



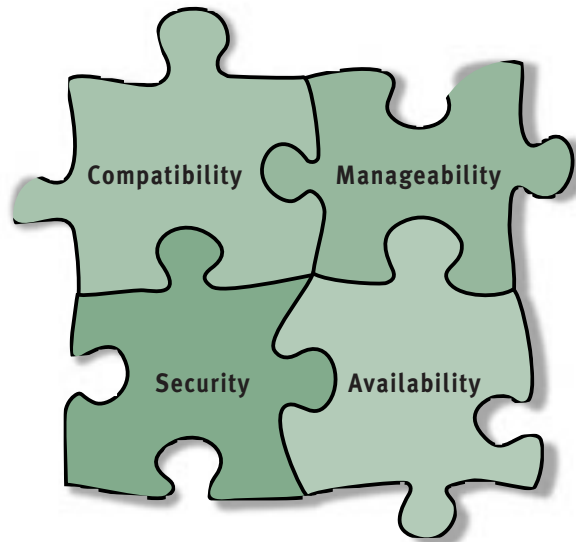
**Product information begins on page 2.**

Lucent and Ascend have merged.

With the Lucent-Ascend merger, customers gain a broader and more powerful portfolio of next-generation data, voice, fax, and video services and products. To access up-to-the-minute information about our products, see page 2.

We also invite you to contact us with your questions directly at: [info@ascend.com](mailto:info@ascend.com)

# Virtual Private Networks for the Enterprise



**A Resource Guide for  
Information Technology and  
Network Managers Worldwide**



Where Network  
Solutions Never End™

# TABLE OF CONTENTS

<b>1. Executive Summary.....</b>	<b>1</b>
<b>2. The VPN Advantage .....</b>	<b>4</b>
<b>3. VPN Requirements .....</b>	<b>11</b>
<b>4. VPN Building Blocks.....</b>	<b>23</b>
<b>5. Appendix .....</b>	<b>38</b>
VPN Case Study .....	38
Ascend MultiVPN Product Information.....	40
VPN Implementation Checklist .....	41
Reference Material.....	46

## TABLE OF DIAGRAMS

Figure 1.	The VPN Concept.....	2
Figure 2.	VPN Driving Forces .....	5
Figure 3.	The Population Pyramid .....	8
Figure 4.	A Global Remote Access/Branch Office VPN .....	9
Figure 5.	Accessing Private and Public Resources.....	9
Figure 6.	Distance Learning Training Class Via IP Multicast .....	10
Figure 7.	The VPN Essentials.....	11
Figure 8.	Tunneled Packet Format .....	14
Figure 9.	How Tunneling Works .....	15
Figure 10.	End-To-End Tunneling .....	16
Figure 11.	Encrypted Tunnel Mode Packet .....	19
Figure 12.	Three Forms of QoS .....	20
Figure 13.	Proxy RADIUS Configuration.....	22
Figure 14.	Dependent VPN Architecture .....	23
Figure 15.	Independent VPN Architecture .....	24
Figure 16.	VPN Building Blocks.....	25
Figure 17.	Enterprise Equipment Building Block.....	26
Figure 18.	Piecemeal Solution of Network Access .....	28
Figure 19.	Integrated VPN Approach .....	28
Figure 20.	Major Site Connectivity .....	29
Figure 21.	Before DSL.....	31
Figure 22.	After DSL.....	31
Figure 23.	The Management Building Block.....	32
Figure 24.	The Network Access Switch Building Block.....	33
Figure 25.	The NSP Backbone/Internet Building Block .....	35
Figure 26.	An Enterprise-Wide Virtual Private Network .....	37

*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](mailto: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.*

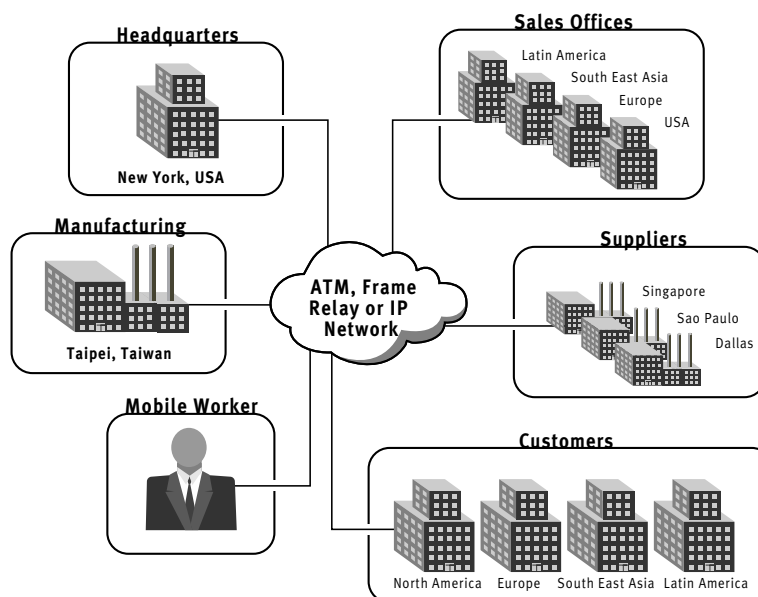
*Ascend and the Ascend logo are registered trademarks and all Ascend product names are trademarks of Ascend Communications, Inc. Other brand and product names are trademarks of their respective holders.*

## 1. EXECUTIVE SUMMARY

Businesses large and small have come to appreciate the value of the Internet for promoting and selling products and services, supporting customers, exchanging e-mail internally and externally, conducting research, collaborating with business partners and more. After years of successful experience with the Internet, many organizations are now wondering: can the vast power and presence of public networks be leveraged for private networking applications? The answer is a resounding yes for a growing number of enterprise needs.

The public network, which includes the Internet and its underlying Frame Relay and Asynchronous Transfer Mode (ATM) infrastructures, indeed presents an intriguing possibility for the enterprise: the Virtual Private Network, or VPN. The essence of a VPN is its use of the Internet, Frame Relay or ATM as a Wide Area Network (WAN) backbone to supplement or replace the costly long-distance leased or dial-up links in a private network. Sending private information via these new public networks is not much different than using the Public Switched Telephone Network (PSTN) for internal communications or sending confidential correspondence by mail. Organizations benefit tremendously by being able to depend on these public services without having to take on responsibility for their operation. It is this need to simplify—and save money—that make VPNs a compelling alternative to the privately architected enterprise network.

## The VPN Concept



*Figure 1 — A VPN based on the more efficient new public network provides a more capable, flexible and affordable alternative to the purely private network for many enterprise applications.*

A VPN can link all of an organization's offices, telecommuters, traveling employees, and even its customers and suppliers around the globe. Due to the Internet's worldwide presence, users just about anywhere can connect through a local switched or dedicated service. By eliminating long-distance charges, consolidating equipment needs and minimizing network management responsibilities, Forrester Research estimates companies can achieve a savings of up to 60% over private networks. The VPN also leverages user familiarity with the Internet, and enhances overall flexibility based on the Internet's ubiquitous presence and easy access. For these reasons, and others outlined later, VPNs offer businesses a more attractive solution to many enterprise networking needs.

A majority of enterprises will use VPNs to supplement or replace existing private network links, and to implement new forms of communications. According to the International Data Corporation, 90% of organizations already plan to use the Internet to give employees remote access to internal information. Many also want to use VPNs for remote office internetworking and even enterprise-wide intranets. The Internet's multicast capability, with its any-to-many connectivity, will enable organizations to implement new collaborative work and distance learning applications easily and affordably. And the advent of Voice over IP (VoIP) has given the Internet voice, video, fax and "multimedia" capabilities. The almost limitless possibilities make VPNs the next logical step in enterprise networking.

The enormous potential afforded by VPNs has motivated Network Service Providers (NSPs) to enhance the public network infrastructure, making VPNs suitable for most enterprise networking needs today. Tunneling techniques now allow the Internet Protocol (IP) to carry a wide range of popular non-IP traffic. Virtual IP routing now improves flexibility and control. Virtual private trunking with direct access to Frame Relay and ATM services is now available in an increasing

number of locations. Encryption and authentication security provisions now put the private in Virtual Private Networking. Performance enhancements in the public network backbone and access equipment now provide the Quality of Service (QoS) and Service Level Agreements (SLAs) needed to compete with privately architected networks. Customer network management systems that seamlessly integrate provider (carrier, service provider) and subscriber (an enterprise) capabilities now make VPNs just as manageable as private networks. And all of these enabling technologies are based on standards that yield end-to-end interoperability.

One thing is clear: nearly all organizations will use VPNs eventually. The benefits are quite compelling and even irresistible. The sooner your organization begins to exploit the public network's immense potential for private communications, the sooner you will benefit from the many advantages.

This resource guide can help Information Technology (IT) managers understand and plan a successful Virtual Private Network. Chapter 2 assesses the many advantages of VPNs and highlights some typical applications. Chapter 3 outlines the four basic requirements of a VPN and provides an overview of some key enabling technologies. Chapter 4 describes the five building blocks in an end-to-end VPN, giving you practical information for implementing your very own VPN. The Appendix provides useful supplemental material, including a case study, an introduction to Ascend's MultiVPN™ solution, a VPN Implementation checklist and a list of additional references.



