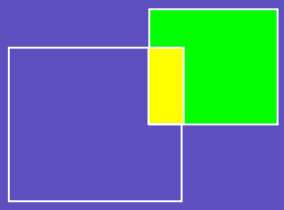
March 2002



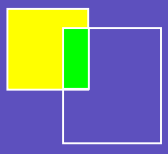
Expanding the IP VPN Value Proposition

An Introduction and Analysis of Network-Based Service Delivery

Colorado Office
1317 Cherry Street
Denver, CO 80220
303.355.1982

Oklahoma Office
1307 South Boulder Avenue
Suite 120
Tulsa, OK 74119
918.382.0007

Texas Office
2208 Columbia Drive
Flower Mound, TX 75028
972.874.7791



www.telechoice.com

The Strategic Catalyst™
TeleChoice
for the Telecom Industry

Enabling the Enterprise

The Internet revolution and rise of public networking has dramatically altered the networking requirements and opportunities of the enterprise. The deployment of new IP (Internet Protocol) applications and the availability of ubiquitous Internet connectivity promise to facilitate the exchange of critical information both within the enterprise and throughout its sphere of influence. However, this opportunity to expand the value of the network as a business asset does present challenges.

The network vision is the ability to connect multiple company sites, mobile users, business partners and customers in a manner that best enables the enterprises' business objectives. As many IT managers are painfully aware, the primary objective in today's current economic environment is fast becoming cost control. However, cost savings cannot be achieved at the expense of the network's flexibility, performance and security components, but should be realized in concert with the company's network vision. Increasingly apparent to many enterprises are the shortcomings of traditional technologies—such as private lines and frame relay—to deliver across all of these fronts.

As a result, a number of enterprises have looked to IP Virtual Private Networks (VPNs) enabled through specialized hardware and software on their premises as the solution. Flexible, secure and cost-effective in comparison to traditional solutions, IP VPNs exhibit many of the traits enterprises are seeking. However, demand from enterprises for IP VPNs has not lived up to industry expectations to date. Enterprise concerns including complexity, vendor interoperability, IP network performance and total cost of ownership remain roadblocks to widespread implementation.

This paper introduces the concept of enabling enterprise IP VPNs from within the edge of the service provider infrastructure, commonly referred to as network-based IP VPNs. In addition to evaluating the benefits of the network-based approach in place of or in combination with premises-based IP VPN solutions, a comparison to familiar legacy technologies such as private line and frame relay is provided. By leveraging network-based service delivery as a core element to enabling enterprise IP VPNs, several service providers are looking to expand and improve upon the IP VPN value proposition. One such service provider is Virtela Communications, whose service offerings and customer case studies are referenced in order to provide real-world examples of the benefits of network-based VPNs.

Shifting Enterprise Requirements

While traditional enterprise networking requirements such as reliability and cost of ownership continue to be important factors, new challenges and opportunities must increasingly be considered in the public environment including:

- Distributed Applications
- Widely Distributed Locations and Users
- Security
- Business-to-Business Communications
- Application Performance

Distributed Applications

The expanding adoption of client/server systems has heavily shaped the distributed computing environment. This architecture is most pronounced within the growing number of IP-centric applications, typically web-based programs such as CRM and ERP tools and email. Enterprises have gravitated to these types of applications for their competitive advantages, ease of use, flexibility, rapid development/deployment, and overall lower projected costs in comparison to legacy systems (such as mainframe based computing). As companies grow more and more reliant on the distribution of these applications as critical elements of their business, network connectivity and last mile bandwidth requirements increase significantly.

Widely Distributed Locations and Users

From a physical location perspective, enterprises must contend with the growing number of remote locations and users—enabled by the distributed business applications previously mentioned—requiring access to central sites or application hosting centers. Remote sites range from larger branch offices to small offices/home offices (SOHOs) to mobile "road warriors" requiring dialup connectivity from various locations. In particular, the trend towards telecommuting and the need to extend the business day by working additional hours from home have significantly increased the number of remote users. In addition, many of these locations may also be in a position to leverage the benefits of emerging broadband access technologies such as DSL, cable, Gigabit Ethernet and fixed wireless. Regardless of where applications reside or the access method most beneficial for the location, enterprises require the ability to provide access seamlessly, securely, reliably, and cost-effectively.

The geographic distribution of these remote sites and users for many enterprises continues to shift from local to national and even global arenas as business trends demand it. While addressing a distributed environment has its challenges regardless of geography, global companies face some of the biggest hurdles in terms of available coverage area of individual service providers, quality of service over wide distances, lack of a local IT presence, and a high cost to deliver service. Reducing these costs while providing the security, support and service quality required has been a major challenge to the global enterprise.

Security

Security concerns have been an impediment for migrating business-critical traffic to IP networks as well as an IT challenge from a mobile user/telecommuter perspective. In particular, recent events cause concern for public networking, such as DDOS attacks, reported break-ins tampering with or stealing data, and the constant threat of viruses. Mission critical applications need to be available, protected, and secure if a business is to operate successfully. In some sectors, confidentiality of sensitive data needs to be ensured in the face of legal ramifications to the enterprise. This is particularly the case in the U.S. for breaches of corporate or personal financial data, an individual's health records as protected by HIPAA regulations (Health Insurance Portability and Accountability Act of 1997) and/or academic records.

Business-to-Business Communications

The Internet model of connectivity and application simplification has given rise to business-to-business (B2B) commerce. Enterprises electronically exchange data with suppliers, solutions partners, customers, and other entities at much higher levels than previously with legacy technologies. These business communications range from basic document exchange via email to complex business Extranets enabling electronic supply chain integration. While obviously attractive to businesses, the implementation of such communications is complex and expensive with the traditional technologies most utilized today.

Application Performance

QoS requirements have also increased as more critical business traffic runs over IP networks. The Internet has moved beyond simple store-and-forward or low bandwidth applications to latency- and jitter- (variation of latency) sensitive applications such as voice and video. Enterprises are looking to leverage these advanced services at near private line quality but at significantly less cost. Enterprises are increasingly turning to IP networks and the Internet as their performance measurements and guarantees demonstrate that IP networks can support critical business applications.

