RESOURCE GUIDE

Ascend

RESOURCE GUIDE

VPN Cost Savings Analysis for the Enterprise

ASCEND

VPN Cost Savings Analysis for the Enterprise

A Resource Guide for Information Technology and Network Managers Worldwide

ASCEND

Where Network Solutions Never End™

Table of Contents

Table of Diagrams

Ascend Communications, Inc. develops, manufactures and sells wide area networking solutions for telecommunications carriers, Internet service providers and enterprise customers worldwide. For more information about Ascend and its products, please visit the Ascend Web site at http://www.ascend.com, or e-mail info@ascend.com.

Ascend markets the B-STDX, CBX, GRF, GX, IP, MAX, Multiband, MultiDSL, Navis, Pipeline, SA, SecureConnect and STDX families of products. Ascend products are available in more than 40 countries worldwide.

I. Executive Summary

Virtual Private Networks, or VPNs, are the future of enterprise networking. The reason is simple: VPNs can cut the operating and management costs of wide area networking in half, while offering substantially greater flexibility and worldwide reach.

The essence of a VPN is its use of the Internet, Frame Relay or ATM networks as a Wide Area Network (WAN) backbone to supplement or replace the costly long-distance leased and dial-up links in a traditional private network. Sending private information via these new public networks – either domestically or internationally – is similar to using the Public Switched Telephone Network (PSTN) for internal communications, or sending confidential correspondence by mail. Enterprises can benefit tremendously by using these new, more advanced public networks, which are operated and managed by Internet Service Providers (ISPs) and carriers.

Ascend has developed the industry's most comprehensive VPN strategy with its MultiVPN™ solutions. MultiVPN leverages the presence and power of the new public network with a choice of services and options that make VPNs suitable for a wide range of commercial networking needs. MultiVPN from Ascend allow companies to:

- Replace existing private network segments, subnets or entire wide area topologies
- Supplement private networks by offloading certain applications or meeting backup/overflow needs
- Increase the overall stability and reliability of the enterprise network
- Add new applications without disrupting the existing private network
- Extend the reach of corporate communications by adding new geographically-dispersed locations quickly and easily, especially international sites, which could otherwise take months to bring on-line
- Offer remote access for traveling employees and full/part-time telecommuters
- Provide internetworking for all branch offices and divisions
- Create extranets with buyers and suppliers

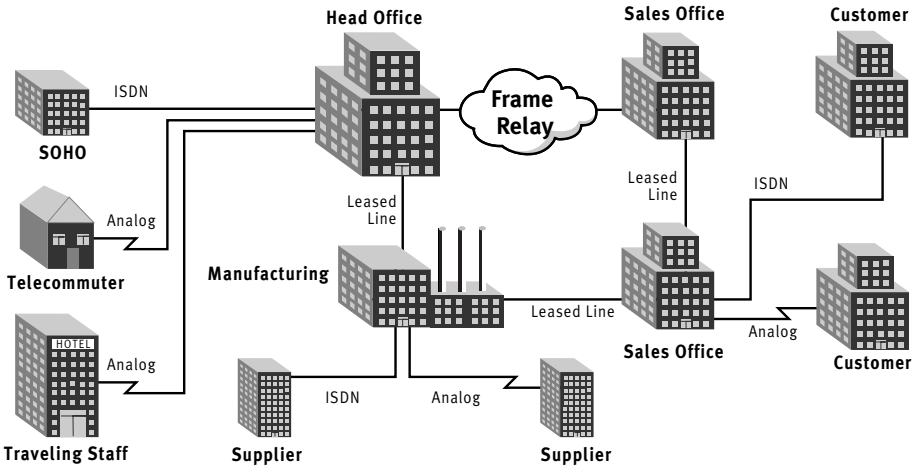
MultiVPN from Ascend

Ascend is the first vendor to break down the remaining barriers to widespread VPN adoption in a strategy that matches private enterprise-wide needs with carrier-class public network services. Ascend's enabling MultiVPN strategy, with its visionary provider/subscriber approach and broad interpretation of VPNs, has three equally important dimensions:

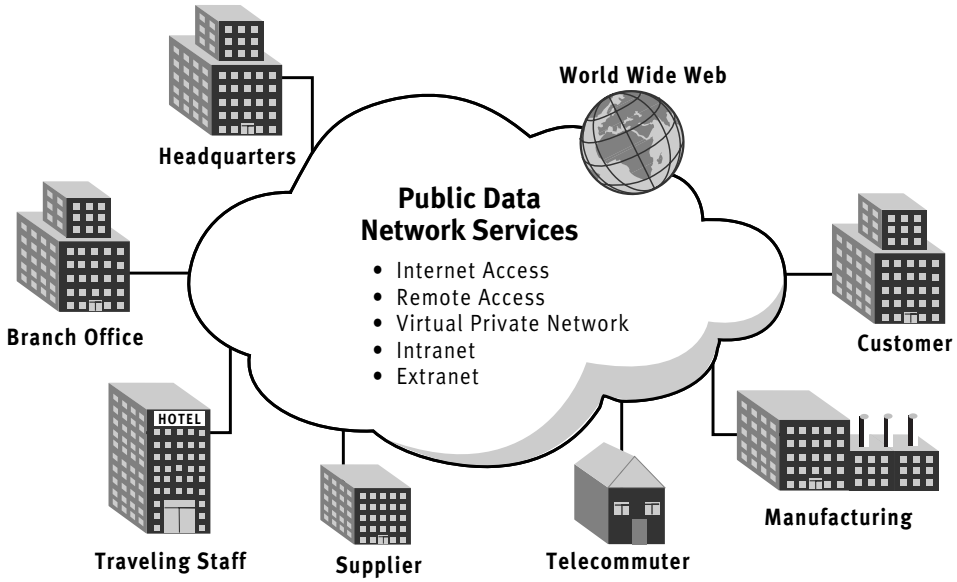
- *Creating the industry's first comprehensive set of fundamental VPN architectures that can utilize IP, Frame Relay and/or ATM services seamlessly*
- *Overcoming the concerns organizations have regarding enterprise-wide VPNs, including compatibility, security, availability and manageability*
- *Satisfying the unique needs of service providers responsible for the infrastructure*

MultiVPN adds special capabilities to the public network infrastructure, and enhances enterprise equipment to take full advantage of these new services. Of particular appeal to the enterprise is MultiVPN's broad compatibility with popular enterprise applications, robust security, Quality of Service and Service Level Agreement performance guarantees, and VPN-oriented Customer Network Management, which is able to manage the entire VPN, including the private portions of the public network infrastructure.

Private vs. Virtual Private Network



Today's Typical Enterprise Network



The Enterprise Network of the Future

Figure 1 – A VPN replaces the complex and expensive private network topology with a single, cost-effective per-site connection to access a private enterprise network, the semi-private extranet with buyers and suppliers, and the public Internet.

MultiVPN Benefits for the Enterprise

- *Lower costs – from 30 to 80%, according to industry analysts and real-world experience – for data networks and, optionally, voice/video/fax telecommunications*
- *Achieve high reliability through the carrier-class redundancy and resiliency of the public network infrastructure*
- *Increase flexibility and simplify operations with a single per-site connection to the enterprise network, an extranet and the Internet*
- *Maximize interoperability using IP-based extranets with buyers and suppliers*
- *Leverage enhanced and expanded services unavailable in the PSTN, such as multicast for any-to-many communications*
- *Gain control in and through the public network with the power of VPN Customer Network Management (CNM)*

VPNs offer substantial savings over PSTN-based private networks. Here are projections by three leading industry analyst firms:

- Infonetics Research estimates a savings of 20-40% for branch office VPNs and 60-80% for remote access VPNs. Infonetics believes that, by 2001, one-third of US remote access users and one-quarter of branch offices worldwide will use a VPN, and that over 90% of extranets will be implemented using VPNs.
- Gartner Group expects VPNs to offer a savings of at least 50% for remote access and, owing to this substantial savings, 70% of Fortune 500 companies will use VPNs for remote access by 2003.
- Forrester Research found the following 60% savings when comparing private and virtual private solutions for a 2000-user remote LAN access network:

	Private Network	VPN
T1 Lines	$48,000	$68,400
Routers & Servers	208,000	44,800
Phone & ISP Charges	2,160,000	1,080,000
User Support	600,000	(Included) 0
TOTAL	$3,016,000	$1,193,200

Note the major savings in three distinct areas: equipment consolidation (“Routers & Servers”); elimination of long-distance services (“Phone & ISP Charges”); and management expenses (“User Support”). The only area where VPN costs are higher is the local access lines, which need to operate at a higher data rate with the consolidation to single line access for the Internet, the extranet and intranet VPN.

