Virtual Private Networks:

How Can They Help My Business?

1 INTRODUCTION

It seems that everyone these days is talking about VPNs. But what is a VPN and how can it help your business? This paper explores these questions and demonstrates how you can reduce costs and improve business communications both internally and externally using Cabletron's VPN products.

2 WHAT IS A VIRTUAL PRIVATE NETWORK?

A Virtual Private Network (VPN) is a network which uses the Internet or other network service as its Wide Area Network backbone. In a VPN, dial-up connections to remote users, and leased line or Frame Relay connections to remote sites, are replaced by local connections to an Internet service provider (ISP) or other service provider's point of presence (POP). A VPN allows a private intranet to be securely extended across the Internet or other network service, facilitating secure e-commerce and extranet connections with business partners, suppliers and customers. There are three main types of VPN:

- **Intranet VPNs** allow private networks to be securely extended across the Internet or other public network service, and are sometimes referred to as site-to-site or LAN-to-LAN VPNs.
- **Remote Access VPNs**, also referred to as dial VPNs, allow individual dial-up users to connect to a central site across the Internet or other public network service in a secure way.
- **Extranet VPNs**, an extension of Intranet VPNs with the addition of firewalls to protect the internal network, allow secure connections with business partners, suppliers and customers for the purpose of e-commerce.

A Virtual Network

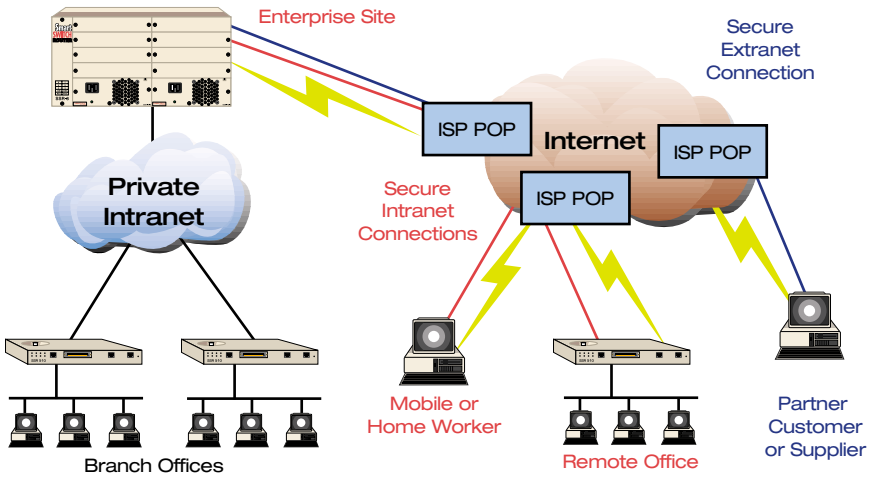

Figure 1: A Virtual Private Network

All of the above types of VPNs aim to provide the reliability, performance, Quality of Service, and security of traditional WAN environments, using lower cost and more flexible service provider connections. VPN technology can also be used within an intranet to provide security or to control access to sensitive information, systems or resources, restricting access to financial systems, or ensuring that sensitive or confidential information is sent securely.

3 THE BENEFITS OF VPNS

VPNs offer considerable cost savings over traditional solutions. Find out how much you could save.

VPNs cost considerably less than traditional leased lines, Frame Relay or other services, because long-distance connections are replaced with local connections to an ISP's POP, or local connections to a service provider or carrier network.

Reduced Costs

VPNs based on IP tunnels, particularly Internet-based VPNs, also allow greater flexibility when deploying mobile computing, telecommuting and branch office networking. Many corporations are experiencing explosive growth in the demand for these services. VPNs provide a secure, low-cost method of linking these sites to the enterprise network. Due to the ubiquitous nature of ISP services, it is possible to link even the most remote of users or branch offices to the network.

Flexibility

VPNs offer network managers a way to reduce the overall operational cost of wide area networking through reduced telecom costs. In the case of a managed VPN service the savings can be even greater, as the ISP or service provider manages the WAN equipment, so that fewer networking experts are needed to manage the security aspects of the VPN. In many cases, implementing a VPN also means that better use is made of existing dedicated Internet connections.

