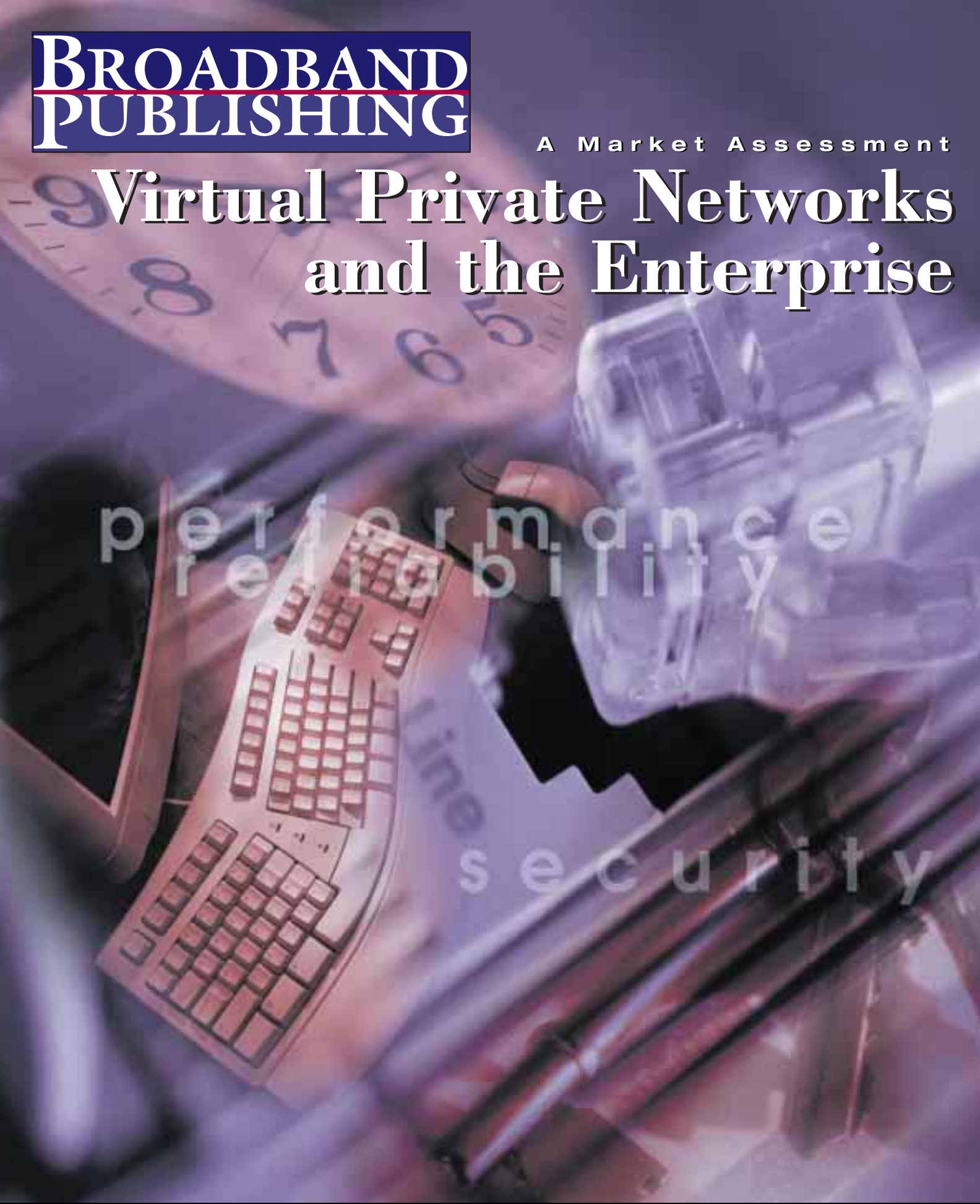
BROADBAND PUBLISHING

A Market Assessment

Virtual Private Networks and the Enterprise



A Special Report

Letter from the Editor

Dear Reader:

Having covered the communications and IT industry for over a decade now, I should be used to the lightning speed with which new technologies are developed and embraced. Yet, I somehow can't help but be awed by how rapidly the Internet – and its IP-based progeny – are transforming the very foundations, not just of the data and telecommunications sector, but of corporate America at large.

One thing is clear, we are witnessing the first stages of a communications revolution, namely the transition from circuit-switched networks designed for voice, to packet-switched networks designed to integrate voice, video and data. While many technologies, ranging from Frame Relay and ATM to Broadband Wireless, will be used to build out this next-generation network infrastructure, it is a single protocol, IP, that will enable the convergence of all higher layer protocols and applications onto a common platform.

Which brings me to the topic of this special report on Virtual Private Networks. Over the past 18 months the IP-based VPN phenomenon has sprung onto the data networking stage with a force that I have not seen since the explosion of the World Wide Web. Clearly, the emerging trends in IP networking are going to have a profound impact on the three main components of our industry – the equipment makers, the carriers, and the enterprise customers.

As a journalist, the VPN story is fascinating, not just because it is news – but because it promises to forever change the way companies share and process information internally and externally. Indeed, VPNs are blurring the lines between inter and intra-corporate communications – linking suppliers, manufacturers and consumers in the process. After much talk in the late '80s about the rise of the virtual enterprise, it is just recently that VPNs have allowed these enterprises to flourish.

In the pages that follow, our editorial team takes a look at the key elements driving demand for VPN services, and analyzes the impact that VPNs are having on enterprise business strategy. We also take a close look at how one company – AT&T – is positioning itself to service and develop this rapidly growing market.

I hope you find reading about VPNs as interesting an experience as we found reporting and writing about them.

Sincerely,

David Hold
Editor-in-Chief

Contents

Publisher: Karen P. Hold, BPC
Executive Editor: David F. Hold, BPC

Editor: Lane F. Cooper, WNB
Reporters: John Harney and Monica Fuertes, WNB
Art and Design: Rick Aleman, Barbieri & Green
Senior Copy Editor: Joan Fitzgerald

This report was written and produced by the Broadband Publishing Corporation and the Washington News Bureau, an independent editorial service based in Washington, DC.

To contact the Publisher, please call 208-725-0600 or send email to karenh@atmreport.com.

Enterprise Virtual Private Networks

Secure, Affordable, Powerful And About To Boom

In an age of global competition, international companies will do business virtually, using secure remotely accessed applications, intranets and extranets. Data VPNs make this possible by combining key networking attributes like security, power, scale and reach. It is the largest international telecom carriers that will provide the worldwide infrastructure, deep resources, expertise, and economies of scale capable of supporting true business-class VPN services.