Real-world experience confirms these anticipated cost savings. One company achieved a 67% savings with a remote access VPN for 150 users. The private network had a monthly operating cost of $48,000 with usage of 2 hours/day per user. With the VPN, monthly operating costs decreased $30,000 to only $18,000 – a savings of $360,000 per year. Another company reported an annual savings of $252,000 for a 100-user remote access VPN. By taking advantage of $19.95/month unlimited Internet access, yet another organization was able to save a whopping 78%, primarily by eliminating long-distance charges. For companies that already provide such Internet access for employees, the user side of a remote access arrangement is effectively "free" with a VPN!

VPN Paybacks and Benefits

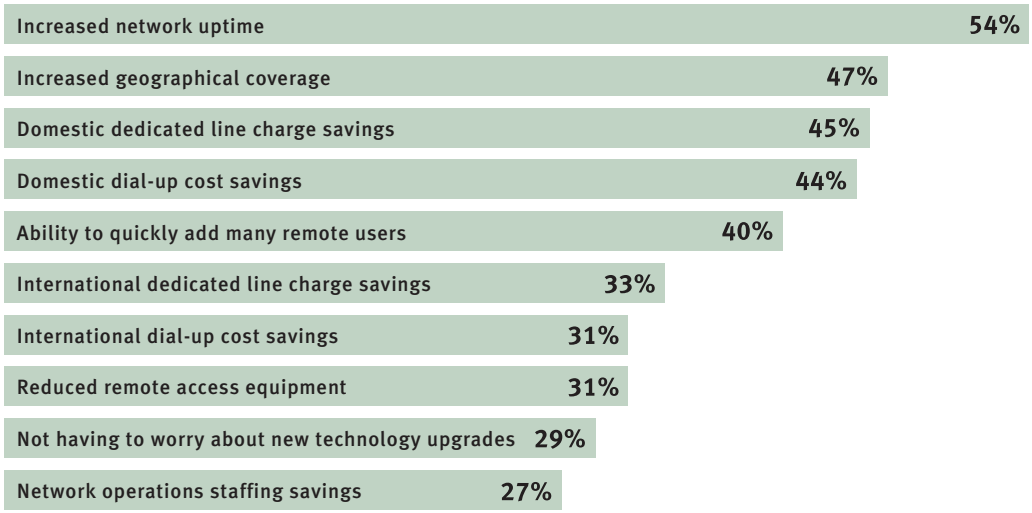


Figure 2 – An April 1998 Infonetics Research survey of enterprise organizations revealed these many additional advantages of a VPN.

In these and other examples, there are two general conditions that strongly favor use of an Internet-based VPN: First is the existence of numerous locations, including both individual users and multiuser offices. Second is when these users/sites are spread across long distances, especially multinational locations. If your organization has a wide area networking application that meets these criteria, you have an ideal candidate for a VPN.

This guide will help you estimate the cost savings your organization could realize with a Virtual Private Remote Network (VPRN), which utilizes the Internet for the VPN's backbone. The analysis covers two popular VPN applications: remote LAN access and branch office internetworking. There are, of course, other applications for VPNs and other ways Ascend's MultiVPN solutions leverage the public network infrastructure, both of which may provide additional savings or advantages.

The discussion begins with an overview of the options and considerations involved in planning a VPN. The analysis section investigates both initial equipment expenditures and on-going operating costs. Because VPN equipment is priced about the same as similar systems used in private networks, focus is placed where the savings are: the major on-going costs of WAN services, and the management of all connections and equipment.

The analysis employs a useful "VPN Cost Savings Worksheet," developed by Ascend, for estimating the operating cost of a VPN. The worksheet also compares the operating cost of the VPN with that of an existing, equivalent private network. A "typical" example is offered to outline the methodology.

Finally, at the end of the document in the appendix, is a list of additional resources available from Ascend and others for learning more about VPNs. A printout of the basic VPN Cost Worksheet and an overview of Ascend's MultiVPN product offering are also included in the appendix.

VPNs are indeed the future of enterprise networking. The sooner your organization begins migrating to a VPN for part or all of your needs, the sooner you will be able to achieve the cost savings and other advantages of a VPN.

Ascend's Credentials

Ascend's expertise in VPNs derives from the company's many strengths and achievements:

- *Broad experience in the deployment, utilization and management of public networking solutions with 28 of the 30 largest ISPs using Ascend solutions and nearly 5 million ports installed worldwide*
- *Comprehensive family of field-proven VPN products with industry-leading features and international certification for worldwide interoperability*
- *High degree of integration, including built-in firewall to simplify installation, operation and management*
- *Tremendous flexibility with a choice of VPN architectures, equipment configurations, security provisions, performance guarantees and management techniques*
- *Quality of Service (QoS) and Service Level Agreement (SLA) assurances guaranteeing all three dimensions of availability: throughput, latency and uptime*
- *Powerful VPN Customer Network Management (CNM) that lets enterprises and their service providers jointly, completely and securely manage the end-to-end VPN*
- *Delivery of "multimedia" VPNs that integrate voice, fax, video and data communications, including the any-to-many capability of IP multicast*

II. VPN Options and Considerations

With anything new, there is a certain element of risk. For VPNs, that risk can be reduced substantially – and potentially eliminated – by paying careful attention to these four critical areas: compatibility, security, availability and manageability.

Compatibility with existing applications is crucial. While the Internet protocol (IP) is becoming increasingly popular for commercial applications, many continue to use long-established protocols like SNA, IPX and NetBEUI, among others. Even when IP is used, the address scheme is often private (unregistered addresses, such as 10.x.y.z), making the enterprise IP application incompatible with the public Internet.

Unlike other VPN solutions that provide tunneling alone, Ascend's MultiVPN solutions afford three fundamental ways to achieve compatibility, each defining a basic architecture for a VPN:

- ***Virtual Private Remote Networking*** (VPRN) employs multiprotocol tunneling to make the public Internet compatible with private IP and many non-IP applications. Popular tunneling protocols include: the Point-to-Point Tunneling Protocol (PPTP), created in a strategic partnership between Ascend and Microsoft; the Layer 2 Tunneling Protocol (L2TP), an industry standard based on PPTP; and the Ascend Tunnel Management Protocol (ATMP), an enhanced implementation of standard Generic Routing Encapsulation (GRE).
- ***Virtual Private Trunking*** (VPT) makes the powerful capabilities of Frame Relay and ATM switches in the new public network infrastructure available directly to the enterprise VPN. VPT goes beyond traditional virtual circuits, permanent and switched, to make the VPN compatible with most higher layer protocols and more suitable to enterprise needs. Existing Frame Relay users may want to check with their service provider(s) to learn more about the benefits and availability of Virtual Private Trunking.
- ***Virtual IP Routing*** (VIPR) extends private route tables and address spaces from the enterprise into the public network. Essentially, a virtual IP router is a logical partition of a physical IP router or switch in the service provider's infrastructure. Of particular appeal to the enterprise is VIPR's ability to use private IP addresses and create individual broadcast domains.

Variations and combinations of all three techniques can exist in a single VPN. An enterprise-wide VPN, for example, might use VPRN tunneling for remote access by individual telecommuters, and Virtual IP Routing to interconnect all multiuser sites. For sites that have NetWare servers with IPX, tunneling can be combined with Virtual IP Routing. Frame Relay and ATM "trunks" are often more suitable for the largest sites in the enterprise, such as the headquarters and major divisions. The service provider will need to interface the various networks to one another, but having done so, the VPN operates transparently to all users and sites thereafter.

