Frame Relay vs. IP VPNs
Table of Contents

Introduction 2

Definition of Terms 2

“Virtual” Privacy and the Value of Shared Networks 3

The Three Definitions or Distinctions of VPN 3

The Case for Frame Relay 4

The Case for IP Virtual Private Networks 6

Conclusion 8
Introduction

Welcome to one in a series of white papers brought to you by Sprint. We believe it is important to inform you on issues in the industry and to keep you updated on our current endeavors.

A major challenge in today’s data transport market is that businesses wanting to implement a Virtual Private Network (VPN) are faced with a dizzying array of options and have few guidelines from which to make an educated decision. The sheer breadth of available VPN offerings can be overwhelming, especially for those unfamiliar with the relative merits and capabilities of all the alternatives.

To answer this challenge, Sprint has developed this series of VPN white papers designed to help customers and prospects navigate the VPN decision-making process. Each paper in the series compares and contrasts different types of VPN solutions and highlights the various communications needs they can — and cannot — address. This white paper not only identifies the communications needs that can be solved by VPNs, but also examines the relative capabilities of frame relay and IP VPNs in delivering solutions.

Sprint has extensive knowledge and experience in this industry category. In fact, Sprint and Cisco are currently working together to develop, market and deliver nationwide IP and broadband solutions. The joint effort combines Cisco Systems’ best-in-class networking technology and equipment with Sprint state-of-the-art network infrastructure and customer service capability. The companies are initially focused on dedicated Internet access, IP VPN, IP Telephony solutions, content delivery networks and metro Ethernet solutions. By joining forces on this project, Sprint and Cisco intend to define and establish IP industry standards.

Definition of Terms

The following definitions will be used in this white paper:

**VPN — Virtual Private Network** is a private communications network that uses a shared network as its Wide Area Network (WAN) backbone, thereby offering the appearance and functionality of a dedicated private network at a reduced price.

**IP VPN** — An IP Security (IPSec)-based VPN that uses encryption and authentication to offer the appearance and functionality of a private data network over a shared IP network such as the Internet. In this paper, IP VPN will be discussed in terms of both Sprint CPE-based IP VPNs and Network-based IP VPNs. It will not be discussed in relation to IP-enabled frame relay or MPLS VPNs.

**QoS — Quality of Service** refers to the consistent performance of a network as supported by the network Service Level Agreements (SLAs).

**CoS — Class of Service** refers to traffic differentiation. CoS provides the ability to treat packets differently based on the packet’s importance.
"Virtual" Privacy and the Value of Shared Networks

It wasn’t long ago that dedicated leased lines were the only viable option for businesses requiring secure data transmission among multiple remote locations. At the time, this solution addressed most organizations’ communications needs; but the associated costs and complexities could be considerable — especially for businesses with geographically dispersed employees or a large number of branch offices.

With the advent of Layer 2 technologies like frame relay, more cost-effective shared networking solutions became available. Such solutions were seen as breakthroughs because they allowed businesses to leverage a service provider’s shared network resources to build “virtually” private networks. These networks could mimic the appearance and functionality of leased line services at a fraction of the cost.

Currently, most companies run at least a portion of their WAN over shared facilities. The key advantage is seen in the potential cost savings. With the rise of Internet and IP usage for business applications, the role of shared networks has accelerated in today’s corporate data networking environment.

The Three Definitions or Distinctions of VPNs

At the most basic level, all VPNs serve the same purpose — they permit organizations to securely share data with key stakeholders. This includes:

- Sharing a particular subset of data with all stakeholders
- Sharing all data with a particular subset of stakeholders
- Sharing a particular subset of data with a particular subset of stakeholders

The following table shows which stakeholder groups are served by each of the three fundamental types of VPNs.

