INTRODUCTION

The plethora of wide area network (WAN) options available in the United States continues to grow as technology advances. While new options and changing technologies give U.S. companies and their WAN managers more choices to solve problems, these new options also add complexity. The result is often an increasing number of WAN managers scratching their heads trying to find the right WAN technology fit for their increasingly complex networking needs.

This white paper is designed to help WAN managers navigate the choices available in today's wide area networking environment. The paper focuses on the two primary WAN options used today: frame relay and network-based IP virtual private networks (IP VPNs).

The term VPN refers to the use of shared facilities under software control such that it gives the appearance and benefits of a private network, including continuous availability and reliability. VPNs provide network-based features and management capabilities that are not found in private networks.

Voice VPNs have been available since the 1980s and are widely used by many large and mid-sized businesses for communications across their geographically dispersed locations. Voice VPNs usually include network-based features, such as customized routing, advanced numbering plans, and remote access. This simplifies intracorporate communications by enabling features such as 4-digit dialing to reach any corporate site on the VPN.

Data VPNs have been available since the 1970s from carriers that built private data networks to support multiple customers through intelligent virtual networking. In the 1980s, data VPNs were built through the use of X.25 protocols. In the 1990s, frame relay became the preferred choice for data VPN transport protocols. By the late 1990s, several carriers began offering VPN services by carving safe and reliable channels through the public Internet, thus enabling enterprises to use the public Internet in a private, secure environment. The latest iteration of VPNs are carrier-based IP VPNs. The IP VPN value proposition was enhanced as carriers built private IPs that didn't route through the Internet. This approach could be professionally managed and controlled on an end-to-end basis, thus creating a much higher quality solution for corporate IP VPN requirements.

OVERVIEW OF FRAME RELAY AND IP VPNs

Today, frame relay and IP VPNs are the two most popular types of VPNs used by businesses in the United States.

Frame relay has been on the market for over 10 years. It relies on both a telecom carrier's network infrastructure and on edge equipment located at the customer's premises. The edge equipment encapsulates data into frame relay packets for transfer across the WAN. Frame relay, as a Layer 2 (link layer) technology, can
transmit a wide range of protocols, including IP, mainframe, and voice, and can also be used to deliver Internet access. As a connection-oriented technology, data travels over a set path, which allows the carrier to engineer the network in a way to guarantee quality of service, and also provides for excellent security and reliability.

Frame relay customers have dedicated access, but within the long-haul transmission network, data shares the carrier's physical network infrastructure.

IP VPN is a WAN newcomer. The network-based version of IP VPN, in which no special equipment must be installed on the customer's premises, is comparable to frame relay in many ways. Either technology may be the ideal WAN solution for connecting sites.

Figure 1 shows the basic architecture for frame relay and network IP VPN, as well as the similarities/differences in their WAN features. Frame relay networks offer high security, predictable performance, and guaranteed reliability. However, a permanent virtual circuit (PVC) must be established between each site connected, and PVC capacity must be monitored and adjusted for the amount of data flowing between the sites. This is costly to implement and maintain. When traffic patterns and site applications change, a new PVC must be created.

**Figure 1**
A Comparison of WAN Architectures and Features

<table>
<thead>
<tr>
<th>Frame Relay</th>
<th>IP VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permanent Virtual Circuits</td>
<td>On-demand Circuits</td>
</tr>
</tbody>
</table>

**Table:**
- **Security**
- **Performance**
- **Reliability**
- **Staffing Requirements**
- **Implementation Complexity**
- **Cost**

Source: IDC, 2003
In contrast to frame relay, connectionless network IP VPNs do not require PVCs. Each site simply connects to the network cloud via multiple access methods (such as frame relay, private line, DSL) and can talk to all other connected sites in an any-to-any traffic pattern. IP VPN ports are less costly than frame relay ports, and network management and optimization can be done quickly, easily, and cost effectively. IP VPN can provide substantial cost savings over private lines as long as security and performance issues can be satisfactorily addressed.

Frame relay networks are efficient for stable spoke-to-hub traffic patterns. They work best where traffic flow is steady and predictable from points B, C, and D to the hub at point A. However, a new service feature, called IP-enabled frame relay, enables fully meshed network using multiprotocol label switching (MPLS) or virtual routing overlay to the frame relay network. Today IP-enabled frame relay is a fairly new feature with limited availability, but IDC expects it to account for 25% of frame relay ports within three years. IP VPNs are preferred solutions where users have any-to-any traffic patterns.

**REGULATION**

Since the 1982 consent decree that broke up AT&T, government regulation has kept the local (intra-LATA) and long distance (inter-LATA) markets in the United States largely separate. That situation changed with the Telecommunications Act of 1996, which allowed long distance carriers and competitive local exchange carriers (CLECs) to operate in any market, but kept local incumbents (BellSouth, Qwest, SBC, and Verizon) out of the long distance market until sufficient competition existed in the local markets.