What Constitutes a VPN?

A VPN is a private network that utilizes the public network infrastructure. Of course, all enterprise networks use some public services. Historically, such capabilities were available only in the Public Switched Telephone Network(PSTN). But the PSTN was designed for voice communications, making it increasingly unsuitable – and expensive – for today's demanding applications. VPNs, therefore, generally refer to private networks that employ newer public network technologies, such as the Internet (IP), Frame Relay and Asynchronous Transfer Mode (ATM). Organizations that have begun migrating to Frame Relay from leased and dialup PSTN services already have a VPN, although they may just consider these segments to be part of the "private network." Eventually, the need for the term "VPN" will diminish as enterprises become more comfortable with the newer public network services. In the meantime, however, there is a need to distinguish "private networks" (that use the Public Switched Telephone Network, and according to some, public Frame Relay services) from "virtual private networks" (that use the new public network technologies designed to handle data communications more effectively – and affordably).

Security is often cited as the primary concern regarding VPNs. By taking the necessary precautions, however, a VPN can be made just as secure as any private network, and even more secure than most.

The foundation of VPN security is the firewall. A firewall passes only authorized traffic for all trusted users, and blocks everything else. In other words, all unknown or untrusted users are denied access, and the two-way traffic of trusted users is screened to ensure it is expressly permitted. This important form of protection must be provided for every user and site, even when Virtual Private Trunking or Virtual IP Routing services are employed. Why? Because if you don't have security everywhere, you don't have security anywhere. Just as a chain is only as strong as its weakest link, so too is a VPN security system.

While the firewall is the only essential element of VPN security, several additional provisions are available, including:

- IP Security, or IPSec, with packet encryption and digital signatures for data confidentiality, integrity and authenticity, along with key management for administering security policies
- Virtual IP Routing's separate route tables and closed user groups for another layer of protection for private traffic
- Virtual Private Trunking's inherent security, with its use of dedicated resources, isolates VPN traffic from all other traffic in the public network
- Single- and two-factor token authentication hardware and software mechanisms utilizing secret passwords and dynamically changing passcodes
- Security systems at Internet Service Provider (ISP) Points of Presence (POPs), such as PAP, CHAP, Calling Line ID (CLID), Dialed Number Information String (DNIS) and others

Availability has three equally important dimensions: throughput, latency and uptime. Guarantees for one or all three are available from most service providers. Quality of Service (QoS) assurances normally cover throughput, including maximum packet loss, and a not-to-exceed latency. A Service Level Agreement (SLA) assures a specified minimal uptime, typically in excess of 99 percent. Some service providers reduce monthly fees proportionately whenever QoS and/or SLA performance falls short of contractual levels.

An often overlooked performance factor with VPNs is the overhead associated with tunneling, encryption and authentication, all of which add to packet length and take time to process. The overhead may be negligible, but for an existing link that is already saturated, selecting a slightly higher data rate for the VPN connection may be prudent.

Interestingly enough, early adopters of VPNs have found that this concern actually turns into an advantage. The number one benefit they cite of migrating to VPNs is improved network reliability. Considering how much simpler VPN configurations are, such a result should be expected. The simpler configurations also makes management easier.

Manageability should not be taken for granted with a VPN, however. VPNs do minimize the management burden placed on the enterprise. But to achieve the full potential of a VPN – complete with satisfaction for all users and peace of mind for network managers – the enterprise should participate in managing the end-to-end configuration jointly with the service provider(s). Such joint control is available with Customer Network Management (CNM) gateways in the service providers' infrastructure. Through the familiar Web browser interface, CNM gives the enterprise a real-time, around-the-clock window into the infrastructure to view, monitor, reconfigure, troubleshoot and otherwise manage its entire VPN, including its private portion of the public network.

VPN Building Blocks

There are, essentially, five building blocks in any VPN:

- The service provider's backbone or the Internet itself
- The network access switch at the service provider's POPs
- Equipment at the enterprise sites
- Local WAN services connecting enterprise sites to POPs
- The management applications and tools

VPN Building Blocks

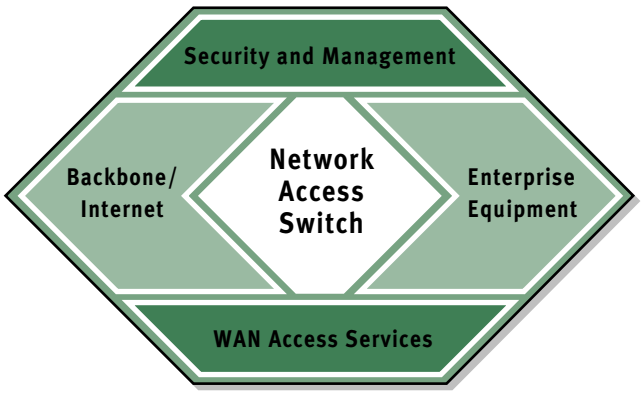


Figure 3 – Every Virtual Private Network is made up of these five fundamental building blocks.

To keep the various considerations at a high level, the network access switch and backbone elements are combined into "service provider facilities" and local WAN services are ignored, leaving three critical elements. Local WAN services are, however, included in the cost calculations in the next section. Presented here are considerations and a comprehensive checklist for each of the three critical elements.

Enterprise Equipment

Four alternatives exist currently for VPN-capable equipment for the enterprise: separate firewalls; router "add-ons"; server-based adapter cards; and fully integrated solutions.

Separate firewalls have the advantage of leveraging the existing private network configuration, and are ideal for individual users with modems. But the potential up-front savings can increase long-term management costs. Central site firewalls can be quite expensive and require a dedicated server, both of which minimize any up-front savings. And because some solutions offer limited integration with authentication systems, directory services, tunneling, encryption and QoS/SLA facilities, the organization may be unable to optimize its VPN configuration and performance. While a firewall is an essential element of any VPN, a firewall in and of itself does not constitute an enterprise VPN.

Router "add-ons" also attempt to leverage the existing private network. These devices can be installed either on the LAN side or the WAN side of a router. Most merely add tunneling and/or IPSec packet encryption/authentication. But just as with the firewall-based VPN, this approach adds more devices to the network, thereby increasing the long-term management costs. There is little integration with the router or separate firewall, so initial configuration and troubleshooting tasks can become quite complicated.

Server-based adapter cards are similar to router add-ons. The idea here is to use the NOS server as a VPN gateway or router. While such a configuration may be acceptable for a limited number of users, it is difficult to secure and almost impossible to scale. The processing burden of routing, tunneling, encrypting, authenticating and firewalling – all on a general-purpose PC platform – requires substantial system resources. As a result, the server must often be dedicated to VPN communications, making it an expensive attempt at a fully integrated solution.

Fully integrated systems are the only viable alternative for business-critical VPNs. The single device replaces a conventional WAN router with a VPN-capable router that integrates a firewall, tunneling, authentication, IP Security provisions and network addressing support, including RADIUS, TACACS+, Network Address Translation (NAT) and the Dynamic Host Configuration Protocol (DHCP). These systems cost little more than a conventional WAN router, allowing users to create "VPN-ready" private networks to facilitate a site-by-site migration to an enterprise-wide VPN. Systems are available for both individual users (typically ISDN BRI at 128 Kbps) and multiuser offices (at speeds up to 6.144 Mbps with multirate T1).

Important Features for Enterprise Equipment

Here is a checklist of required and desired features found in fully integrated VPN-capable routers. A VPN router is needed for all multiuser sites; special models are designed for small office/home office (SOHO) environments and full-time telecommuters.