## 2. THE VPN ADVANTAGE

The success of the Internet is bringing about a change in private networking. Private networks and the public network now exist in parallel. There are many circumstances now causing these separate infrastructures to converge toward Virtual Private Networks. Five forces in particular are driving this convergence:

1. **The high cost of implementing and maintaining private networks** has no light at the end of the tunnel. Long-distance charges for leased lines and switched services mount daily. IT organizations are being asked to do more with less. The dependence on networked applications requires separate backup and overflow provisions, further expanding the already burdensome private network infrastructure. And rather than provide relief, most new technology only makes private networks more sophisticated – and more expensive.
2. **The increasingly dispersed and mobile workforce** is making private networks unmanageable. Now more than ever, traveling personnel need dial-up access around the world, and employees are increasingly working at home. Such mobility requires at least two network connections for each worker. Full-time telecommuting arrangements dramatically increase the number of permanent “remote offices” a company must interconnect. Acquisitions, mergers and expansion add even more sites and nodes. As a result, many private networks have become unwieldy – and unmanageable.
3. **Business applications will become dependent on the Internet.** Indeed, the ubiquity of the Internet and its IP-based applications create numerous opportunities for commercial users, such as promoting products and services, supporting customers and interacting with suppliers (see [Potential Internet Applications for the Enterprise](#) sidebar below).
4. **The need to interact “on-line” with customers and suppliers** adds a new dimension of complexity, where multiple private networks must be interfaced in a delicate balance of integration and isolation. The individual networks normally use different protocols, different applications, different carriers and different network management systems. With so few common denominators, interfacing private networks can be a major challenge.
5. **New applications continue to emerge**, especially those involving bandwidth-intensive multimedia and collaborative work. Many of these applications, which cannot run cost-effectively on the point-to-point PSTN, require the advanced any-to-any and any-to-many multicast capabilities of the public network.

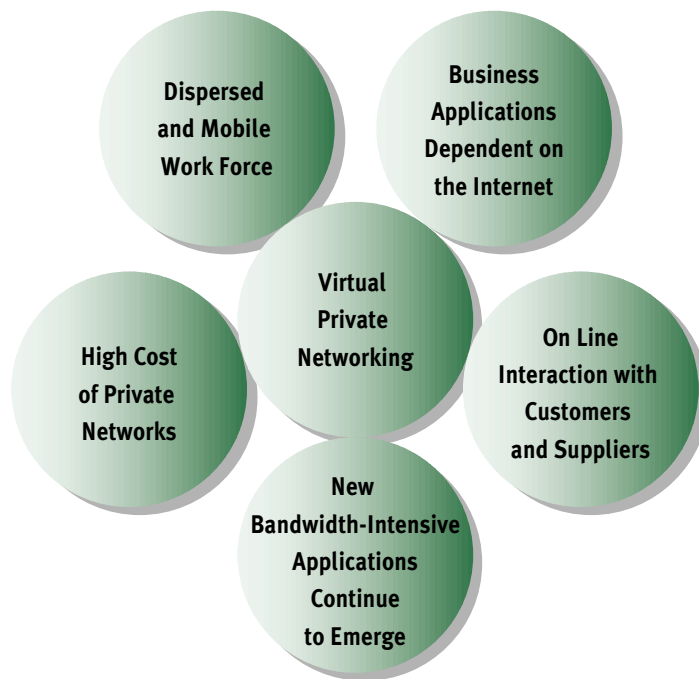
### Potential Internet Applications for the Enterprise

*Is your organization using the Internet only for Web-based marketing? If so, consider just a few of the Internet's other uses:*

- Supporting customers via the Web
- Exchanging internal and external e-mail
- Performing market and engineering research
- Receiving news and other timely information
- Placing telephone calls using Voice over IP
- Sending faxes long distance and internationally with local calls
- “Broadcasting” videos or events in real-time
- Conducting training classes and distance-learning seminars
- Collaborating with strategic partners and outside project teams
- Buying and selling products with new forms of electronic commerce or conventional Electronic Document Interchange (EDI) technology

---

## Virtual Private Network Driving Forces



---

*Figure 2 – These driving forces are making Virtual Private Networks a compelling alternative to private networks for most enterprises*

## Tapping the Public Network's Full Potential with VPNs

PSTN-based private networks have been the most cost-effective way to implement enterprise-wide data communications – until now. Today Virtual Private Networks that utilize the more efficient new public network infrastructure offer all of the very same capabilities – and more – at a fraction of the cost.

Essentially, a VPN is a private network that utilizes the new public network to carry all traffic in the WAN. The most widely available, least expensive, high-speed public network is the Internet. With its worldwide presence and unparalleled price/performance, the Internet is an excellent foundation for any VPN. Atop this foundation, organizations can employ virtual IP routing and virtual private trunking, with direct use of Frame Relay and/or ATM services, to meet enhanced performance and security needs.

Whether using the Internet, Frame Relay or ATM, a VPN is virtual because it appears to the organization as a dedicated private network, with exclusive use of the intermediate infrastructure. In reality, traffic from other VPNs and the Internet itself traverses the public network infrastructure on a packet-by-packet, frame-by-frame and cell-by-cell basis. But it does so in such a way that ensures the appropriate traffic, and only the appropriate traffic, arrives at the appropriate, and only the appropriate destinations. Because all organizations see only their own traffic, the network appears to be theirs – and theirs alone: a Virtual Private Network.

### The VPN concept is not new.

*Indeed, the phrase “virtual private network” is also used to describe integrated voice/data networks offered by some carriers. Although these offerings are packaged as VPNs, they resemble true private networks in both their costs and capabilities.*

*Technically, any private network could be considered “virtual” because it uses the Public Switched Telephone Network for both leased line and dial-up communications. But such a view is based on semantics and not on network characteristics or requirements, which are quite different for PSTN-based private networks and a VPN that utilizes new public network services. Special needs for VPNs exist in four key areas – compatibility, security, availability and manageability – which are covered in detail in Chapter 3: VPN Requirements.*

### VPNs allow companies to:

- Support full- and part-time telecommuting programs
- Handle all branch office interconnectivity on a dedicated VPN
- Move an existing application from the private network to a VPN
- Add sites not already on the private network
- Provide backup and overflow capacity for private networks using the Internet as a secondary “carrier”
- Perform overnight backup or software distribution of applications and/or data
- Institute virtual project teams with outside partners using inter-organizational “members only” groupware

## VPN Benefits

*Organizations with VPNs are able to save up to 60% over equivalent private networks, according to a study by Forrester Research. VPNs save money because they:*

- *Eliminate long-distance leased lines among major facilities, including those needed for alternate or “mesh” paths*
- *Eliminate long-distance switched calls via the PSTN for analog modems and ISDN access equipment*
- *Allow companies to pay only for actual usage or traffic sent*
- *Require less equipment because a single solution provides both Internet and VPN access, eliminating the need for separate modem banks, terminal adapters, remote access servers and so on. The consolidation also permits utilization of cost-effective, high-speed trunk lines.*
- *Minimize end-user network design and management responsibilities*

*VPNs exploit the new public network infrastructure's inherent robustness to provide a more capable and dependable alternative to private networks:*

- *Service providers in nearly every city create a worldwide presence*
- *Local access improves throughput by minimizing line noise*
- *Mesh redundancy and fault tolerance afford end-to-end reliability*
- *User familiarity simplifies training needs*

*The Internet's global presence also makes VPNs more flexible than private networks. With VPNs, end-user organizations can:*

- *Add and delete connections instantaneously*
- *Provide permanent, periodic or temporary connectivity as needed*
- *Integrate third-party users, such as customers and suppliers, almost effortlessly*
- *Select optimal data rates ranging from analog modem to T1/E1 speeds, and beyond with Digital Subscriber Line technology*

*Because VPNs offer a more affordable, capable, dependable and flexible alternative to private networks, nearly all organizations surveyed by IDC and other industry analysts expect to employ the Internet for internal data communications needs. VPNs are indeed the next step in enterprise-wide networking.*

## Identifying VPN Applications

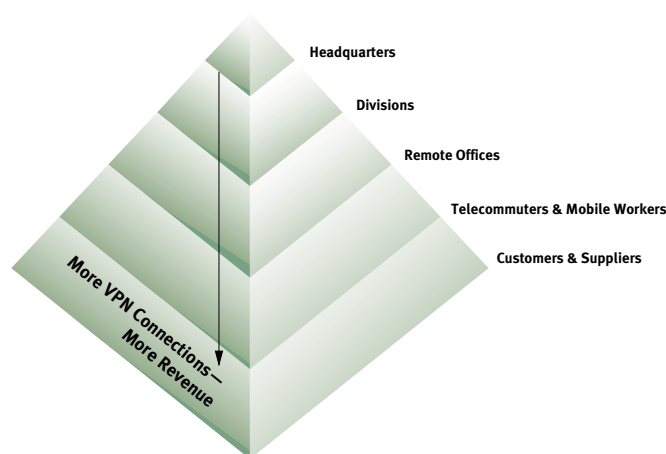
The presence and power of the public network make VPNs suitable for a wide range of commercial networking needs. A VPN can:

- Replace existing private network segments, subnets or entire wide area topologies
- Supplement private networks by offloading certain applications or meeting backup/overflow needs
- Handle new applications without disrupting the existing private network
- Extend the reach of corporate communications by adding new geographically-dispersed locations, especially international sites

There are two general conditions that strongly favor use of a VPN: The first is the existence of numerous locations, including both individual users and multiuser office sites. The second is when these users/sites are spread across long distances, especially multinational locations.

---

## The “Population Pyramid”




---

*Figure 3 — The cost-savings potential of a VPN increases with both the number of and distance between users and sites.*

Three applications – worldwide remote LAN access, intranets/extranets and collaborative work – are particularly well-suited for Virtual Private Networks. Each provides a total access solution, and can be implemented as a small “pilot” or trial application to gain experience and confidence.

1. **Worldwide remote LAN access** for mobile employees and those working at home is an obvious use of the Internet. Rather than employ long-distance calls to a centralized corporate facility, a user's local call to a local NSP Point of Presence (POP) provides access to the company's VPN via the Internet. The employee can now run business-critical applications, such as exchanging e-mail, catching the latest news, updating a price list, entering orders, or performing other tasks. The same arrangement can provide remote access for full-time telecommuters, as well.