Currently, local carriers have been granted approval to enter the long distance market in about half of the 50 states. We expect the process to be wrapped up in 2003, with the remaining restrictions lifted on local incumbent carriers selling long distance service. For the frame relay and IP VPN customer, this means more choice of carriers and greater competition. Since the data market carried the same local/long distance restrictions as the voice market, this meant frame relay customers often needed to buy both a local and long distance frame relay service from different providers. Local carriers could not offer network IP VPN at all; they were limited to customer premises equipment (CPE)-based IP VPNs.

Now that the regulatory restrictions are being substantially lifted, we expect the local incumbents to excel in offering regional long distance services in both voice and data. They will also be able to better address the needs of local business customers, as the lifting of regulatory barriers permits the local incumbents to offer bundled services of local and long distance voice and data that had been previously restricted.

**FRAME RELAY IS THE LEADING CORPORATE WAN BACKBONE**

Frame relay, launched in 1991, was a $7.3 billion market in the United States in 2002, and the market is projected to reach almost $9 billion in 2007 (see Figure 2). Frame relay continues to grow because it has remained flexible by adding new features as it matures, such as frame relay-to-ATM interworking, priority PVCs, voice-over-frame relay, multicast PVCs, and IP-enabled frame relay.
Frame relay works best when used to interconnect the local area network (LAN) in a company's headquarters to LANs in the company's branch offices. A typical American frame relay network is 20 sites, but it can range from five or six sites to thousands.

Typically, companies have installed frame relay as a replacement for private lines because frame relay offers the same quality and security as private lines but at lower cost. Figure 3 shows a comparison of frame relay and private line network configurations.

To build a fully meshed network, on which every site talks to every other site, network planners employ the formula N x (N-1)/2 to determine the total number of links needed, where N is the number of sites to be connected. For instance, in a five-site network as shown in Figure 3, each site must have a line linking it to each of the other four sites. This would require a total of 10 links among the five sites, as well as the necessary access links to reach the service provider's point-of-presence (POP).
The big advantage of frame relay over private lines is that the network formula — $N \times (N-1)/2$ — applies only to the PVC. The number of ports in a frame relay network is equal to the number of sites connected, not an order of magnitude beyond the actual number of sites. The PVC logical connections represent an improved flexibility over private lines — it is easier and cheaper to move a logical connection than a physical connection.

While cost is a principal driver of demand for frame relay over private lines, it has several other attractive features, including performance reliability, low latency, multiprotocol support, management maintenance, and ubiquity.

- Frame relay is an extremely reliable service, with many carriers offering 99.999% availability guarantees, or service level agreements (SLAs). Corporate network managers can be contractually guaranteed that their mission-critical applications will be properly supported on frame relay networks.

- Frame relay offers low latency — the roundtrip transit time for traffic to travel between point A and point B. This makes frame relay suitable for real-time voice, videoconferencing traffic, and low-latency mainframe communications. Some frame relay carriers offer class of service allowing latency-sensitive traffic to take priority.
Frame relay is a Layer 2 (link layer) technology, meaning that it can carry any type of Layer 2 or 3 (network layer) protocol, including transmission control protocol/Internet protocol (TCP/IP), systems network architecture (SNA), or voice (while a Layer 3 IP VPN can only carry IP traffic). SNA is a common mainframe technology that a hospitality company might use for a central reservations system. This traffic could coexist, for example, on the same frame relay link with SAP application data from the hospitality company’s planning department and with email traveling over TCP/IP.

Large companies are attracted by frame relay’s ubiquity. It is available in every corner of the world. Companies can buy frame relay from different carriers around the world, and the service will interconnect and work together because it is based on international standards.

**FRAME RELAY USERS AND APPLICATIONS**

Who uses frame relay? In a word, everyone. It is the most popular WAN technology in the United States. According to IDC’s WAN Manager Survey, which interviewed 400 medium and large companies in spring 2002, frame relay is the number 1 choice for WAN backbone technology, with one out of three U.S. corporations using it for their primary WAN backbone platform (see Figure 4). This is consistent across most industry sectors, with frame relay being the predominant WAN choice for manufacturing, transportation, healthcare, and banking industries (see Figure 5). Retail/wholesale was the only vertical in which frame relay came in second place to IP VPN. IP VPN received high marks as a secondary WAN technology, indicative of companies implementing IP VPN for remote access or IP-based applications such as email or Web access.

**FIGURE 4**

PRIMARY WAN TECHNOLOGY (% OF RESPONDENTS)

Q. *Which configuration does your company use as its primary WAN platform?*

<table>
<thead>
<tr>
<th>Configuration</th>
<th>% of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame relay</td>
<td>3.3</td>
</tr>
<tr>
<td>IP VPN</td>
<td>25.6</td>
</tr>
<tr>
<td>Private lines</td>
<td>24.5</td>
</tr>
<tr>
<td>ATM</td>
<td>4.7</td>
</tr>
<tr>
<td>Transparent LAN over Ethernet</td>
<td>3.5</td>
</tr>
<tr>
<td>Other</td>
<td>6.6</td>
</tr>
<tr>
<td>Don’t know</td>
<td>1.8</td>
</tr>
</tbody>
</table>

N = 400

Note: Results are weighted to reflect US company size and vertical market distribution.