Since mid-decade, it has become clear that the Internet is going to play a profound role in how companies of all shapes and sizes bring products to market. Indeed, the commercialized Internet has overhauled the entire consumer/vendor relationship of major industries, creating unprecedented opportunities for new entrants as business models are reshaped to accommodate the digital economy.

More recently, leading-edge companies both large and small have begun to harness the power of the Internet, or more precisely the Internet Protocol (IP) that underpins it, to completely redefine the economics of inter- and intra-corporate networking. The flexibility and ubiquity of IP networks is contributing to the proverbial paradigm shift in how companies manage the flow of data—and soon, voice and video—within and between organizations.

As an alternative to building closed networks based on proprietary specifications, IP is evolving into a robust multimedia networking technology that can be used for a variety of applications and situations. Moreover, the rapid pace of change associated with IP applications and specifications is creating a consensus among strategic planners: companies may be better off leasing IP-based services rather than owning them outright. As a result, we are seeing the birth and rapid rise of the Virtual Private Network.

> ***We believe that the VPN opportunity is the largest single opportunity for public data services.***
>
> —Tom Nolle, CIMI Corporation

VPNs Defined

Like any hot buzzword or technology, defining precisely what VPNs are can be tricky. Its definition is subject to change, and even controversy. Just in the past two years, the highly successful voice VPN services have receded into the background as data VPNs rose in popularity.

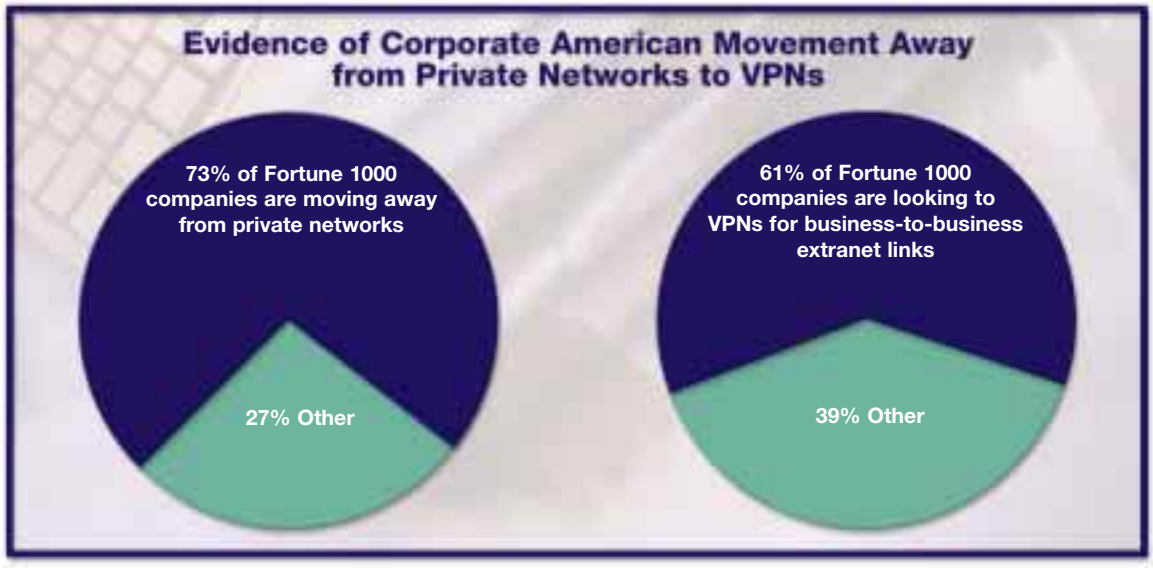
The Internet Engineering Task Force (IETF) defines VPN as: “the emulation of a private wide area network (WAN)...using IP facilities, including the public Internet or private IP backbones.”

The first wave of these were based on Layer 2 services such as Frame Relay and ATM. Here, companies typically attached routers, firewalls and other CPE types to the physical and logical pipes provided by carriers and service providers.

The latest wave of VPNs, based on the Layer-3 IP protocol, are generally independent of the underlying communications technology. These IP networks can include a mix of dial-up and dedicated circuits, which facilitate any-to-any connectivity. This flexibility provides road warriors and tele-commuters alike with remote access to the same resources enjoyed by workers at the corporate headquarters.

But at the core, VPNs are data networks that leverage the public telecommunications infrastructure, using elaborate security measures and so-called tunneling technology (see sidebar p.4) to ensure the privacy and safe passage of the transmission over a shared public network. Security mechanisms such as encryption, authentication and authorization are thus critical to the successful deployment of a corporate VPN. But the

Enterprise Virtual Private Networks



Source: Forrester Research

primary value-proposition of VPNs is that they can deliver the functionality, performance, and reliability of de-dicated networks at a fraction of the cost.

The Business Benefits

VPNs thus allow businesses to leverage IP networks as a low-cost global communications infrastructure. This is a promise that is as meaningful for large multinational corporations competing for new business in the international economy, as it is for small start-ups eager to capture their own share of the global market.

VPNs promise to drive time and distance out of companies' business cycles. Using a VPN to support an intranet, for example, a global sales force can:

- access changing price quotes, submit orders, and post monthly sales via the public Internet;
- process this data much faster than using phones or traditional messaging methods; and
- accomplish this more cost-effectively than companies who have built their own dedicated networks to interconnect branches and trading partners.

It now can take the same time, effort and cost for an office in Japan to do business with the headquarters in New York, as it does for workers in nearby New Jersey.

Outsourcing vs. Owning

Central to the VPN concept is outsourcing. This represents a fundamental shift in how corporations of all sizes view their IT investments. After years of being told that the Information Age will make information and communications management a core corporate activity for all companies in all industries, executives are hearing a new tune from management consultants: outsource as much IT processing as possible and concentrate on the core business.

Corporate America appears to be listening, as researchers at International Data Corporation predict that demand for outsourced network management services will rise from $2.4 billion in 1998 to approximately $4.7 billion in 2002. (See chart, p.5)

This market, says Richard Brewer, senior analyst with IDC's Network Support and Integration Services, will be highly competitive as a variety of service providers scramble to meet demand.

Competitors today are entering this market segment from the regional and long-distance telephony spaces, as well as the WAN equipment manufacturing and integration sectors. Vendors of all sizes and backgrounds are currently positioning for this market, but their offerings can vary widely due to factors such as geographic reach, market experience and access to R&D resources, he says.