## A Global Remote Access/Branch Office VPN

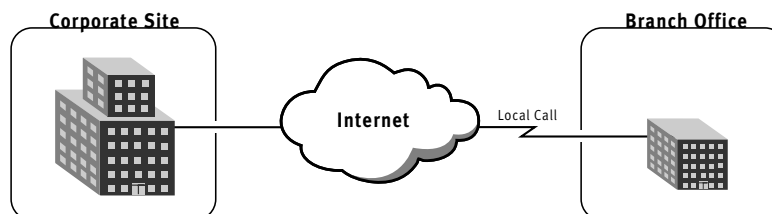


Figure 4 — Long-distance calls, along with racks-full of modem banks and other equipment, are things of the past with an Internet-based VPN for worldwide remote LAN access.

**2. Intranets and extranets** are quite symbiotic with the Internet. From a single network connection and a single application interface, users have access to Internet-based public resources, intranet-based private resources and extranet-based communications with buyers and suppliers. For example, an employee can search the World Wide Web for publicly-available background information on a current project, then correlate this with private information on one of the company's Web-enabled servers, and finally check with a supplier on availability or other details. The result is easily posted for others to review before presentation to management.

## Accessing Private and Public Resources

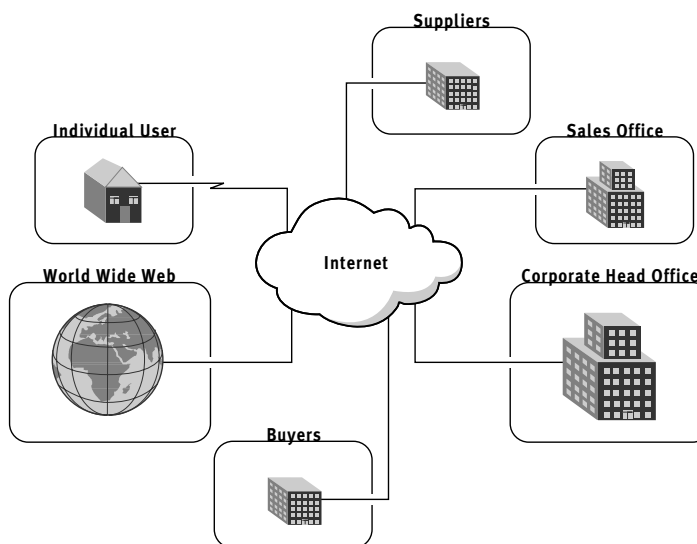


Figure 5 — An Internet-based VPN intranet/extranet gives users seamless access to private, semi-private and public resources — all from the friendly and familiar Web browser interface.

3. **Collaborative work** or distance learning/training applications are ideal for Internet-based VPNs. The Internet's powerful multicast capability can "broadcast" material to any number of sites, allowing users around the globe to participate in a meeting or attend a class from the convenience of their own offices. The multicast material could be as simple as a shared whiteboard, or as sophisticated as full-motion video and audio. Such applications, which are generally cost-prohibitive in private networks, can boost productivity substantially – and inexpensively – with an Internet-based VPN.

### Distance Learning Training Class Via IP Multicast

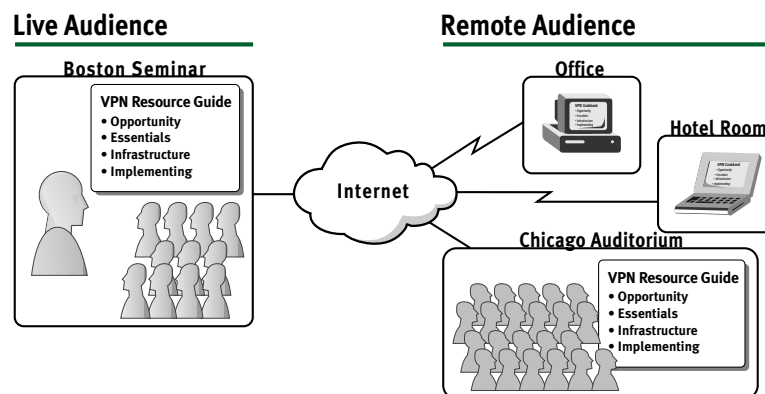


Figure 6 – By capitalizing on the Internet's multicast capability, a VPN lets users participate in a virtual meeting or attend a class.

### Multicast in the Internet

Multicast capabilities will dramatically expand the applications potential of the Internet. The optimal way to handle IP multicast in the Internet is a topic of intense scrutiny at this time. The Multicast Backbone (MBone) has proven itself quite successful, but now only covers a portion of the world. Basically, IP multicast employs the equivalent of a "group address" administered by the Internet Group Management Protocol (IGMP). Users wanting to participate in a multicast session register with the nearest multicast-capable router as a member of that session. This router then directs the session's multicast traffic from the Internet to the unique IP addresses of its member participants. All such "edge" routers must, in turn, register with other routers all the way back to the multicast source using special protocols that allow multicast traffic to reach all participants without duplication on the mesh topology of the Internet itself. The technology is robust enough for an NSP's own IP backbone today, and will eventually extend to every corner of the Internet.

### Multimedia VPNs using Voice over IP

IP is not just for data any more. Indeed, the ever-increasing ubiquity of IP assures its use in many other and innovative ways. Voice over IP (VoIP) adds voice, video and faxing capabilities to IP-based networks, including VPNs, using the H.323 standard. H.323 provides interoperability with PSTN, allowing business and residential customers to use existing telephone equipment, videoconferencing systems and fax machines. And because the new public network can deliver toll-quality performance, most users will be unable to notice their calls are being carried in IP packets! VoIP makes it possible to implement "multimedia" intranets, extranets and VPNs that can offer even greater savings by reducing long-distance voice and fax calls.

### 3. VPN REQUIREMENTS

While there are numerous and varied requirements for any network, four present special considerations with VPNs: compatibility, security, availability and manageability. Because private and virtual private networks are so similar, most other network needs are essentially identical. This section, therefore, focuses on the four special areas that now make the public network robust enough for most enterprise networking needs.

#### The VPN Essentials

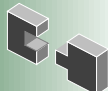



	<b>Compatibility</b>
	<b>Security</b>
	<b>Availability</b>
	<b>Manageability</b>

Figure 7 – A Virtual Private Network has these four special requirements.



#### Compatibility

Public Frame Relay and/or ATM networks can often be used directly for both IP and non-IP applications. Virtual private trunking, for example, which uses Frame Relay or ATM services directly, is fairly compatible with multiprotocol environments (see Virtual Private Trunking sidebar). Basically, all that is required for a VPN based on virtual private trunking is wide area internetworking equipment with Frame Relay or ATM capabilities. The popular choices include Frame Relay Access Devices (FRADs), or routers with Frame Relay or ATM interfaces. Standards such as RFC 1490 permit IP and SNA, for example, to be combined on single virtual circuit. Multiple permanent or switched virtual circuits can accommodate virtually any mix of protocols and topologies. And some NSPs even offer advanced capabilities that go beyond virtual circuits with an ability to dedicate infrastructure capacity or resources to a particular VPN.



To use the Internet for any portion of a VPN, the application must be made compatible with the Internet Protocol, or IP, at the International Standards Organization (ISO) Layer 3. The obvious way to achieve Internet compatibility is to use IP and IP applications with officially-assigned IP addresses. And indeed, private networking applications that meet these requirements can use the Internet “as is” for a VPN – provided appropriate security measures are taken. But because most private networks are multiprotocol or use unofficial “private” IP addresses, they cannot take advantage of the Internet without special provisions. There are numerous options for making these private networks compatible with the Internet; the four most popular are:

- Convert existing IPX, NetBEUI, AppleTalk or other protocols to IP and Internet addresses
- Convert private inappropriate/invalid IP addresses to official “Internet” addresses
- Install special IP gateway software on servers
- Employ general-purpose tunneling techniques
- Utilize virtual IP routing

The organization’s current situation and long-term networking goals determines which of these possible options is best for the VPN.

### Virtual Private Trunking

*Virtual Private Trunking (VPT), which directly accesses the powerful capabilities of Frame Relay and/or ATM services, is suitable for both IP and non-IP needs. Permanent virtual circuits (PVCs), for example, might be used to link all sites in an intranet, while switched virtual circuits (SVCs) could serve to link the many sites in an extranet. Some NSPs deliver trunking capabilities that go beyond traditional virtual circuits by provisioning actual lines as dedicated to or shared services, depending on enterprise subscriber needs and service provider resources. Dedicated bandwidth in the form of reserved lines might be used to link major enterprise facilities, including the headquarters and larger divisions, while shared capacity would more efficiently internetwork numerous branch offices. The full spectrum of frame and bit rates, with their respective price/performance attributes, can be employed to create an optimal VPN configuration. Organizations concerned about using the Internet for enterprise networking will find VPT’s enhanced performance and security appealing. VPNs that involve mostly non-IP applications is another situation where accessing Frame Relay and ATM services directly may be preferable to the exclusively IP Internet.*

**Internet addresses** are the “official” IP addresses administered and assigned by the governing body InterNIC. Of course, any user organization can simply select 32-bit IP addresses at random or as part of a rational scheme, and these addresses will work just fine in a private IP network. But these private addresses will not work in an Internet-based VPN (see [Private IP Networks](#) sidebar).

This option is viable for organizations with existing private IP networks, and is even suitable for applications that can be converted to IP. What is needed in either case is a compatible internal internetwork of local routers and switches. The internal internetwork can support multiple protocols, as long as it supports IP.

Converting an organization’s entire network to official Internet addresses is unnecessary for a limited VPN because official Internet addresses can coexist with private IP addresses on the organization’s internal internetwork of routers and switches. In other words, a “private” IP client can still access an “official” IP server via the local internetwork with no special provisions. Even where enterprise-wide conversion is desirable or inevitable, the organization may choose wait for the next generation (IP version 6) to avoid double work: converting now with IPv4 and again with a new block of assigned addresses when IPv6 comes along in a few years.