Source: IDC’s US WAN Manager Survey, 2002
The leading application for frame relay is connecting LANs in different cities or within a metro area. Typically, a frame relay PVC is purchased between headquarters and multiple branch locations, and occasionally between branch locations. At each end of the frame relay connection, there is an edge device (a CSU/DSU) that terminates the traffic and converts it from frame relay packets to LAN ethernet packets. The edge device can either be owned and maintained by the business or leased from and maintained by the service provider as a managed service, depending on the IT expertise and resources of the customer.

**FIGURE 5**

**PRIMARY WAN PLATFORM BY VERTICAL MARKET (% OF RESPONDENTS)**

<table>
<thead>
<tr>
<th>Vertical Market</th>
<th>Frame relay based (%)</th>
<th>Other (%)</th>
<th>IP VPN (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking/Finance/Insurance/Real Estate</td>
<td>32.4</td>
<td>13</td>
<td>32.4</td>
</tr>
<tr>
<td>Manufacturing/Mining</td>
<td>38.3</td>
<td>26</td>
<td>33.8</td>
</tr>
<tr>
<td>Retail/Wholesale/Trade/Business</td>
<td>28.9</td>
<td>28.9</td>
<td>7.9</td>
</tr>
<tr>
<td>Services/Hospitality</td>
<td>33.8</td>
<td>28.9</td>
<td>7.9</td>
</tr>
<tr>
<td>Transport/Utilities/Media</td>
<td>34.9</td>
<td>28.9</td>
<td>7.9</td>
</tr>
<tr>
<td>Healthcare</td>
<td>34</td>
<td>33.8</td>
<td>34.9</td>
</tr>
<tr>
<td>Education/Nonprofit</td>
<td>24.6</td>
<td>18.9</td>
<td>9.1</td>
</tr>
<tr>
<td>Government</td>
<td>18.9</td>
<td>3.3</td>
<td>3.3</td>
</tr>
<tr>
<td>Other</td>
<td>33.3</td>
<td>0</td>
<td>33.3</td>
</tr>
</tbody>
</table>

Note: Results are weighted to reflect US company size and vertical market distribution.
Source: IDC's US WAN Manager Survey, 2002

Data transmitted in frame packets provides a higher degree of security, data integrity, and transmission reliability than Internet packets. Because of these qualities, corporations utilize frame relay to interconnect their LANs to transmit their mission-critical applications like credit card authorizations, supply chain data, online ordering systems, accounts receivables, and voice over IP. Frame relay is also often used as
the link layer for dedicated Internet access and to distribute Internet access to branch offices.

A range of speeds is available with frame relay — from 56Kbps, which may be appropriate for credit card authorizations, to T1 (1.544Mbps) and T3 (45Mbps), used by large corporations for customer relationship management systems or supply chain data.

**FRAME RELAY HAS MANY FEATURES AND CHARACTERISTICS**

Frame relay was designed specifically for data communications, while private lines were designed for voice. Two important features that optimize frame relay for data traffic are PVCs and committed information rates (CIRs).

The PVC, as discussed above, is a cheaper alternative to private lines because it reduces the number of physical circuits and equipment needed. Frame relay uses a connection-oriented architecture so that all traffic follows a predetermined path through the network. The paths are called virtual circuits because different virtual circuits share the same physical infrastructure. This characteristic enables the service provider to "over book" the bandwidth and thereby reduce the cost for all users. At the same time, by predetermining the traffic path, the service provider can guarantee quality of service.

Data communications tend to travel in bursts, and frame relay uses statistical multiplexing to increase the efficiency of the network. Traffic parameters, such as CIR and maximum burst, are used to police traffic to ensure that network resources are not overloaded. If a customer exceeds its contracted CIR by sending too many packets, the extra packets are tagged as discard eligible. If network congestion occurs, those discard-eligible packets are dropped. If the network is not congested, the extra packets are successfully sent.

This system maintains quality of service for all customers who share the carrier's frame relay infrastructure. This system also allows service providers to offer strong SLAs, guaranteeing parameters such as network availability, latency, frame delivery ratio, and mean time to repair.

Unlike private lines, frame relay continues to evolve with a steady stream of new enhancements:

- Frame relay class-of-service and/or priority PVCs give time-sensitive traffic, such as voice or mainframe (SNA) traffic, priority over less time-sensitive streams of traffic, such as email or file transfer. This enhancement vastly improves the performance of time-sensitive applications, while no one notices if their email arrives 30 seconds later.