With both supply and demand for outsourcing apparently secured, VPNs are poised to experience exponential growth. ❑

Secure Tunneling:

Tunneling refers primarily to mechanisms that separate the contents of a packet and its header from the addressing used to route the packet across an IP network. The IP tunnel acts as an overlay across the IP network. One tunneling method is to encapsulate a data packet within an IP packet for forwarding. This allows the encapsulated packet, including its header, to be encrypted for security. Since the encapsulated packet need not be IP, tunneling thus supports multi-protocol traffic, albeit at the cost of additional overhead. A flow of proposals, including IPSec (IP Security Protocol) and the Point-to-Point Tunneling Protocol (PPTP), which defines how encryption and authentication technology can be used, are being evaluated by the Internet Engineering Task Force (IETF), which develops Internet standards.

Frame Relay—ATM—IP

Some people believe that Frame Relay and ATM are incompatible with IP, and that one can only gain at the expense of the other.

"Nonsense," says Joe Lueckenhoff, Vice President, AT&T Data Networking, explaining that IP can run over dedicated, dial-up or Frame/ATM services, and that many organizations are building hybrid networks consisting of mixed services and access methods.

"IP VPNs are a means to extend the reach and scalability of legacy Frame and ATM networks, not a replacement for these services," he adds.

Jim Daugherty, General Manager of Data Services Marketing at AT&T, agrees, noting that the service interoperability that allows dial-IP connections to terminate on Frame Relay, also supports access to the Internet over virtual circuits.

All three services will thrive, these executives believe. Frame Relay offers a highly reliable and efficient alternative to leased lines for data transport, while ATM is best for higher-bandwidth and real-time applications requiring quality of service. IP is best for maximum, any-to-any connectivity and scalability.

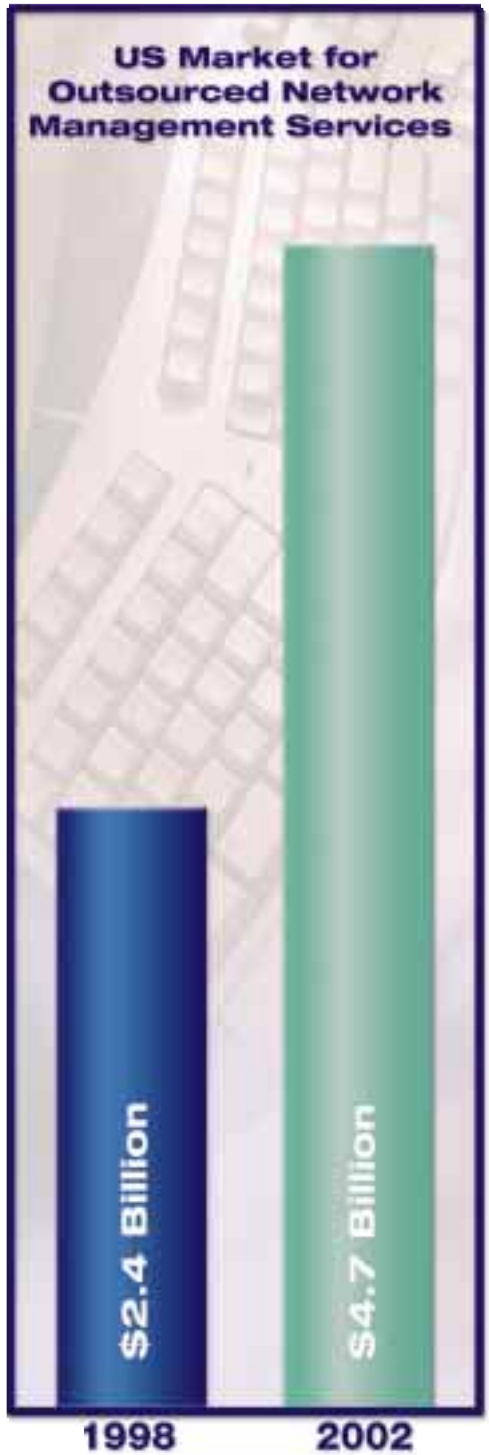
Growing The Whole Pie

Frame Relay, ATM and IP services are all high growth services with IP expected to explode over the next few years. Frame Relay is still growing at double digits, while ATM service revenue is expanding at near triple digit rates. And IP services, although in their early days, are expected to surpass all others in long-term growth.

IP services, although in their early days, are expected to surpass all others in long-term growth.

Switching Labels

"The next major technological advance," Daugherty says, "is Multi-Protocol Label Switching (MPLS), currently an IETF draft specification slated for completion early in 1999." MPLS offers the prospect of more closely integrating Frame Relay and ATM (Layer-2) with IP (Layer-3) services. By adding virtual circuit-like paths for IP flows, MPLS will enable Business Class IP services and advanced traffic engineering. ❑



Source: International Data Corporation

Choosing a VPN Service Provider

With the boom in VPN services, users will benefit from a service-oriented networking environment. The elite VPN providers of the next century will differentiate themselves by excelling in several or all of the key value-added capabilities: reliability, capacity and scalability, reach, and interoperability. Ultimately, fully managed VPN services will become the new status quo.

Reliability

The emergence of IP as the convergence protocol that integrates all corporate traffic–voice, data and video, including multi-protocol traffic, raises significant reliability issues.

IP VPNs now interface with more communications and computing elements than ever before. IP traverses and integrates remote dial, LANs and WANs, desktops and MIS applications, intranets and extranets, web sites and application hosting environments. To guarantee bulletproof reliability, carriers will have to make these various elements interoperate smoothly while maintaining each element's integrity and independence. Corporate customers must be assured that while all segments of the VPN infrastructure plug and play, if one segment crashes the rest will not.

There are significant advantages in outsourcing this responsibility to a carrier with proven network and network management expertise. If the service provider can operate a network that meets, and preferably exceeds, their Service Level Agreements (SLAs), customers will receive near 100% reliability.

No network is immune to failure, since nature always sides with the hidden flaw, thus businesses should have a backup plan that incorporates several layers of redundancy and resiliency. Examples include redundant physical access facilities at important sites, and diverse routing plans to make sure that all traffic is not subject to a single point of failure anywhere in the network. A full-service carrier will have the resources to prepare and implement contingency plans in the unlikely event disaster strikes.

Capacity and Scalability

When a VPN goes global, it creates new capacity and scalability concerns. In general, network activity increases exponentially with the number of end-users connected. At the same time, overseas networks tend to be more bandwidth limited than domestic nets (the future looks better; international bandwidth, especially to and within Europe, is on the rise). So instead of creating more space for network traffic, it's not uncommon for global networks to attract more traffic to fill capacity.

