service providers. These fully managed services offer cost savings, scalability, and flexibility not found in VPNs managed by the customer. This report describes the different types of carrier based VPNs and highlights their strengths and limitations for business customers.

**Report Contents:**

- Executive Summary
- Issues to Consider
- Analysis
- Recommendations
- Web Links

**Executive Summary**

A virtual private networks (VPN) is a dedicated network link that is provided over a shared network, using encryption and authentication techniques to provide privacy and security. The earliest VPNs were provided over frame relay and provided private subnetworks using permanent virtual circuits (PVCs). These types of networks were difficult to configure and expensive to maintain. Although frame relay is certainly robust enough to provide VPN services for enterprise customers, virtual private networks really began to grow in popularity when carriers introduced services based on IP tunneling. Today, IP-enabled VPNs--either over an IP network or as an IP-VPN provided over a frame network--are emerging as next-generation alternatives.

VPNs allow traffic from many sources to traverse the same network in private data streams. The data streams can be differentiated, permitting routing to different destinations and provision of different levels of service. A VPN can operate over the Internet or on IP, frame relay, or ATM networks.

**Types of VPNs**

There are three types of IP VPNs:

- **Frame Relay**--Frame relay uses PVCs linked to Internet gateways. The quality of service for
frame-based VPNs is good, but it is difficult to provide any-to-any connectivity because the PVCs need to be manually configured every time network technology changes.

- **Customer Premise Equipment (CPE)**—CPE-based services are the most popular. The service provider or enterprise customer deploys access routers onsite using Point-to-Point Tunneling Protocol (PPTP), Layer-2 Tunneling Protocol (L2TP) or IPSec. A variety of equipment may be used, including IP VPN routers, standard routers with added VPN software, IP VPN gateways that work with routers, IP VPN appliances, or firewalls acting as IP VPN gateways.

- **Network-Based IP VPNs**—Network-based IP VPNs are delivered from a carrier’s network edge to the customer’s premise over a no-frills connection. This type of service does not require any additional CPE other than a standard network router, allowing the service provider to house all of the necessary equipment within the network. This lack of customer premise equipment has obvious cost advantages to the service provider. Network-based VPNs have the greatest possibility for future growth. A network-based VPN enables the same services as a CPE-based VPN, including application proxy firewall, encryption, intrusion detection, and tunnel termination—but it integrates them into a single carrier-based platform, permitting support of thousands of subscribers simultaneously with customized VPN services.

The market direction is toward IP VPNs, whether running over IP, frame relay, or ATM backbones. IP provides a unifying protocol for today’s data services. Increasingly, VPNs are provided by carriers as managed products running on high-speed backbones with service equivalent to leased lines at a fraction of the cost. Businesses are increasingly taking advantage of these services, and carrier managed VPNs are experiencing rapid growth.

**Carrier Managed VPNs**

Telecommunications carriers offering managed VPN services connect customers over their own backbone networks, avoiding any connections—and potential problems—through the public Internet. Customers enjoy the same security, traffic prioritization, manageability, and reliability that they would receive if they build out their own network. Obviously, in a carrier managed deployment, the service provider must have a footprint large enough to cover all of the customer’s sites.

Telecom carriers can provide an entire VPN solution for customers, including design, installation, and support. As a result, the technical expertise required of in-house IT personnel is much less. With encryption, digital certificates, and Public Key Infrastructure (PKI) playing such a prominent part in VPNs, the needed security expertise is in great demand and difficult to obtain. Carrier VPN providers, however, have the necessary expertise, and they are able to set up secure networks simply and rapidly. In some solutions, the network might already be in place and require very little effort and expense to connect and interconnect customers’ internal networks.

**Issues to Consider**

Carrier managed VPNs do have some drawbacks, but the benefits outweigh them for enterprise customers.

**Benefits**

Carrier VPNs offer a number of benefits to businesses:

- Cost savings.
- Scalability.
- Flexibility.
Adoptive to business relationships.

Connections to remote users are much less costly than the links provided by corporate WANs and traditional remote access servers with modem banks. These cost savings come from the elimination of leased lines, long distance charges, and the large amounts of equipment required to set up corporate WANs. In addition, remote users require considerable support outlays, because they have varying technical abilities and use a wide variety of different equipment. When remote access is obtained through carrier VPNs, these support responsibilities can be shifted to the VPN provider. Many of these providers have maintenance staff in widespread locations.

Equipment installation, maintenance, and obsolescence costs are also reduced, since a single interface with the VPN provider can serve multiple purposes. Equipment costs can be further reduced if a network-based strategy is used. Corporations can expand geographically without investment in leased lines or equipment, and less equipment means less exposure to obsolescence.

Carrier managed VPNs can be scaled by changing the configuration at the interface with the VPN provider. External suppliers and business partners can be added and removed from the network, providing additional flexibility.

Network-Based VPNs. The network-based VPN integrates VPN functionality and applications into the service providers’ IP cloud, eliminating the need for premises-based VPN hardware and software. VPN functionality is not limited to what CPE vendors are now offering, because it can evolve to cater to changing requirements. With a network-based VPN, the subscribers’ router routes packets, while VPN services and functionality are deployed from the carrier's POP. This means service can be rolled out easily and cheaply without affecting daily operations, and services can be turned on and billed immediately.