- Multilink frame relay was introduced as a standard in 1999 and addresses the big jump in port speed from DS1 (1.544Mbps) to DS3 (45Mbps) by enabling bonded T1s to offer additional port speeds between DS1 and DS3. Multilink gives companies more economical options when they need to upgrade a port above T1. In addition, several carriers offer subrate T3 offerings, which also deliver intermediate port speeds by rate-limiting a T3 port.

- Several disaster recovery applications are available with frame relay. The most widely available is ISDN backup service, in which an ISDN circuit would take over in case of an outage in the frame relay network. There are also features, such as intelligent PVCs, that are used if a company's network hub experiences a disruption. The intelligent PVC immediately reroutes traffic to a backup site.
Web-based interfaces allow customers to monitor and manage their frame relay network online. Monitoring the network allows the customer to improve efficiency and get more value from the network by catching issues that impact network performance. For instance, if low-priority, large file transfers occur during peak network times in the middle of the morning instead of the middle of the night, this would crowd out high-priority data and cause network congestion and dropped packets. Monitoring software allows the network manager to see what applications are impacting the network in a particular way. Without network monitoring, the solution to network congestion is often to upgrade to a higher port speed. With monitoring, the applications consuming network resources can be tweaked so that full use is made of existing resources. Monitoring also allows the network manager to ensure the carrier is meeting SLAs and to take corrective action if it is not.

IP-enabled frame relay allows any-to-any connectivity between all frame relay sites, instead of the traditional hub-and-spoke architecture of frame relay. Using either MPLS or virtual routing as an overlay technology, each site is connected by a single PVC. These IP-enabled PVCs then deliver the frame relay packets to routers in the core of the network, where they can be transferred to any other IP-enabled PVC on the frame relay network.

**FRAME RELAY IS ESPECIALLY SECURE**

Frame relay is an especially secure networking technology, on par with the security of a private line network. Even though frame relay shares physical network resources among different customers, its connection-oriented architecture makes it immune from the address spoofing, denial of service, and other security concerns associated with Internet protocol.

Expanding on the connection-oriented nature of the technology, frame relay is a Layer 2 protocol, running at the data link layer of the Open Systems Interconnection (OSI) Seven Layer Model. In other words, frame relay networks are aware of the physical networks on which they are running. (Internet protocol networks at Layer 3, such as IP VPNs, are not aware of the physical network.) Each frame relay packet contains information specifying the route it must travel on a point-to-point path known as a PVC. While multiple PVCs can be provisioned between sites, the data can only follow a path defined by a specific PVC. Unlike Internet packets, frame relay packets cannot be spoofed or hacked because they have to travel on a specific pathway.

The only security vulnerability in frame relay is one that is shared by all technologies — the physical layer. And for this, customers must look at the efforts of their service provider to keep its switches and other transmission facilities secure. For companies needing ironclad security against a physical security issue, encryption is possible at the frame relay layer, but it is rarely implemented.

While frame relay networks are immune from hackers, viruses, and denial of service attacks that plague public Internet access, for the reasons discussed above, precautions should be taken when frame relay is used to distribute public Internet access. As with any public Internet access, firewalls and virus detection are prudent.

**FRAME RELAY COST ISSUES**

To implement a frame relay network, there are both equipment costs and service costs. The service costs are in four main categories: equipment, port, PVC, and access. Each site connected to the network needs a CSU/DSU. This can either be bought or leased. As frame relay is standards based, equipment can be bought from any vendor. Each location needs a frame relay port, which is the connection to the carrier's frame relay network. While discounts are usually available, monthly intra-
LATA frame relay port charges might range from $45 for a 56Kbps port to over $3,000 for a DS3 port. In addition to the port, each location needs at least one PVC, which is the point-to-point path between two ports over which the data will travel. PVCs are available in many increments, and intra-LATA frame relay PVCs might range from $8 per month for a 32Kbps PVC to over $2,000 for a 45Mbps PVC.

Inter-LATA (long distance) ports and PVCs are significantly more expensive than intra-LATA (local) ones. Compared to the local port charges mentioned above, a long distance port may range from $470 per month for a 56Kbps port to $8,700 per month for a DS-3 port. Likewise, long distance PVCs are more expensive than local ones. A 32Kbps long distance PVC would be $102 per month, and a 10Mbps PVC would be $9,225 per month.

Priority PVCs that offer class of service or PVCs with other special features would cost more than traditional PVCs. The last significant service cost is access. This is the physical link, usually a private line or DSL connection, between your site and the carrier's nearest frame relay point of presence.

In addition to the basic equipment and service fees, several additional features can be purchased, each with its own monthly fee:

- **Backup/disaster recovery.** An ISDN backup network or intelligent PVCs to a backup host site.
- **Public Internet access.** Many companies use their frame relay network to deliver public Internet access to their branch offices.
- **Customer network management.** Allows the customer to use Web-based tools to monitor and manage the frame relay network online.
- **Personnel and training costs.**

Frame relay, like other telecommunication services, is generally based on multiyear contracts, with two to three-year terms being the most common.