- *Support for multiprotocol L2TP, PPTP and ATMP tunneling*
- *IP Security (IPSec) provisions add packet encryption and authentication to multiprotocol tunneling, or can be used for its own IP tunneling capabilities*
- *Integrated and certified dynamic firewall protection*
- *Software upgradable to conform with emerging VPN standards*
- *Remote download of software upgrades, via the VPN*
- *Robust local and remote management to maximize uptime at minimal cost*
- *Adequate capacity to handle anticipated traffic volumes*
- *An Ethernet LAN interface for attaching to the local network*
- *Support for the most cost-effective local WAN option desired, such as T1/E1, ISDN PRI/BRI, xDSL, X.25, Frame Relay and ATM*
- *Optional dial-up backup and overflow bandwidth for large and/or critical sites to maintain communications in the event of VPN saturation or failure*
- *Built-in compression to maximize throughput, and dynamic bandwidth management for enhanced performance*
- *Ability to accommodate IP multicast applications, like Internet audio and video*
- *Compatibility with any advanced capabilities offered by the service provider's facilities (see the checklist on page 12) to magnify the benefits of a VPN*
- *Compatible family of scalable products to suit a variety of site types and sizes*
- *Certification for operation with local carriers*

Note: Modem users, especially mobile workers, will need a software-based firewall. Ideally, the firewall will be certified and integrated with IPSec encryption and authentication provisions, and will be compatible with the PPTP tunneling that is now included with the Windows 95 and above operating systems.

Service Provider Facilities

Service provider facilities, which include both the POP and backbone building blocks, become the wide area network for the VPN. As such, it is vitally important to evaluate service providers thoroughly. The right service provider will maximize the flexibility of the VPN, with a full spectrum of alternatives ranging from support of in-house designs to fully outsourced solutions.

Enterprise/Service Provider Relationship Responsibility[1]

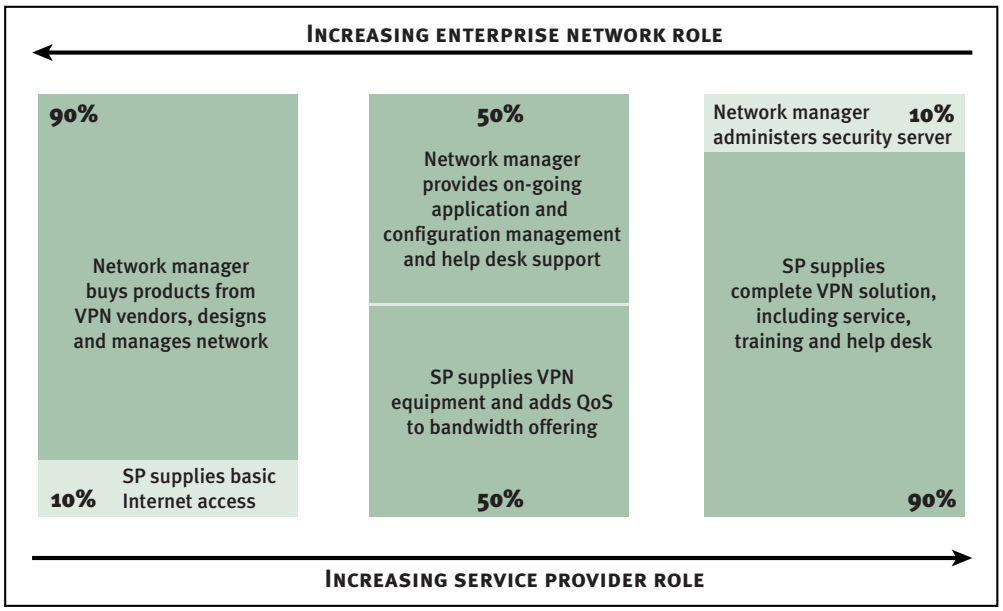


Figure 4 – Selecting the right service provider affords tremendous flexibility in the operation and management of the VPN. Start by managing the VPN mostly in-house, for example, then gradually turn over this responsibility to the service provider.

[1]Exhibit 5 of Infonetics Research, Inc. Partnership Report

Service Provider Evaluation Criteria

When evaluating service providers, be sure to investigate the following capabilities:

- Choice of VPN architectures: Virtual Private Remote Networking, Virtual Private Trunking and Virtual IP Routing
- Comprehensive security provisions, including Proxy RADIUS, IPSec encryption and authentication, closed user groups, and logical segmentation of physical resources
- Support for L2TP, ATMP, PPTP and IPSec tunneling to accommodate existing protocols and applications
- Service Level Agreement (SLA) uptime guarantees and confirmation reporting
- Tiered Quality of Service (QoS) options ranging from "best effort" to an "absolute" guarantee of throughput and latency
- End-to-end monitoring, operating and troubleshooting capabilities (see checklist on Customer Network Management, page 13)
- Value-added features such as Voice over IP (VoIP) and IP multicast
- Value-added services, including consulting, design, systems integration, on-going support, extranet management, data backup, Web hosting and electronic commerce
- State-of-the-art technology based on industry standards for maximum compatibility, flexibility and performance
- POP locations near all users and sites, or national/international "roaming" agreements with other service providers, to eliminate or minimize long-distance calls
- Central site or distributed pricing and billing arrangements, including bundled and managed service offerings
- Long-term financial stability and viability

VPN Management

Management of VPNs is normally a shared responsibility between the service provider and the enterprise organization (the subscriber). The subscriber must be able to manage its own equipment and its virtually private portion of the provider's network, including all system resources and links. Specific tasks involve the installation, configuration, monitoring and troubleshooting of the network equipment and all interconnections.

A capable provider/subscriber Customer Network Management (CNM) system should possess the following features for managing the total VPN:

- Utilization of a Web browser interface for intuitive ease of use that minimizes training requirements
- Robust partitioning and security measures, including the ability to set read (monitor only) or write (monitor and control) access to all databases and network equipment status registers
- Auto-discovery and dynamic mapping of the end-to-end network topology with both physical and logical groupings of all equipment and links
- Real-time network monitoring of physical and logical WAN links and traffic conditions, with fault alert/alarm generation based on user-defined thresholds
- Monitoring that offers a way to assess actual throughput on WAN lines to help control delivery of contracted Quality of Service (QoS) and Service Level Agreements (SLAs)
- Capacity planning and performance trending through collection and analysis of traffic statistics that show both the level and patterns of usage by all users/sites
- Base-lining of normal operating conditions to help determine overall network "health" and for capacity planning needs
- Integrated, statistical accounting to track network traffic by user/department/site for billing, accounting, auditing or other purposes
- Remote configuration management for bringing new locations on-line, as well as coordinating network-wide updates and changes
- A means of comparing actual vs. intended equipment configurations
- Traditional device-oriented fault detection and diagnostics for pinpointing and troubleshooting specific equipment problems
- A trace function that tracks traffic through the network, end-to-end, to help isolate bottlenecks and other problems
- A way to examine the WAN's Physical and Data Link layers, as well as assess actual throughput of dial-up and dedicated WAN links
- RADIUS, TACACS and TACACS+ database support for maintaining the security profiles for all VPN members

III. Estimating VPN Cost Savings

This section assesses the overall VPN costs and cost savings in two typical project phases: the initial equipment expenditure and the on-going operating expenses. A qualitative analysis is given first for each, followed by a quantitative example. The VPN Cost-Savings Worksheet used in the example is included for making your own estimate.

Economies of Scale Make VPNs Less Expensive

Modem banks became obsolete with the advent of digital access concentrators. The access concentrator affords both operating and management efficiencies that cut remote LAN access costs in half. VPNs take these economies of scale to the next level with carrier-class access concentrators supporting thousands of ports and tens of thousands of users. Individually, very few enterprises could justify such an expenditure. But collectively, through VPNs, enterprises are finding they can cut their costs in half with a more capable and reliable solution.

Initial Equipment Expenditure

The table below shows how VPNs can save money from the outset. The total remote networking needs of the enterprise involve site-to-site internetworking, remote LAN access for telecommuters and mobile workers, Internet access for all employees, and optionally, an extranet with buyers and suppliers. With a VPN, the enterprise gets everything in a single connection for each site/user. By consolidating and eliminating equipment, a VPN minimizes both the initial expenditure and the on-going system maintenance costs.