Global traffic volume also tends to surge at different times in different places. When a multinational's European work force heads home, its American employees are ramping up their morning networking activity; when American traffic tails off, Pac Rim traffic picks up, and so on. Global carriers must employ techniques to adapt to these traffic patterns. Caching and mirroring are good examples of techniques that reduce the time an employee waits to retrieve a Web page.

Reach

An international carrier can provide multinationals with global reach and—as importantly—variable global reach. Most multinationals need dedicated high bandwidth connectivity between heavy traffic locations, often around major cities or manufacturing sites in different countries. A subset may also

Choosing a VPN Service Provider

require dial-up IP connectivity throughout individual countries. Global carriers should provide both kinds of reach, either through direct ownership of international facilities, joint-ventures with overseas carriers, or partnership relationships with in-country service providers.

Since the Internet is global and growing rapidly, it can provide the widest geographic reach for non-mission critical applications. Lacking inherent high bandwidth capabilities, though, it can't adequately service locations with high bandwidth needs. These will typically require dedicated facilities, such as IP over Frame Relay or ATM.

Interoperability

Network-to-network interoperability happens when Frame Relay, ATM and IP networks are interworked to accommodate multi-protocol traffic from all the component networks. A high-level of interoperability is a prerequisite for network-to-application and application-to-application communication.

Network-to-application interoperability, like automated customer service, lets customers access a host company's intranet application via the Net to electronically service themselves in real-time. The company gains an automated response and ordering system to relieve the workload in its manned customer service call center, which reduces order processing costs while actually improving service quality.

Application hosting is an important subset of VPN network-to-application activities. Marty Gruhn, Vice President of Summit Strategies Internet Business Solutions, defines this as the ability to rent applications off the Internet. This will allow small to medium-sized companies to lease their ERP (Enterprise Resource Planning) systems, allowing smaller companies to compete up-market by accessing expensive enterprise functionality like accounting, human resource and engineering applications without making the huge up-front investment that only the Fortune 1000 companies can afford.

Service providers will differentiate themselves by providing local access facilities in addition to long distance network services.

Gruhn says application hosting will drive VPN deployment because no organization will port mission-critical applications with vital company data over the unsecured Internet. This trend will accelerate the outsourcing of both applications and VPNs. It doesn't pay an ERP application hosting specialist to stray from core competencies by trying to become a networking specialist. So while customers outsource applications, the specialist will outsource VPN services to a proven network services provider.

Meanwhile, application-to-application interoperability lets members of an automated supply chain exchange data via an extranet between different legacy applications and message queuing software. Thus, a supplier's Windows NT-based inventory control application can be linked by Microsoft Exchange to the host company's UNIX-based manufacturing applications. At the same time GroupWise applications can communicate with mainframe-based accounting applications in a Notes environment.

Carriers and systems integrators will increasingly be asked to interwork these disparate environments, integrate the diverse applications and manage the complexity of the resulting heterogeneous environment to provide an end-to-end solution.

Managed Services

The future of VPNs will be predominantly shaped by incremental improvements in managed services. As the line of demarcation moves further into the enterprise, fully managed services will include installing, managing, maintaining and upgrading the CPE. Service providers will also differentiate themselves by providing local access facilities in addition to long-distance network services.

Future Trends

In the early phases of VPN market development, providers will wage technology battles. Once the functionality issues are settled, service providers will refine their service strategies to offer customers better solutions to business—not technology—problems.

But VPN technology development cycles will not slow down while carriers and customers refine their terms. Most businesses won't be able to keep up with the pace of technology change and the attendant equipment, technical support and training costs. Focusing on their core businesses, they will increasingly seek VPN solutions from full-service providers. ❑

1 800 FLOWERS
The Sweet Smell of Virtual Success

The world's largest florist needed a better VPN. They turned to AT&T VPN Service. Now business is virtually blooming.

When you're the largest retail/wholesale florist in the world, your profits are keyed to volume sales, managing slim margins, and bringing to bear economies of scale. So the Virtual Private Network that 1 800 FLOWERS depends on for order submission, fulfillment and distribution must be bulletproof. Outages can easily translate to huge losses of orders worldwide. Most of the floral industry found this out first-hand on Mother's Day, 1996. That's when the Mercury Net went down. For 12 hours. On one of the biggest business days of the year.

Back then, Mercury Net was the industry's de facto WAN backbone for doing virtual business in the flower business. It was a shared network that connected florists throughout the network, but it was owned and operated by one of the biggest players in the industry, and it used a dedicated network that was simply not fault-tolerant or redundant enough. If it could crash on Mother's Day, what could be expected on any given Valentine's Day?

Executives at 1 800 FLOWERS knew they had to face facts and develop an alternative strategy, or watch business wither on a million stems due to the vagaries of an undependable network.

But that was then.

Over the past two years the company has built its own extranet to do business with florists throughout the country. Dubbed BloomLink, the network supports flower order, fulfillment and distribution functions using AT&T Business Dial Service.