Carrier VPNs can also provide Service Level Agreements (SLAs) to provide quality guarantees for VPN service corporate users will enjoy. Currently, business users can buy carrier VPN services with SLAs from individual service providers, but these guarantees do not usually cover traffic that flows across multiple service provider networks. Techniques are becoming available that allow SLAs to be guaranteed for VPN traffic across multiple networks. One of the principal techniques makes use of Multi-Protocol Label Switching (MPLS), which assigns a label to each packet that enters a carrier's network. The label includes information on packet type and class, allowing the carrier to apply different service priorities to different packets, and thus control the quality of service for VPN traffic. Settlement systems allow multiple service providers to share revenues from VPN traffic that crosses their networks.

Difficulties with in-house VPNs have been slowing their adoption by businesses. VPN software does not always work smoothly with existing networking hardware and software. Modifications that are specific to each end user’s configuration can drive up installation and support costs. PKIs are complex and suffer from interoperability between gear from different vendors. All of these difficulties are exacerbated when businesses extend VPNs to form extranets connecting them with customers, suppliers, and other trading partners.

Limitations

Outsourcing VPNs to a carrier is not an unmixed blessing. It does have some potential disadvantages. Companies that outsource will have limited control over VPN hardware. In some cases, the connection to the provider's network may be unencrypted. This problem can be overcome by having the VPN start on company premises with a VPN server that the provider controls, and such a server should be isolated from the corporate network with a firewall. In all cases, the company using the VPNs will have to monitor the security practices of the provider.
Carrier managed IP-VPNs continue to exhibit strong growth. The market for IP-VPNs was valued at $2.3 billion in 2002, and it is expected to grow to $7.2 billion by 2006. About 50 percent of all mid- and large-sized businesses now have some form of IP-VPN service. The service is inexpensive enough that it is an attractive option to smaller businesses, and as these companies are signing contracts, more carriers are getting involved in the market. Network-based configurations are more attractive to smaller businesses than CPE-based once since they cost less and require less technical expertise.

Remote access and site-to-site connections are the primary applications for IP-VPNs and are expected to remain so in the future. The target industries remain those buying at the present time, retail, banking and transport. Mid-market sized companies represent an important segment for growth as do frame relay and ATM customers for potential conversions.

VPN hardware and software now make it possible for providers to separately handle traffic from different customers, guaranteeing the quality of VPN service for corporate customers, capturing information for billing VPN services, and sharing revenues between carriers when VPNs traverse more than one carrier network. The continued development of MPLS is providing further impetus to VPN growth. IP VPNs based on MPLS offer an easy migration from frame relay VPNs. While there continues to be some resistance from carriers, supporting reasons include better scalability and manageability, plus support for value added differentiated service--which might include firewalls, virus protection, caching, and other services.

There are significant economies of scale in centralized, managed services. These economies will drive an increasing number of businesses toward the network-based model over the CPE-based model. CPE-based VPN solutions require expensive and management-intensive devices on the subscriber premises, and there is little opportunity for ongoing value-added services from the carrier. By eliminating CPE, costs can be lowered at every stage. Capital equipment investment is reduced, and service provisioning is rapid, with simplified maintenance. For carriers, this also provides opportunity to create and sell incremental IP services.

With VPNs provided as a standard carrier service, all of the efficiencies of large scale operation can be brought into play, and POPs for remote links can be made available worldwide. Use of a carrier-based system is also consistent with global trends toward outsourcing IT infrastructure.

The top 10 IP-VPN service providers are as follows:

- AT&T.
- Equant.
- Infonet Services.
- Genuity.
- MCI.
- Qwest Communications.
- Savvis Communications.
- SBC Communications.
- Sprint.
- XO Communications.

There is intense competition among the range of providers, including major and 2nd tier carriers, local ISPs and value added resellers.
Recommendations

The popularity of VPN will continue. VPNs are rapidly replacing expensive leased lines and high-maintenance WAN facilities. Any network-related decision for an enterprise is extremely important. This is especially true when converting an existing network or changing the configuration. The advantages must be significant enough to choose new or upgraded technology. The managed IP-VPN offering is attractive in a variety of situations. Several issues must be addressed before a final decision is made. If the existing network is frame relay or ATM based there can be a significant cost saving by implementing an IP-VPN. If the enterprise method of remote access were dial-up then an IP-VPN would be much less costly. The required level of security is also a factor in any decision. The security level can only be delivered if a single provider's network is used for all locations. The network based IP-VPN is better suited for a headquarters or regional office than needs guaranteed service levels in connecting with a number of remote sites. The decision process should examine what option is best for the majority of its sites. Most of the larger companies deploy a mix of CPE and network based VPNs. The level of staff expertise must also be considered in evaluating a managed solution. The level of outsourcing has increased among companies and the economy makes it difficult to retain support staff, which favors the carrier-managed system. There is a higher level of confidence in the security software options than early VPN technology.

About the Author

Mr. Podsedly is an independent consultant in the area of forecasting and business intelligence. He has more than 30 years of experience in the telecommunications industry. Before starting his consulting business, he was Director of Forecasting and Planning at BellSouth. He has presented papers at National Forecasting Conferences and taught undergraduate courses in economics and management. He holds an M.B.A. from the University of Alabama at Birmingham.

Web Links

AT&T: http://www.att.com/
BellSouth: http://www.bellsouth.com/
Cisco Systems: http://www.cisco.com/
Equant: http://www.equant.com/
Infonet Services: http://www.infonet.com/
MCI: http://www.mci.com/
Qwest Communications: http://www.qwest.com/
Savvis: http://www.savvis.com/
SBC Communications: http://www.sbc.com/
Sprint: http://www.sprint.com/
Verizon Communications: http://www.verizon.com/