**FRAME RELAY MIGRATION STRATEGY**

Companies look to migrate from traditional frame relay for a variety of reasons:

- **Save money.** In the first years of IP VPNs, companies often considered migrating because they could save money with IP VPN instead of frame relay. While this was certainly true when IP VPNs were first launched, IP VPNs have exerted considerable price pressure on frame relay over the past 3–4 years, and the cost differential has shrunk.

- **Remote access.** Remote access is the leading reason why a company using frame relay adopts IP VPN, as this is something that IP VPN does very well and frame relay does not. IDC's research has found the most common scenario is for a company with an existing frame relay network to add IP VPN for remote access functionality and keep frame relay for mission-critical applications that require high quality of service. This is why IDC's 2002 WAN Manager Survey shows frame relay as the most popular primary WAN technology, and IP VPN is the most common secondary WAN technology.

- **Fully meshed network.** The need for a fully meshed network is a distant third place as a reason to migrate from frame relay. Traditional frame relay architecture is a hub-and-spoke configuration, where branch offices are all connected to and communicate through a headquarters hub. For some IP
applications, any-to-any connectivity might be desirable, but with traditional frame relay, the number of PVCs needed to attain a fully meshed network is prohibitively expensive. This is the $N^2$ logical circuit problem, where the full mesh requires $N(N-1)/2$ connections. IP VPN, with its routed carrier infrastructure, delivers any-to-any connectivity.

But there is also a way to deliver any-to-any connectivity using a company's existing frame relay network that does not require the purchase of any different equipment on the part of the corporate customer. IP-enabled frame relay uses either MPLS or virtual routing as an overlay technology to deliver the same any-to-any connectivity as IP VPN. Instead of multiple PVCs per site for a fully meshed network, IP-enabled frame networks have just one PVC per site, and the MPLS or virtual routing technology in the core of the carrier network routes the data at Layer 3 to the appropriate site. With IP-enabled frame relay, the customer gains any-to-any connectivity at a reasonable cost without expensive changes or forklift upgrades to the customer's CPE. And even if a customer needs only partial meshing on a long distance frame relay network, IP-enabled frame relay is often more cost effective than purchasing traditional PVCs at long distance prices.

IP-enabled frame relay is primarily a long distance offering at present, as regulatory restrictions have prevented local incumbents from offering it. However, since these regulatory restrictions are now being lifted, we expect local carriers will launch IP-enabled frame relay services in 2003 and 2004.

**FRAME RELAY OUTSOURCING/INSOURCING OPTIONS**

Most frame relay customers have chosen the insourcing path and manage their own network because they are so simple to manage. This means that most companies buy their own edge equipment, manage it with in-house staff, and then buy frame relay circuits from a telecommunications carrier. They configure the equipment themselves and might also do some degree of monitoring and/or traffic shaping.

Outsourcing is used for about a third of frame relay ports in the United States. This often entails leasing the equipment from a carrier, with the carrier being responsible for the initial installation and configuration. Most carriers offer three levels of managed services. The basic level usually includes monitoring, proactive notification, reporting, router configuration, and change management. An intermediate level would add network design and audit. An advanced level would entail the carrier running an entire network for the customer.

Companies typically purchase a managed frame relay service when they find the cost too prohibitive to do so internally due to insufficient IT staff. To reduce some of the expense, it is common for companies to manage their own networks at their headquarters and for them to outsource the network management of branch locations or of certain locations that are in a different time zone from headquarters. Managed frame relay is also popular among companies created through mergers or acquisitions, where the network planning to integrate two or more networks can be complicated.

Managed frame relay has grown in popularity in recent years, due to reasons discussed above and because firms face tight capital budgets with which to purchase networking equipment. Leasing equipment through a managed service is a way to conserve capital funds and to stretch the cost of equipment over a number of years.
An IP VPN is a private network constructed over a shared packet network backbone. The network infrastructure may use ATM, frame relay, or native mode IP to transport IP VPN packets. Network IP VPNs utilize technologies to ensure privacy of data. Sites may be connected to IP VPNs through traditional Layer 2 access methods — frame relay, private lines, DSL — or through dial-up connections. This means both large corporate sites and remote users can easily access an IP VPN.

Since IP VPNs burst on the scene in a big way in 1999, they have rapidly grown. IP VPNs are used by 26% of U.S. corporations as their primary WAN platform (refer back to Figure 4), which makes it the second most popular WAN technology after frame relay. IP VPN's popularity is seen across the economy, and the potential customer base is literally every company in the United States.

However, some industries have adopted IP VPNs faster than others. Retail/wholesale trade, healthcare, and manufacturing are the most intense users of IP VPNs to date (refer back to Figure 5). Some of these industries face particular sets of factors that IP VPNs address well. One example is the healthcare field, in which new federal regulations about patient privacy mandate additional security in the WAN, since patient data is increasingly transmitted from clinics to hospitals to doctors' offices.

