Network-Based vs. CPE-Based IP VPNs
Table of Contents

Introduction 2

Definition of Terms 3

“Virtual” Privacy and the Value of Shared Networks 3

The Three Definitions or Distinctions of VPNs 4

Cost 4

Security 5

Availability of Service 6

Reliability 6

Obsolescence of Equipment 7

How Hybrid Solutions Leverage Advantages of Both Offerings 7

Conclusion 8
**Introduction**

We believe it is important to inform you of issues in the industry and to keep you updated on our current endeavors.

Looking at the business environment today, we recognize many challenges. The rapid growth of the Internet as a key business tool has created demand in IP-enabled applications, especially those maximizing the benefits of scaled, high-speed communications. The evolution of enterprise resource planning tools and remote user access has spurred a concurrent demand for more bandwidth capacity and greater intra-enterprise connectivity. Most important, there is a growing need for more stringent network security. In response, IP Virtual Private Networks (VPNs) have emerged as the pre-eminent Wide Area Network (WAN) technology to meet the new business drivers.

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. Cisco and Sprint 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.

It’s important to note, that two varieties of IP VPN exist: VPNs that require equipment to reside at the customer location, or Customer Premises Equipment (CPE)-based IP VPNs; and VPNs that begin at the edge of the service provider’s network, called Network-based VPNs. Within both CPE and Network-based VPNs, customers may choose from a myriad of options. The task of determining the best match between features, functionalities and business requirements can be very confusing, particularly if you are not familiar with the nuances of the category.

This white paper is designed to help sales representatives navigate through the complex VPN decision-making process. It will describe the differences between CPE-based and Network-based IP VPNs that use the IPSec protocol to secure communications. The areas of concentration include issues of:

- Cost
- Security
- Availability of Service
- Reliability
- Obsolescence of Equipment

We will conclude with a discussion on how Network-based IP VPN and CPE-based IP VPN solutions work together in a hybrid network. This arrangement allows customers to consider either CPE or Network-based IP VPN options for each of their office locations, depending on the mix that best meets their business needs.
Definition of Terms

The following definitions will be used in this white paper:

**VPN** — A Virtual Private 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. We will use IP VPN to refer to both CPE-based IP VPNs and Network-based IP VPNs. The term will not be used to refer to other VPNs, such as frame relay or MPLS VPNs. (Please see the previous white papers in this series for more about those technologies.)

**CPE-Based IP VPN** — An IP VPN that initiates IPSec tunneling and encryption at the edge of the customer’s network for dedicated locations and on the remote user’s PC for remote access users.

**Network-Based IP VPN** — An IP VPN that initiates IPSec tunneling and encryption at the edge of the service provider’s network for dedicated locations and on the remote user’s PC for remote access users.
“Virtual” Privacy and the Value of Shared Networks

Until recently, 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 business 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) and Layer 3 technologies (like IPSec), more cost-effective shared networking solutions became available. Such solutions allowed businesses to leverage a service provider’s shared network resources to build “virtually” private networks. The great advantage was that these networks could mimic the appearance and functionality of leased line services at a fraction of the cost.

Today, most companies run at least a portion of their WAN over shared facilities. The potential cost savings remain compelling. In addition, the rise in IP usage for business applications has further solidified the role of shared networks in the contemporary 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

Below are the three fundamental types of VPNs and the stakeholder groups that can benefit:

- **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.)

**Cost**

Although service attributes (such as value-added offerings and customer support) are very important, pricing still plays a key role in the decision-making process for IP VPNs. For this reason, Sprint suggests that cost-conscious customers consider Network-based IP VPN service over CPE-based IP VPN service. This can lead to lower overhead costs associated with outsourcing equipment and
network management.
Customer premise equipment has evolved into feature-rich and multipurpose devices to better support VPN services. This equipment is placed at every customer location in a CPE-based IP VPN environment and can be added to pre-existing Internet transport. Each piece of equipment requires ongoing maintenance and management, which translates into more headcount and expertise. It’s not unusual for customers to outsource their IP VPN service to Sprint which could reduce added personnel and related costs. Sprint leverages economies of scale in order to minimize customer expenses.