- **Intranet** — employees at fixed locations (HQs, branch offices, small offices/home offices, etc.)
- **Remote Access** — employees “on the go” (telecommuters, mobile users, business travelers, etc.)
- **Extranet** — key business partners (suppliers, distributors, resellers, etc.)
The Case for Frame Relay

Frame relay is a Layer 2 communications protocol that enables the establishment of multiple independent circuits, or data links, over a single physical connection. The protocol accomplishes this by packaging data into variable length frames at their source location, and then merging these frames into a single data stream for transmission over a shared network resource. This merging process, called statistical multiplexing, ensures efficient use of capacity on the shared facilities and minimizes the end-to-end delay of frame delivery.

In a frame relay network, each individual logical connection is called a Permanent Virtual Circuit (PVC). Beyond cost savings, PVCs have two distinct advantages over leased lines:

- PVCs are software defined, so they can be created, altered or dismantled in a matter of hours. This represents a tremendous time savings over leased lines, which require days, weeks or even months to deploy the physical components.

- Every PVC has an associated Committed Information Rate (CIR) that defines the amount of bandwidth a customer is provided on the shared network facility. However, customers have the ability to transmit data on their PVC at rates up to the full port speed. This means customers can “burst” above standard capacity as needed for certain bandwidth-intensive applications. Sprint is one of the service providers that offers 0-CIR PVCs, which provide SLA guarantees on all traffic transmitted.

Frame relay networks are considered private because each customer’s individual traffic is separated into a predetermined path, the PVC. Unintended recipients cannot view traffic that is not deliberately sent to them. In fact, there is no way to misdirect traffic without physical access to network facilities. In order to intercept or corrupt traffic traveling on a frame network, an individual would need to physically tap into the transport medium in question — an intrusion that is easily detected using widely available monitoring tools.

Key Strengths

Ability to support multiple Layer 3 protocols. Frame relay is a Layer 2, or data link, technology, and thus can support any Layer 3 protocol. Businesses running applications based on non-IP protocols, such as IPX, SNA or AppleTalk, should strongly consider implementing — or sticking with — a frame relay network. For companies running purely IP-based applications, this isn’t a key decision factor.

Ability to address Internet security concerns with a single firewall. Many corporate frame relay networks are built in a hub-and-spoke arrangement with a single Internet connection at the hub site. This architecture requires all remote (spoke) offices to access the Internet via the central (hub) site. In this scenario, the company can protect their entire network from unauthorized access via the Internet by using only one firewall located at the hub site. The upside to such a configuration is the need to pay for and manage no more than one firewall, which can be a significant benefit for customers looking to save money and headaches on Internet security. However, businesses whose employees send and receive a considerable
The Case for Frame Relay:

amount of Internet traffic should think twice about this type of configuration. The inefficient use of bandwidth as Internet traffic traverses the frame network to and from the hub site could end up costing more than deploying Internet connections and firewalls at each remote location.

**Ability to provide predictable performance for delay-sensitive traffic.** Since the frames that carry data in frame relay networks are variable in length, network congestion problems can arise when larger data blocks queue up ahead of delay-sensitive traffic, such as voice. To help alleviate this problem, the Frame Relay Forum has ratified procedures to break down larger frames into a series of smaller ones. While such methods are not official CoS protocols, they can provide predictable delay patterns and therefore maintain the integrity of delay-sensitive traffic. Companies concerned about the quality of any delay-sensitive traffic sent over their network may feel more comfortable with a frame relay (as opposed to IP) solution. However, frame relay does not guarantee true traffic prioritization. This is important because frame relay may not offer better performance for delay-sensitive traffic versus IP solutions backed by competitive SLAs.

**Key Limitations**

**High cost and complexity of meshed configurations.** Businesses that want to allow their remote or spoke locations to communicate with each other without connecting through a hub site must have PVCs between each pair of remote sites in question. For businesses with many sites, a large number of PVCs can be required to achieve this type of meshed configuration. Since more PVCs translate to additional cost and complexity, companies interested in enabling direct communications between multiple locations should consider alternatives to frame relay networking.