Challenges with Current Solutions

Traditionally, the enterprise has addressed the problem of connecting multiple sites by using legacy technologies such as private lines, frame relay and ATM (Asynchronous Transfer Mode). However, with the shifting enterprise requirement landscape these legacy technologies fall short as the future of networking for many enterprises. The following table outlines the key advantages and drawbacks of these technologies:

Technology	***Advantages***	***Disadvantages***
Private Line	As a dedicated pipe it has very high level of performance Highly secure: as a private, dedicated infrastructure, privacy breaches only occur through tapping physical links	Almost always the highest cost solution. Dedicated circuits are the most expensive form of networking Less flexibility in designing network redundancy and meshing within a company and in B2B settings as it requires additional dedicated circuits Meshing of multiple sites together is not economically practical Integrating standalone remote access users requires additional infrastructure No support for burstable speed. Enterprises can only buy fixed speed lines, forcing them to pay for maximum expected bandwidth utilization

Frame Relay	Links from site to site created within the frame relay network through software defined virtual circuits. Service provider builds in redundancy within the network Virtual connections create a lower cost alternative to private line Good alternative for sites with low bandwidth requirements Virtually any speed service available	An expensive solution for large meshed networks as each site-to-site connection requires a PVC (Permanent Virtual Circuit) Network administration in maintaining a meshed network is still a difficult task Not conducive for B2B solutions due to the lack of interconnectivity between frame relay providers Integrating standalone remote access users requires additional infrastructure Frame providers hand off circuits at multiple points, introducing performance and trouble spot ownership concerns
ATM	Leverages virtual circuit concept of frame relay for lower costs Inherent Class of Service improved overall service quality from Frame Relay Good for higher bandwidth connections	Network administration and integration challenges similar to Frame Relay Generally more expensive than Frame Relay Received lots of hype but did not result in a large number of subscribers due to complexity

Introduction to IP VPNs

In general, legacy solutions provide basic connectivity in a reliable fashion, but are costly and difficult to manage as the enterprise attempts to force fit them into the IP-centric world. With the emergence of IP networking and related security needs, native IP solutions have become the focal point. As a result, the industry has introduced IP VPNs as a solution.

An IP VPN establishes a base network, including physical access to each site, secure transport over a wide area network, and IP connectivity and routing between locations. IP VPNs leverage three key functions to ensure security—authentication, encryption and tunneling (the trait they are associated with most often).

- **Authentication.** Authentication is the process of verifying the identity of a user or host on a network. RADIUS is a standard authentication mechanism used by most every service provider and many enterprises. Stronger methods of authentication involve issuing digital certificates through some type of Public Key Infrastructure (PKI) or token-based solution.

- **Encryption.** Encryption is the process of ensuring data packet privacy during transport by encoding the data to ensure confidentiality. Encryption marks a data packet, transforms its contents, and reformats the data for transmission. The most common encryption algorithms are the DES (56 bit) and 3DES (168 bit) standards.

- **Tunneling.** Tunneling is the process of creating a secure connection between two points by enveloping a packet within a packet. ESP (Encapsulation Security Protocol) is the standardized IPsec tunneling protocol and is leveraged by most IP VPN service providers today.

The business intelligence component of an IP VPN is the creation and maintenance of a policy set. The policy set configures the IP VPN to meet business objectives, mapping desired behaviors to functional components. For example, a policy can determine which users and systems may establish a connection through the firewall, whether this connection is secured with encryption, and which applications can be used over this connection. Establishing and modifying the policy set is required for successful operation. This can be a daunting task, but managed IP VPN service providers that offer expert policy management alleviate this burden.

The First IP VPN: CPE-Based Solutions

The first deployments of IP VPNs have been based on CPE (Customer Premises Equipment) software and hardware. Enterprises have adopted these solutions either on a do-it-yourself (DIY) basis or by subscribing to a managed solution from a service provider. The CPE-based IP VPN is widely deployed among enterprises today, and has several key benefits and challenges, as presented in the following table:

Benefits	***Description***
Enterprise Control	IT organizations generally favor self-control over their networks, particularly the newer services. With a CPE-based IP VPN the enterprise can control the policies, management, and selection of vendor used. As a dedicated device, the enterprise also is not concerned with sharing processing power and network capacity with other enterprise customers of the service provider
End-to-End Encryption	There is a perceived security benefit of encrypting traffic from premise to premise. Highly security-conscious entities prefer this architecture as no data leaves the site unencrypted, providing peace of mind in having the solution onsite under physical control of the IT department
Service Provider Independent	The functionality of the IP VPN is processed by the premise-based solution, separating it from the network component. An enterprise can switch service providers without impacting the CPE infrastructure substantially
Challenges	***Description***
Complexity to Install, Configure and Manage	In this model an enterprise needs to deploy a premise-based solution to each site. Installation requires an on-site presence often resulting in a long time to deploy. Maintaining configurations over a large network is difficult particularly when security policies change (each premise-based device requires updating). Managing the hardware/software upgrades also generally requires onsite presence. The time required to perform these functions reflects a cumbersome network infrastructure