The Sprint Network-based IP VPN service places the VPN functionality in the Sprint network. Many customers and customer locations will use the same equipment resources. Ongoing management and maintenance is then limited to fewer physical pieces of equipment. These efficiencies decrease the per-location total cost of ownership to both the service provider and the customer when compared to a CPE-based IP VPN solution. Sprint Network-based IP VPN will still require some CPE; however, this will consist of a simple router that forwards traffic between the customer’s office and the Sprint network.

**Security**

IP VPNs use IPSec to securely transmit data over public IP networks that make up the Internet. IPSec is a security protocol that uses tunneling, encryption and authentication to ensure data confidentiality, integrity, and authenticity. Access control is another security mechanism that must be employed when a customer’s private network is connected to a public network. Both Sprint CPE-based IP VPN and Network-based IP VPN implementations use IPSec to secure data; the key difference being where the use of IPSec begins and ends.

The Sprint CPE-based IP VPN encrypts/decrypts the traffic at the edge of the customer’s network. As soon as data leaves a customer’s LAN, it is encrypted. This provides a higher level of data confidentiality since data is always encrypted when it is beyond the customer’s direct control.

Sprint Network-based IP VPN encrypts/decrypts the traffic at the edge of the service provider’s network. What this means is that data will be transmitted in the “clear” or unencrypted over the local loop. The local loop resides between a customer’s LAN and the Sprint network. Data confidentiality is provided in this situation by the private nature of local loop facilities which are used by only one customer, like a private line. This is the same level of local loop data confidentiality present in frame relay or ATM networks. For Network-based IP VPNs, once traffic reaches the edge of the Sprint network it is then encrypted and transmitted over the public infrastructure.

Access control is an additional security precaution that should be taken by networks connected to the Internet or any public Layer 3 network. IPSec provides access
Reliability:

control by ensuring that only authenticated users have access to the customer’s network via IPSec tunnels. Additional precautions should be taken if a customer wishes to use the Internet for more than just an IP VPN transport medium. A firewall is a common way of providing this access control. The firewall may be part of the customer’s premise equipment or in a network device.

Availability of Service

Both Sprint CPE-based IP VPN and Network-based IP VPN ultimately send traffic over the Internet or private IP network; however, they have different access options. Sprint CPE-based IP VPN can use any type of dedicated Internet access method, including broadband options like DSL. Even non-Sprint Internet access is supported. This means that CPE-based IP VPN is limited only by the availability of worldwide CPE installation and maintenance support.

Sprint Network-based IP VPN devices reside in the Sprint network and is therefore limited by where Sprint has access to its IP backbone network. That means Sprint provides all the transport that connects the customer’s network to Sprint Network-based IP VPN service. This transport includes options beyond pure IP connections, such as Sprint Frame Relay or ATM PVCs.

With either IP VPN solutions, remote access provides for excellent flexibility for connecting mobile employees. You should note that remote users are not constrained by the need for onsite maintenance support since they are mobile in nature.

Reliability

In order to ensure high reliability, IP VPN solutions support a number of redundancy strategies. Popular methods include redundant local loop access, service provider points of presence (POPs), Internet Service Providers, devices and backup access types such as ISDN. Sprint Network-based IP VPN and CPE-based IP VPN both support reliability mechanisms. However, Sprint CPE-based IP VPN can deliver more options for disaster recovery.

Sprint Network-based IP VPN supports redundant local loops and some backup access. Customers can use multiple local exchange carriers, or LECs, to provide more than one local loop connection, as long as all local loops lead back into the Sprint network. Backup access that establishes a direct private connection between CPE at two customer locations can also be used to re-establish connectivity. Backup access methods that connect to a public network are not desirable since no IPSec would be in place to protect customer data.