### NETWORK-BASED IP VPN VERSUS DO-IT-YOURSELF IP VPN

IP VPN functions can be performed either in the carrier network or on the customer premise through a "do-it-yourself" (DIY) approach. With the carrier network-based IP VPN, all IP VPN functionality is performed in the "cloud" (i.e., the carrier's network). The DIY approach is used by companies that implement an IP VPN using their own equipment and that manage it using in-house staff without the aid of a third-party service provider.

The advantages of a carrier network-based IP VPN are:

- No new customer premise equipment (CPE) is required.
- It is relatively easy and painless for the customer to establish it.
- It is very cost effective when compared with managing CPE internally with an already over-extended IT staff.

Customer spending on network IP VPN services is projected to grow from $676 million in 2002 to $935 million in 2007 (see Figure 6). This compares to CPE-based spending of $8.4 billion in 2002 to $12.5 billion in 2007.
Network-based IP VPNs use an IP network and IP connection for transporting corporate data between sites. The most common form of network-based IP VPN uses MPLS, which partitions one company's data traffic from others on the carrier's network.

**NETWORK IP VPN USERS AND APPLICATIONS**

Network-based IP VPNs are ideal for customers who have remote sites, users, and partners they wish to interconnect. Since network VPNs are built on Layer 2 access (see Figure 7), the VPN user would only need to connect to a VPN service provider's network (typically, through a central office) to have VPN access. (Note: VPNs over the Internet are IPSec [a system of Internet protocol security measures that include tunneling, authentication, and data privacy] and not necessarily network based.)

Other factors that make network VPNs ideal include:

- A need to share IP applications among dispersed users
- Too few IT resources in-house
- A need to accommodate telecommuting employees

Because IP VPNs travel well, telecommuters using a DSL connection at home can add the security features of an IP VPN and connect directly to the corporate LAN. Road warriors or traveling employees can use IP VPN software on laptops to cheaply connect to local phone numbers around the world and dial in to the corporate LAN in a secure way. In short, IP VPN is a dynamic technology that allows a company to change corporate sites or change the location of corporate users in a painless way. IP VPNs are an adaptable technology that meets the needs of sites and remote users.

IP VPNs are particularly useful for companies in which data traffic has several destinations. For instance, companies with many different corporate sites, all of which are communicating with each other, are ideal candidates for an IP VPN. The reason is that paths for data traffic can be created from one location to another and torn down again quickly and easily. Each location has its own connection to the carrier's IP
network, and the traffic is routed to the destination corporate site without any special effort on the part of the WAN manager.

**FIGURE 7**

**IP VPN DIAGRAM**

*Source: IDC, 2003*

**NETWORK IP VPN FEATURES**

Business continuity and disaster recovery are built into the IP networking standard. IP was originally designed by the U.S. Department of Defense to allow for communications during a nuclear exchange. Needless to say, IP is resilient. The reason is that no fixed path through the network is predefined. Each IP packet takes the best route through the network available at the time.

The features and characteristics of network-based IP VPNs include the following:

- Dynamic technology moves and changes as sites/users/network configurations change.
- The IP connection exists on the corporate site to allow for Internet access for employees.
- Each corporate site has a single connection to the carrier IP network and authenticates itself to the corporate network, allowing for the secure transmission of data traffic from that site to all others on the IP VPN.
Each remote or traveling employee has access to the corporate LAN via software contained in laptops and other devices, allowing them to securely access LAN data.

MPLS allows for quality of service, meaning that companies can specify applications that are allowed priority access to available bandwidth in the WAN.

IP applications in the LAN remain IP in the WAN with no need for protocol conversion from IP into frames and back again.

**IP VPN SECURITY ISSUES**

IP VPNs by definition add security to an IP connection or transmission. Network IP VPN security is done by partitioning one customer's traffic from that of others to keep them separate across the LAN. Encryption can be layered on top of MPLS partitioning to add an additional layer of security in the network.

Network-based IP VPNs have special security issues because by definition the security functions of the IP VPN are performed once the traffic hits the carrier's network. As a result, the data is secured across the carrier network but is not secure over the local loop between the corporate site and the carrier network access point. However, other Layer 2 technologies have the same issues.

Some security-conscious WAN managers may find any such solution impractical for their needs and require end-to-end security of their data. Others point out that each local loop is dedicated to a single customer, so there is no mingling of data among different customers. Whether a company views the local loop issue as a major problem or not, depends largely on the individual views of the company and its WAN manager.

**IP VPN COSTS**

The cost of implementing an IP VPN and operating it varies by the size of the company, size of its WAN, and its bandwidth requirements at each site. A network-based IP VPN is considerably more cost effective than a solution that requires the deployment of special IP VPN equipment on each corporate site. Network-based IP VPNs do not require a major capital outlay upfront, since the equipment needed is almost always available on all corporate sites, usually a router. The primary cost for a network-based IP VPN service is the IP connection to each site. IP costs have decreased over time, and a T1 port typically runs less than $1,000 depending upon location.