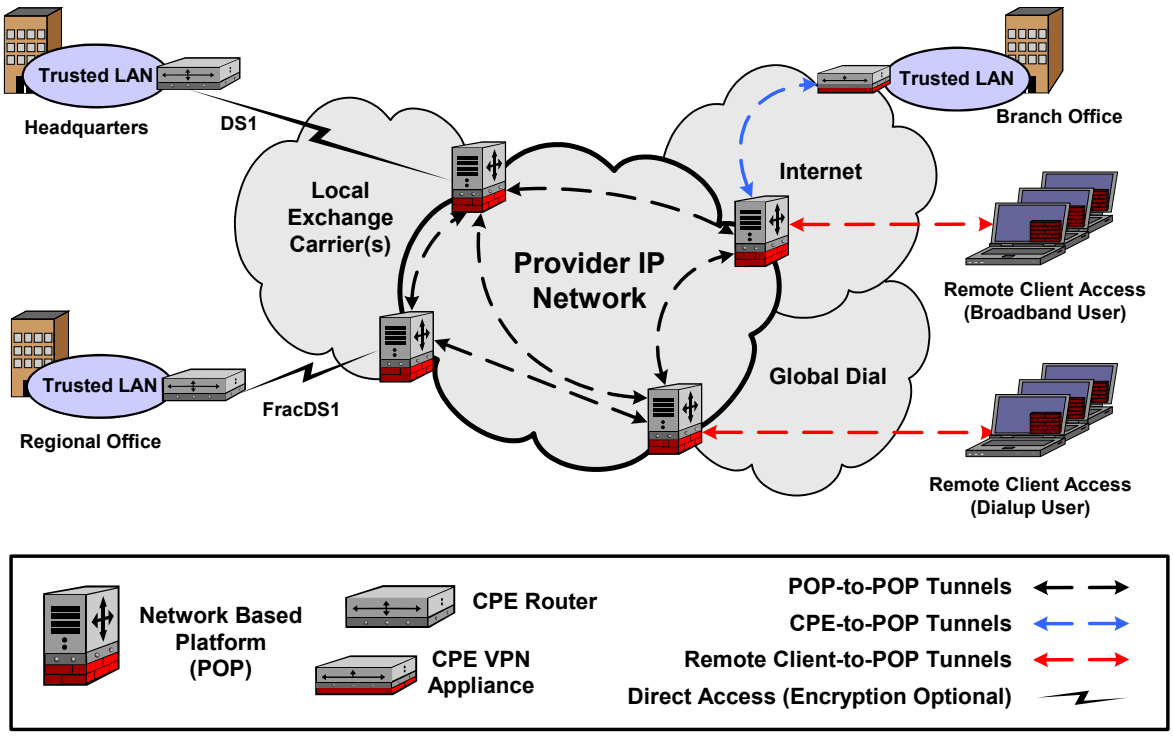
Increased Cost	The increased complexity described above also translates to higher support costs for the IP VPN infrastructure. Additionally, each site requires a device or software solution that is either leased or purchased. For large enterprises with many sites, these costs add up quickly
Vendor Interoperability	Enterprises are not only challenged to provide a secure solution that works for their own sites, they may be required to interconnect with other networks (such as those of a trading partner, expanded company resulting from a merger, etc.). These disparate networks are often supported by solutions from different vendors; integrating them can be extremely difficult
Scalability	As a new site is added to a fully meshed network, each device requires reconfiguration to allow access, establish tunnels, etc. This condition is known as the `n(n-1)/2` problem where network complexity increases exponentially, hampering network growth and increasing operational costs. This is a similar issue to creating and managing PVCs in a meshed frame relay network – fully meshing sites is not practical for large networks
Configuration Constraints	By selecting a particular make and model of CPE for a specific site, the enterprise is constrained by the specifications of that device in terms of functionality (number of tunnels, encrypted throughput, simultaneous users and/or firewall sessions, etc.) and would necessitate a hardware/software upgrade should requirements change. Additionally, IP VPN CPE generally lacks the reliability levels of carrier-grade platforms
Limited QoS Options	Most CPE solutions do not offer QoS controls. Some offer limited options such as rate limiting, etc.

Despite these disadvantages, many companies have successfully deployed CPE-based IP VPNs. However, for some businesses, the disadvantages inherent in these solutions have impeded or prevented widespread implementation. For the early adopters, CPE-based IP VPNs were the only option available. With the more recent innovations in vendor platforms enabling the service provider, enterprises now have an alternative to and/or an augmentation of the CPE-based approach: network-based IP VPN services delivered from the service provider's "cloud."

Network-Based IP VPN Service Delivery

Availability of network-based IP VPN solutions is being driven in large part to address the manageability, scalability and cost challenges of premise-based IP VPN solutions. The concept of delivering services from the network is not innovative in itself, as many voice services (such as Centrex) have been delivered from a service provider's central office for years. Likewise the intelligence of the legacy data services described above (e.g., frame relay) is contained within the network and passed on to the customer. Network-based IP VPNs are a relatively recent alternative that simplifies and reduces the cost of enabling IP VPN service to the enterprise and its end users. This approach enables services within the network and does not require the enterprise to deploy and maintain expensive CPE devices at each location. This substantially reduces capital and operational costs and expedites service delivery.

What is needed for a network-based IP VPN implementation? Similar to other solutions, it begins with network access and transport, with speeds generally ranging from 128K to DS-3. A traditional router is deployed on the customer premise to enable IP connectivity and protocol translation from an access technology to a LAN protocol (such as Ethernet or Token Ring). The next step is to establish the policies defining the key parameters of the IP VPN (as discussed earlier). With network-delivered services, the core IP VPN functions of authentication, encryption and tunneling take place at the edge of the service provider's network rather than within equipment on the enterprise's premises. This is illustrated in the following diagram:



Note: The diagram demonstrates the flexibility of a potential hybrid IP VPN to meet the needs of each enterprise location. Providers such as Virtela support this hybrid configuration. The network–based solution is the preferred method for a majority of sites, followed by CPE-based for off-net or highly security-conscious sites and remote dial access with software client for travelling users.

A key component of the network-based IP solution is the virtual router on a network-based platform (such as an IP service switch). A virtual router is a software instance of the enterprise's routing table implemented upon a shared service provider maintained platform. In effect it moves the routing function and associated management headache from the enterprise premise into the service provider's network. The service provider can customize each virtual router to meet the specific needs of the enterprise IP VPN. The virtual router not only allows routing policy, but it can also be configured to deliver security services from the service provider network (such as firewall, intrusion detection, encryption, tunneling, etc.). Furthermore, the virtual router is more easily managed and replicated across the network than touching the configuration of multiple physical routers at each company site.

With certain network-based offerings, such as Virtela VPN, enterprises can layer these services onto their existing access networks (such as Private Lines, Frame Relay, DSL, etc.). Being "access neutral" allows the enterprise to customize its IP VPN to support its various user locations with different configurations as shown in the previous diagram.

Service Highlights:

Virtela™ Communications

The Virtela Approach: Customized network-based IP VPN solutions that leverage an optimized and redundant, carrier- and access-neutral network

Virtela's IP Service Fabric℠: A unique infrastructure for transport optimization of enterprise traffic across *multiple*, best-in-class IP backbones resulting in greater reliability and performance.