While supporting the same redundancy strategies as Sprint Network-based IP VPN, Sprint CPE-based IP VPN offers a few additional options. Backup access that directly connects to a public network is a secure option for Sprint CPE-based IP VPN, since
Hybrid Solutions:

encryption takes place at the edge of the customer's network. Fully redundant Internet access from different Internet Service Providers is also an option, since Sprint CPE-based IP VPN service is independent of Internet transport service. Another advantage is that Sprint CPE-based IP VPN equipment can be duplicated to add an extra layer of reliability to the network.

**Obsolescence of Equipment**

From desktop computers to wireless telephones, technology is always subject to becoming obsolete. As new hardware, software, features and service trends become available, many devices quickly seem outdated. In other cases, the customers' requirements simply outgrow the capacity of the equipment in a short period of time. Considering the issue of obsolescence, Sprint Network-based IP VPN can offer greater protection for businesses than the Sprint CPE-based IP VPN.

Since CPE-based IP VPN equipment will become outdated, as will any piece of hardware, customers may need to purchase new software and equipment. New features may require new additions to existing devices, and sometimes it is necessary to purchase entirely new equipment. Customers can choose to rent equipment in order to offset some purchasing risks of CPE; however, rental fees may still increase if the customer upgrades equipment. Modular CPE, which is composed of generic interchangeable parts, can help protect a customer from having to purchase or rent entirely new equipment, but there are still costs involved. The Sprint Network-based IP VPN equipment will be aggressively maintained and upgraded. Upgrades will be required to only a handful of large modular devices that are shared by many customers. As new features and services become available, they can be easily added to Sprint Network-based IP VPN equipment and seamlessly offered to customers. By placing the IP VPN devices in the network, the capital costs of the IP VPN enabling equipment can be offloaded to Sprint, which can allow you to invest your capital elsewhere.

**How Hybrid Solutions Leverage Advantages of Both Offerings**

Sprint CPE-based and Network-based IP VPNs can be easily combined into one network since both offerings are using the same standards-based technology: IPSec. Customers can leverage the strengths of each solution to their advantage. Moreover, a network built with IPSec provides the ability to migrate individual office locations from one of these IP VPNs to another, without requiring physical changes to the rest of the network.

Sprint Network-based IP VPN can be used for the core sites of the customer's network. These sites generally make up the most expensive CPE costs, so the pricing benefit of Network-based IP VPN has the largest impact. As new services and hardware
advances become available, a customer’s core site can seamlessly incorporate new features with Sprint Network-based IP VPN. Finally, Sprint Network-based IP VPN can receive connections from other networks like frame relay and ATM, so the customer can efficiently merge all these network services if they should choose to do so.

Some customer locations, particularly global locations, may not have access to Network-based IP VPN transport and they have the option to keep pre-existing transport. Other locations may want to use transport from another service provider and that option is also available. Some office locations may require encryption to be used as soon as data leaves their LAN or they may need higher reliability measures — all of which can be accomplished through Sprint CPE-based IP VPN.

**Conclusion**

Both IP VPN solutions can meet most customer requirements, so the decision has to be based on the priorities of the individual business. Customers who need geographically-dispersed and diverse Internet access options, or higher security and reliability measures, can choose to use CPE-based IP VPN. For companies that want to minimize their cost investment in IP VPN services, and want to efficiently scale technology and service enhancements, Network-based IP VPN may be the better solution.

Since business requirements ultimately drive the technology choice, Sprint closely evaluates your needs before recommending the best solution for each individual location and application. In many cases, an entirely CPE-based or Network-based IP VPN is not the best solution for the customer. Sometimes, a hybrid of the two may provide the best of both worlds. Please refer to the other white papers in this series for additional information on VPNs. We also invite you to contact a Sprint representative to discuss your specific business requirements.

**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’s 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.