Examples

The following examples, based on real-life costs, show how you can enjoy significant savings by implementing VPN-based solutions. The first example shows the cost of a dial-up VPN service compared to a traditional remote access solution, while the second example

CABLETRON SYSTEMS

shows the cost of an Intranet VPN solution compared to a traditional WAN solution. The final example shows the costs of an international VPN service based on an encrypted 128 Kbps Frame Relay connection compared to a 64 Kbps dedicated leased line.

Example 1—Dial VPN versus Traditional Remote Access

There are two areas where savings can be achieved with a dial VPN solution, as compared to a traditional remote access solution:

- **Telecom costs.** Companies can reduce telecom costs as users start dialing into the network through local calls to ISPs instead of direct long-distance calls to the company. Typically, a company has a dedicated high-speed connection to the Internet and one or more T1/E1 or ISDN PRI connections to support remote dial-up users. Market research of Fortune 1000 companies done by Forrester reveals that more than 70 percent of company sites have more than one high-speed connection. This multiple line approach is common even in small branch offices. A VPN can reduce the number of these lines, since dial-up traffic terminates at the service provider's POP and is delivered via the high-speed Internet link. In many cases, implementing a VPN means that more use is made of an existing dedicated Internet connection.
- **Staffing and equipment costs.** Rather than maintaining a remote access server (RAS), modem banks and ISDN terminal adapter pools for remote access, as well as a router for Internet access, a VPN can combine all of the traffic over the connection used by the router for Internet access. Instead of managing these many devices, network staff now manage a higher-performance router that offers VPN services. In the case of an outsourced VPN service, the router can also be managed by the ISP or carrier, possibly reducing costs even further.

According to Forrester's research, the cost savings of an Internet-based dial VPN solution compared to a traditional RAS approach are staggering, as shown in table 1 below.

However, to assess the cost justification completely, we must also consider the potential costs of making the switch to a VPN. A VPN may not make sense if, for example, nearly all of a company's remote users need only make a local call to access the network. This is especially true in the United States where local calls are free.

In most European countries, however, this is not the case and a remote access solution based on ISDN may actually be cheaper than a dial VPN solution. In many European countries, ISDN tariffs are low and extensive use of time cutting, protocol spoofing and filtering can dramatically reduce ISDN costs.

Moving to a dial VPN solution means that each remote user requires an ISP account, and the POPs must be local to the majority of the users. The cost benefits might not be as compelling if users are switched to an ISP account with a flat monthly rate but then must incur long distance call charges to connect to the ISP's nearest POP.

Example 2—Intranet VPN versus Leased Line and Frame Relay

There are two areas where savings can be made with an Intranet VPN solution compared to a traditional WAN solution:

- **Telecom costs.** Companies can reduce telecom costs by using leased line or Frame Relay connections to local ISPs and relying on the Internet for long-distance connections. Typically, a company implements a private WAN using many long-distance T1/E1 leased line or Frame Relay connections. Studies by Cabletron have found that an Intranet VPN can reduce the cost of leased line or Frame Relay connections considerably.

Average Annual Cost	Dial VPN Costs	Traditional RAS costs
Phone/ISP Charges	$0.54M	$1.08M
User Support	$0.00M (included in user access costs)	$0.30M
Capital Expenses	$0.02M	$0.10M
T1 Lines	$0.03M	$0.02M
Total	$0.59M	$1.50M

(Cost per 1000 users) *Source: Forrester Research, 1998*

Table 1: Remote Access VPN Saving Estimates

- **Staffing and equipment costs.** Rather than maintaining multiple routers at many small branch and SOHO sites, companies can use an outsourced VPN service where the routers are managed by the ISP or carrier to reduce costs even further.

Based on the results of a Cabletron study, table 2 below shows the average annual savings per site on the cost of Intranet VPN access compared to the cost of traditional leased line access for different types of site.