Core VPN Solutions:

- **Direct VPN Access (Network-based IP VPN)**
  - Direct TDM, DSL, Cable, Gigabit Ethernet, Fixed Wireless connections to the Virtela Network
- **CPE VPN Access**
  - Network based IP VPN implementations using CPE and Internet connectivity to access the Virtela Network
- **Secure Remote VPN Access**
  - IPsec based mobile dial and telecommuter broadband remote IP VPN access

Virtela Solution Attributes:

- **Network Design and Coverage**
  - Carrier and Access neutral
  - Worldwide footprint
- **Redundancy**
  - Automatic fail-over
  - Redundant hardware architecture
- **Security**
  - Secure IPsec tunneling
  - Integrated firewall and IDS
- **Interoperability at All Levels**
  - With legacy infrastructures
  - With multiple CPE vendors
- **Performance**
  - Performance-optimized routing
  - Load balancing
- **Service Delivery**
  - Fast provisioning intervals
  - Service creation within network core

Source: Virtela Communications

Capabilities and Features of Network-Based Services

Network-based IP VPN services can be viewed as the platform for delivery of layered services. Once the IP VPN base is created, an enterprise can meet its business requirements more optimally by layering on additional features such as firewall, intrusion detection and prevention, virus scanning, and QoS assignments by application type and/or location:

- **Firewall.** A network firewall secures the perimeter of a network from unwanted ingress or egress. Rules or policies are set to control ingress/egress behaviors for a customer network. By securing a firewall in the network-based scenario, the enterprise protects its LAN and reduces unwanted traffic from consuming bandwidth on the last mile. A network-based solution provides economical firewall services for all sites, versus having one or two firewalls within the enterprise network and needing to hub all Internet-bound traffic back to those sites.

- **Intrusion Detection and Prevention.** From the network edge, known attacks are stopped by the state of the sessions. For example, the intrusion detection system monitors for hacker behaviors such as port scanning for network weaknesses. These attacks from inbound intruders are stopped before reaching the enterprise LAN, conserving enterprise resources and reducing threats.

- **Virus Scanning.** The enterprise can add protection to its network by screening for viruses at the provider network edge. Many enterprises currently use virus scanning on servers and desktops. This network-based complementary service additionally filters at the most common entry point for viruses (particularly for Internet connections). Using a combination of network-based and client-based scanning maximizes protection against viruses.

- **Assignment of QoS.** Specific applications and IP addresses can be designated as a particular class or level of service. Applications are given a particular level of service based on their business importance and/or their technical nature (i.e., ability to handle latency). This feature allows the IP VPN to support higher-level applications such as voice and video. End-to-end QoS is achieved through techniques such as Diffserv on the customer router.

Additional services can be created and layered for more security and closer alignment with business and network objectives as configurations change, security techniques and technologies are updated, etc. The network-based IP VPN supports IT departments as they enable new services to meet end user application requirements.

Customer Case Study:

Virtela™ Communications

Leading Wireless Service Provider

THE CHALLENGE: Providing Highly Secure, Reliable Connectivity between Branch Offices, Remote Workers, Strategic Vendors and Business Partners

One of the largest wireless carriers in the U.S. needed to provide secure, cost-effective remote access to their world-class corporate technology laboratory. The lab's existing connectivity consisted of dedicated T1 circuits, a DS-3 connection and Frame Relay network. The wireless company's employees, vendors and partners often need rapid access to the lab to test a new piece of equipment or proof-of-concept, and ordering a new T1 circuit to accommodate them could take six weeks to six months depending on the location.

THE SOLUTION: Implement a Fully Managed, Secure IP Virtual Private Network (VPN) to Add New Sites Quickly at a Much Lower Cost

The customer turned to Virtela to provide and manage a secure remote access VPN, initially connecting remote offices in locations such as Seattle, New Hampshire, Washington, D.C., Los Angeles and Vancouver, Canada. Virtela tailors its VPN solutions to each customer, and in this case, blended Virtela's network-based VPN with existing customer premise equipment. Virtela's network-based solution inherently provides expedited service delivery; Virtela has brought up new sites for the customer within as little as six business days and continues to add sites every week. Virtela's solution delivers an average monthly savings of 60 percent over the legacy solution.

THE RESULTS: Delivering Fast, Secure Access Without the Management Headache

Since Virtela manages the remote access environment, the director of lab operations now has more time to dedicate to his primary responsibility – evaluating new technologies that will ultimately better serve the company's millions of subscribers. "If someone in the Chicago office wants to use the lab and needs a connection within a couple of weeks, now they get it and it doesn't require much work on my part," he added. "Virtela handles the entire process. It's terrific."

Source: Virtela Communications

Network-Based IP VPN in Action

An enterprise may ask, "So what? What's in it for me?" The following applications are examples of how the IP VPN service and layered features might be leveraged to meet a specific business need:

- **Legacy Network Migration.** Network-based IP VPN is expected to have a lower total cost of ownership for the enterprise. As more traffic moves to IP, a native IP architecture is logically the best infrastructure alternative to leverage. As a lower cost option, this solution is particularly applicable to small to medium enterprises with legacy networks in place to connect smaller sites.
- **SOHO and Telecommuter Connectivity.** Enterprises are looking for a cost-effective solution to add the growing number of these locations to a corporate network. The network-based IP VPN provides this connectivity at lower cost and faster deployment times than traditional solutions. IP VPNs are the only secure method of leveraging high-speed broadband Internet access, such as DSL and cable, for enterprise networks. Traditional solutions, such as Frame Relay, do not easily or economically support these situations. In addition, network-based VPNs can be provider agnostic—a real benefit when some locations have either DSL or high-speed cable access.
- **Secure Access to Hosting Centers.** The rise of outsourced data center space and managed application hosting requires secure connectivity. Using network-based IP VPNs, enterprises can connect to a data center to securely access mission critical applications such as ERP, CRM, etc. In another example, enterprises with hosted web servers require secure connectivity to administer these servers and to manage hosted content.
- **Site-to-Site Voice.** Voice traffic is prioritized, encrypted and sent over the network-based IP VPN infrastructure rather than using the PSTN. The advantages of this application are significantly lower costs for long distance traffic (i.e., no LEC termination charges, no long distance charges), single network to manage, etc. The incremental cost for running VoIP is essentially zero since an enterprise is already paying for IP bandwidth. A specific example of site-to-site voice over IP is connecting two or more call centers or connecting branch offices to the headquarter site.
- **Global Video Conferencing.** Enterprises use video conferencing for a number of reasons ranging from reduced travel cost to a higher degree of contact than standard phone calls. To date, video conferencing solutions have been either low quality (i.e., insufficient bandwidth, too difficult to use and implement) or too expensive (i.e., costly analog circuits and a usage-based model that becomes cost prohibitive to do international conferencing). Attempts to reduce costs by utilizing IP based video compounded the service quality issue, as IP networks did not have adequate controls to minimize latency and jitter. The network-based architecture leverages QoS techniques that look to ensure that high quality video can be supported on the network. These costs and QoS issues are multiplied when the endpoints are international.