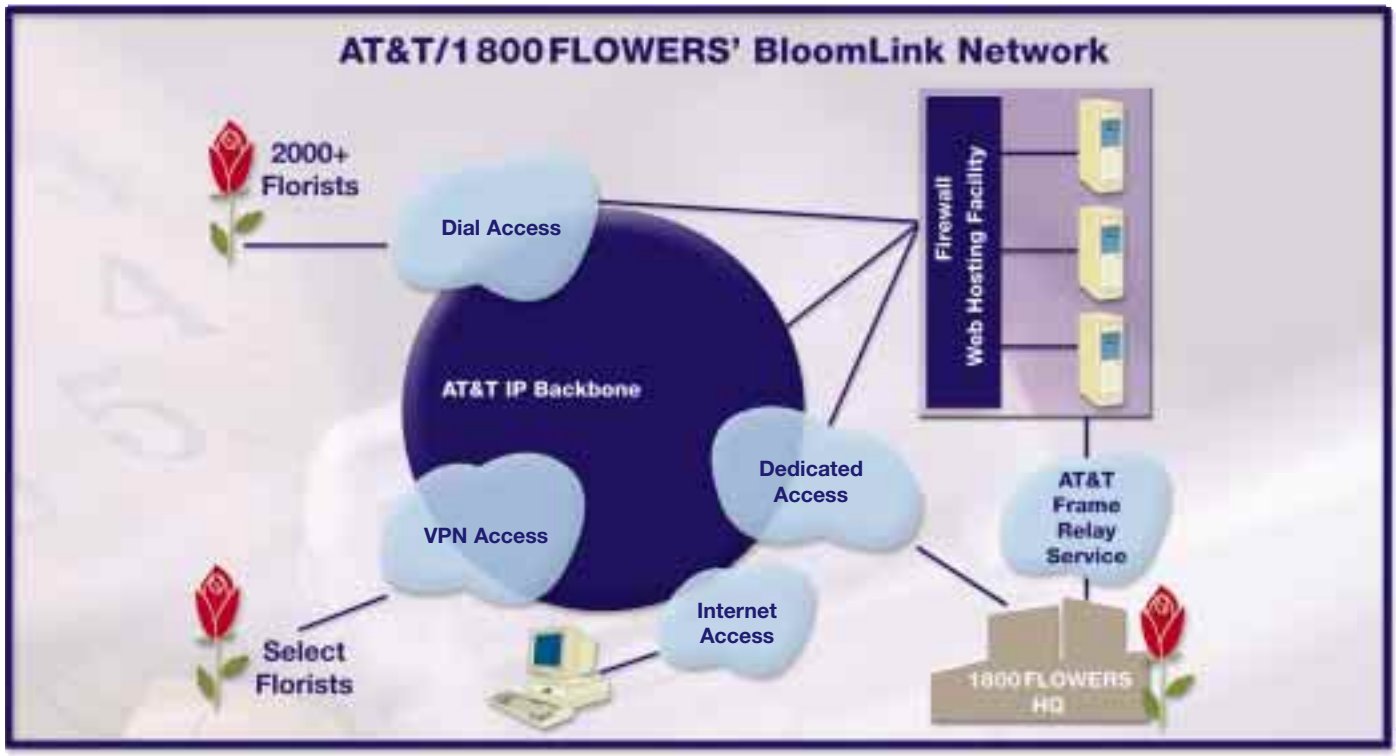
How It Works

Orders arrive at the company in a variety of different formats depending on whether consumers log in to the www.1800flowers.com website, or call in through the 1 800 call center. All of the order entry systems are integrated to support end-to-end consumer electronic commerce transactions. Customers can submit orders via the Internet to the 1 800 FLOWERS web-site, whereupon back-office applications transfer the data to BloomLink via a T-1 Frame Relay connection provided by AT&T.

Given the high volume of business that depends on this web site, the company has instituted several back up options to ensure that continuous operation is not disrupted by network failures. In the event that the main link goes down, there is instant fail-over to open-net Internet access. As a further insurance, the site has dial-access capability to bring the service back on-line, and a second Frame Relay connection is also planned. The next step will be to migrate to AT&T VPN Service, which will insulate the on-line business from the vagaries of the public Internet with specific performance guarantees that never waver.

Integrating Networks With Applications

Orders that are called in via the call center are manually entered. At that



1 800 FLOWERS

point 1 800 FLOWERS can either directly fulfill orders through their own facilities or distribute the requests to independent local florists who have elected to participate in the BloomLink network.

Though receiving, fulfilling and distributing orders between florists is BloomLink's core application, it is comprised of multiple components. Back-office applications enable order entry, while a business-to-business application controls order distribution, and a retail shopping application lets florists provision their stores.

You'd think a network integration project of this magnitude would be enormously time consuming and fraught with management headaches. Not so. 1 800 FLOWERS brought in Norman Dee, Director of Network Services, who developed and deployed BloomLink "from concept to market in seven months." And today, the majority of the company's business comes in via BloomLink.

Cost-Free Center

What's more, the new network service transformed the company WAN from a cost center to a cost-free center. BloomLink has become a strategic company asset that enables 1 800 FLOWERS to conduct business virtually.

The network now processes more orders at a cheaper rate per order. Dee says that florists are incented to use BloomLink because "they can send and receive orders at less than half the cost." Based on this level of confidence, company managers project the number of florists using their service to encompass all their partner florists this holiday season.

However, order processing, though the backbone of BloomLink, is only part of the story. 1 800 FLOWERS' goal is to build an online community of florists who participate in chats, online wholesale ordering, and other web-based commerce. ❑

NovaCare Inc.
Transitioning to Prospective Payment with a VPN

Many industries have had to deal with rapid changes in their business environment. However, few have experienced as far-reaching and dramatic a paradigm shift as the healthcare industry. To accommodate new federal mandates to maintain – if not elevate – the level of care while simultaneously reducing costs, NovaCare, a rehabilitation provider, turned to VPNs to lend a healing hand.

For thirteen years King of Prussia, PA-based NovaCare Inc., has provided occupational, physical and speech therapy through its Contract Rehabilitation Division. Today, one in every five patients in long-term care facilities receive care from a NovaCare therapist in some 2,000 nursing homes and assisted living facilities in 45 states. Everyday, 40,000 patients are served by NovaCare healthcare professionals.

"We manage the rehabilitation therapy practice for nursing homes around the country. We provide therapists and systems to those facilities and manage the therapy that is provided to the geriatric patients," says Steve Wise, NovaCare's CIO.

"It became clear that we needed a system that could track the therapy provided, manage the clinical practice, handle the reimbursement of those services from Medicare to our nursing home clients and support the necessary reporting activities," he says. Beyond this, he adds, NovaCare needed an accurate and timely way to bill its customers—the nursing homes – for the therapy that was being performed on a contract basis. Thus, in 1994, NovaCare's IT staff deployed a client-server system to support the daily activities of their distributed practice, making use of dial-up technology and a centralized data center located at its headquarters.

Dubbed NovaNet PLUS, the system was deployed in the following manner: Each facility in which NovaCare had a practice was equipped with a PC dedicated to the therapists' needs. At the facility, the therapist entered information on a daily basis about the clinical practice.

Every night the PC would spend about two to three minutes dialing into the data center in King of Prussia using analog modems over regular long-distance toll lines to upload the therapist's reports, and then download information that is relevant to the practice or facility.

It became clear that we needed a system that could track the therapy provided, manage the clinical practice, handle the reimbursement of those services from Medicare to our nursing home clients and support the necessary reporting activities.

NovaCare Inc.

"During the communication session all clinical records were sent to the central database and all electronic mail, data on new employees and new contract information for the facility was communicated in a two-way session," says Wise.

Once a week headquarters produced management reports for NovaCare field managers providing a clinical and business perspective on how the operation was running. And on a monthly basis, information was collected to bill the nursing homes for services rendered.