Based on a cost comparison alone, the reasons for moving to an Intranet VPN are compelling. However, a traditional WAN based on leased lines or Frame Relay provides guaranteed levels of service. Replacing a traditional WAN between branch offices and central sites with an Intranet VPN is unlikely to provide the same levels of performance and QoS to users unless the service provider is able to give throughput and latency guarantees as part of a Service Level Agreement.

Example 3—International VPN versus International Connections

The savings are particularly evident in the cost of international connections. A 128 Kbps VPN link between London and Tokyo provided by an international ISP costs around $20,000 per year, while a 64 Kbps leased line provided by a traditional carrier can easily cost around $160,000 per year. Even an international VPN service based on Frame Relay provided by a traditional carrier costs around one third of the cost of the 64 Kbps dedicated leased line.

4 INTERNET VPNS

VPNs based on the Internet are becoming widely available, especially as an alternative for dial-up remote access.

When people talk about VPNs, they generally refer to an Internet-based network as an alternative to a private network based on public network services such as T1 leased lines or Frame Relay. The Internet has become so ubiquitous and ISPs so numerous that it is now possible to obtain connections in all but the most remote locations. Although some countries still restrict access, most countries now have ISPs offering connections to the Internet. It is therefore possible for many organizations, both large and small, to consider the Internet not just for external communication with customers, business partners and suppliers, but for internal communications as well using a VPN. The following diagram shows an Internet-based VPN that uses secure IP tunnels to connect remote clients and devices.

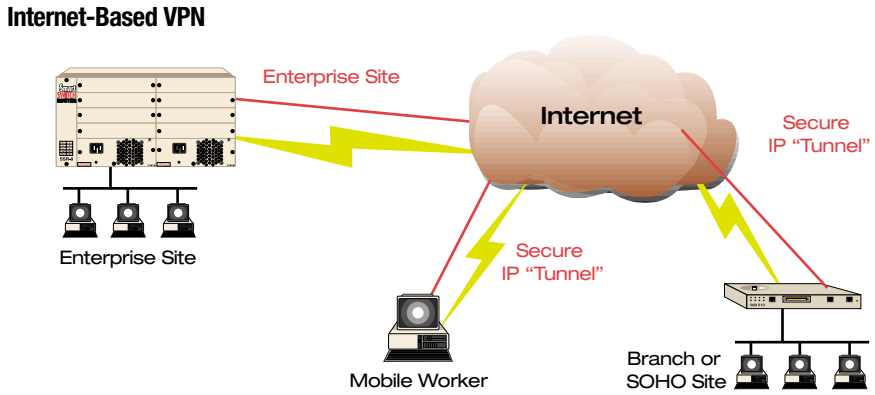

Figure 2: Internet-Based VPN

Internet-based VPNs can be used to outsource remote access with significant cost savings and enhanced flexibility. Modem racks, remote access servers and other equipment necessary to service the needs of remote and mobile users can be replaced with a managed service provided by an ISP.

Average Annual Line Cost per Site	Intranet VPN Annual Cost	Traditional WAN Annual Cost
Central Site	$19,300	$70,300
Regional Site	6,700	30,100
Branch Site	2,600	14,900
SOHO Site	260	1,450
Total	$28,860	$116,750

Note that the costs shown are for bandwidth costs only. *Source: Cabletron 1999*

Table 2: Intranet VPN Saving Estimates

While Internet VPNs are suitable for remote access needs, there are still problems to overcome before moving to a full Intranet VPN solution. Although most VPN products now offer adequate levels of security, the issues of Quality of Service and Service Level Agreements still remain. While most VPN service providers can offer guarantees for connectivity and uptime, few can offer adequate throughput and latency guarantees. In addition, there are few agreements between ISPs, so unless you can use a single ISP's IP backbone for all your connections, you are likely to suffer service degradation where connections cross boundaries between ISPs. Most users will not want to give up the levels of service currently offered by leased lines, Frame Relay or ATM networks for something inferior.

In the long term, however, these problems will be overcome and Internet-based VPNs will become much more widespread for Intranet as well as Remote Access VPNs. In a few years, global VPN services based on the Internet will become as cost-effective and as highly available as global Frame Relay and other public network services.