Private Network vs. VPN Equipment Requirements

	Private Network	VPN
Headquarters		
Site Internetworking	Multiport WAN Router	**Single Router with Integral Firewall**
Remote LAN Access	Access Concentrator	
Internet Access	Separate Router and/or Firewall	
Buyer/Supplier Extranet	Separate Router and/or Firewall	
Division or Branch Office		
Internetworking	WAN Router	**Single Router with Integral Firewall**
Remote LAN Access	Modem Bank or Small Access Concentrator	
Internet Access	Separate Router and/or Firewall	
Buyer/Supplier Extranet	Separate Router and/or Firewall	
SOHO or Individual User		
Full-time Telecommuter	ISDN Router	**Same as Private Network With the Addition of Software-based Firewalls**
Part-time Telecommuter	Modem or ISDN Router	
Mobile Worker	Modem	

Figure 5 – Private networks require more equipment – and are, therefore, substantially more complex – than the equivalent single-connection-per-site VPN.

As mentioned earlier, the cost of a VPN-capable WAN router is no more than a conventional router, which helps underscore the importance of building "VPN ready" private networks in preparation for the inevitable. When ready to implement the VPN – now or in the near-term future – the VPN-specific options, such as a firewall, tunneling and IPSec provisions, can normally be added through software upgrades to the router.

VPNs also help save on configuration changes, upgrades, enhancements and additional expenditures over time because the new public network's global power and presence makes VPNs tremendously flexible. With a VPN, enterprises can:

- Add and delete connections instantaneously (including those locations where companies are on waiting lists to get private network lines)
- Provide permanent, periodic or temporary connectivity as needed
- Integrate third-party users, such as customers and suppliers, almost effortlessly

Other implementation-related costs (not addressed here, but important to mention) include obtaining a block of IP addresses, conducting a VPN pilot, training, planning, account set-up fees, installation, configuration and troubleshooting expenses.

On-going Operating Expenses

The on-going operating expenses of any network, private or virtually private, constitute approximately 80% of the total cost of ownership. The two major on-going expenses are WAN services and network management. Facilities, such as equipment space, and Heating, Ventilation and Air Conditioning (HVAC), also create an on-going expense, which is substantially less than either WAN services or network management. As the table below shows, VPNs offer savings in all three areas. Note that two costs are slightly higher (at some sites) with a VPN: the Internet connection and its associated local access fee. Both result from the need for more bandwidth to handle the consolidation of Internet, intranet and extranet applications.

	Private Network	VPN
Network Services		
Local Access (at each end) Leased Line		The Same or Slightly to More Expensive with VPNs
Leased Line (IXC or LEC)	Major Expense	Eliminated with VPN
Dial-up Monthly and Usage Fee		Same as Private Network
Dial-up Long Distance Charges	Major Expense	Eliminated with VPN (Possible Roaming Fees)
Internet Connection(s)	Required[1]	More Expensive with VPNs
Management/Support		
Network	Major Expense	Much Less with VPN
User		Less with VPN[2]
Facilities		Less with VPN

[1] *Internet connections are generally required for all users and sites in the enterprise today, so this expense should be included in the cost of a private network.*

[2] *Some user support (basic network connection) can be outsourced to service providers; enterprise applications continue to be supported by the organization.*

Figure 6 – VPNs eliminate or minimize the major on-going expenses of enterprise networks.

WAN Services

VPNs minimize WAN service fees primarily because – with service providers in nearly every city worldwide – they eliminate long-distance leased and switched connections. The only need for these expensive services is optional dial-up backup and overflow bandwidth for the VPN, which is only needed when the VPN is overloaded or fails. Local WAN access charges (from the enterprise site/user to the service provider's POP) are relatively inexpensive, and are only slightly higher at those VPN sites needing higher speed access. So the big difference is in the distance – and that difference can be substantial.

VPNs help reduce WAN service charges for these additional reasons:

- Individual users with existing, unlimited $19.95 Internet access effectively get VPN/intranet and extranet access for "free"
- Consolidation of multiple access links into higher speed lines offers superior price/performance
- Optimal data rates – ranging from analog modem to T1/E1 speeds, and beyond with Digital Subscriber Line technology – eliminate oversubscription
- Usage-based services minimize costs for low volume sites/users
- Expensive redundancy and mesh topologies can be eliminated while maintaining high end-to-end reliability

Network Management

The International Data Corporation estimates that one support technician is required for every 60 LAN-attached users, whereas one technician can support only half as many, or 30, remote users. These ratios take into account user support for the PC, all applications and the network. The major reasons for this two-to-one difference include additional network complexity, reduced economies of scale and the need for users to participate in the sometimes-sophisticated problem resolution process. VPNs can alter the ratio to the point where supporting remote users involves the same effort as supporting local users, effectively cutting these costs in half.

Strategic Networks Consulting conducted a separate study of just the network portion of remote user support, which is more relevant to the comparison in this analysis. The average ratio of users to support personnel is 90:1. In other words, one support technician can support an average of 90 users.

VPNs enhance staff productivity, either to handle existing users with a smaller staff or accommodate growth with existing personnel, in the following ways:

- VPNs present fewer problem scenarios and minimize end-user network design, operation and management responsibilities
- With intuitive browser-based Customer Network Management, technicians are required to master a smaller set of management tools
- Reconfiguration of a VPN and individual user capabilities can be accomplished almost exclusively in software (rather than hardware) via the network management console
- The VPN's integration – with a single system and a single connection for Internet, intranet and extranet – simplifies the task
- Service providers normally provide user support for basic network connectivity, much like an outsourcing arrangement, leaving the enterprise responsible only or primarily for company-specific applications
- Familiarity with Internet access minimizes training needs and equips users to participate more productively in problem resolution
- The emerging "universal" browser interface further minimizes user applications-level support

VPNs do involve some special responsibilities, such as administration of IP addresses and VPN membership profiles. But tools like NAT and RADIUS minimize the effort, which is no more complex than handling similar tasks in a private network.

Facilities

Finally, although dwarfed by WAN service and management costs, the elimination and consolidation of equipment in a VPN leads to a corresponding reduction in space, power and HVAC needs.

Quantitative Example

This section compares the on-going costs of a "typical" private network with the equivalent virtual private network. Applications include site internetworking, remote LAN access and Internet access. For the sake of simplicity, there is no extranet with buyers or suppliers. The network is enterprise-wide with two international sites, 50 domestic branch offices (totaling 3350 remote users) and 500 domestic dial-up users as follows:

- The Headquarters
- 2 International Sites (with 100 users each)
- 5 Major Divisions (with 500 users each)
- 10 Large Branch Offices (with 50 users each)
- 35 Small Branch Offices (with 10 users each)
- 50 Single-user Small Office/Home Offices
- 100 Full-time Telecommuters
- 350 Part-time Telecommuters and Mobile Workers

As with any quantitative cost comparison, circumstances and service rates vary substantially from company to company and from location to location. Nevertheless, the methodology is accurate and universal. Please let this example serve as both a realistic comparison and a model for conducting your own evaluation of VPN cost savings.

The Private Network

The on-going costs of the hypothetical private network are outlined in the table, showing all assumptions and WAN service fees. All costs are monthly unless otherwise indicated.