Management and support costs for a network-based IP VPN also benefit from this lack of special equipment at each corporate location. The carrier will manage all the changes, additions, subtractions, and problems for the end user, since the IP VPN equipment and functions are located in the carrier's network. The IP connection and IP VPN management fees for network-based IP VPN run from hundreds to thousands of dollars per site depending upon the bandwidth at each site. Management fees for a T1 are typically equal to or slightly less than the cost of the IP port, which ranges from $800–$1,000 per T1 site. The cost per remote user is based on the amount of time each employee spends online. The cost of these management fees can be compared to the cost of an internal do-it-yourself IP VPN, which should include salary, health, and other benefits paid to those internal employees.

**IP VPN MIGRATION CONSIDERATIONS**

IP VPNs are usually the WAN technology companies migrate to rather than migrate from. Companies seeking to migrate from traditional data solutions like frame relay to
an IP VPN are well served by the network-based IP VPN option. Network-based IP
VPNs are similar to frame relay in that traffic is partitioned in the carrier network as
the security mechanism, a carrier is ultimately responsible for the service’s proper
functioning, and an in-house staff is not needed to run the WAN on a day-to-day
basis.

Hybrid networks – in which both frame relay and network-based IP VPN are used –
are fairly common. Companies may desire to keep their traditional frame relay
network in place but find that certain locations are difficult to reach with frame relay or
expensive to do so. In such cases, the ubiquity of IP networks may fill the gap nicely,
and the corporation can add new sites with an IP VPN.

Another manner in which frame relay and IP VPN are used in tandem is connecting
corporate sites with frame relay and remote users with IP VPNs. IP-enabled frame
relay delivers such functionality well.

**IP VPN OUTSOURCING CONSIDERATIONS**

Network-based IP VPNs are typically an outsourced solution, since IP VPN security
functions are performed in the carrier’s network. Outsourcing the network-based IP
VPN to a carrier has significant bottom-line advantages, since the company does not
need to buy, ship, and install new equipment at its corporate sites or deploy security
software. The operational costs of an outsourced solution vary by company. The
survey data available to IDC shows that there is no consensus among companies as
to which option is the most cost effective — outsourcing or insourcing. The cost of
carrier management may seem high to some companies that view their own
employees as pre-existing costs and are not included in the comparison. The cost of
outsourcing may seem low to companies that look at the costs involved with hiring
personnel to run the WAN, including their salary, benefits, etc.
COMPARISON OF FRAME RELAY AND IP VPN
ADVANTAGES/ DISADVANTAGES

Both frame relay and IP VPN have a set of advantages and disadvantages. These are summarized in Figures 8 and 9, respectively.

FIGURE 8
FRAME RELAY ADVANTAGES/DISADVANTAGES

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality of Service</td>
<td>Remote access</td>
</tr>
<tr>
<td>High-level security</td>
<td>Requires CPE at each site</td>
</tr>
<tr>
<td>Efficient for hub-and-spoke configurations with stable traffic patterns</td>
<td>Expensive and time-consuming to reconfigure</td>
</tr>
<tr>
<td>Ubiquity – ability to interconnect local, national, international networks</td>
<td>Expensive and difficult to manage in fully meshed network configurations</td>
</tr>
<tr>
<td>Mature technology with solid track record and experience</td>
<td>Higher cost relative to IP VPN (at some speeds)</td>
</tr>
<tr>
<td>Experienced personnel plentiful in work force</td>
<td></td>
</tr>
<tr>
<td>Backup and disaster recovery options</td>
<td></td>
</tr>
<tr>
<td>Support of multiple Layer 3 protocols</td>
<td></td>
</tr>
</tbody>
</table>

Source: IDC, 2003
FIGURE 9

NETWORK IP VPN ADVANTAGES/DISADVANTAGES

Advantages

- Scalability and flexibility — sites can be easily added or removed
- Remote access
- Efficient for many-to-many network configurations with varying traffic patterns
- Growing IP standardization — more and more applications are based on IP technology
- Leverages investment in Internet access
- WAN is easily outsourced
- No special CPE is required

Disadvantages

- IP connections have shorter reliability track record.
- IP VPN is new product still experiencing experimental phases.
- There is a perception by some of a connection with the public Internet. However, network-based IP VPNs typically use a private IP network.
- IP VPN security is not passed through to the local link, just as with Layer 2 technologies.

Source: IDC, 2003

ADVANTAGES

The biggest advantage of frame relay is quality of service. Frame relay has a strong reputation for providing excellent quality and reliability of service that can be enforced through measurable SLAs. There are many products on the market that enable customers to do real-time monitoring of network performance and SLA compliance using Web-based interfaces.

Scalability and flexibility are prime advantages of IP VPN. New corporate sites can be added or removed from the IP VPN with relative ease. The other great power of IP VPN is the ability to support remote access. Remote users or telecommuters can access LAN resources in a secure way, unlike with frame relay and other technologies that are designed for corporate sites only. As companies invest in more IP-based IT applications to run their business, it is efficient for the WAN to operate in the same protocol environment. In addition, all meshing is provided in the network without the need to reconfigure CPE as sites or users change.