A less ambitious endeavor involves sharing a small block of Internet addresses among a much larger number of users. Address-sharing techniques are similar to modem pools, because they leverage the fact that not all users will need Internet access at the same time. Two industry standard solutions – the Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) – are available, each taking a slightly different approach. DHCP assigns an Internet address to a PC dynamically, as the name implies, when it boots up. NAT substitutes an Internet address for a private IP address as necessary, also in a dynamic or “leased” fashion. Both let a relatively small allotment of addresses serve a fairly large user population. And each can provide an additional layer of security by hiding internal address from discovery on the Internet.

### Private IP Networks

*Many organizations that use IP have “private” IP addresses. The reason is simple: obtaining a block of official Internet addresses large enough to facilitate subnetting is impossible. Subnets simplify address administration and router/switch management, but “waste” precious addresses.*

*This practice is so common that a standard was published (RFC 1597) to set aside or sanction certain IP addresses for private use. Three such address blocks, or subnets, are available to suit any size organization:*

- 10.0.0.0 - 10.255.255.255 (24 bits for nearly 17 million addresses)
- 172.16.0.0 - 172.31.255.255 (20 bits for about 1 million addresses)
- 192.168.0.0 - 192.168.255.255 (16 bits for slightly over 65,000 addresses)

*Routers in the Internet block these sanctioned private IP addresses to avoid any ambiguity among private networks. Note that private IP address schemes that do not use the sanctioned private subnets must be carefully administered with similar blocking or filtering techniques. If two nodes have the identical address (one official, one not) serious problems can result for both users.*

*The next generation IP (IPng, which is also known as version 6 or IPv6) will eliminate the need for private address schemes. IPv6 quadruples the current 32-bit address space. Even with waste from rampant subnetting, 128 bits is generous enough to yield 50,000 registered IP addresses for every square meter of land on Earth!*

**IP Gateways** are another option for making private networks compatible with the Internet Protocol. A gateway works by translating a non-IP protocol to IP, and vice versa. Because the typical IP gateway operates at Layer-3, it should be called an IP relay – technically speaking, according to ISO. But the popular terminology is, and will likely remain, the IP gateway.

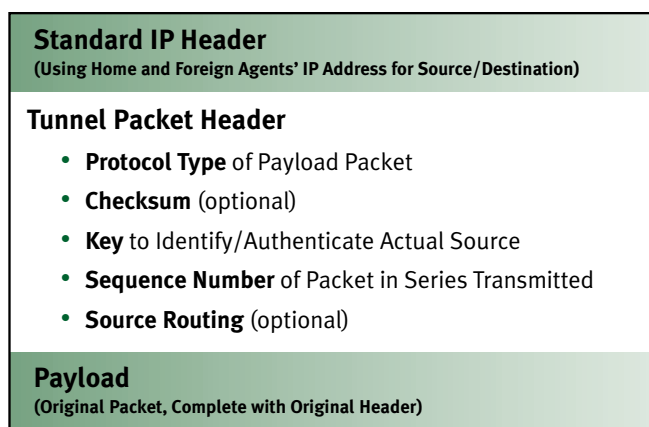
IP gateway software is available from most network operating system (NOS) vendors that have proprietary “native” protocols. The gateway software – installed on each server to support all clients assigned to it – converts traffic to/from the proprietary protocol from/to IP. Novell’s IP gateway for NetWare, for example, lets clients running browser-like applications on the proprietary IPX protocol access Web servers on the Internet. IP gateways employed for Internet access can be used without modification for Internet-based VPNs. Because most NOS vendors, including Novell, now offer robust support for “native” IP, the need for these specialized gateways will diminish over time.

**Tunneling, or Virtual Private Remote Networking**, is generally the best option for making non-IP and even private IP networks Internet-compatible. Tunneling methods and various encapsulation techniques have been used for years to integrate different network protocols on a common backbone. These proven technologies have now been optimized for use with Internet-based VPNs.

Tunneling occurs at both ends of a connection. The source end encapsulates the other protocol's packets in IP packets for transit across the Internet. The encapsulation process involves adding a standard IP header to the original packet, which is then referred to as the payload. A corresponding process at the destination end decapsulates the IP packet by removing the IP header, leaving the payload – the original packet – intact. (See the [How Tunneling Works](#) sidebar for a more detailed description of the process.)

---

## Tunneled Packet Format




---

*Figure 8 — All tunneling and encapsulation techniques add special headers to the original packets – whether IP or not – for transmission via the Internet.*

Because tunneling is relatively simple, it is often the most cost-effective and easily managed alternative for making nearly any private network, including a private IP network, operate as an Internet-based Virtual Private Network. Another advantage of tunneling is that it can be implemented in the NSP's point of presence (POP) or in enterprise equipment – or in some combination of both. Many network access switches, remote access servers and WAN routers already support interoperable tunneling standards (see [Tunneling Protocols](#) sidebar).

## How Tunneling Works

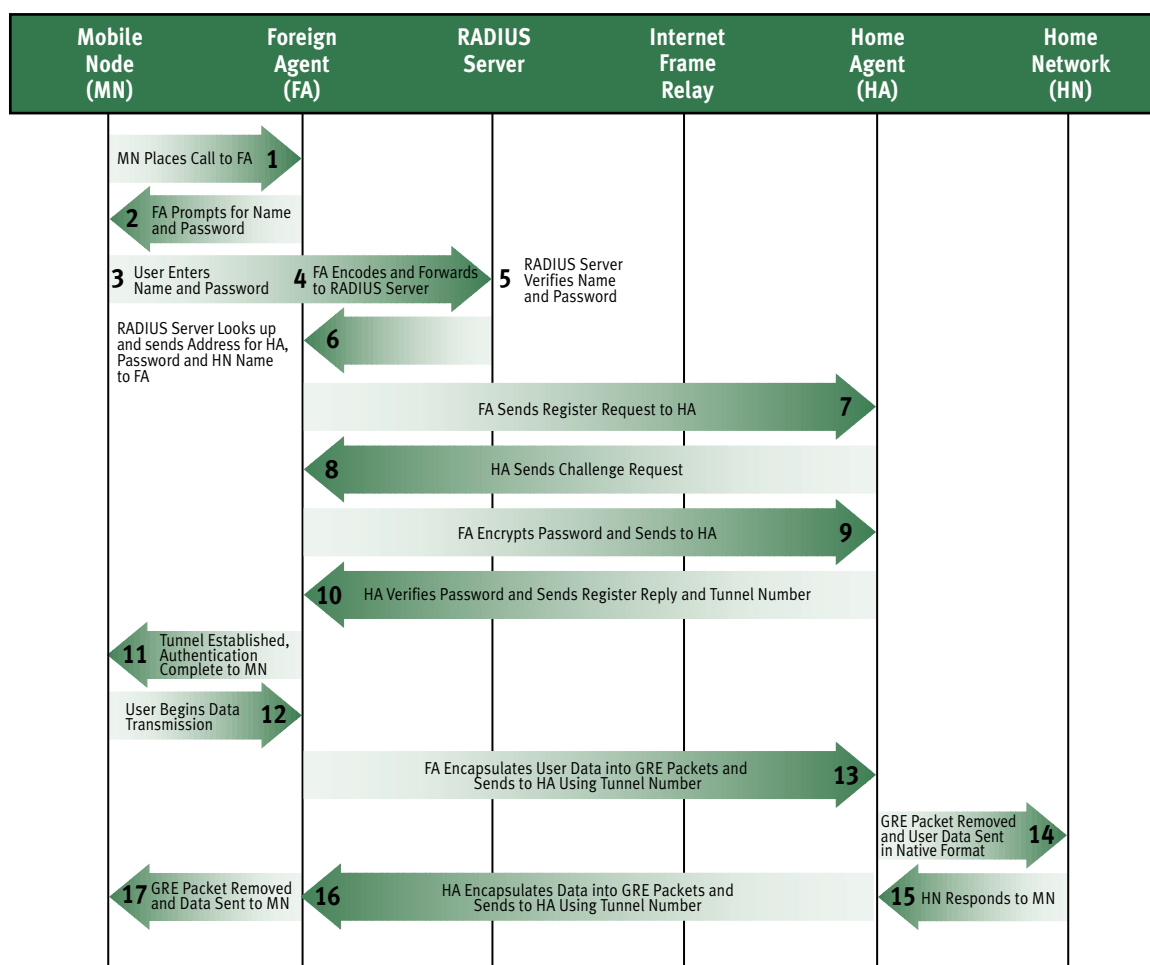


Figure 9 – This flow chart shows the detailed handshaking exchange of the GRE-based Ascend Tunnel Management Protocol (ATMP)

All end-to-end tunneling protocols have up to four special entities – depending on where tunnels originate and terminate – with names similar to these:

- The Mobile Node is the remote client or server initiating the VPN session. Mobile Nodes may be stationary, i.e. attached to a LAN, or truly mobile, e.g. a traveling employee's PC.
- The Home Network is the private network containing the resources the Mobile Node wishes to access.
- The Home Agent resides in the network access equipment at the Mobile Node's Home Network site or in the destination server.
- A special Foreign Agent, which acts on behalf of a Mobile Node or Home Network client or server, resides in the network access equipment at the local site or NSP POP – at either or both ends of the connection.

Tunneled packets are sent across the Internet from agent to agent using each agent's Internet address in the header to designate source and destination, depending on the direction. The source agent (Home or Foreign) creates the tunnel's header; the destination agent (Foreign or Home) removes the tunnel header, and delivers the original packet to the Mobile Node or the Home Network, respectively. The tunnels can either be static or dynamic. Static tunnels, which remain active for extended periods of time, are acceptable for site-to-site VPNs. Dynamic tunnels are activated only as traffic requires, and are, therefore, more secure.