Network-based IP VPN solutions apply to many more business and network applications than are cited above. Each enterprise will have specific uses for an IP VPN and unique reasons for utilizing and benefiting from an IP VPN delivered by the service provider's network.

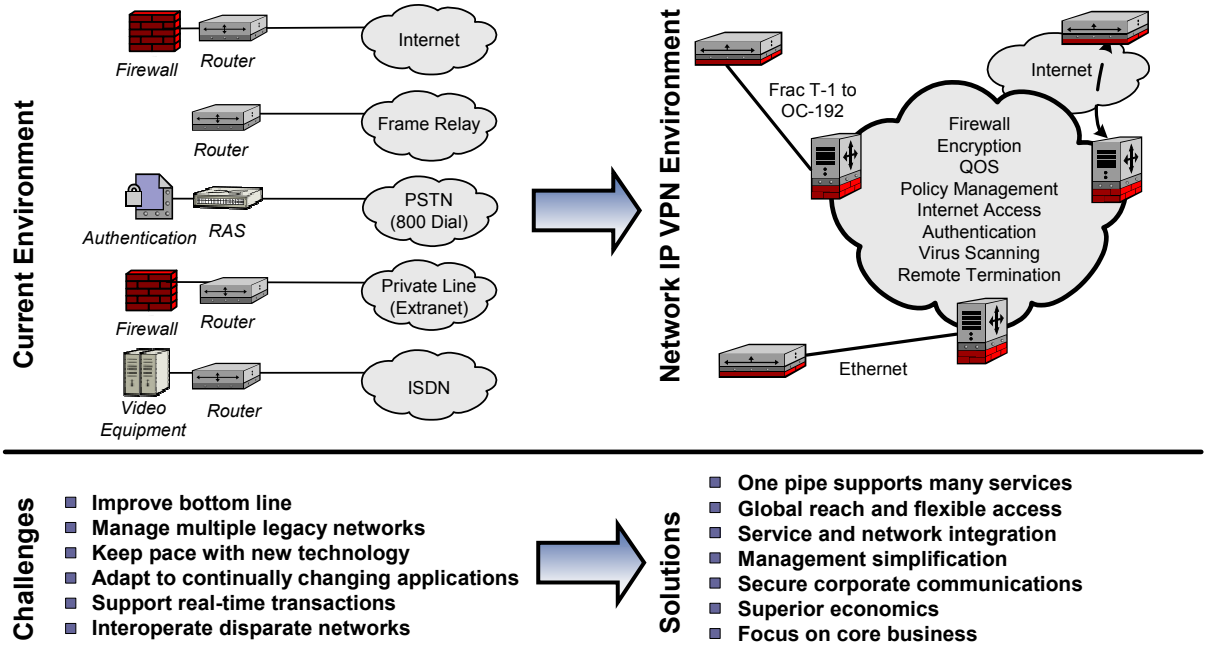
In Comparison with Traditional Solutions

The traditional solutions cited earlier in this document were effective because they worked well for the applications and networks at the time of their introduction to market. How applicable are they in today's environment? The following table outlines some of the strengths and weaknesses of legacy services and the IP VPN architectures.

Criteria	***Legacy Services***		***IP VPN Services***	
	Private Line	***Frame Relay***	***CPE-Based Only***	***Network-Based***
Perceived Cost	Highest cost solution	Viewed as cost effective for hub-and-spoke networks	Viewed as cost effective in comparison to legacy	Lowered capital expenditure and operational expenditure (due to limited number of VPN devices at customer premise). Viewed as cost effective in comparison to both legacy and CPE-based IP VPN
Scalability	Least scalable solution	Scalable for hub and spoke designs	IP is scalable, but configuring individual location CPE is an administrative challenge	Highest scalability for large networks Network-based IP VPNs are fully meshed in nature and pre-configured; IP VPN virtually defined by the provider within its network
Converged Video, Voice and Data Support	Well suited for individual applications on dedicated pipes or channelized circuits	Strong support for data applications. Voice and video endpoints have to be on the same Frame Relay network	With recent innovations in QoS and service delivery, IP VPNs are increasingly suited for converged, multimedia networks	
Perceived Security	Perceived to be secure due to dedicated circuits, but lack encryption and authentication	Perceived to be secure, but lack encryption and authentication	IP in general has real and perceived security challenges— CPE-based solutions viewed as more secure IP VPN	Basic configuration perceived as secure from POP to POP and on par with frame relay— optional but less secure than CPE-based as the last mile is "in the clear" Optional encryption over the last mile makes this alternative as secure as CPE-based solutions

Any-to-Any Connectivity	Static connection-oriented technologies are less conducive to any-to-any connectivity		Inherent in IP, including international and dial. Network-based and CPE-based VPNs cover most every type of customer site Network Based VPN (only): The network based infrastructure acts like an intermediary for multi-vendor equipment connectivity. Supported vendor devices communicate with the "neutral" network-based IP VPN rather than connecting directly to each other	
Network Availability	Redundant links require dedicated circuits – expensive and difficult to maintain	More resilient in nature than private line solutions, yet carrier outages impact the entire network	Diversity of IP networks and the Internet provide for multiple paths through multiple carrier networks. IP networks dynamically route around network problems	
Key Distinctions	Dedicated circuits are more controllable, have highest perceived security, but at highest cost	Cost-effective alternative to private lines. Good for multi-protocol traffic like SNA	Flexibility of IP with higher perceived levels of security and control. Harder to maintain and more expensive than network-based	Cost-effective, secure and simplified native IP connectivity

A key benefit of IP VPN services over the traditional networking alternatives is the consolidation of services and applications to a single network and reduced complexity on the premise. The current environment requires multiple networks and multiple devices to support various applications. The preponderance of nodes results in more complex administration, operations and maintenance – translation: higher costs.