5 PUBLIC NETWORK VPNS

Public networks such as ISDN, Frame Relay and ATM can carry mixed data types including voice, video and data.

A Public Network VPN can also be used to provide VPN services by using ISDN-B channels, Permanent Virtual Circuits (PVCs) or Switched Virtual Circuits (SVCs) to separate traffic from other users.

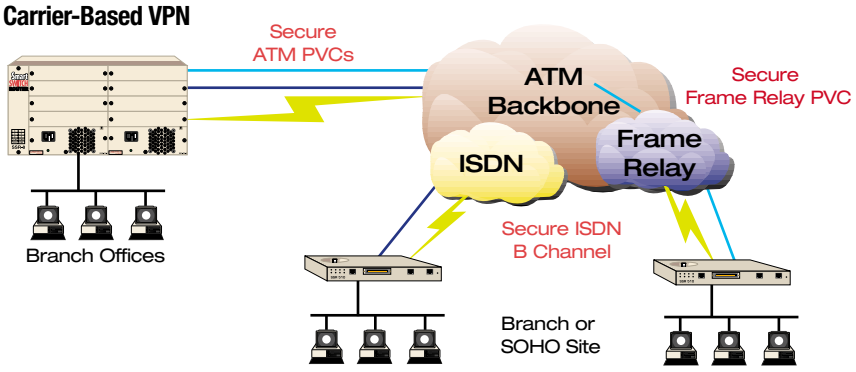

Figure 3: Carrier-Based VPN

Optionally, authentication and encryption can be used where the identity of users and the integrity of data needs to be guaranteed. Using PVCs, SVCs or ISDN-B channels makes it easier to provide additional bandwidth or backup when needed. The traffic shaping capabilities of Frame Relay and ATM can be used to provide different levels of QoS, and because these services are based on usage, there is significant opportunity to reduce telecom costs even further by using bandwidth optimization features. Frame Relay in particular has become a popular, widespread and relatively low-cost networking technology that is also suitable for VPNs. Running VPNs over a Frame Relay network allows expensive dedicated leased lines to be replaced and makes use of Frame Relay's acknowledged strengths, including bandwidth on demand, support for variable data rates to support bursty traffic, and switched as well as permanent virtual circuits for any-to-any connectivity on a per-call basis. The following diagram shows a carrier-based VPN that uses ISDN-B channels and Frame Relay PVCs to connect remote clients and devices.

Frame Relay's built-in buffering and its ability to handle bursty traffic means that it makes optimum use of available bandwidth, something that is important in a VPN environment where latency and performance are concerns. Frame Relay can be used to create a VPN in two ways:

1. **By creating a mesh of Frame Relay connections between sites.** These connections are essentially point-to-point links and are similar in concept to dedicated leased lines. Data is kept separate from other Frame Relay users as each connection uses a separate virtual circuit.
2. **By using IP tunnels over Frame Relay connections between sites.** As above, these connections are essentially point-to-point links similar in concept to dedicated leased lines, and each connection uses a separate virtual circuit. However, several separate IP tunnels can be run over each connection, and each tunnel can be encrypted and authenticated to provide additional security.

Frame Relay is an end-to-end protocol that can be run over a variety of access technologies, such as ISDN, DSL (Digital Subscriber Loop), and even POTS dial-up lines. New access methods such as switched virtual circuits, ISDN access and backup mean that Frame Relay is now a much more reliable and cost-effective solution. Frame Relay can also run over, and interoperate with, ATM backbones, making it one of the most widely available public data networking services worldwide. As a result, major service providers and carriers have created global Frame Relay networks that are cost-effective and offer high availability. When coupled with tunneling, encryption and authentication, these attributes make Frame Relay an ideal candidate for global VPN services. Therefore, a network management system must give managers immediate notice when something goes wrong.

Network managers often carry a pager—and they would rather be paged automatically by the management system than by complaining users. Some systems incorporate applications that will perform this kind of notification automatically, notifying the network manager—by phone, fax or pager, of any network problems. But this only happens when the application and the network management system can be set up to communicate with each other reliably.