The location of the agents determines where tunnels originate and terminate. The diagram shows two examples. With the Point-to-Point Tunneling Protocol (PPTP), the Home Agent that originates/terminates the tunnel is in the server (Windows NT or NetWare). With the more advanced Layer 2 Tunneling Protocol (L2TP), the agents can be in clients (Mobile Node), servers (Home Agent) or network access equipment (Foreign Agent) at either the NSP's POPs or at the organization's sites. Network access systems that originate and/or terminate tunnels also have special names, such as L2TP Access Concentrator ("LAC") and L2TP Network Server ("LNS").

### End-To-End Tunneling

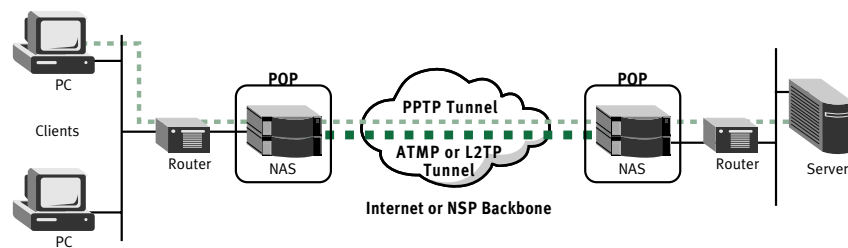


Figure 10 – Tunnels originate and terminate in different places, depending on the location of the Home and Foreign Agents. Shown here is an example of POP-to-POP tunneling with L2TP, and client-to-server tunneling with PPTP.

**Virtual IP Routing (VIPR)** extends private route tables and address spaces from the enterprise into the service provider's routing/switching infrastructure. Essentially, a virtual IP router is a logical partitioning of a physical IP router owned and operated by the service provider. Naturally, a single physical router can support numerous individual VPNs. The virtual routers that define a particular VPN are configured and managed as physical routers, making VPN implementation and operation integrate seamlessly with existing systems and procedures. All of the facilities for managing physical routers, for example, are available to manage virtual routers and, hence, the VPN itself. Each virtual router is configured with its own closed user group, which adds a layer of security beneath any other provisions (discussed in the next section). Of particular appeal to the enterprise is VIPR's ability to use private IP addresses. Finally, some virtual routers are able to dedicate physical elements, such as WAN interfaces and links, to a particular VPN, which is attractive to organizations with particularly demanding applications.

**Combinations and permutations** of the various compatibility options are permitted in a single VPN. An enterprise-wide VPN, for example, might use tunneling for remote access by individual telecommuters and virtual IP routing to interconnect all multiuser sites. Virtual private trunking is 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 should operate transparently to all users and sites thereafter.



## Security

Security provisions put the “private” in Virtual Private Networks. Providing adequate security is often the primary concern for organizations considering use of an Internet-based VPN. Many IT managers have become accustomed to the inherent privacy afforded by private networks, and may consider the Internet “too” public for private networking needs. With the proper security provisions, however, a VPN can be made even more secure than the typical PSTN-based private network. Virtual IP routing and virtual private trunking are inherently more secure than the Internet, but VPNs using these services can still benefit from additional security provisions.

There are three P’s that, together, constitute total network security:

- **Protection** of resources through a dynamic firewall defense
- **Proof** of identity through both user and packet authentication
- **Privacy** of information through snoop-proof packet encryption

All three P’s are equally important in any enterprise network, including a VPN. Exclusively private networks may use only simple passwords for proof of identity, and take for granted both protection of resources and privacy of information. But any time a private network interfaces to a public network, none of the three P’s can be taken for granted. So in any VPN, a firewall should exist at every interface to the public network, and authentication and encryption should be used as needed on an application-by-application basis.

### VPN security provisions should meet the following three objectives:

- **Furnish adequate security** – A minimal security system should have a firewall at every site and authenticate users with passwords to protect VPN-accessible resources from unauthorized access. The addition of encryption and packet authentication protects data in transit. Other levels of security are available, and the more levels provided, the more secure the VPN becomes.
- **Afford simple and secure administration** – The VPN security provisions chosen should be easy to both set up initially and maintain over time. The security system’s administrative functions must also be secure from tampering by users.
- **Create no burden for users** – Even legitimate users may attempt to circumvent security methods that are difficult to use, so the security system should make logging on to the VPN as easy as logging on at a LAN-attached workstation.

### Tunneling Protocols: Making the Virtual Paths in Virtual Private Networks

- *Point-to-Point Tunneling Protocol (PPTP), created by Microsoft and Ascend Communications, is an extension to the Point-to-Point Protocol (PPP) for Windows NT and NetWare client/server environments.*
- *Layer-2 Tunneling Protocol (L2TP) is a proposed industry standard that will combine the best features of PPTP and Layer-2 Forwarding (L2F) to accommodate IP, IPX, AppleTalk, NetBIOS, NetBEUI and other PPP-supported protocols.*
- *Ascend Tunnel Management Protocol (ATMP) defined under RFC 2107 which implements both PPTP and Generic Routing Encapsulation (GRE) as defined in RFCs 1701/1702.*
- *Data Link Switching (DLSw), originally defined by IBM and now an industry standard, encapsulates SNA traffic (the LU 6.2 protocol) in IP.*
- *IP Security (IPSec), which adds packet encryption and authentication to other tunneling protocols, also has a Tunnel Mode of operation to provide basic tunneling on its own.*

**Firewalls** are essential in any VPN. A firewall passes only authorized traffic for all trusted users, and blocks everything else. In other words, all attempts at access by unknown or untrusted users are stopped, 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 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 network security system. Any "unlocked door" makes resources throughout the enterprise vulnerable.

The biggest single limitation of most firewalls is that securing every single connection becomes cost-prohibitive, thus negating the cost-saving advantages of a VPN! The ideal firewall solution, therefore, should meet all of the following criteria:

- It should be integrated with the remote access equipment to make the protection both effective and affordable, thereby preserving the VPN advantages.
- An optional unprotected "de-militarized zone" (DMZ) LAN interface should be available, on the Internet side of the firewall, for Web and other public servers.
- A low-cost, software-only version should be available for individual users with ordinary analog modems.
- The firewall should strictly enforce a policy of "that which is not expressly permitted is denied."
- The design should employ state-of-the-art dynamic stateful inspection for maximum protection.
- The offering must be certified by the International Computer Security Association (ICSA).

**IP Security**, or simply IPSec, is defined in a series of initially emerging standards (RFCs 1825-1829) and Internet Drafts to provide data authentication, integrity and confidentiality. There are two aspects to IPSec's protection: the Authentication Header (AH) and the Encapsulating Security Payload (ESP), which can be employed individually or in combination. AH adds a digital signature to the header using the Message Digest (MD) or the Secure Hash Algorithm (SHA). AH authenticates the packet with a digital signature and assures data integrity by enabling detection of any alteration during transmission. The Certificate Authority (CA) is a trusted third party that certifies the digital signatures. ESP encrypts and decrypts either the entire packet (Tunnel Mode) or just the data (Transport Mode) using the Data Encryption Standard (DES) or Triple DES (3DES). ESP keeps transmitted data strictly confidential, and can provide adequate user authentication and data integrity for most applications. Both AH and ESP employ digital "keys" at each end of the connection that are known only to authorized clients and servers.

## Encrypted Tunnel Mode Packet

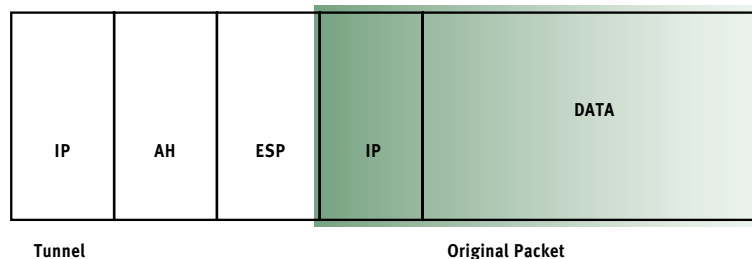


Figure 11 – IPsec’s Encapsulating Security Payload (ESP) encrypts or “scrambles” transmitted data to ensure confidentiality. IPsec’s Authentication Header (AH) adds a digital signature for integrity. Keys, which are long strings of characters known only to authorized users, are employed to lock and unlock the packets.

For managing security provisions, the industry-standard RADIUS (Remote Authentication Dial-In User Service) database maintains user profiles that contain passwords (authentication) and access privileges (authorization). For managing the keys that “lock” and “unlock” encrypted packets, IPsec uses a combination of the Internet Security Association Key Management Protocol (ISAKMP) and the Oakley key determination protocol, which together make up the Internet Key Management Protocol (IKMP) or Internet Key Exchange (IKE) standard. Optionally, the Diffie-Hellman standard of public key encryption can be employed to establish and exchange private keys.

Additional security options may be supported by some NSPs, such as calling line ID (CLID) and callback. Certain other security standards being proposed for Internet commerce are not required but can be used with VPNs; these include the Secure Sockets Layer (SSL), Secure HTTP, Secure MIME, Secure Electronic Transaction (SET) and Private Communications Technology (PCT). For example, you can implement SSL over an IPsec encrypted VPN.



## Availability

Availability has three equally critical dimensions – uptime, throughput and latency – and private networks offer inherent assurances for all three. For VPNs, uptime assurances are generally covered by a Service Level Agreement (SLA). Throughput and latency are elements of Quality of Service (QoS) provisions. Together, uptime, throughput and latency assurances make a VPN perform as well as, if not better than, a fully-redundant private network configuration.

- **Uptime:** The PSTN, the basis for most private networks, is remarkably reliable. So too, are the Frame Relay and ATM networks offered by the public carriers. The Internet may or may not be so reliable, depending on the arrangement with the service provider. In all situations, uptime assurances in excess of 99% are available, with money-back guarantees when the service provider fails to deliver. Organizations concerned about the dependability of VPNs should insist on some form of service agreement with the service provider(s).