"The system gathered critical clinical information to produce reports on how our practice was performing. These outcome reports, as they are called, provided extremely useful information for our patients, customers and our clinical group. These reports showed our patients the meaningful progress they were making, helped our customers market their facility in the community and deal with their existing payers and helped NovaCare show prospective customers how well our clinical programs perform," says Wise.

New Politics and Economics of Healthcare

For nearly four years everything worked smoothly. Then in 1998, Congress and the Clinton Administration passed a balanced budget for Fiscal Year 1998.

"In so doing, the federal government changed the reimbursement model for nursing homes. They moved from a fee for service model – which our system was designed to track – to a Prospective Patient System (PPS) model – in which a fixed cost is allocated to patient care based on his or her level of need," explains Wise.

While the existing system had served NovaCare well, the fact that all of the metrics were about to change elevated the importance of tracking and managing more information on the clinical steps taken to improve the health of patients.

"We decided that having a system deployed in 1,000 facilities over which we had limited control created a very cumbersome environment—in terms of management and maintenance. Every time we needed to do a software upgrade we had to send out software packages to every PC on the system and hope that they were properly installed by therapists who had little or no background in information systems. We had no IT support to offer them," says Wise.

NovaCare's IT team decided that it was time to move to a distributed computing model based on intranet access.

"If we could have the applications reside on a centralized server that could be accessed by therapists who dialed in, then we could not only maintain a real-time data base, but we could simplify application management and support," he says.

Wise did have concerns about security. If people were going to sign on to an application through an intranet—often dialing through the internet itself—NovaCare needed to make sure that measures were in place to ensure patient confidentiality. "We needed a service that would ensure that we were secure from an applications standpoint, and that we did not open up the patient records to the entire Internet community," says Wise.

After a lengthy analysis he concluded that there were two choices: NovaCare could develop its own private data network; or it could look into using a VPN.

Enter the VPN Solution

When all was said and done the company decided to go with AT&T Virtual Private Network Service.

"From a security standpoint I was satisfied that you would have to be properly configured and have the proper sign-on authorization to reach this application in this VPN environment. AT&T demonstrated that the data could not be seen by the general Internet community."

Wise was particularly impressed with AT&T's Closed User Group function—which only allows access to certain TCP/IP addresses that have properly gone through specific sign-on procedures.

"It ensures security by locking the system out of normal Internet traffic and gives us the control that we would get if it were a private network."

Once that was demonstrated, AT&T showed that the VPN could meet NovaCare's dial-up performance requirements—which right now must support 28.8 to 56 Kbps access.

Wise is taking AT&T up on an end-to-end service availability guarantee. If NovaCare reports that the VPN's dedicated access connection is unavailable during any single day, AT&T will credit NovaCare. AT&T is able to deliver on this guarantee because its high-speed, low latency connections are engineered for speed with lower delay and higher throughput than solutions built on non-IP technologies. This solution is designed to support a guaranteed low latency between two AT&T managed customer sites. Dial access is available from 300+ local dial points of presence or via 800 service. AT&T supports

NovaCare Inc.

56K modem access as well as nationwide ISDN.

"The VPN is helping to secure savings by eliminating the need for therapists to synchronize their databases with the central PC in the facility," says Wise.

In the old system, therapists would have to spend time making sure that the data stored on their PCs was synchronized with the Central Data Center to ensure that decisions were made using the latest data. The VPN has allowed the NovaNet PLUS network to move away from the batch transmission methodology, by having the therapists enter the information on-line in a real-time environment.

This saves time and creates an opportunity for therapists to see more patients, which increases revenues.

NovaCare is also removing the costs associated with maintaining and supporting software upgrades on the client PCs because the VPN supports a distributed "thin-client" computing model, rather than a traditional "fat-client" server model. In other words, all of the applications are stored on the server, and shared with the client PC for the duration of the communications session.

"When we want to put a new version of our software out, we put it on the server here, and the next person that dials in works with the latest data and application. Diskettes do not have to be made or mailed out. We do not need to engage in trouble-shooting because the programs were not properly installed. Software deployment costs are reduced to nearly zero," he says.

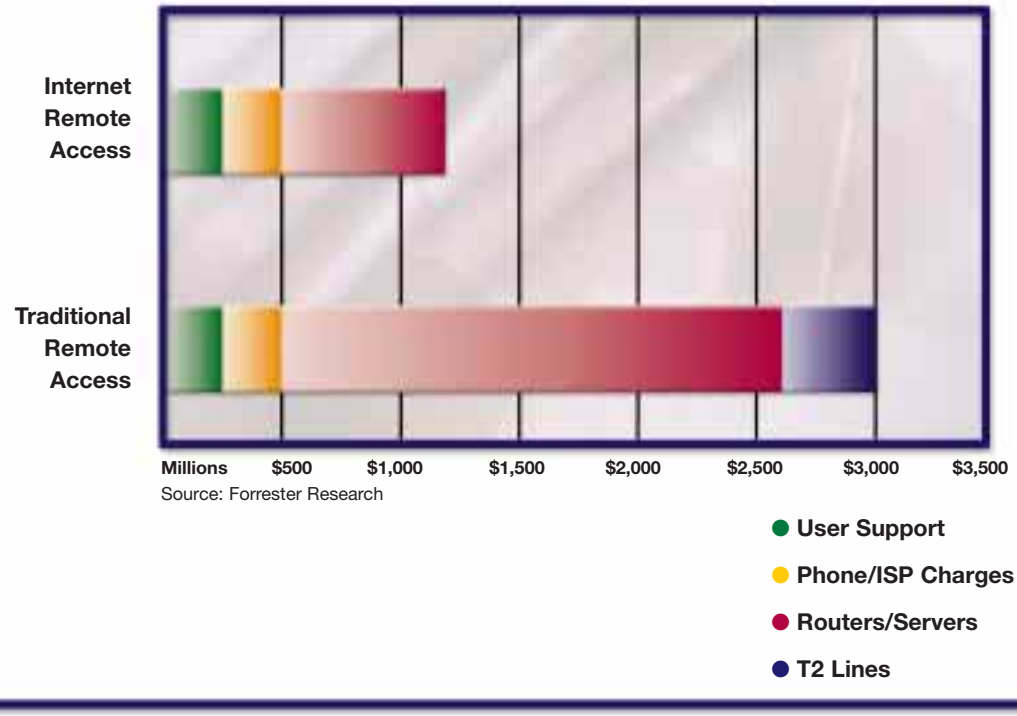
Indeed, Wise estimates that total savings made possible by the new system utilizing VPN will run between $500,000 and $1 million per year.

