A DETAILED ANALYSIS OF FR-VPNs vs. IP-VPNs

VPNs

Frame Relay

A Comparison of IP-VPN and Frame Relay Services

Description

Say "VPN" and most people think Internet technology. Generically defined, a Virtual Private Network (VPN) is a means of transmitting digital information over a shared public network infrastructure in which secure and reliable connectivity, management and addressing is equivalent virtually to that of a private network.

Despite the recent excitement about IP-VPNs, Layer 2 VPNs have been available since the mid to late 1980s as VPDNs. Current managed frame relay services run mission-critical applications and provide secure, stable predictable and highly manageable solutions.

Several market drivers are fueling the euphoria surrounding IP-VPNs. A comparison of IP-VPN and frame relay services in relation to these market drivers may serve to clarify the current situation.

For More Information:

World Wide Web
http://www.frforum.com

E-mail
frf@frforum.com

Phone
510-608-5920

FAX
510-608-5917

Frame Relay Forum
www.frforum.com

Secure Transmissions

Today, one way IP-VPNS are being deployed is through ISPs who are building IP tunnels through their backbones as special, secure paths for customers' traffic. However, users trust frame relay Permanent Virtual Circuits (PVCs) to provide adequate security for most applications without having to create tunnels and use encryption as default. PVCs inherently provide a "tunnel" of sorts in that the network operator (within the company or service provider) establishes the DLCIs associated with a different access device. In addition, packets with corrupted addressing information are systematically discarded.

A VPN service provisioned using PVCs on a frame relay access platform, eliminates the need to acquire special tunneling and performance enhancing options to accompany it. Current frame relay networks support many thousands of concurrent active PVCs with high levels of availability, scaling and forwarding performance, and minimal, predictable delay and jitter.

Cost Savings

The potential savings of IP-VPN technology over other technologies should be examined on the basis of total cost of network ownership. For example, IP-VPNs do not preclude the need for security relationships to be defined and established between each pair of hosts that may need to communicate. This means that network administrators must configure the rules by which individual users communicate with each other, requiring an exponential number of configurations. The savings can quickly evaporate as the cost to hire, train and retain the scarce expertise required for the configuration and administration of complex networks is added to the total cost equation.

On the positive side for frame relay, several factors will continue to drive tariffs down. Potential savings of alternative services and carriers may constitute a strong value proposition for price-sensitive customers willing to give up SLA and security, a consideration that "traditional" carriers will not underestimate.

With the potential threat of new entrants, carriers will have a strong incentive to protect their installed base and resulting revenue. The ISP/carrier consolidation will also push the service providers to rationalize and position their own offerings within their product line so as to minimize cannibalization effects.

Flexibility and Any-to-Any Connectivity

The IP-VPN promise of any-to-any connectivity is an attractive benefit, especially for extranet and remote users. Frame relay Switched Virtual Circuits (SVCs) offer some of the same benefits. SVCs can extend the reach of secure and feature-rich frame relay services to remote users and extranet sites, such as trading partner locations, without using expensive leased lines.

Frame relay SVC services are available in the U.S. and Europe, and CPE supporting frame relay SVCs is on the market today. Particularly in Europe, SVCs provide an alternative to IP-VPNs because some major service providers offer parity pricing for SVC and PVC services (for equivalent aggregate CIRs). Greater proliferation of frame relay SVCs may also be driven in Europe by X.25 conversion. According to Vertical Systems, SVC-based X.25 network services represented a $2.7 billion worldwide market in 1999.

Frame relay SVC users also have the benefit of a secure environment using Closed User Groups (CUG), which is now a standard within the ITU – X.36. CUGs are applicable for national (NCUG) and international (ICUG) networks.

In spite of the benefits, however, frame relay SVC usage is growing slowly. Point-to-point and star topologies are still the primary implementation of PVCs today, as indicated by

a 1999 Distributed Network Associate Survey, in which 79 percent of the respondents stated they were still using the two types of network layouts. One possible reason for slow SVC adoption is that frame relay SVC services have not yet been deployed or priced attractively by all carriers. In the final analysis, the drivers that limit the adoption of SVCs as a replacement for current network topologies are the same market drivers that affect IP-VPN usage.

Mixed Protocol Environments

Not all traffic is IP-based. The Infonetics Research 1998 survey showed that 44 percent of survey respondents required support for their IPX traffic and 20 percent needed SNA/APPN support. A recent Frame Relay Forum survey completed by Distributed Networking also showed that TCP/IP represented only 48.3 percent of the total traffic volume on frame relay networks. Other protocols included IPX, SNA/SDLC and other legacy protocols.

This less than homogeneous environment is also a problem for IPSEC, the Layer 3 tunneling protocol designed to securely tunnel IP traffic only. Multiprotocol support for IPSEC requires a proxy server to do the necessary protocol translation to IP, which represents additional burden of overhead (10 to 30 percent higher than frame relay) and processing. Another approach is to combine IPSEC with L2TP tunneling, or use DataLink Switching (DLSw).