- **Throughput:** Bandwidth requirements range from analog modems, that operate in the 28.8-56 Kbps range, to leased lines operating from 56 Kbps to 1.54 Mbps and beyond. Naturally, larger sites require greater bandwidth. In the PSTN, bandwidth is available as dedicated or switched circuits in increments of 64 Kbps. In the Internet, Frame Relay and ATM networks, bandwidth is available on demand or as permanent/switched virtual circuits in virtually any amount.
- **Latency or Delay:** With such generous bandwidth in the new public network, latency and variations in latency become the determining factors for certain applications, especially voice and host/terminal communications. Anyone who has experienced a telephone call via satellite can appreciate the need for minimal latency. A single-hop satellite link adds about a quarter second one-way delay that, while not seeming like much, is noticeable – and annoying – in a conversation. Similarly, many host/terminal protocols, such as those in IBM's System Network Architecture (SNA), have similar “real-time” requirements. The more demanding of the two is voice, where the threshold for acceptable latency is about one-third of a second.

**Service Level Agreements** guarantee network uptime will exceed 99 percent, and some even add QoS assurances to cover throughput, latency and even packet/frame/cell loss. Meeting such stringent service levels requires resiliency and redundancy in the backbone switching infrastructure. So if dependability is a concern, look for service providers that have the following carrier-class redundancy features in their networks:

- Fully redundant, hot-swappable control processors, I/O modules, power supplies and cooling fans – all with automatic failover
- Trunk and access line redundancy, with the option to aggregate switched links for on-demand backup bandwidth
- Powerful rerouting capability that automatically reroutes any failed or congested circuit to an alternative backup path, with the option to designate reroute preferences for maximum efficiency

**Quality of Service**, with its two dimensions (throughput and latency), comes in three levels or classes: best effort, relative and absolute. (See [Supplemental VPN Performance Boosters](#) sidebar for additional ways to maximize performance.)

- Best effort is, essentially, the absence of QoS; neither throughput nor latency is assured. Most users of the Internet today receive best effort service.
- Relative QoS prioritizes traffic using the Type of Service (ToS) field in the IP header. The Internet's ability to deliver on such a request depends on two factors: the current network load and the percentage of traffic requesting prioritization. Hence the reason this service is relative. And even if the bandwidth can be delivered, relative QoS has no provision for minimizing latency.
- “Absolute QoS” guarantees delivery of both sufficient bandwidth and a not-to-exceed latency with no ifs, ands or buts – in other words: absolutely.

Class of Service	Throughput Assurance	Latency Assurance
Best Effort	No	No
Relative	Maybe	No
Absolute	Yes	Yes

Figure 12 – The table summarizes the three forms of QoS. “Absolute” QoS is necessary for voice and certain host/terminal applications because it is the only class of service that offers minimal latency.

Each type of QoS serves a different market segment. Best effort is best for basic \$19.95 consumer or business Internet access. Relative is ideal for extranets and non-critical remote LAN access needs. Absolute is essential for real-time voice over IP, SNA VPNs and business-critical VPNs. The typical organization might employ all three levels of service to meet its total enterprise networking needs cost-effectively.

## Supplemental VPN Performance Boosters

*The following capabilities help maximize performance of any VPN:*

- ISDN bandwidth-on-demand with the Multilink Protocol (MP) and the Multilink Protocol Plus™ (MP+)
- Digital modem technology to improve analog modem performance, including use of new asymmetric 56 Kbps modems
- Digital Subscriber Lines (DSL) for high-speed continuous access
- Standard STAC or other data compression
- Hardware-assisted encryption and compression
- IP multicast efficiency for any-to-many “multipoint” applications
- Frame Relay Direct to channel IP tunnels through virtual circuits in the NSP’s Frame Relay backbone, rather than route traffic unnecessarily as IP packets
- Enterprise equipment with integral PSTN-based dial backup and overflow provisions



## Manageability

Organizations have always wanted to manage their enterprise networks end-to-end, including those portions of the in-between public network. But this powerful provider/subscriber capability has remained elusive, until now. Surprisingly, management is one area where VPNs are often superior to private networks. Most private networks are managed “edge-to-edge” only by both the service providers and their subscribers. The typical service provider manages its network up to the edge of the enterprise network; the subscriber manages its enterprise network up to the edge of the service provider’s WAN.

VPNs make it possible to eliminate this traditional “separation of powers” with advanced capabilities that permit provider and subscriber systems to work in concert to manage the entire private/public VPN end-to-end. This Customer Network Management (CNM), implemented by the service provider lets subscribers supervise their private portion of the public network infrastructure, and gives service providers the ability to manage, if required, all the way into the customer premises.

With a provider/subscriber management system, the organization’s network manager can monitor, reconfigure, troubleshoot and otherwise manage the entire VPN. The more powerful CNM capabilities include controlling network access at the edges, real-time status and performance monitoring through the public network’s core, and accounting of end-to-end service levels. Finally, a good solution will also ensure that no other organization can access anything that will interfere with your organization’s VPN.

**Security and accounting administration** is about as capable, yet simple, as possible with the Remote Authentication User Dial-In Service (RADIUS) standard. RADIUS handles all security, accounting and other administrative needs with individual profiles for all VPN members. RADIUS employs a client/server architecture with network access switches as the clients, and the RADIUS database as the server. Proxy RADIUS capability lets a server at the NSP POP query the organization's server to access VPN member profiles. In this way the organization maintains total control over access to its VPN resources, while allowing the security provisions to be enforced at the NSP POPs. This ability to handle distributed management with centralized control makes RADIUS ideal for VPNs of any architecture.

### The Role of RADIUS in VPNs

- RADIUS (Remote Authentication Dial-In User Service) is a standard for maintaining authentication, authorization, accounting and auditing information for remote access networks, including Virtual Private Networks
- RADIUS employs a client/server architecture: RADIUS is the server; network access equipment become its clients
- "Proxy RADIUS" lets one server become a proxy for accessing another RADIUS server at any location in the network (see diagram)
- Normally both the organization and its NSP(s) have RADIUS servers
- The organization's RADIUS server is the point of control for authentication and authorization, i.e. it is the repository for individual profiles of all VPN members
- Each profile identifies a particular node's Home Agent and Home Network, as well as any applicable user password(s) and access privileges
- For workers who travel (truly mobile Mobile Nodes), separate profiles are used for dial-out and dial-in capabilities

### Directory Enabled Networks

The Directory Enabled Network (DEN) initiative is an effort to standardize how network directory information is acquired, disseminated, stored and used. DEN affords a fully distributed directory architecture that is compatible with the Lightweight Directory Access Protocol (LDAP), Novell Directory Services (NDS), X.500, RADIUS and other popular directory services.

DEN takes a policy-based approach to all aspects of networking, including user profiles, networked applications, security, service provisioning and accounting. The standard is expected to become the preferred way to control network resources and user access capabilities. When available, DEN will afford a powerful yet simple way to establish and maintain VPNs. In the meantime, proprietary vendor solutions will be available. There will be a short term requirement to upgrade equipment to support these specific vendor solutions.

### Proxy RADIUS Configuration

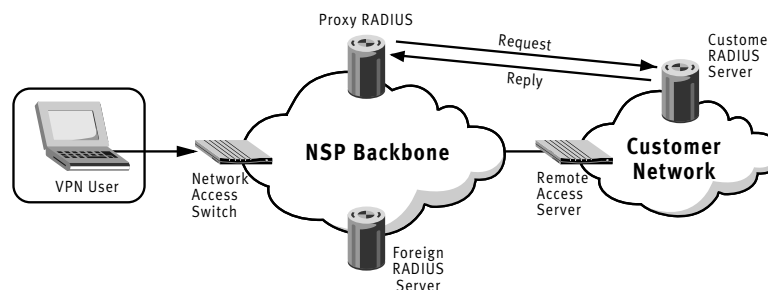


Figure 13 – The primary RADIUS server can be used as a proxy for reaching other RADIUS servers, anywhere in the network. A common use of Proxy RADIUS is for a server at the NSP POP to access VPN member profiles on a server at the organization's site.



With a dependent VPN the organization can – and probably should – administer all user security and access capabilities, which is quite easy to do. The NSP's RADIUS server acts as a proxy for the organization's RADIUS server, which contains the database of user profiles. The alternative would be for the organization to turn over all necessary internal information – with regular updates – which may actually reduce the effectiveness of security. Gathering, “publishing” and distributing employee lists with sensitive security-related information is a risk-filled endeavor. Maintaining user profiles on a RADIUS database is a task best kept in-house, even with a dependent VPN.

An **independent VPN** is where the organization handles all VPN requirements on its own equipment, relegating the NSP to the role of an Internet “carrier”. The NSP sees only Internet traffic, and does not concern itself whether the traffic is for the Internet itself or for the VPN.

With an independent VPN, all participating sites exchange IP traffic with the local POP. If tunneling is employed, all traffic is encapsulated and decapsulated – and optionally encrypted and decrypted – at the organization's sites.

The independent approach is ideal for organizations that believe the VPN is too important to turn over completely to an NSP. Independent VPNs allow the organization to maintain direct control over day-to-day operations, while the total costs – both internal and external – may not be that much more than a dependent VPN architecture. NSPs can, of course, still provide certain complementary services, and the independent architecture can migrate to a hybrid one or even to a dependent one over time.