"The VPN-intranet application has reduced the time a clinician spends on the computer, allowing therapists to spend more time with patients, even as it eliminates the cost of application deployment. It also reduces break/fix costs and provides a more reliable interface to billing and payroll," says Wise.

Currently in pilot mode, the system is on track for a scheduled deployment in February that will result in national availability to all of NovaCare's therapists on March 1, 1999. ❑

VPNs Offer Estimated 60% Cost Savings

Remote Access Cost Comparisons for 2000 Remote Users



Source: Forrester Research

Mission-Critical VPNs Need More Than Virtual Security: They Need Bulletproof Assurance

Important advances in security protocol definition and network performance guarantees are accelerating organizations' willingness and ability to move from private data networks to VPN services that take advantage of the flexibility inherent in the IP protocol at a fraction of the cost.

There is a general perception that the public Internet lacks adequate security safeguards. In many cases, these concerns can be alleviated by keeping all VPN traffic on a service provider's IP backbone where bandwidth and service levels can be guaranteed. That's because the Public Internet does not provide the security measures that a VPN service environment will provide.

The IETF (Internet Engineering Task Force) has recognized three layers as the most important battle grounds for security protocol development and has defined a set of specifications for VPN devices and services it calls IPSec (IP Security Protocol). Here's a look at what the standards have helped accomplish:

Level 1: Identification and Authentication

Level 2: Access Control and Authorization

Level 3: Confidentiality and Integrity.

Level 4: Physical and Administrative Audits

Level 1: Identification and Authentication

Knowing who is communicating with whom and that people are who they say they are is perhaps the most basic starting point for a VPN security strategy. Identification requires that a user identify himself and authentication requires that a user attempting network access can prove that the ID is accurate.

At the physical level, identification can be achieved with a user password, a magnetic card access, or in the future, an increasing array of biometric techniques such as hand scans, fingerprint ID and retina scans. IPSec has a variety of methods for establishing authentication. The most secure techniques often involve the use of public key encryption, including public/private pairs, combined with digital certificates to bind public keys to an identity and ensure validation.

A secure VPN service can also protect privileges on the corporate intranet.

Level 2: Access Control and Authorization

Determining which privileges users have to access appropriate network resources is the next critical element that security strategists must consider. This is really about controlling access to the different information systems resources available throughout an extended enterprise network. As the remote access concept continues to build up steam, mastering and managing access control will not be limited to tracking employees; it will also require managing the way trading partners, such as resellers and customers, are let in to the corporate or inter-corporate network to maximize commerce while simultaneously mitigating risk.

Level 3: Confidentiality and Integrity

Protecting data from interception and tampering as it travels across a network or group of networks is a very real issue for companies that are rolling out VPNs. Encryption technology used by military applications and commercially for many years, has contributed to the ability to make protected communications nearly impossible to "crack."

When purchasing a VPN service from a service provider, there is one additional level of performance that contributes to the robustness of the service. This is:

Level 4: Physical and Administrative Audits

This ensures that the physical security of the overall network, the ability to track the overall security and the ability to establish for certain that the entire network has not been compromised.

An Evolving Standards Environment

As the Internet grows and continues to develop, standards will continue to evolve to ensure security and compatibility. Today, however, any VPN service should, at a minimum, contain support for these specifications. Additional specifications such as IPSec, L2TP (Layer Two Tunneling Protocol), and QoS (Quality of Service) are being promoted as innovative technologies to build VPNs. These standards are currently being accepted by the industry. ❑

AT&T Virtual Private Network Service

AT&T Virtual Private Network (VPN) Services have been created to take advantage of the reach, reliability and scalability of AT&T's global network. According to Bill Gewirtz, AT&T Global Business IP Services Vice President, AT&T's VPN Services have deployed advanced logical and physical networking to address three emerging VPN applications:

- **Remote LAN access for mobile workers and telecommuters**
- **Intranets for intra-company transactions**
- **Extranets for supply chain management**

This broad product portfolio allows AT&T to meet the needs of customers who at one end of the spectrum want to concentrate on their core business competencies and outsource their networking needs to a VPN provider, all the way to those customers at the other end of the spectrum who would prefer to build their own VPN with modular layers of service and equipment. For all customers, the appropriate VPN service is determined by whether the incremental benefits outweigh the complexity of implementation.

Gewirtz also identifies performance, global reach and security, as critical minimum entry points for a VPN provider. AT&T differentiates itself by being the most reliable and secure network in the market. He points out that AT&T over-engineers its platform by 50 percent to assure 100 percent availability with less than 1 percent packet loss and maximum cross-country latency of 80 milliseconds. Should an errant backhoe take out a crucial link, the patented AT&T FASTAR® System (Fast Automatic Restoration) technology can restore interrupted service in seconds.

AT&T has built fully redundant network management centers performing both in-band and out-of-band failure diagnostics. The in-band diagnostic tools ping routers periodically, while out-of-band systems dial around them to monitor customers' CPE. There are 58 SONET rings providing nationwide SONET coverage. Graduated, standards-based IP security range from simple firewalls and packet filtering to advanced encryption and tunneling.

AT&T backs up its technology with SLAs on both its VPN and customer CPE that ensure a day's service reimbursement for outages.

Sophisticated software, that ensures calls from business customers are never blocked, has contributed to AT&T's impressive dial-up statistics (see sidebar) and is positioning this carrier as the best-in-class provider of dial-up connectivity. ❑

Inverse ISP Benchmark Test

(Test period: December 1 through December 15, 1998)

MEASURE	AT&T RATINGS AND SCORES	INDUSTRY AVERAGE RATINGS AND SCORES
24-HOUR CSR*	A+ = 98.5%	A = 95.0%
EVENING-HOUR CSR*	A+ = 97.7%	B = 91.5%
BUSINESS-HOUR CSR*	A+ = 97.8%	B = 94.5%
INITIAL MODEM SPEED	C = 27.0 Kbps	B = 28.0 Kbps
TIME TO LOG IN	A = 25.5 sec	B = 29.5 sec
DNS LOOKUP	B = 421.5 msec	C = 576.0 msec
DOWNLOAD TIME	C = 32.4 sec	C = 33.9 sec
WEB THROUGHPUT	A = 2.9 Kbytes/sec	B = 2.8 Kbytes/sec
WEB FAILURES/TIME-OUTS	A = 1.44%	B = 1.56%

* CSR = Call Success Rate. No ratings were adjusted down for failing to meet the additional "threshold" criteria.