Service Level Guarantees

When network performance problems occur, bottom-line profitability and competitive edge is negatively affected. With the increase of business dependence on networked systems, the cost of degraded application response time (most strategic) and unplanned downtime (most important) escalates.

Performance management and monitoring are an absolute requirement for companies to address different internal needs. Current frame relay performance management tools provide the means to quantify performance on a given link down to the virtual circuit and determine if performance is equal to levels specified in a contract with a service provider, or in agreement between users and IT departments.

Standard (see FRF.13) frame relay Service Level Management "killer-applications" are widely available today. They enable service level verification and management, capacity planning and trending, bandwidth optimization, preemptive warnings of over-subscription, automatic troubleshooting, and more.

On the IP-VPN side, service providers have started to offer Service Level Guarantees (SLGs), but they are limited because there are limited standards for backbone engineering or for network management. Therefore, any SLGs that exist tend to be fairly limited in scope and in their ability to report on the individual customer's network.

In addition, service providers have been cautious in their own rollouts, carefully evaluating the technological and financial risks. Their challenge is to meet a whole set of user needs in a complete and economical manner. A technologically superior approach alone will not suffice.

The dominant design for the infrastructure will be one that offers a superior price-performance combination, and one that enables the delivery of services that will match, at a minimum, the business class, secure, feature-rich, and high-performance solutions frame relay offers today.

Ensuring certain levels of service is tied closely to traffic engineering, capacity planning, equipment interoperability and performance. Service providers face the non-trivial challenge of anticipating the growth and demand in bandwidth, which compounds the difficulty in providing predictable and reliable services. Designing and tuning their networks for optimum performance and operation while minimizing complexity and operating costs is a significant task.

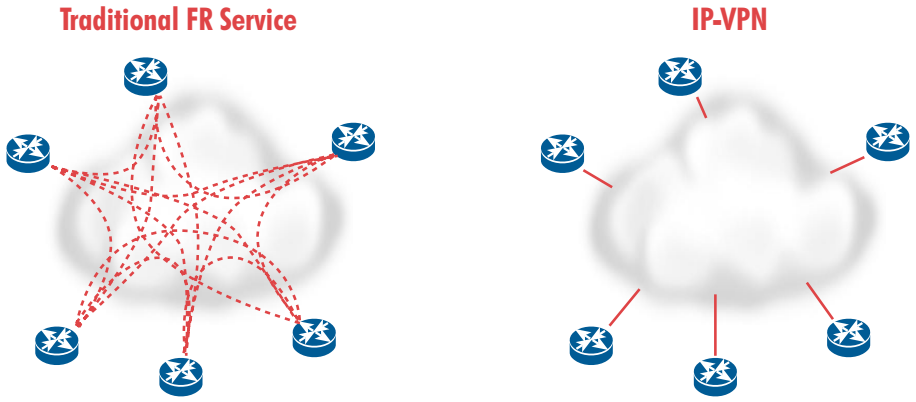
For managed services, providers also need the expertise and resources to determine IP-VPN requirements, manage day-to-day operations, operate helpdesk, manage security (carrier liability, international legislation, key management and web of trust), select, install and test VPN products (interoperability) and monitor and guarantee service levels (transit delays and jitter, throughput) on a per tunnel basis.

The connectionless nature of IP does not allow service providers to determine traffic patterns because packets can take unpredictable paths through the network. This makes capacity planning quasi-impossible until standard traffic-engineering technologies are deployed and quality of service and performance-oriented policies established and mastered in the backbone, which is not likely to happen soon. Technical knowledge (experience curve) among carriers still needs to grow and diffuse, especially when it comes to the complex and diverse IP-VPN-enabling technologies, such as MPLS (RSVP, CR_LDP), ICS, Diffserve, Terabit routers, etc.

Multi-vendor Environments

There is also a need for more integration and consolidation in terms of product lines with multi-vendor interoperability (maturing of embedded technologies). Current IP-VPN CPE possibilities are indeed confusing, and implementers should be cautious about interoperability issues when combining servers, functions-specific hardware, firewall

Traditional FR-VPN vs IP-VPN



- Each router connected to every other router via frame relay PVC
- Bandwidth guaranteed between sites via FR CIR

- Each router connected to carrier's network via a single FR PVC
- Bandwidth guaranteed on access, but not between sites

and router-based equipment. Equipment will need to be upgraded or enhanced (hardware encryption acceleration) to provide wire-speed encryption and tunneling, as the IP-VPN CPE will create network bottlenecks. Scaling is also a major issue facing CPE vendors and indirectly, service providers.

IP Market: Still Maturing

Initially characterized by the lack of standards and proprietary approaches, poor quality, wide variety and specialized distribution channels, the current IP-VPN market seems typical of a new and still maturing industry segment. The maturing of the market is indicated by recent consolidations and partnerships across different industry segments (carriers/ISPs, product/technology integration, etc.).