Site/User	Local WAN Access	Long-distance	Internet Access
Headquarters	$7000 (10 T1 lines at $700 each)	N/A (Charged to remote users/sites)	$3500 (for LEC and ISP T1 access)
5 Major Divisions	$3500 ($700 T1 line at each site)	$25,000 ($5000 T1 line for each site)	$8000 ($1600 for LEC and ISP 128 Kbps FT1 access per site)
2 International Sites	$4000 ($2000 E1 line at each site)	$7,000 ($3,500 E1 line for each site)	$8000 ($4000 for PTT and ISP 128 Kbps access per site)
10 Large Branch Offices	$4000 ($400 128 Kbps FT1 line at each site)	$21,000 ($2100 128 Kbps FT1 line for each site)	$12,000 ($1200 for LEC and ISP 64 Kbps FT1 access per site)
35 Small Branch Offices	$2975 ($85 ISDN BRI line at each site)	$33,600 ($960 for 8 hours/day at 10¢/minute for each site)	$4725 ($135 for LEC and ISP ISDN BRI access per site)
50 SOHO	$4250 ($85 ISDN BRI for each site)	$18,000 ($360 for 3 hours/day at 10¢/minute for each site)	$2500 ($50 for ISP only for ISDN BRI access per site)
100 F/T Telecommuters	$8500 ($85 ISDN BRI line for each user)	$36,000 ($360 for 3 hours/day at 10¢/minute for each user)	$5000 ($50 for ISP only for ISDN BRI access per user)
350 P/T Telecommuters & Mobile Workers	$12,250 ($35 POTS line for each user)	$42,000 ($120 for 1 hour/day at 10¢/minute for each user)	$7000 ($20 for ISP only for modem access per user)
Monthly Subtotals	$46,475	$182,600	$50,725
Annual Totals	**$557,700**	**$2,191,200**	**$608,700**

Management for the above network, including user support, is estimated to be $2,880,000 per year, or $240,000 per month, reflecting an around-the-clock staff of 45 at an average burdened cost of $64,000/year each to support the 4050 remote users. Note that the ratio of users to support personnel is approximately 90:1 to cover only the network-related costs, and not the total costs of user support (which include the PC and all applications).

The total annual operating cost of this network (including local and long-distance charges, Internet access and network management) is $6,237,600, or about $1540/user.

The Equivalent VPN

The table below shows the initial cost of configuring each site and user with a fully integrated VPN solution. The configuration for each site may include many of the following: an integrated firewall (Ascend's Secure Access™), tunneling, and authentication (included with the Secure Access Firewall), and all necessary management agents and applications.

Site/User	Equipment Needed	Initial Expenditure*
Headquarters	MAX TNT (FT3 @ 15 Mbps) with Access Control and NavisConnect	$93,745
2 International Sites	MAX 6000 (E1)	$38,070
5 Major Divisions	Pipeline 220 (T1)	$33,725
10 Large Branch Offices	Pipeline 130 (FT1 @ 128 Kbps)	$29,950
35 Small Branch Offices	Pipeline 50 (ISDN)	$48,825
50 SOHO	Pipeline 85 (ISDN)	$79,750
100 F/T Telecommuters	Pipeline 75 (ISDN)	$149,500
350 P/T Telecommuters and Mobile Workers	Intragy Access (with Secure Connect client)	$26,500
TOTAL		**$500,065**

**Pricing based on sample configurations and is subject to change.*

The results from the VPN Cost-Savings Worksheet for this example are shown below.

	WAN	ISP	Monthly Costs	Annual Total
Existing Private Network				
WAN Services (LEC & IXC)			$229,075	$2,748,900
Internet Access (ISP)			$50,725	$608,700
WAN/User Management			$240,000	$2,880,000
Total Annual Cost (Existing Private Network)				**$6,237,600**
Proposed VPN (Site/User Connections)				
1 Fractional T3 (15 Mbps)	$8,000	$14,000	$22,000	$264,000
2 E1 (2.048 Mbps)	$2,000	$4,000	$6,000	$144,000
5 T1 (1.544 Mbps)	$700	$2,800	$3,500	$210,000
10 Fractional T1 (256 kbps)	$450	$1,700	$2,150	$258,000
35 Fractional T1 (128 kbps)	$400	$1,200	$1,600	$672,000
150 ISDN BRI (64-128 kbps)	$85	$50	$135	$243,000
350 Modem/POTS (33.6-56 kbps)	$35	$20	$55	$231,000
				$2,022,000
50% VPN/User Management			$120,000	$1,440,000
Total Annual Cost (Proposed VPN)				**$3,462,000**
Estimated Cost Savings				
Annual Dollar Savings				**$2,775,600**
Percentage of Annual Savings				**44%**

The on-going costs of operating the VPN (local WAN service charges, Internet access and network/user management) are provided by completing the VPN Cost-Savings Worksheet.

As indicated by the VPN Cost-Savings Worksheet, this "typical" VPN offers an annual savings of $2,775,600, or 44% over the equivalent private network. The results are in line with industry analyst expectations and real world experience with VPNs. The payback in this example, to fully recover the initial equipment expenditure of $508,215 (excluding other implementation-related expenses), is just a little over two months.

The ROI Option

Many organizations now consider their networks to be an investment, rather than an expense, that provides a financial return to the company. While such a calculation is not the intent of this analysis, it may be a worthwhile exercise. This is especially true of a VPN, which offers a ready-made solution for communicating with customers, suppliers and other business partners.

An ROI analysis often involves what some refer to as "intangibles" because the economic benefits, while real, are difficult to quantify precisely. If you do conduct an ROI analysis, be certain to include the following considerations:

- *Faster time-to-market or greater marketshare*
- *An extranet's increased customer satisfaction, and improved productivity with suppliers and business partners*
- *New applications, such as collaborative work and distance training, that further enhance employee productivity*
- *Reduced down-time from enhanced network resiliency*
- *Fax/voice/video applications over IP*

IV. Concluding Thoughts

A VPN really can cut your organization's wide area networking costs in half, while giving you more capabilities and much greater flexibility. The example in this analysis utilizes the Internet for all communications, but your organization may benefit more with Virtual Private Trunking or Virtual IP Routing.

In addition to conducting your own analysis (the VPN Cost-Saving Worksheet is included), you may want to check out some of the additional resources listed in the appendix, and talk to your service provider(s) to learn more and get the latest information on VPNs. You might even designate a "VPN evangelist" or committee to investigate the impact on your organization.

Finally, consider launching a VPN pilot. A pilot is an excellent way to learn about VPNs and experiment with various service providers and their offerings. Often the best course of action with a pilot is to bring new sites and/or users into the enterprise network. Once these prove successful, existing sites and users can be added, and your organization can begin realizing the cost savings and other advantages of the incredible, inevitable VPN.

Appendix

1. The VPN Cost Savings Worksheet

Following are instructions for performing your own VPN cost savings analysis using the VPN Cost-Savings Worksheet. The worksheet is optimized for the most common type of VPN – an Internet-based Virtual Private Remote Network that employs multiprotocol tunneling – but can be used with modified pricing for a VPN that uses Virtual Private Trunking or Virtual IP Routing.

Complete the cost savings worksheet on page 25. Section-by-section instructions as well as an explanation of the limitations of the worksheet are also included.

Existing Private Network Section

In this section input the monthly costs (in the Monthly Costs column) for the existing private network, consisting of:

- WAN Services for both local access (LEC) and long distance (IXC) for all dial-up and leased lines in the private network
- Internet Access charges (ISP and LEC) for all multiuser sites and individual users that currently have an Internet account
- WAN/User Management costs for the private network

If the current cost information you have is on an annual basis, be certain to divide by 12 to get *Monthly Costs*.

Note that the costs here pertain to the operation and management of the wide area network (WAN) only, as well as to all user support for the network itself. An enterprise WAN includes site-to-site internetworking, remote LAN access for telecommuters and mobile workers, Internet access for all employees, and optionally, an extranet with buyers and suppliers. If replacing only a portion of the enterprise WAN with the VPN, include only that portion in the monthly costs. Specifically excluded is the Local Area Network (LAN) and user support for PCs and all applications, as these costs should be comparable between the private and virtual private networks being compared.

Because the Internet, especially for e-mail and the Web, is an essential element of any enterprise network, this cost should be considered an existing private network expense. Access to the Internet might be provided with a single, high-speed link for the entire enterprise or, more likely, through numerous lower speed links for individual users and multiuser sites. Be sure to include all such accounts in the monthly *Internet Access* cost.

Finally, if your existing WAN employs Frame Relay services, you already have a VPN, and may find that the savings of an Internet-based VPN are insignificant. Likely, your Frame Relay VPN uses switched or permanent virtual circuits. If so, it may be worthwhile to check with your service provider(s) to learn about the benefits and availability of Virtual Private Trunking services.