6 REMOTE ACCESS VPNS

Remote Access VPNs are rapidly replacing traditional remote access solutions, as they are more flexible and cost less.

Remote Access refers to the ability to connect to a network from a distant location. A remote access client system connects to a network access device, such as a network server or access concentrator. When logged in, the client system becomes a host on the network. Typical remote access clients might be:

- Laptop computers with modems used by mobile workers
- PCs with modems or ISDN connections used at home by telecommuters
- Laptop computers on a shared LAN. For example, some hotel chains are now offering LAN connection points in hotel rooms so that Ethernet cards can be used, with no need for a modem card.

We can divide remote access connections into two groups: local dial and long-distance dial.

For traditional, private, remote access networks, local area users connect using a variety of telecommunication data services. Remote access long-distance users rarely have a choice other than modem access over telephone networks. The aggregation devices that the clients connect to typically use channelized leased line and primary-rate ISDN, offering dedicated, circuit switched access.

With VPNs, local area users typically have a wider range of data services to choose from, regardless of the enterprise or central site VPN equipment. However, long-distance connections are currently via modem access. What VPN carriers currently offer corporations are "Work Globally, Dial Locally" services. The VPN equipment will use high-speed leased lines to the nearest POP of the chosen VPN carrier, and all remote access traffic can be aggregated or routed as IP datagrams over this single link.

Advantages of Remote Access VPNs

- **Cheaper dial-service costs for long-distance users.** When a company partners with a VPN carrier to provide global remote access, the employees are issued information on local telephone number access points in each country supported. Since local calls are significantly cheaper than national and international calls, this would appear to offer a sizable saving. This saving does of course depend on the throughput achieved and the relative cost of local, national and international calls. In most regions of the world, local calls are not free, and this may mean that real savings are not achieved. For example, if local calls offer a 50 percent saving over national calls, but the VPN throughput means that it takes twice as long to copy mail from a central office than it would have done using a direct-dial call, then no telecommunication savings have been made and company time has been wasted. For local users with telephone lines (or ISDN), a VPN offers no immediate dial-in cost savings for the user.
- **Better data rates for modems.** Because long-distance VPN users can dial a local modem at the VPN carrier's office, the data rate achieved by the modem should be better than for a long-distance or international direct call. Again, partnering with a VPN carrier to provide a service is important. For example, international VPN throughput can deteriorate badly when using the Internet as a carrier.