* The "Business-Hour" is defined as Weekdays 9 a.m. to 5 p.m. local time

* The "Evening-Hour" test period is defined as 6 p.m. to midnight local time

The thirteen national ISPs that made up the industry average are:
AOL, AT&T, Cable & Wireless, CompuServe, Concentric, Earthlink, GTE, IBM, Microsoft Network, MindSpring, NETCOM, Prodigy, and UUNET.

AT&T backs up its technology with SLAs on both its VPN and customer CPE that ensure a day's service reimbursement for outages.

Q & A with Kathleen Earley

Vice President, AT&T Internet Services

Kathleen B. Earley, Vice President, AT&T Internet Services, is responsible for leading AT&T's IP networking initiatives in the global business market. AT&T Internet Services provides its customers with IP-networking capabilities, electronic messaging services and industry-leading web hosting. AT&T's family of IP services include AT&T Business Dial, AT&T Managed Internet Service and AT&T Virtual Private Network Service. We sat down with Kathleen to discuss the future of the VPN market and the role that AT&T intends to play in its development. Here is what she had to say:

BPC: Much has been said about VPNs and the revolutionary impact they are going to have on corporate America. How do you see the market for this technology developing, and how do you think it will be embraced?

Earley: The Virtual Private Network concept has been a veritable moving target. Over the last few years we have seen its meaning evolve, expand and contract as technology developers, carriers and enterprise customers struggle to determine its parameters and its implications. Some people have tried to keep it tightly defined to remote access to corporate intranet servers, while others have tried to stretch it out to incorporate extranet access. Still others have tried to pigeon hole it into one of a series of functional areas: premise-to-premise, application-to-application, or dial-to-application.

But as the dust finally settles around this very important technology, a general sense is emerging that, in the final analysis, VPNs are all about offering a series of permissions for different layers of access in a secure manner, leveraging the presence of the most cost-efficient network ever created, namely the Internet. In so doing, VPNs are being designed to support applications and activities that were previously carried by proprietary dedicated networks, be they 800 number call centers, dedicated modem banks, leased lines, Frame Relay networks, etc.

It has immediately become evident that one of the biggest beneficiaries of the VPN revolution are those companies in the so-called middle market—medium-sized companies, that have been excluded by pricing from deploying sophisticated corporate networks based on ATM and Frame Relay technology to support and advance their business objectives.

For these companies VPNs offer up a set of resources and capabilities on a worldwide basis that, a few years ago, could only be accessed by the elite group of players of the Fortune 1000. By leveraging the shared economics of IP, these companies now have an opportunity to compete with any entity anywhere, and be measured not by the size of their topline, but by their ability to solve problems or deliver service in a cost-effective manner.

BPC: How are these companies going to accomplish their objective?

Earley: It is going to be accomplished by re-thinking their business processes in light of the new technological capabilities. One of the most exciting areas being opened up by the VPN revolution is application-to-application connectivity. I expect this to be a very

One of the most exciting areas being opened up by the VPN revolution is application-to-application connectivity.

important 1999 phenomenon, as companies begin to realize that the Internet is not only changing the rules of marketing and distribution, but also providing an opportunity to deliver heretofore unimagined improvements in operational productivity. Here is what I mean. In electronic commerce, many companies are only now getting over being wowed by the marketing potential offered up by the Internet, and are waking up to the impact that it can have on their own workflow.

Consider the 'Buy Now' button at a site. The technology is now available to immediately link the order request, not just to payment authorization and processing applications, but also to inventory management systems, logistics, and even decision support systems that can completely transform the competitiveness of companies of virtually any size. This type of inter-application integration was promised by the JAVA programming language, but it is going to be realized by VPNs that remotely, yet securely, link customers all over the world to back office operations. VPNs will not only do this for an individual company, but by using the extranet model, link up an entire channel of distribution.

The implications for enterprises are profound. It is going to force companies to engage in serious soul searching in order to make decisions about what, fundamentally, constitutes core corporate activities. As companies redouble the efforts around those competencies that truly differentiate them in the marketplace, VPNs should facilitate their subsequent need to outsource non-core functions to those companies that are willing and able to form tight digital partnerships that respond on a real-time basis to changes in market conditions. Finally, these companies will be able to get off the sidelines and actively participate in the global economy.

There is a growing list of companies that have just emerged to establish phenomenal brand recognition with remarkably few resources. These companies have been fleet of foot and have delivered on the promise of the time-to-market paradigm. Indeed, companies like E*Trade and Amazon.com are not just pioneering Web-based commerce, they are fundamentally changing the nature of the traditional brick and mortar industries that they have brought into cyberspace. The marketing and distribution channels have been entirely redefined. Amazingly, huge firms like Merrill Lynch and Barnes & Noble, are following their lead, not the other way around.

Simply put, VPNs will provide the vehicle through which companies manage internal, external and public IP resources to get to market better, faster and cheaper. The pace of adoption will explode as IP moves from primarily being a store and forward technology to a real-time medium. And along the way early adopters face the real prospects of capturing market share and significantly reducing the cost of goods sold.

Simply put, VPNs will provide the vehicle through which companies manage internal, external and public IP resources to get to market better, faster and cheaper.

BPC: What do these trends mean for AT&T?

Earley: AT&T intends to be the largest ISP in the world, and everything we have done to date is designed to position us as the premier provider of communications services. That is the thinking that has gone behind our acquisitions of TCG, TCI and most recently the IBM Global Network. It is also the fundamental force driving our joint venture with British Telecom.

These developments have created unprecedented scale in the communications services space, and the VPN offer is unquestionably enriched because of them. This spate of M&A activity not only gives us a worldwide presence, you will be hard pressed to land in a country in which AT&T can not provide a dial tone, but it also allows us a unique capability to offer robust VPN services across the entire spectrum of prospective clients. We do understand that we have a heterogeneous client base, and each of the acquisitions we have made are designed for every one of them in a tailored fashion. ❑

Editor's Note: Kathleen Earley was named to **Telephony's** *10 To Watch On The Carrier Scene* in the magazine's December 21, 1998 edition.

internet. intranet. extranet.

who could ever make them work together?

we can.

With AT&T, all your networks can work together as one.

Whether you're running your business on a private corporate network or on the internet, AT&T makes networks work better. AT&T builds networks your business can depend on. Now with AT&T, you can get the flexibility and speed of the internet with the security, management and control of a private network. All backed by the industry's best customer support. AT&T is the one company that can bring it all together for your company today—and well into the future. **For more information visit www.att.com/ipservices.**

It's all within your reach.®

AT&T IP Services