**Potentially high network delay.** Depending on the topology of a customer's frame relay network, packets traveling over a frame relay network may experience high latency relative to IP networks with any-to-any connectivity. For example, in a hub-and-spoke configuration, traffic must first travel to a hub site before reaching its final destination. This added distance can slow the delivery of data. Once again, customers looking for fast, direct connections among many remote locations may be better served by solutions other than frame relay.

**Limited interoperability.** Frame relay backbones in existence today are managed by different carriers and are restricted in their abilities to interoperate with one another. While providers can interconnect their networks using Network to Network Interfaces (NNIs), PVCs across NNIs are complex and can be difficult to manage. Another complication is that many carriers do not have NNIs with their competitors, which means customers are rarely free to mix frame relay from multiple transport providers. This restriction should be of greatest concern for businesses considering implementing an extranet, since it is highly unlikely that third-party businesses will all have networking solutions from the same provider.
Inability to inherently address remote access. Frame relay cannot inherently support mobile users who need to connect to the corporate network while away from the office. To address the needs of these users, companies with frame networks must deploy a separate remote access infrastructure, such as dial-up services. While this is a viable and acceptable option for many, those companies with an increasingly mobile workforce would benefit from the “built-in” remote access capabilities of an IP VPN.

The Case for IP Virtual Private Networks

Since its inception, the Internet has grown from a private project of the military and academia to a worldwide communications medium that serves up mail, news, entertainment, audio, video and other forms of information to millions of users on a daily basis. The flexibility and ubiquity of the Internet has made it a logical substitute for the private lines or other WAN solutions that many companies use today to connect their remote locations. One obvious drawback, however, is the fact that a network this widely accessible is not inherently secure. So, how can communication across such a network be accomplished without sacrificing privacy?

The answer is to establish an IP VPN using security measures specifically developed for the Internet. IP VPNs use a protocol known as IP Security, or IPSec, to ensure the privacy of data traveling over the public Internet. The Internet Engineering Task Force (IETF) developed this protocol to authenticate and encrypt data within an IP network.

Key terms are defined as follows:

Authentication — This verifies that network users are who they claim to be. It can be achieved using passwords, a shared “key,” that only the proper session participants possess, or digital certificates issued by a trusted third party. Authentication can also verify that data sent between two users has not been altered by a third party along the way.

Encryption — These are coding techniques used to make information sent across a public network unreadable by anyone other than the intended recipient(s). Encryption allows sensitive information to traverse a public network without compromising the confidentiality of the data.

Access Control — This third Internet security measure addresses a problem not fully covered with IPSec. This concept focuses on blocking unwanted users from gaining access to an organization’s or individual’s internal network. Access control is typically achieved through authentication for IPSec traffic, or the use of a firewall for regular Internet traffic. Firewalls can be implemented independent of an IP VPN, but are an important component of a secure Internet networking solution.

Key Strengths

Any-to-any connectivity. When a company connects its sites to the Internet, each site can directly communicate with every other site without the need to specially provision independent connections. Secure IPSEC “tunnels” must be established between sites, but unlike frame relay, no PVCs must be purchased. Although the cost savings over frame PVCs can vary depending on the type of the IP VPN solution, companies looking for maximum flexibility in their network communications should explore the various IP VPN options available today.

Variety and cost-effectiveness of bandwidth option. Internet access is now available at speeds from 56k to OC-12 and beyond, while frame relay is only available at speeds from about 56k to DS3. This may
not be of much concern to businesses sending minimal traffic between their locations, but it’s important to remember that, as bandwidth requirements grow, high-speed IP port charges are more cost-effective than high-speed frame relay port and PVC charges. So, even companies whose current bandwidth needs can be met by frame relay, may find IP VPNs the better long-term solution as their business continues to grow.