Bottom Line Benefits and Value Proposition

The network-based IP VPN compares favorably with alternative technologies as well as with CPE-based IP VPN solutions depending upon the needs of the enterprise. The enterprise can leverage the following advantages of an IP VPN delivered from the network:

- **Centralized Policy Control and Management.** All of an enterprise network's rules and policies are stored and accessible in a centralized manner. In addition, upgrading software codes and versions can be a much faster process from within the network. For example, an enterprise with 200 locations would have to upgrade each box individually. With a network-based VPN, the service provide can upgrade its switches in the core without having to interfere with an individual enterprise's equipment.

  Network-based VPNs also allow for the stateful monitoring of IPsec tunnels. A service provider can monitor the health of each IPsec tunnel and proactively troubleshoot any potential issues.

- **Operational Cost Savings.** Network-based IP VPNs reduce operational costs for enterprise customers through simplified management performed in the network. Configuration changes are made more quickly than CPE-based solutions. Additionally, an enterprise using a network-based solution requires less hardware, which translates into reduced operational, maintenance and troubleshooting costs.

- **Lower-priced Service.** Not having to buy additional hardware for VPN results in lowered total cost of ownership for the enterprise customer. Although the service is lower-priced, overall quality is not compromised.

Customer Case Study:

Virtela™ Communications

Winphoria Networks, Inc.

The Challenge: Providing Low-Cost, Secure Connectivity Between International Locations and U.S. Headquarters

Winphoria Networks Inc., a core infrastructure company for mobile wireless service provider networks, needed a more efficient way provide development teams in Madrid and Bangalore with email and access to key centralized resources residing at its corporate headquarters in Tewksbury, MA. Since other private network approaches would have been extremely cost-prohibitive and time-consuming for international connectivity, Winphoria turned to a Virtual Private Network (VPN) model. However, an initial in-house VPN deployment was limited to dial-up connections and managing the environment had become a drain on internal IT resources.

The Solution: Choosing a Fully Managed VPN to Provide Secure, Flexible Connectivity

Winphoria chose Virtela to provide a fully managed VPN solution that offers the widest array of access methods on the market. Virtela leveraged Winphoria's existing Internet connectivity and provided CPE access to the Virtela VPN, substantially reducing the time and cost to bring up new connections. This Virtela VPN approach is estimated to save Winphoria up to 75 percent over deploying a Frame Relay network.

Virtela supports every customer with a 24x365 Network Operations Center (NOC) that provides expert monitoring and maintenance of all Virtela customer network sites. Now, Winphoria's U.S. IT staff is no longer disturbed in the middle of the night by network issues overseas. At the same time, the staff has the flexibility to monitor and control their Virtela VPN via VirtelaView^{SM}, a secure, web-based management portal.

"I have looked at VPN offerings from larger carriers, and they were too big for me to accomplish what I need to accomplish," said David Heafey, IT manager at Winphoria. "Virtela is very flexible, and created a support plan for us around what we need."

The Results: More Reliable, Less Expensive Connections for International Sites

Winphoria's international users have fast access to business-critical corporate resources without security or reliability concerns, while its IT staff can focus attention on other projects by relying on the expertise of Virtela's NOC management. Winphoria is also exploring the opportunity to leverage additional services over their Virtela VPN, such as VirtelaVoice^{SM}, which enables cost-effective domestic and international calls between company locations, and VirtelaVideo^{SM}, which provides secure, TV-quality videoconferencing between enterprise sites.

- **Capital Cost Savings.** Since it requires less equipment, the enterprise has less asset-related expense from equipment purchase or lease costs. The service provider bears this capital burden.

- **Scalability.** CPE-based VPN devices are limited by the number of tunnels they can support. Equipment that can support several hundred simultaneous tunnels gets very expensive and time consuming to manage. Network-based VPNs offer fully meshed, pre-configured tunnels thereby increasing scalability. It is much easier to add virtual routers, security policies and links in the network than configuring devices on premise. This reduces the time to bring a site online and allows it to start contributing to company productivity.

- **Service Provider Responsibility.** The service provider maintains the hardware and software configurations and is responsible for the service reliability beyond just the network links. The enterprise generally has the option to leverage a CNMS client to maintain its own policies.

- **Flexible Integration.** Innovative IP VPN service providers, such as Virtela, are able to integrate with traditional networks and CPE solutions to offer a smooth migration path. An existing frame relay network can be IP VPN enabled by a network-based solution. Enterprises with a CPE-based IP VPN solution at a central site can easily and cost effectively add small sites to this IP VPN by using a network-based architecture.

Service Provider Benefits of Network-Based IP VPNs

Service providers benefit from network-based IP VPNs as well as enterprises. Some of these benefits are as follows:

- More scalability to deliver services
- Reduces truck rolls, saving time and cost
- Centralized service provisioning and management
- A profitable alternative to address small sites previously not attractive to service providers
- Improved capabilities to create new services for subscribers
- Similar security as Frame Relay and ATM services and a migration path for users of these services

Enterprises subscribing to network-based IP VPN services reap these benefits in terms of lower cost, less time focus required and improved service quality.

Despite the above advantages there are some potential challenges to address when deploying network-based VPNs, as discussed below:

- **Ensuring Security.** Because a basic implementation may not include last mile encryption or premise-based firewall, some enterprises see this as a deficiency. Using a shared service provider edge device where security takes place is also viewed by some companies as a security liability. However, network-based VPNs offer a higher level of data privacy than a frame relay network, where data is not encrypted anywhere on the network. For enterprises that require a higher level of security, service providers such as Virtela and others support network-based IP VPNs configured in a hybrid solution. These configurations combine all the security benefits of the network-based solution plus encryption over the last mile via a less expensive device than traditional CPE-based approaches (see below).

- **Some Solutions May Require a CPE Component.** A CPE solution may be required for applications needing encryption at the premise. Some enterprises prefer the firewall at the demarcation point rather than in the network. However, the last mile can be viewed as a private extension of the LAN to the network.

Additionally, QoS can be delivered end-to-end with premise routers that are part of a network-based solution (described above). Flexible service providers support hybrid approaches that best meet the specific needs of each enterprise location.

- **Implementation Intervals.** Network-based VPNs require the provisioning of a circuit to the service provider's point-of-presence (POP) which may increase implementation time. Leading providers offer an array of access options to help speed implementation.

The benefits of a network based VPN far outweigh these limited drawbacks. For sites where network-based deployment is not an optimal solution, select service providers such as Virtela can implement hybrid architectures by deploying CPE at these sites. This "best-of-both worlds" model allows the enterprise to push functionality to the premise when needed, and to select its choice of ISPs globally.