Remote Access VPN versus Traditional RAS

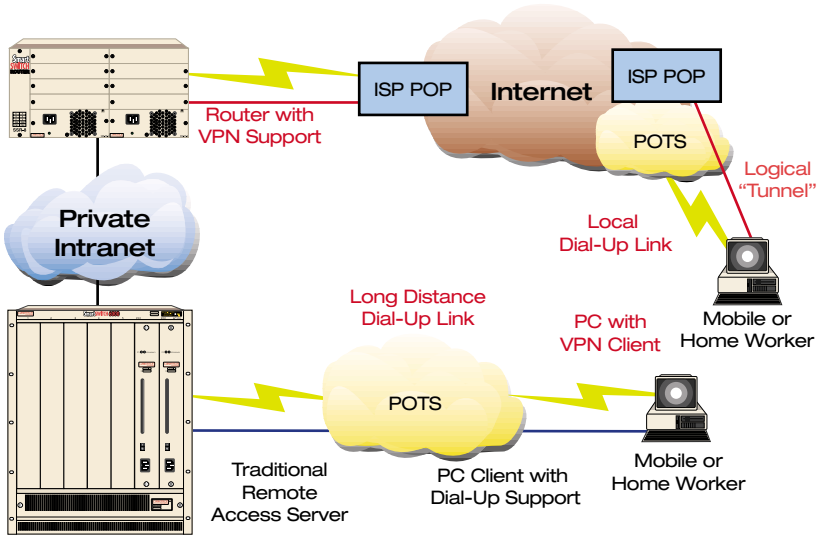

Figure 4: Remote Access VPN

- **Scalability.** Adding 100 users to a modem pool typically presents more problems to the network manager than adding 100 users to an enterprise Security Gateway that only deals with IP datagrams over a high-speed leased line.
- **Less upgrading needed to the equipment at an enterprise or central site.** As modem technology improves and new local loop services become available, new hardware would be required at a "modem pool" site. With VPNs, this problem is handled (and paid for) by the VPN carriers.
- **Improved local access services.** With a traditional direct-dial remote access network, the data services that can be used by the remote users are dictated by the data services supported by the aggregation device. With a VPN, the user can choose the best local loop service available, for example, cable modems or xDSL. This advantage is only a reality for home workers currently, but may eventually apply to mobile users.
- **Better utilization of bandwidth at the enterprise or central site.** With the traditional approach, each user is typically allocated fixed bandwidth, for example, an ISDN B-channel or a 56K channel on a T1 circuit. Most remote working sessions have very low overall utilization of the reserved bandwidth allocated. Also, with a circuit switched approach, there is also a fixed number of users that can be supported before new users are completely blocked. With a VPN approach, it is possible to fully utilize the available bandwidth; as the number of connected users increases, the service to each user gradually decreases but is not completely blocked. Users equipped with high-speed local access services may also more easily take advantage of any spare capacity.
- **Using the link for both company and private business.** If the connection from a small office/home office (SOHO) to a central site uses the Internet as a carrier, it is possible to use the link for company and private business. It is also possible to send external mail using the ISP's mail servers and other features (e.g. fax, voice-mail, DNS, direct browsing) without burdening the company-owned servers. This does have the downside, however, of raising billing and security issues.

7 INTRANET VPNS

Intranet VPNs can be used to provide cost-effective branch office networking and offer significant cost savings over traditional leased-line solutions.

Intranet, or site-to-site, VPNs apply to several categories of sites, from SOHO sites to branch sites to central and enterprise sites. SOHO sites could be considered as remote access users where dial services are used, but as SOHO sites often have more than one PC, they are more accurately referred to as small LAN sites. In an Intranet VPN, expensive long-distance leased lines are replaced with local ISP connection to the Internet, or secure Frame Relay or ATM connections as shown in the following diagram.

Local ISP connections can be provisioned using many technologies, from dial-up POTS and ISDN for small sites, to leased lines or Frame Relay for larger sites. New emerging "last-mile" technologies such as DSL, cable and wireless provide both low-cost and high-speed access. Many ISPs and service providers are now starting to support these emerging technologies for Internet access, particularly for home users and SOHO sites.

The intranet market is one where traditional WAN carriers are likely to compete heavily with ISPs. Traditional WAN carriers can offer a VPN service similar to a Frame Relay service with Quality of Service based on Committed Information Rate. Traditional WAN carriers are well placed to push their advantage in providing secure, reliable, low-latency, intranet links by adopting their current services to support routed VPN links.