Finally, another advantage is that since IP VPN is a Layer 3 transport, myriad access types are supported and customers have a wide variety from which to choose. Sites can use high-speed dedicated connections, DSL, or even dial-up connections.

DISADVANTAGES

While frame relay is an excellent choice for interconnecting corporate LANs and other applications, mentioned above, its major weakness is in providing remote access to the LAN for telecommuters and other remote employees.
The same Layer 2, connection-oriented network architecture that makes frame relay extremely secure also makes remote access inconvenient. Remote access to the corporate WAN is a strong suit of IP VPN, and one of the main drivers of IP VPN adoption.

Another weakness of frame relay has been in architecture. Frame relay is traditionally configured in a hub-and-spoke configuration. Customers needing a fully meshed network find that to be prohibitively expensive, although IP-enabled frame relay is addressing that issue.

Finally, frame relay is generally more expensive than IP VPN.

The disadvantages of network-based IP VPNs are:

IP VPNs can only handle IP, which is a Layer 3 protocol, so if transport of Layer 2 protocols is required, they must be encapsulated for transmission.

IP VPNs are untested for mission-critical applications. While frame relay is now relied upon by many businesses for transport of mission-critical data applications, IP VPNs offer a relatively new approach. IP connections were primarily used for Internet access — not typically considered mission critical — and thus IP VPNs are not as hardened a technology for mission-critical applications.

IP VPNs are easier to invade from the Internet. And even though network-based IP VPNs add security by partitioning traffic and keeping it on a private IP network to shield corporate data from these threats, the perception that the Internet is being used does concern some WAN managers. This is obviously not a real concern in the view of IDC, since private IP networks are used and not the public Internet – yet the perception remains in the marketplace.

Long repair cycles (48 hours) can be expected if connecting via a DSL local access loop.

The service is relatively new. Other data services are tried-and-true workhorses of data networking. IP VPNs are the new kid on the block, and WAN managers do not have as much experience with them.

Local loop security is determined by the transport type used for the local loop, which is typically a highly secured frame relay circuit. Network-based IP VPNs do not add special security on the local loop, but none is needed if a secure transport is utilized. In addition, the local loop is dedicated to a single customer so the security threat is less than some may think; breaching the local loop requires accessing the physical layer, which requires more the services of a James Bond than a remote hacker.

CONCLUSION

Frame relay and network IP VPNs are both excellent choices for corporate networking. In this white paper, we have highlighted the strengths and weaknesses of these technologies to help you make an informed decision on which is right for you. Which one you ultimately chose must depend on your applications, the locations you have to connect, your budget, uses planned for your WAN, as well as its stage of development.

Over the next five years, WAN technology choices will abound as data networking needs increase among enterprise organizations. No one solution will be right forever. Frame relay may be the foundation of your network but as your network grows, newer applications may drive you to an IP VPN architecture. The wisest network managers
will most likely integrate new technologies, such as IP VPN, into their networks gradually while benefiting from the reliability of older frame relay networks.

WHAT TO LOOK FOR IN A CARRIER SOLUTION

Frame relay:

- **SLAs.** What does the carrier guarantee? Are the credits proactive, or do I have to document any outages? What monitoring is available? What is the carrier's track record on network uptime, packet loss, and other SLA metrics?

- **Responsiveness to repair.** What are their customer service policies? Is there one number to call for repair? What is the speed to response and repair?

- **Management.** Can the carrier manage my network if needed, particularly branch offices?

- **Migration.** What migration paths are available? Does the carrier offer an IP-enabled frame relay service?

- **Geographic reach.** Does the carrier offer service everywhere I have facilities? And if not, can they service me through partners?

- **Track record.** How large is the carrier's frame relay network, and what is their history of rolling out new features and options as technology matures?

- **Features.** How many features are available? What is the cost to add them? Are they easily added? Is billing accurate?

Network IP VPN:

- **SLAs.** What does the carrier guarantee? Just as with frame relay SLAs above, check on credits and track records to ensure credits are proactive, outages are quickly corrected and documented, and monitoring tools are available.

- **Responsiveness to repair.** What are their customer service policies? Is there one number to call for repair? What is the speed to response and repair?

- **Management.** Does the carrier offer options for management, from fully managed to joint management?

- **Geographic reach.** Can the carrier provide you with access to sites and local IP phone numbers for remote users? If not, you will have 800 number or toll charges.

- **Track record.** Is the carrier brand new to IP VPNs and testing it out with you as a guinea pig, or has it thoroughly tested the service and run one for customers?

- **Types of IP VPN.** What kind of network-based IP VPN does the carrier offer? There are multiple forms, with MPLS being the most popular.

- **Features.** How many features are available? What is the cost to add them? Are they easily added? Is billing accurate?
COPYRIGHT NOTICE

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2003 IDC. Reproduction without written permission is completely forbidden.