Making Sense of It All

In the rapidly expanding world of business communications and services, network-based IP VPNs are in the earlier stages of adoption among enterprises and service providers. However, by enabling large numbers of enterprises with high value services in a cost-effective manner for both the enterprise and service provider their success will only increase over time. Network-based IP VPNs are particularly applicable to mass-customized sites such as remote branches, SOHO sites and telecommuter locations and potentially can serve as the sole solution for some enterprises.

Like any other technology however, network-based IP VPNs are not the silver bullet that will meet the needs and requirements of every single enterprise for every one of their locations in all cases. Some enterprises will require the deployment of CPE-based VPNs for heightened security and control, while others will require a composite solution of network-based, CPE-based and remote dial access components in order to address their unique mix of individual location requirements. TeleChoice believes that service providers such as Virtela that are able to offer enterprises these multi-architecture solutions are best positioned to meet the needs of today's and tomorrow's enterprise.

Glossary

3DES. Triple DES is a Data Encryption Standard that applies three 56-bit private encryption keys in succession to each 64-bit block of data in a specific transmission. Triple DES is considered an unbreakable transmission method as each key has 72 quadrillion possible combinations.

ATM. Asynchronous Transfer Mode is a dedicated connection-switching technology that organizes digital data into 53-byte cell units and transmits the cells over a physical medium using digital signal technology. ATM can manage all types of transmissions, including delay sensitive transmissions such as voice and video due to the fixed length nature of the cell technology. Each cell is processed asynchronously relative to other related cells and is queued before being multiplexed over the transmission path.

B2B. Business-to-Business refers to exchange of products, services, or information between two business entities. Direct consumer markets are not considered part of B2B transactions.

Cable Access. Cable Access refers to broadband access delivered via coaxial cable generally through the local cable television provider. Broadband Cable Access is widely used for Internet access and is currently being adopted for local telephone service. Broadband Cable Access operates on a shared network, requiring the use of additional security measures to insure data safety.

Centrex. Central Office Exchange Service is a service from local telephone companies in the United States in which up-to-date phone facilities at the phone company's central (local) office are offered to business users without requiring these users to invest in their own facilities. The Centrex service, which can be likened to a community Private Branch Exchange (PBX), effectively partitions part of its own centralized capabilities among its business customers. The customer is spared the expense of having to keep up with fast-moving technology changes (e.g., having to continually update its PBX infrastructure), and the phone company has a new set of services to sell.

CNMS. A Customer Network Management System CNMS refers to a system that allows a customer to access information concerning its specific network. Customer Network Management Systems vary from simple view access to very complex management tools that allow customers to modify parts of their network or billing interactively.

CPE. Customer Premises Equipment refers to equipment residing on the customer's premises that is necessary for access to the Wide Area Network (WAN) or Public Switched Telephone Network (PSTN). Examples of CPE include but are not limited to routers, PBX systems, Internet appliances, and firewalls.

CRM. Customer Relationship Management is an information industry term for methodologies, software, and usually Internet capabilities that help an enterprise manage customer relationships in an organized and effective way. For example, an enterprise might build a database containing information about its customers that described relationships in sufficient detail so any internal employee could access information, match customer needs with product plans and offerings, remind customers of service requirements, know what other products a customer had purchased, and so forth. Many companies also employ CRM systems to provide information directly to customers.

DDOS. DDOS refers to a Distributed Denial Of Service attack on a computer system. The attacker essentially floods the target system with incoming messages or requests, causing it to overload and deny service to legitimate users.

DES. Data Encryption Standard is a widely used method of data encryption using a private (secret) key that the US government judged so difficult to break that it was restricted for exportation to other countries. DES is the single step replicated in triplicate when employing 3DES. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

DiffServ or DS. Differentiated Services is a protocol for specifying and controlling network traffic by class so that certain types of traffic receive precedence over other traffic types. Using DiffServ, voice traffic might get precedence over other kinds of traffic such as data traffic, which is more delay tolerant.

DIY. Do-It-Yourself refers to internally developed resources or systems. DIY resources are also referred to as "Home Grown." Often, DIY systems are the incumbent solution and a major barrier to entry for new systems solutions.

DSL. Digital Subscriber Line is a technology for bringing high-bandwidth access services to homes and small businesses over ordinary copper telephone lines. DSL is categorized into many variations, including ADSL, HDSL, and RADSL, all of which are referred to in general as xDSL. Availability of xDSL services is subject to distance limitations measured from the central office. Based on distance and signal quality, xDSL services can typically range from 128Kbps to 1.544Mbps. In some cases, data rates as high as 6Mbps can be attained. xDSL service is commonly used for broadband Internet access.

ERP. Enterprise Resource Planning refers to the broad set of activities supported by multi-module application software that helps a manufacturer or other business manage the important parts of its business. Dependent on the business, these could include product planning, parts purchasing, maintaining inventories, interacting with suppliers, providing customer service, and tracking orders. ERP can also include application modules for the finance and human resources aspects of a business.

ESP. Encapsulating Security Payload supports both authentication of the sender and encryption of data. The specific information associated with each of these services is inserted into the header of the packet following the IP packet header.

Ethernet. Ethernet is the most widely-installed Local Area Network (LAN) technology. Specified in IEEE standard 802.3, Ethernet was originally developed by Xerox and then developed further by Xerox, DEC, and Intel. An Ethernet LAN typically uses coax or special grades of twisted pair wires. The most commonly installed Ethernet systems are called 10BASE-T and provide transmission speeds up to 10Mbps.

Extranet. An extranet is a network that utilizes the public infrastructure to securely share information and communications between a business and its partners, vendors, customers, or other businesses. Extranets require the use of security devices such as firewalls and encryption to maintain the integrity of the transactions across the public network.

Fixed Wireless. Fixed wireless refers to the operation of wireless connections between fixed locations. In contrast to mobile wireless systems that are generally battery operated, fixed wireless systems use standard utility-grade power sources. Fixed wireless systems can operate at higher bandwidths than mobile wireless.

Frame Relay. Frame Relay is a packet-based transmission technology designed to provide more efficient, cost-effective data transmission for bursty traffic types than private line services. Frame Relay uses variable length packets to traverse a public backbone. Customers subscribe to a Port and a Permanent Virtual Circuit (PVC). The port grants access to the network while the PVC establishes a path across the network. Frame Relay services are available at speeds from 56Kbps to 45Mbps.