Site-to-Site VPN versus Traditional WAN

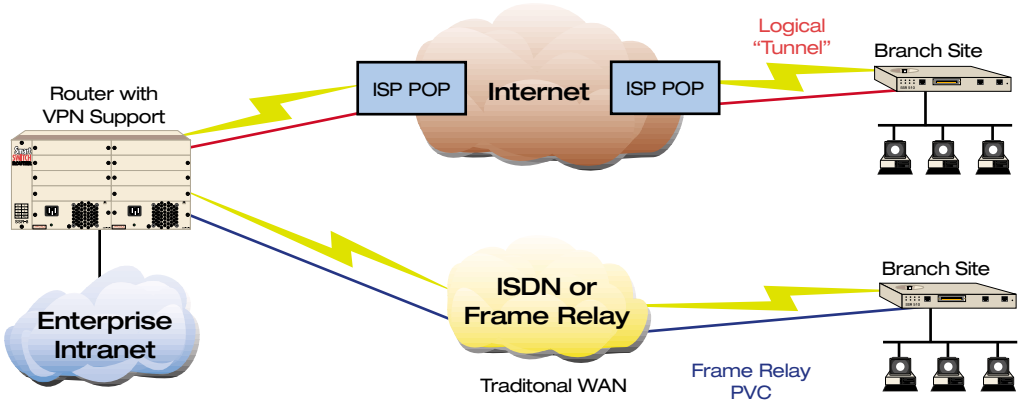

Figure 5: Site-to-Site VPN

Advantages of Intranet VPN Solutions

- **Cheaper line rental.** Typically, VPN carriers provide a leased-line feed by contracting to a traditional carrier company. Since leased lines often have a distance-related cost structure, connecting to a local POP will provide savings compared to a direct long-distance or international link.
- **Scalability**. Unlike leased lines and Frame Relay PVCs, there is no additional cost for new peer-to-peer links. However, in order to offer Frame Relay-style Quality of Service, VPN carriers may need to introduce a per-virtual-link factor to cover costs.
- **Cheaper backup.** If a company sticks with traditional carrier, end-to-end data services for primary intranet links (which is advisable), the VPN carrier service may offer cheap "get what you can, when you can" bandwidth, backup or low-priority data routing. To do this effectively, the tunnels need the support of dynamic tunnel monitoring. If the VPN tunnel is used in partnership with a private data service which had a use-based tariff, for example Frame Relay, then this solution could offer considerable savings.
- **Cheaper high bandwidth over last mile.** Renting high-bandwidth leased lines—for example, T1/E1 or T3/E3—is expensive, and cheaper options exist for last-mile connections in some areas such as cable, xDSL, wireless, and satellite.
- **Cheap global virtual backbone.** For companies that do not already have a national/international backbone, there is no cheaper option than setting up a virtual backbone using VPN carrier services.

8 QUALITY OF SERVICE

What Quality of Service can you expect from your VPN service provider and how can you measure what you are getting?

Most data services, such as Frame Relay, provide guarantees for uptime and availability, as well as throughput and response time. These guarantees, or Quality of Service metrics, are defined in the Service Level Agreement with your service provider.

While most managed VPN services provide a certain level of guaranteed uptime and availability, many do not provide comparable performance and latency guarantees, nor do they offer throughput guarantees. There are several different schemes used to provide Quality of Service, some of which have been developed specifically with a particular technology or protocol in mind, such as Ethernet or ATM. Other schemes are specific to the IP protocol and are being developed by the IETF. Examples of different QoS schemes are:

- **ATM and Frame Relay traffic shaping schemes.** These bandwidth reservation mechanisms are built into the ATM and Frame Relay standards. Examples are ATM ABR and CBR, and Frame Relay CIR.
- **IEEE 802.1p and 802.1q.** IEEE specifications that allow Layer 2 switches to provide traffic prioritization over Ethernet and Token Ring LANs.
- **Differentiated Services (DiffServ).** An IETF standard that defines ways of assigning specific service levels and priorities to IP traffic using the IP TOS field.
- **Multiprotocol Label Switching (MPLS).** A method of encapsulating and tagging IP traffic to improve efficiency and control of routed networks.
- **Resource Reservation Protocol (RSVP).** An IETF standard that defines how routers and other network devices should reserve bandwidth across the network on a hop-by-hop basis.

If you are considering a managed VPN service, you need to pay particular attention to the QoS metrics specified in the SLA from your service provider. If the service provider is unable to provide adequate SLA guarantees, you may need to reconsider how you deploy VPNs in your environment. Some applications, such as dial-up remote access, are very suited to the VPN approach as users are unaccustomed to guaranteed uptime and availability and are less demanding of the service. However, replacing dedicated leased line or Frame Relay connections between branch offices and central sites with an Intranet VPN is unlikely to deliver the same levels of performance and QoS unless the service provider is able to give throughput and latency guarantees.

9 CABLETRON'S SMARTVPN SOLUTIONS

Cabletron's SmartVPN solutions allow small businesses and enterprise customers to cost-effectively connect their own sites (small offices, branch offices, and larger sites) and provide a secure link to business partners across the Internet and other IP-based networks.

Cabletron's SmartVPN products provide high-performance, optimized VPN capability, and offer unique VPN services across the complete set of "last-mile" or access technologies such as T1/E1 leased lines, ISDN, Frame Relay, DSL, and cable.