Proposed VPN Section

The *Proposed VPN* section takes advantage of a VPN's single connection per site and user to define the enterprise-wide virtual private network configuration. A variety of types and speeds of connections are listed, including two "placeholders" each for leased line and dial-up services. Each provides Internet access for a Virtual Private Remote Network that employs multiprotocol tunneling.

The required input for this section involves filling in the number of connections for each type/speed of service listed. Note that number of connections for each type/speed of service should include those required for both sites and users. This is particularly true of ISDN BRI, which is a popular service for small multiuser offices, SOHO environments and individual users.

The *WAN* and *ISP* columns provide "average costs" for these monthly services. Naturally, the pricing for your actual sites and users may vary substantially by location and service provider. These average values do, however, generate a reasonable first-pass estimate. More accurate numbers can be obtained by contacting the actual local exchange carrier(s) and Internet service provider(s) you would be using for the VPN.

You can add "placeholder" services, such as different data rates or Digital Subscriber Line access, or change the monthly WAN/ISP fees for any type/speed of service listed if necessary.

If the *Estimate Costs Savings* calculations result in negative numbers, check the following two likely causes:

- The monthly costs entered for the *Existing Private Network* are inaccurate. Be sure to include *all* WAN (LEC and especially IXC), Internet access and WAN/user management expenses.
- The total number of connections in the Proposed VPN exceeds the number of individual locations. With a private network, many sites may have multiple leased and/or dial-up links. But with a VPN, each site/user only requires a single connection for public Internet access, semi-private extranet access and private intranet/VPN access.

It is possible, that for some applications, an Internet-based Virtual Private Remote Network would result in little or no savings. For example, an existing Frame Relay network is already a VPN that saves substantially over the equivalent network constructed of leased and dial-up lines. Migrating from one VPN architecture to another, however, is unlikely to offer the same level of savings, and may even result in higher costs.

Limitations

The **VPN Cost-Savings Worksheet** takes certain "short cuts" to maximize simplicity and utility. It is important that you understand each of these limitations:

- The worksheet focuses on those areas where VPNs and private networks differ the most: the on-going costs for WAN services and network management. All other costs, which should be roughly the same for both the *Existing Private Network* and the *Proposed VPN*, are ignored, including the initial implementation expenditure (equipment purchases, training, installation, set-up fees, etc.) and the on-going costs of equipment maintenance. Facilities costs, as an on-going expense, are also ignored, even though they should be less with a VPN (owing to its consolidation of equipment).
- The implementation costs of the proposed VPN can be calculated separately to determine the payback period. Simply divide the one-time implementation costs by the *Annual Dollar Savings* to obtain the payback period.
- The monthly *WAN* and *ISP* costs for the *Proposed VPN* are based on "average rates" for a Virtual Private Remote Network that uses the Internet and/or a carrier's own IP network as its wide area backbone. The worksheet could be used to estimate the costs and cost savings of VPNs based on other services, such as Virtual Private Trunking or Virtual IP Routing, provided the appropriate monthly costs are entered in the *WAN* and *ISP* columns.
- Similarly, the monthly *WAN* and *ISP* costs for the *Proposed VPN* reflect "average" U.S. pricing, which can vary substantially in other parts of the world. For multinational VPNs it may be necessary to check with local carriers and enter these values in the "placeholder" rows.
- *Monthly Costs* for the *Existing Private Network* are required to estimate both the *VPN/User Management* costs and the "bottom line" *Estimated Cost Savings*. Therefore, if no private network exists, or if its costs are not provided, *VPN/User Management* and *Estimated Cost Savings* cannot be calculated. Nevertheless, the worksheet remains useful for calculating the estimated annual cost of WAN and ISP services for a VPN.

VPN Cost-Savings Worksheet

		Monthly Costs	Annual Total
Existing Private Network			
1. WAN Services (LEC & IXC)	*Enter monthly cost for WAN here:* _____	x 12 =	_____
2. Internet Access (ISP)	*Enter monthly cost for Internet here:* _____	x 12 =	_____
3. WAN/User Management	*Enter monthly cost for Management here:* _____	x 12 =	_____
4. Total Annual Cost (Existing Private Network)	*Add above 3 totals:* _____ **A**		

Proposed VPN (Site/User Connections)	**WAN**		**ISP**				
5. Fractional T3 (15 Mbps)	$8,000	+	$14,000	=	$22,000	x 12 =	*
6. E1 (2.048 Mbps)	$2,000	+	$4,000	=	$6,000	x 12 =	*
7. T1 (1.544 Mbps)	$700	+	$2,800	=	$3,500	x 12 =	*
8. Fractional T1 (768 kbps)	$600	+	$2,600	=	$3,200	x 12 =	*
9. Fractional T1 (512 kbps)	$550	+	$2,400	=	$2,950	x 12 =	*
10. Fractional T1 (256 kbps)	$450	+	$1,700	=	$2,150	x 12 =	*
11. Fractional T1 (128 kbps)	$400	+	$1,200	=	$1,600	x 12 =	*
12. Fractional T1 (56/64 kbps)	$400	+	$800	=	$1,200	x 12 =	*
13. Other Leased Line Service	$0	+	$0	=	$0	x 12 =	*
14. Other Leased Line Service	$0	+	$0	=	$0	x 12 =	*
15. ISDN BRI (64-128 kbps)	$85	+	$50	=	$135	x 12 =	*
16. Modem/POTS (33.6-56 kbps)	$35	+	$20	=	$55	x 12 =	*
17. Other Dial-up Service	$0	+	$0	=	$0	x 12 =	*
18. Other Dial-up Service	$0	+	$0	=	$0	x 12 =	*
					Subtotal: _____ **B**		
50% VPN/User Management					*Multiply A by .50:* _____	x 12 =	_____ **C**
Total Annual Cost (Proposed VPN)						*Add B and C:*	_____ **D**

Estimated Cost Savings

Annual Dollar Savings	*Subtract D from A:* _____ **E**
Percentage of Annual Savings	*Divide E by A:* _____ %

** Multiply this annual total by the number of sites/connections, if more than 1*

2. Additional VPN Resources

The following documents contain valuable information on VPNs. These reference documents are available at www.ascend.com

Document	Content
VPNs for the Enterprise	Resource Guide
Building the Enterprise Network of the Future	Resource Guide
Ascend's MultiVPN Strategy	White Paper

3. Ascend's MultiVPN Product Line Highlights

Ascend is making enterprise-wide VPNs a worldwide reality today with next-generation platforms and technologies that are transforming the public network into a cost-saving resource for enterprises.

Ascend's MultiVPN strategy takes a practical approach with incremental and enabling enhancements to the public network infrastructure that build on the existing foundation, much of which already employs Ascend's access, routing and core switching products. These enhancements also satisfy the special needs of enterprises, enabling them to tap the full potential of the public network's power and presence.

Ascend's fully integrated MultiVPN product line includes offerings for both enterprise subscribers and their service providers. This section offers a high level overview of Ascend's MultiVPN product line with little discussion of specific features. Details on these and other products are available at Ascend's Web site (www.ascend.com).

Enterprise Subscriber Offering

Ascend's award-winning Pipeline® family provides the industry's widest assortment of VPN-capable routers for branch offices, small office/home office (SOHO) environments and telecommuters. VPNs benefit substantially from the Pipeline's superb price/performance and low cost of ownership.

Ascend's Pipeline family includes several models to fit applications ranging from single-user home offices to multi-user branch offices of virtually any size. The SOHO models are complete data/voice/fax communications solutions with two analog Plain Old Telephone Service (POTS) ports to connect telephones, answering machines and fax machines. Ascend's flagship SOHO router is the Pipeline 75, which offers the industry's most extensive feature set. The Pipeline 85 adds a 4-port Ethernet hub.