## Independent VPN Architecture

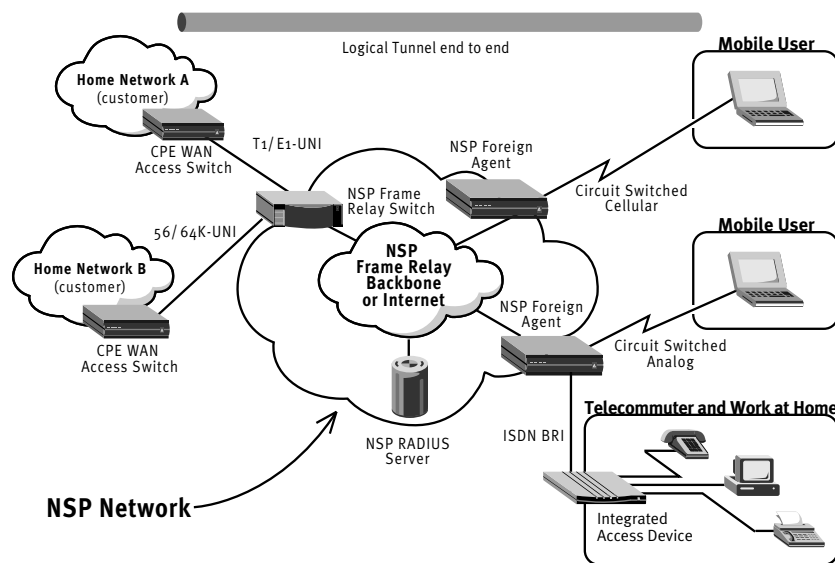


Figure 15 – With an independent VPN, the NSP's role is that of an Internet “carrier” whose only job is to haul IP traffic, much of it being tunnels.

The **hybrid VPN** involves a combination of dependent and independent VPN sites. Each site is one or the other, making the total Virtual Private Network a hybrid. For example, an organization may want to outsource the solution fully, but has some sites beyond the “primary” NSP’s service area. For the sites within the service area, the NSP can handle all VPN-specific requirements in its POPs. At the organization’s sites beyond the primary service area, the NSP can install VPN-capable equipment, then lease everything back to the organization. These VPN-equipped sites then access the Internet, and hence the Internet-based VPN, through another service provider’s POP. Because these specially equipped sites provide all VPN-specific functionality, they are independent from an architectural perspective. But because the VPN involves both dependent and independent sites it is, architecturally, a hybrid VPN. From the organization’s perspective, however, it is a fully outsourced solution that is totally “dependent” on the NSP for all sites – in one way or another. The enterprise equipment can even be managed remotely by the NSP, again as part of a fully outsourced solution. The other service providers merely handle the traffic just as they would any other IP traffic, and might even send monthly statements to the primary NSP for consolidated billing, so the organization gets a convenient, single invoice for the VPN.

## VPN Building Blocks

All Virtual Private Networks are constructed using the five fundamental building blocks depicted in the diagram. The end-user organization is normally responsible for its own equipment. The end user and NSP typically share responsibility for management and local access services. The network access switch and backbone/Internet are always the responsibility of the NSP(s). In a fully dependent VPN architecture, the NSP may take responsibility for everything except, perhaps, the security and some network monitoring and management capabilities desired by the end user. In any event, an end-to-end understanding of VPNs is helpful regardless of which party is responsible for which elements. An overview of all five building blocks is presented in this section.

## VPN Building Blocks

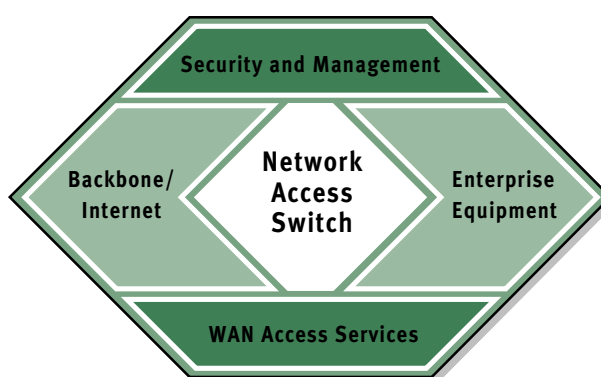


Figure 16 – Every Virtual Private Network is made up of these five fundamental building blocks.

## Enterprise Equipment Building Block

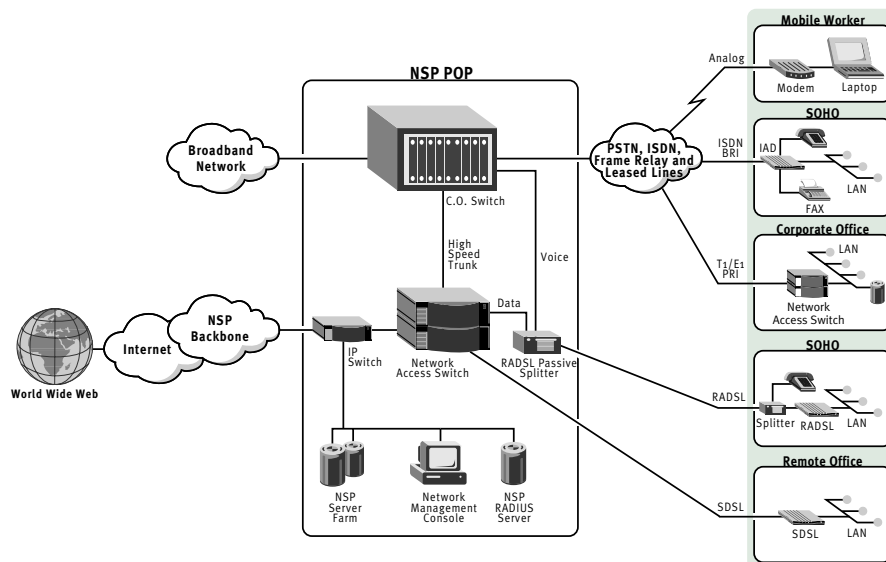


Figure 17 – All five building blocks are represented in this local view, or one end, of a VPN. Customer premises equipment defines the “edge” of the VPN.

## Enterprise Equipment

From the users’ perspective, equipment at enterprise facilities is where a VPN begins – and ends. The rest is left to the NSP. So equipment deployed throughout the enterprise is vitally important in any Virtual Private Network.

The type of equipment required depends on the VPN architecture. With a dependent VPN, the organization can use existing WAN equipment, such as ordinary routers or remote access servers. By contrast, an independent or hybrid VPN architecture requires systems that supports many of the same features needed in a network access switch at the NSP POP, such as provisions for tunneling and security.

This section outlines the required and desired features for enterprise equipment in two stages: a list of general requirements, followed by a discussion of site-specific needs.

General requirements for VPN-capable systems include:

- Support for L2TP, ATMP and PPTP tunneling protocols
- IP Security (IPSec) provisions for adding packet encryption and authentications to the tunneling protocols, and optionally, for its own direct tunneling capability
- Integrated and certified dynamic firewall for protection of local resources
- Software upgradable to conform with emerging tunneling and security standards
- Remote download of software upgrades, via the VPN
- Robust local and remote management to maximize uptime at minimal cost
- Adequate capacity to support anticipated traffic volumes
- An Ethernet LAN interface for attaching to the local network
- Support for the most cost-effective WAN option desired, such as T1/E1, ISDN PRI/BRI, xDSL, X.25, Frame Relay and ATM
- Built-in compression to maximize throughput
- 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 network access switch at the NSP's POP 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

Major sites, such as the headquarters or a large division, should be considered critical installations. These facilities have a large number of users, and some may be Web sites. A single line to such sites, whether in a private network or a VPN, is risky. Dedicated lines, while ideal for such critical applications, regularly become overloaded and can go out of service at any time. Supplemental dial-up bandwidth can handle either situation. A single, supplemental dial-up ISDN BRI line with 4:1 compression provides up to 512 Kbps of throughput – often enough to handle an overload condition or maintain Internet/VPN access until the primary link comes back on-line.

The best solution is a LAN-attached remote access router or network access switch with both primary and secondary WAN ports. The primary link might be a direct connection to the service provider's Frame Relay or ATM network. The secondary bandwidth should be brought into service automatically and transparently when the primary link is saturated or goes down. The secondary bandwidth should also automatically terminate when, in either situation, it is no longer needed. No on-duty attendant should be required once the system has been configured for the desired operation.



## The Piecemeal Approach vs. the Integrated Approach

### Piecemeal Solution of Network Access

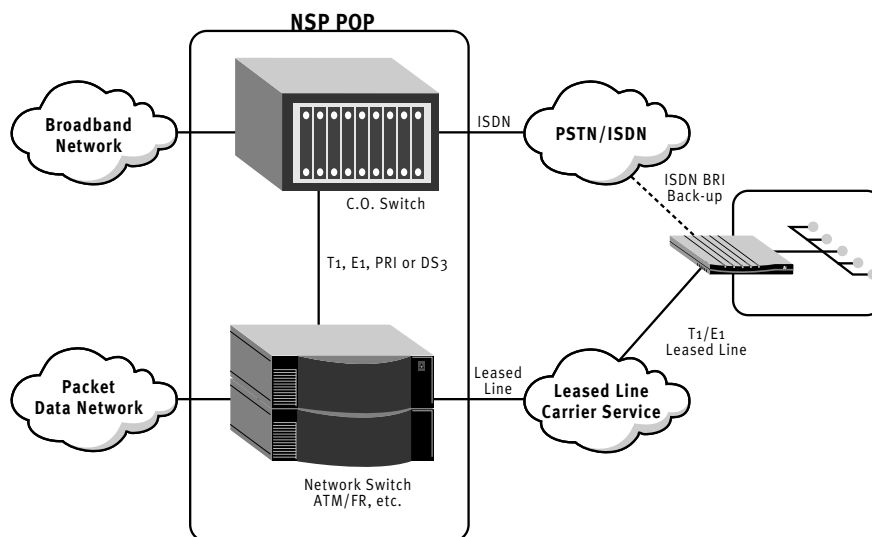


Figure 18 – The dual-WAN configuration offers the mission-critical availability needed by all major facilities in the virtual private network.