The lack of customer knowledge and market infrastructure explain current carrier's "minimal and hybrid" IP-VPN offerings, mostly targeted at early adopters. Product bundling (positioned as solutions) and attractive pricing is the main short -term objective for service providers willing to tap into the VPN revenue stream.

Today, IP-VPN providers can claim only broad and unverifiable network backbone availability and uptime numbers. Service providers do not (and cannot) offer any guarantee on service levels on a per tunnel basis, nor can they guarantee data integrity and security. Potential outsourcing allows much less control over network security policies. Even if those guarantees were available, no service level verification tools are available to measure network performance against the service provider's claims.

Short Term Outlook

The main shift in the value matrix will be a movement along the price and later, performance dimensions, which would indicate IP-VPNs can be characterized as a sustaining innovation. Given that assumption, growth rates for VPNs markets could be predicted, together with trajectories of technological progress, with a reasonable level of confidence.

For the short term, however, it is clear that IP-VPN technology and frame relay services will co-exist in both a complementary and a competitive state. Although ISPs do not provide "native" frame relay services, frame relay provides a service platform and backbone for provisioning access to the Internet. ISP switches reached close to $1.9 billion in worldwide cumulative revenue between 1997 and 2001, and is the fastest growing segment (according to Vertical Systems) with a 22 percent CAGR between 1997 and 2001.

Based on a 1999 Infonetics Research survey on VPNs and managed services, it appears that IP-VPNs are being used to address growing bandwidth needs rather than converting existing site-to-site connections. The findings state that only 22 percent of the respondents perceived the ability to replace frame relay as important for site-to-site VPNs. Cost savings of domestic dedicated line charges was rated highly by 46 percent (20 percent for international) of the respondents, and was perceived as a key benefit to site-to-site VPNs.

These numbers seem to indicate that there is limited direct substitution effect, but growing "opportunity cost" to the frame relay service market in that growth in bandwidth and connectivity needs impact the leased line revenue pool, a $23.8 billion market according to a 1998 Vertical Systems report.

Conclusion

It is unlikely that IP VPNs will upstage frame relay VPNs any time soon. After all, frame relay services have now reached the $10 billion revenue mark and there are over one million ports installed (Vertical Systems). And with frame relay used as the underlying technology, IP-VPNs fuel the growth of the frame relay equipment market.

What is more likely is that new applications suited to the characteristics of IP VPNs will use IP rather than frame relay, so this will limit frame relay's growth over time.

Practically speaking, frame relay carriers have a strong incentive to protect their installed base and resulting revenue; to rationalize and position their product line so as to minimize possible cannibalization effects; and to sustain market position.

As proof of this, frame relay service prices have decreased by an average of 10 to 15 percent over the past years. More recently, various service providers have announced services that combined both IP-VPNs and frame relay in effort to harness the different market forces and define the fit of the two technologies. These services allow frame relay customers to enjoy the Layer 2 virtual private network capabilities that frame relay affords. They also extend a customer's reach outside of the closed user group without adding costly dedicated connections to remote users and trading partner locations across the Internet or shared IP networks.

While the excitement about emerging IP-VPN technology will continue, it is clear that frame relay-enabled VPNs will remain important and central elements in the public network infrastructure for the foreseeable future.

Implementation Agreements

FRF.1.2	User-to-Network Implementation Agreement
FRF.2.1	Frame Relay Network-to-Network Interface Implementation Agreement
FRF.3.2	Multiprotocol Encapsulation Implementation Agreement
FRF.4.1	User-to-Network SVC Implementation Agreement
FRF.5	Frame Relay/ATM PVC Network Internetworking Implementation Agreement
FRF.6	Frame Relay Service Customer Network Management Implementation Agreement (MIB)
FRF.7	Frame Relay PVC Multicast Service and Protocol Description Implementation Agreement
FRF.8.1	Frame Relay/ATM PVC Service Interworking Implementation Agreement
FRF.9	Data Compression over Frame Relay Implementation Agreement
FRF.10	Frame Relay Network-to-Network SVC Implementation Agreement
FRF.11	Voice over Frame Relay Implementation Agreement
FRF.12	Frame Relay Fragmentation Implementation Agreement
FRF.13	Service Level Definitions Implementation Agreement
FRF.14	Physical Layer Interface Implementation Agreement
FRF.15	End-to-End Multilink Frame Relay Implementation Agreement
FRF.16	UNI/NNI Multilink Frame Relay Implementation Agreement
FRF.17	Frame Relay Privacy Implementation Agreement
FRF.18	Network-to-Network FR/ATM SVC Service Interworking Implementation Agreement

For More Information:

World Wide Web
http://www.frforum.com

E-mail
frf@frforum.com

Phone
510-608-5920

FAX
510-608-5917

Frame Relay Forum
www.frforum.com