SmartVPN products are the most cost-effective and secure solution for intranet and extranet connectivity, integrating security services into switch/router products. Customers also

have the flexibility to deploy these solutions behind existing WAN routers or firewalls. Cost is streamlined by providing:

- Flexibility to migrate from private WAN to VPN services according to specific requirements
- Lower equipment costs by integrating VPN gateway and routing capability into a single device
- Lower network management expenses by offering a single set of SPECTRUM management tools to manage both private WAN and VPN environments
- Lower bandwidth costs by allowing customers to select the right combination of private WAN and VPN services
- Greater choice of the appropriate access technology at each site depending on telecommunications tariffs, application requirements and backup requirements

Cabletron's SmartVPN products are implemented via software and hardware upgrades to existing Enterprise WAN products, allowing customers to deploy a VPN with minimal impact to their existing private WAN. Cabletron has also introduced new products—such as the SmartSwitch Router 600—that are designed specifically for the VPN market and allow customers to implement high-performance VPN solutions right away.

SOHO Solutions

Cabletron has a unique set of SOHO products for telecommuters and small branch offices that is designed to provide cost-effective and secure access to the enterprise, leveraging the Internet or other public IP services. These products—the SmartSwitch Router 100 and SmartSwitch Router 200 families—support a range of "last mile" access technologies to Intranet VPN capabilities over ISDN, DSL, broadband cable and wireless.

Branch Office Solutions

Cabletron's branch office solutions are designed to use both traditional WAN and VPN connections. Cabletron's branch site SmartVPN products are specifically designed to use VPN connections for backup of traditional WAN links while offering a cost-effective migration path from your private WAN infrastructure to Intranet VPNs.

The SmartSwitch Router 500 and SmartSwitch Router 600 support a wide range of traditional WAN technologies such as PPP, ISDN BRI, Frame Relay PVCs and SVCs, and X.25, with unique telesaving features that help maximize bandwidth while minimizing costs. In addition, they support the latest VPN standards such as L2TP tunneling, IPSec with DES and 3DES encryption, and Internet Key Exchange (IKE).

Central Site Solutions

Cabletron has a set of central site solutions designed to provide both traditional WAN connections and VPN connections to SOHO and branch sites. The SmartSwitch Router 600 and SmartSwitch Router 710 provide an ideal migration path for customers who have existing private WAN infrastructures but are looking to migrate to Intranet VPNs in order to reduce costs and increase flexibility. Cabletron's central site SmartVPN products are designed to use Intranet VPNs either for primary connections or for backup connections. They include encryption acceleration hardware to ensure that line-speed performance for multiple tunnels can be achieved even under the heaviest encryption load.

SmartVPN Management

Cabletron's multivendor SPECTRUM Enterprise Manager platform will provide five key management services for VPN networks. A consistent, web-based interface will simplify configuration of VPN services across multiple devices, with directory services providing storage of configuration, security and QoS policies on a per-user, application or device basis. Policy-based QoS monitoring will give users a better understanding of VPN performance. SLA monitoring will provide service providers with the information needed to deliver QoS commitments to customers. Traffic accounting of VPN services will enable service providers to generate usage reports and verify delivery of committed service level agreements to their end-user customers.

10 SUMMARY

VPNs are now being embraced as a means of reducing the total cost of providing remote access to the ever-growing number of mobile workers and small branch sites wishing to connect to corporate LANs. VPNs will play an increasing role by allowing extranet connections between organizations and their business partners, suppliers and customers for the purpose of e-commerce. In this environment, throughput, reliability, guaranteed services, traffic monitoring/reporting and accounting are vital.

Cabletron's SmartVPN solutions allow you to build high-performance, Internet-based networks that are flexible, cost effective, easy to manage and aligned with your business. These VPN solutions provide high-performance, optimized intranet or extranet VPN capability over a wide range of access technologies, including traditional T1/E1, Frame Relay and ISDN, as well as new "last-mile" broadband services such as DSL, cable and wireless.

Lit.# 9011637 7/99