**Inherent ability to connect remote users.**
IP VPN remote users can simply dial into their local Internet Service Provider (ISP) or use DSL or cable broadband connections. They then use PC software to establish IPSec tunnels to any of their company’s IP VPN-enabled sites. As a result, no separate dial infrastructure must be deployed or maintained to support remote access capabilities. This can be extremely convenient for companies with mobile employees or even very small branch locations with bandwidth needs that can be addressed by remote access solutions.

**Need for only one connection per site.**
An IP VPN allows a company’s employees to use the same connection for both Internet and WAN connectivity. Combining the two functions in one connection can translate to lower costs since a single high-speed IP port is more cost-effective than multiple lower speed ports. Furthermore, these savings increase with the amount of bandwidth required. This means that businesses looking to either simplify their networking infrastructure or provide their employees’ access to the Internet could realize significant benefits by implementing an IP VPN.

**Greater connectivity options.**
IP VPNs based on equipment deployed at the customer’s premises can run over any carrier’s Internet connectivity. This allows companies to take advantage of cost-effective options like high-speed DSL and Internet access from a wide variety of ISPs when constructing their VPNs. It also means that businesses interested in implementing an extranet do not have to ensure every business partner will access it using the same service provider.

**Key Limitations**

**High base costs for certain types of solutions.** IP VPN customer premises equipment (CPE) is complex because of the need to provide encryption at high speeds and any-to-any IPSec tunneling. With a CPE-based IP VPN solution, customers who do not require high-speed access or meshed network configurations will still pay for these capabilities.

Network-based IP VPNs off-load the complexity to the carrier’s network, thereby decreasing the customer’s base equipment costs to about the same level as a frame relay. However, customers choosing between a CPE-based IP VPN solution and frame relay will usually find frame the more cost-effective for low speed, hub-and-spoke type networks.

**More complex access control options.**
Connecting each company site to the Internet requires that access control to and from the Internet must be addressed at each of those sites. Corporate policy may dictate that all Internet-bound traffic traverse the IP VPN backbone to one or several hub site(s) and exit through a single firewall, as with frame relay. Or, if acceptable, Internet access may be granted at each site. However, this scenario requires that firewalls with appropriate policies be deployed at each connection. Although firewalls built into IP VPN devices can often be utilized, the resulting cost and complexity still increase with such an arrangement.
Conclusion:

“Best-effort” nature of the Internet. Traffic is transmitted across the public Internet at best effort, meaning that IP VPN throughput is not guaranteed in the same way that CIR is provided over a PVC. However, IP networks are rapidly improving in performance. To that point, the Sprint method of creating congestion-free networks is resulting in performance that is at par with most frame relay networks. IP traffic that stays on the Sprint network receives this premium QoS. This high level of performance is provided through Sprint industry-leading SLAs. Nonetheless, some businesses still feel more comfortable with the CIR SLA offered by frame relay PVCs — especially those running a significant amount of mission-critical delay-sensitive traffic.

Conclusion

In order to identify the best communications solution for your company, you must gain a solid understanding of the respective capabilities and advantages of frame relay and IP VPNs. The choice is not always clear, since neither frame nor IP is an inherently “better” WAN solution. Instead, each has its own place in today’s communications networks. Ultimately, those with the greatest knowledge base will be best positioned to realize their organization’s communications goals. This white paper is geared to help you achieve those goals. Please refer to the other white papers in this series for additional information.

About Sprint

Sprint is a global communications company serving more than 26 million business and residential customers in over 70 countries. With approximately 75,000 employees worldwide and more than $26 billion in annual revenues, Sprint is widely recognized for developing, engineering and deploying state-of-the-art network technologies, including the United States’ first nationwide all-digital, fiber-optic network. Sprint award-winning Tier 1 Internet backbone is being extended to key global markets to provide customers with a broad portfolio of scalable IP products. Sprint provides local voice and data services in 18 states and operates the largest 100 percent digital, nationwide PCS wireless network in the United States.

1 The second of the seven layers within the OSI protocol stack.
2 Refer to the upcoming white papers in this series for more information on different types of VPN solutions.