MultiVPN Families

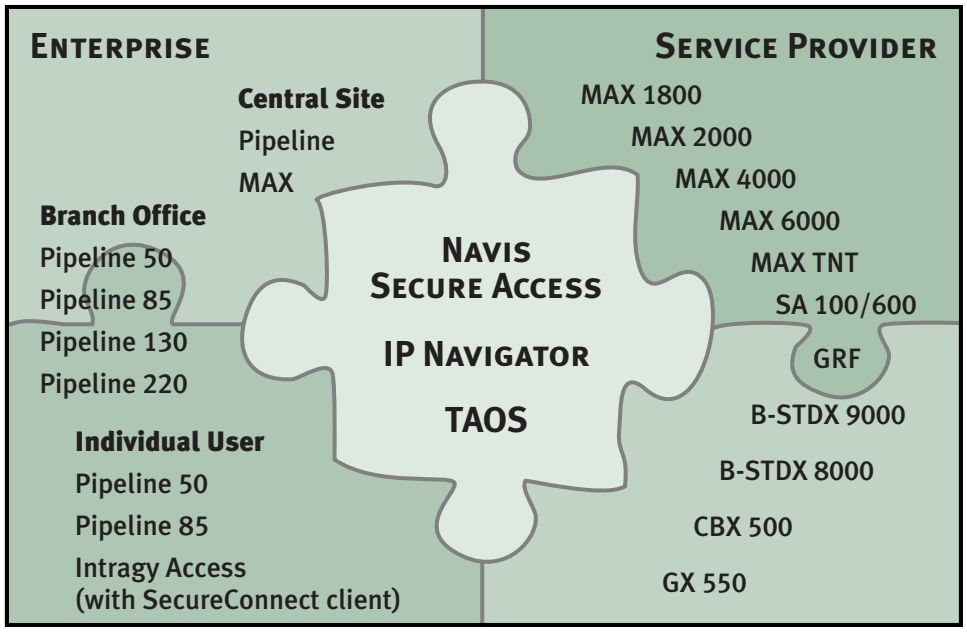


Figure 7 – Ascend's MultiVPN product line is a fully integrated solution with customer premises equipment, infrastructure access, IP routing/switching, core switching, security and management, that together constitute the industry's most comprehensive VPN offering.

Data-only models of the Pipeline are available in switched (ISDN or SW56) and leased line (T1/Fractional T1, DDS56 or xDSL) versions, each with support for Frame Relay. The Pipeline 130 offers both leased line and switched WAN ports for situations that require dial-up bandwidth on demand for backup and overflow needs. The Pipeline 220 adds a second Ethernet LAN port on the Internet side of the optional Secure Access Firewall. The award-winning Pipeline 50, ideal for smaller branch offices, is Ascend's most popular ISDN remote access router.

For larger sites in a hybrid private/virtual private network, Ascend's MAX™ WAN Access Switch offers a total solution. The MAX supports the widest assortment of WAN services in the industry, for both PSTN and VPN services, and is available in a variety of models that range from fractional T1 to T3 data rates. All models offer the capability, scalability and flexibility enterprises need during the migration from private to virtual private networks.

Service Provider Offering

Ascend's comprehensive service provider offering encompasses three related areas: core switching, IP routing/switching and network access.

Core Switching products include B-STDX Frame Relay Switches, the CBX 500 Multiservice ATM Switch and the GX 550 Core ATM Switch. Featuring the highest port density in the industry, the B-STDX is capable of building large-scale, sophisticated public networks with speeds ranging from sub-DS0 to OC-3/STM-1. The CBX 500 is a high performance switch that achieves the vision of ATM as an integrated transport of data, voice and video traffic across a public network infrastructure. True to its name, the CBX 500 offers multiservice support for Frame Relay and IP. The GX 550 combines industry-leading port densities for OC-3/STM-1 and OC-12/STM-4 interfaces with industry-first OC-48/STM-16 high-speed trunking and wave division multiplexing (WDM), affording carriers both capacity for today and investment protection for tomorrow.

IP Routing/Switching products include the IP Navigator™ IP Switch and the GRF® Multigigabit Router. The IP Navigator adds high-speed IP switching to Ascend's carrier-class B-STDX 8000/9000, CBX 500 and GX 550 multiservice WAN switches. IP Navigator is an enhanced implementation of the emerging MultiProtocol Label Switching (MPLS) standard. The design is based on Ascend's proven Virtual Network Navigator (VNN) architecture – an extended version of the OSPF standard – and supports IP multicast through the Distance Vector Multicast Routing Protocol (DVMRP), Multicast OSPF (MOSPF) and Protocol Independent Multicast (PIM). The GRF provides the capabilities of a conventional router, but with an order of magnitude improvement in price/performance. The GRF's unprecedented performance is the result of its distributed architecture and hardware-accelerated route table lookup that occurs at wire speed.

Network access products include MAX WAN Access Switches and SA Broadband Service Units. The MAX, which is the industry's leading digital access concentrator, is installed at over 80% of the world's largest Internet service provider POPs. The MAX supports both traditional PSTN-based forms of access, including Frame Relay, and digital subscriber lines (xDSL). SA systems enable service providers to extend ATM and other broadband services directly and cost-effectively to enterprise sites.

Provider/Subscriber Elements

Security provisions and management systems are common provider/subscriber elements of Ascend's VPN offering.

Security for VPNs is the primary responsibility of Ascend's Security offering, which includes the Secure Access family of products and Ascend Access Control. Secure Access is a dynamic firewall available as an integrated option for Ascend's Pipeline and MAX systems, and is also available in a software-only Intragy Access (with SecureConnect client) for PCs with ordinary modems. Access Control is Ascend's enhanced implementation of RADIUS, which supports Proxy RADIUS for enterprise control of security enforced at service provider POPs.

Management for VPNs is the primary responsibility of Ascend's Navis network management system. Navis components are deployed throughout the service providers' public network infrastructure. Enterprise subscribers can access the wealth of information in the Navis Customer Network Management (CNM) gateway using the familiar Web browser interface.

Navis Management At Work

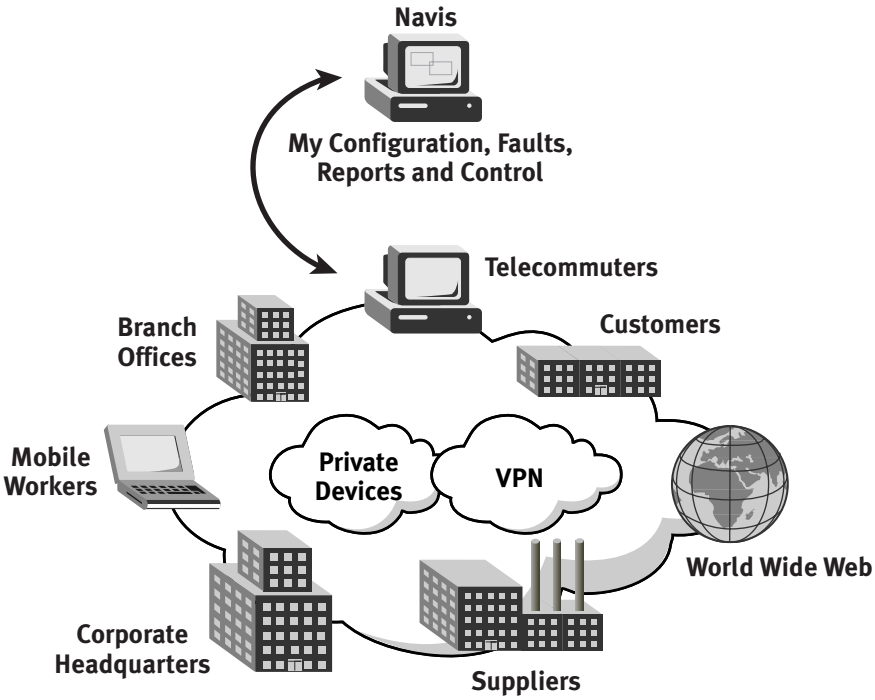


Figure 8 – Ascend's Navis network management system is the industry's only provider/subscriber solution with genuine Customer Network Management for VPNs.

Ascend Communications, Inc.
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502
Tel: 510.769.6001
Fax: 510.747.2300
Toll Free: 800.621.9578
E-mail: info@ascend.com
Fax Server: 415.688.4343
Web Site: http://www.ascend.com

06-16
08/98