Gigabit Ethernet or Gig E. Gigabit Ethernet is a transmission technology based on the Ethernet frame format and protocol used in Local Area Networks (LANs) that provides a data rate of 1 billion bits per second (one gigabit). Gigabit Ethernet is defined in the IEEE 802.3 standard and is currently being used as the backbone in many enterprise networks. Gigabit Ethernet is carried primarily on optical fiber; however, for very short distances, transmission on copper media is possible. Existing Ethernet LANs with 10 and 100Mbps access cards can be connected into a Gigabit Ethernet backbone.

IPSec. Internet Protocol Security is a standard for securing IP transmissions at the network layer. Because the security features are applied at the network layer, IPSec does not require changes to be made to each individual computer.

IP Service Switch. IP service switches are multi-function switches utilized by service providers to expand their IP service offerings. IP service switches allow service providers to deliver value-added services like VPN and firewall on a network-based platform. The utilization of these switches by service providers allows for quicker addition of products to their portfolio, resulting in a quicker realization of revenue.

IP VPN. An Internet Protocol Virtual Private Network is an IP-based network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A Virtual Private Network can be contrasted with a system of owned or leased lines that can only be used by one company.

Jitter. Jitter, which can contribute to latency, is the deviation of some part of an electrical signal. Jitter can be caused by electromagnetic interference and crosstalk.

LAN. A Local Area Network is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area such as a building. Typical LAN technologies include Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI).

Latency. Latency is the amount of time taken by a packet of data to travel from one location to another. Latency is often measured in roundtrip time. While some latency is unavoidable due to processing, propagation, and transmission delays, carriers can control the amount of latency caused by things such as network congestion.

Network-Based Platform. A Network-Based Platform is a services platform, such as a firewall service, that is resident on the service provider network and delivered to the customer premises with little or no additional CPE.

PKI. A Public Key Infrastructure enables users of an unsecure public network such as the Internet to securely and privately exchange data through the use of a public and private cryptographic key pair obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

POP. A Point of Presence is an access point to the Internet or other carrier-based Wide Area Network (WAN) service. A POP has a unique Internet Protocol (IP) address. The Internet Service Provider ISP) or Online Service Provider (such as AOL) has a Point of Presence on the Internet and probably more than one. The number of POPs that an ISP or OSP has is sometimes used as a measure of its size or growth rate. A POP usually includes routers, digital/analog call aggregators, servers, and frequently frame relays or ATM switches.

Private Line. Private Line refers to point-to-point, hard-wired circuits between two fixed locations. While still in use and superior for some applications today, private line services are considered the predecessor to packet technologies such as frame relay, ATM, and IP. Private Lines are capable of any speed and any transmission technology, but much like an extension cord, are only capable of providing service between two fixed points. Private Lines are often referred to as Leased Lines.

PSTN. The Public Switched Telephone Network refers to the global collection of interconnected voice-oriented public telephone networks, both commercial and government-owned. The PSTN also provides the last-mile service to millions of dial-up Internet users.

PVC. A Permanent Virtual Circuit is a software-defined logical connection in a network such as a frame relay network. A primary feature making frame relay a highly flexible network technology is the ability of users (companies or clients of network providers) to define only logical connections and required bandwidth between end points. The frame relay backbone network is responsible for most efficiently utilizing the physical network to achieve the defined connections and manage the traffic.

QoS. On the Internet and in other networks, Quality of Service is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of delay-sensitive traffic such as high-bandwidth video, multimedia services and voice services. Transmitting these types of traffic dependably is difficult in public networks using ordinary best-effort protocols.

RADIUS. Remote Authentication Dial-In User Service is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS is essential in fully securing a network transmission.

SNA. Systems Network Architecture is a proprietary IBM architecture and set of implementing products for network computing within an enterprise. It existed prior to and became part of IBM's Systems Application Architecture and it is currently part of IBM's Open Blueprint. SNA is most widely known for transmission of information between mainframe computing systems. Unlike newer protocols, SNA hosts require regular communications with remote devices, generally achieved through polling.

SOHO. SOHO refers to a market segment including those users in Small Offices or Home Offices. SOHO locations generally support less than 10 users but can be defined slightly differently dependent on other market segments and products.

TDM. Time Division Multiplexing refers to the combination of numerous signals onto one line for transmission. Each separate signal is divided into many short duration packets and sent across the transmission line.

Token Ring. A token ring network is a Local Area Network (LAN) in which all computers are connected in a ring or star topology and a binary digit, or token, passing scheme is used to prevent the collision of data between two computers attempting to send information concurrently. The token ring protocol is the second most widely used protocol on LANs after Ethernet.

VoIP. VoIP refers to Voice over Internet Protocol, or the transmission of voice services using the Internet Protocol. VoIP services can be delivered on either a public or a private IP network backbone or a combination of the two. With VoIP, voice information is sent in digital form in discrete packets rather than in the traditional circuit-committed protocols of the Public Switched Telephone Network (PSTN), which may allow for the avoidance of toll charges generally experienced on the PSTN.

About TeleChoice

TeleChoice is the strategic catalyst™ for the telecommunications industry. Supporting service providers and the technology vendors that serve them, TeleChoice focuses on leading-edge public network technologies. TeleChoice plays a strategic role, enabling our clients to launch new businesses, new markets, and new products and services rapidly and successfully.

Since being founded in 1985, TeleChoice has been differentiated by our proven ability to transform new technologies into successful products and services. Our portfolio of offerings helps our clients conceptualize, launch, market, and exploit the telecommunications market—faster, more efficiently, and more profitably.

About Virtela

Virtela Communications Inc. is a global managed Virtual Private Network (VPN) services and solutions provider that delivers the most cost-effective and secure Internet-based communications between businesses, branch offices, remote workers, and business partners. Founded in April 2000, Virtela is led by industry veterans from Qwest, Sprint, and Global One (now Equant) with extensive experience in the design, delivery, and support of networks and services for multinational corporations and federal agencies. Virtela has received $75 million in equity funding from a diverse set of investors, including Norwest Venture Partners, New Enterprise Associates, Palomar Ventures, RSA Security Inc., Symantec Corp., Juniper Networks, Newton Technology Partners and North Coast Technology Investors.

For more information, please call (720) 475-4000 or visit www.virtela.net.