### Integrated VPN Approach

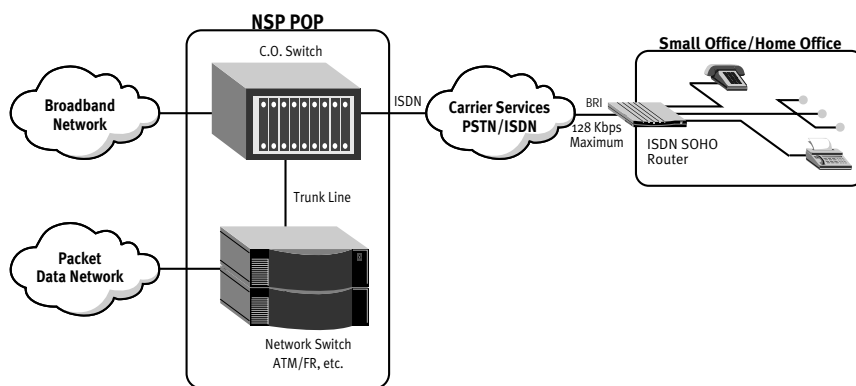


Figure 19 – The ISDN SOHO Router provides a complete dial-up data/voice/fax communications solution on a single BRI line.

## Major Site Connectivity

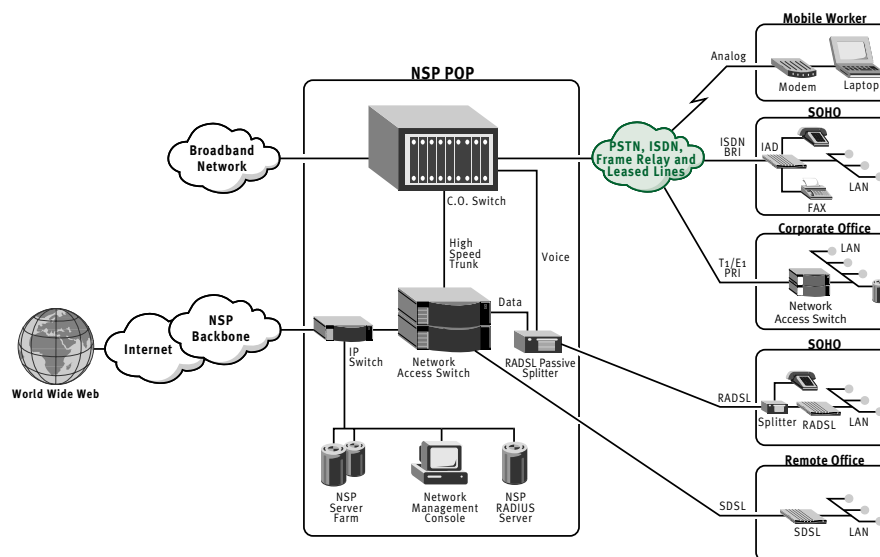


Figure 20 – Local WAN Services connect the user and site CPE to the VPN at the POPs.

**Remote offices** have a choice of ISDN terminal adapters that plug into a card slot on the local Windows NT or NetWare server, or stand-alone remote access routers. The terminal adapter (TA) is less expensive, which may be highly desirable when numerous offices are involved, but it imposes an increased security risk. The TA places devices directly on the Internet unprotected by a firewall similar to your typical modem and PC arrangement.

For a modest additional cost, the stand-alone remote access router provides a much more capable and flexible solution. Because it does not depend on the local server, the remote access router eliminates configuration complexities, consumes no server resources and can be managed remotely because it is always on-line. And one of the best VPN-related features of a robust remote access router is the integral firewall protection it affords. This firewall is a must for full or part-time remote users.

**Individual users** come in two types: mobile and stationary. Mobile workers have little choice but to use analog modems for the foreseeable future. The analog modem is the only remote access device compatible with the Plain Old Telephone System (POTS), and POTS is the only universally available service. Fortunately, for the daily access typical of those on the go, the modem's modest performance is generally quite adequate but H.11 unprotected.

For the full- or part-time stationary telecommuter, however, the better the performance, the better the productivity. ISDN at 128 Kbps, in the form of either plug-in interfaces or stand-alone units, offers excellent price/performance for the small office/home office (SOHO) environment. But a limitation in most homes adds an interesting twist. Many SOHO workers need three or more lines: the home line, a business voice line, a data line and, maybe, a separate fax line. The problem is that many homes and apartments are wired for only one or two lines. In these situations the SOHO router, sometimes called an integrated access device (IAD), provides an optimal solution. The SOHO router uses the two BRI channels as needed to

handle all data, voice and fax communications on a single line. Digital Subscriber Lines also offer integrated voice/data communications on a single pair of wiring (see the [DSL](#) sidebar in the next section for details).

Local WAN Services connect the enterprise with the NSP POPs. There are essentially three choices:

- Dial-up services, such as analog modems and ISDN are best used for part-time access by SOHOs, telecommuters and traveling employees.
- Continuous forms of access, such as that provided by leased lines or Digital Subscriber Lines, which are best for multi-user offices
- Direct Frame Relay or ATM access for larger sites

Beyond these three broad categories, choosing the best alternative is really only a matter of speed: In addition, do you need the integration of phone, fax and data in one box? How much throughput does the site need? When replacing a private network with the VPN, be certain to increase bandwidth by the amount of overhead associated with tunneling and encryption, and conversion to frames or cells. For new applications, an estimate of the traffic volume for each VPN site will be needed. You may want to consider a solution that allows you to consolidate your remote office equipment.

## Digital Subscriber Lines

*Digital Subscriber Line (DSL) technology increases the throughput of ordinary twisted pair wiring in the local loop. Voice telephone services use this same wiring, but employ analog signaling methods that severely limit bandwidth. DSL technologies achieve higher transmission speeds – up to 7 Mbps – by utilizing advanced digital signal processing techniques, similar to those used for ISDN and T1/E1 today. A DSL link, in effect, creates a high-speed “leased line” between the central office and the user site, which is ideal for a VPN. There are many different variations on the DSL theme; however, the three versions that can utilize existing twisted pair wiring and deliver both voice and data services are:*

- *ISDN Digital Subscriber Line (IDSL), pioneered by Ascend, delivers 128 Kbps performance and offers compatibility with existing ISDN access equipment.*
- *Symmetric Digital Subscriber Line (SDSL) furnishes 768 Kbps of throughput as a cost-effective alternative to leased lines.*
- *Rate-adaptive Asymmetric Digital Subscriber Line (RADSL) integrates lifeline analog voice (to power the telephone) with high-speed digital data for a total communications solution on a single pair of wiring. RADSL is available in Carrier Amplitude/Phase (CAP) and Discrete Multi-Tone (DMT) options that provide 64-640 Kbps in the upstream direction (from the subscriber) and 1.54-6.14 Mbps in the downstream direction, where bandwidth is needed the most.*

## Before DSL

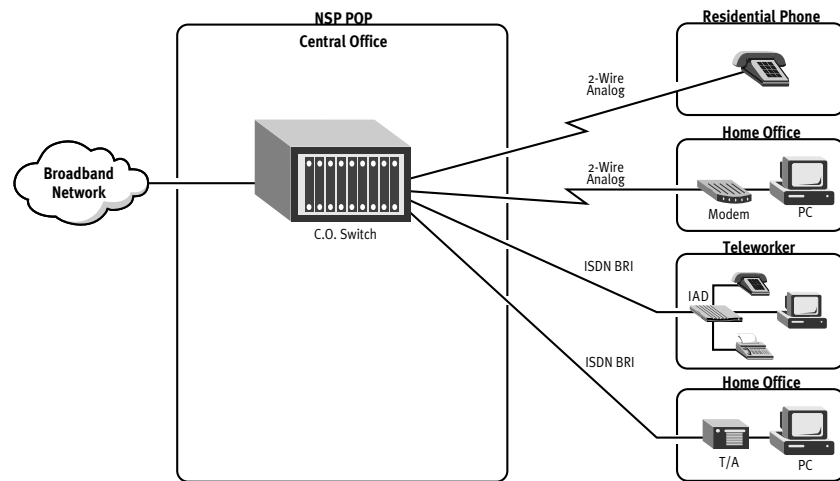


Figure 21 – Data traffic in general is contributing to congestion on PSTN switch.

## After DSL

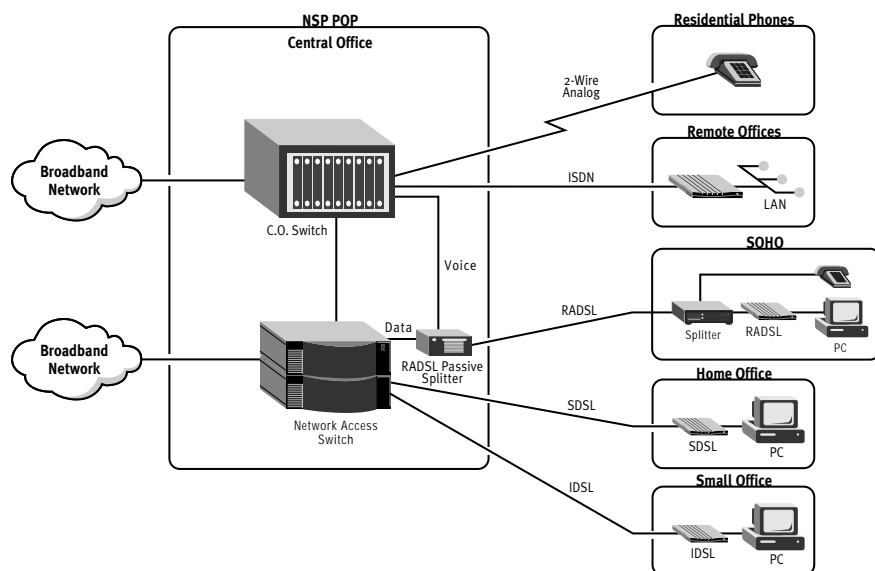


Figure 22 – DSL provides high-speed, continuous access while relieving the PSTN of analog modem and ISDN traffic.

## The Management Building Block

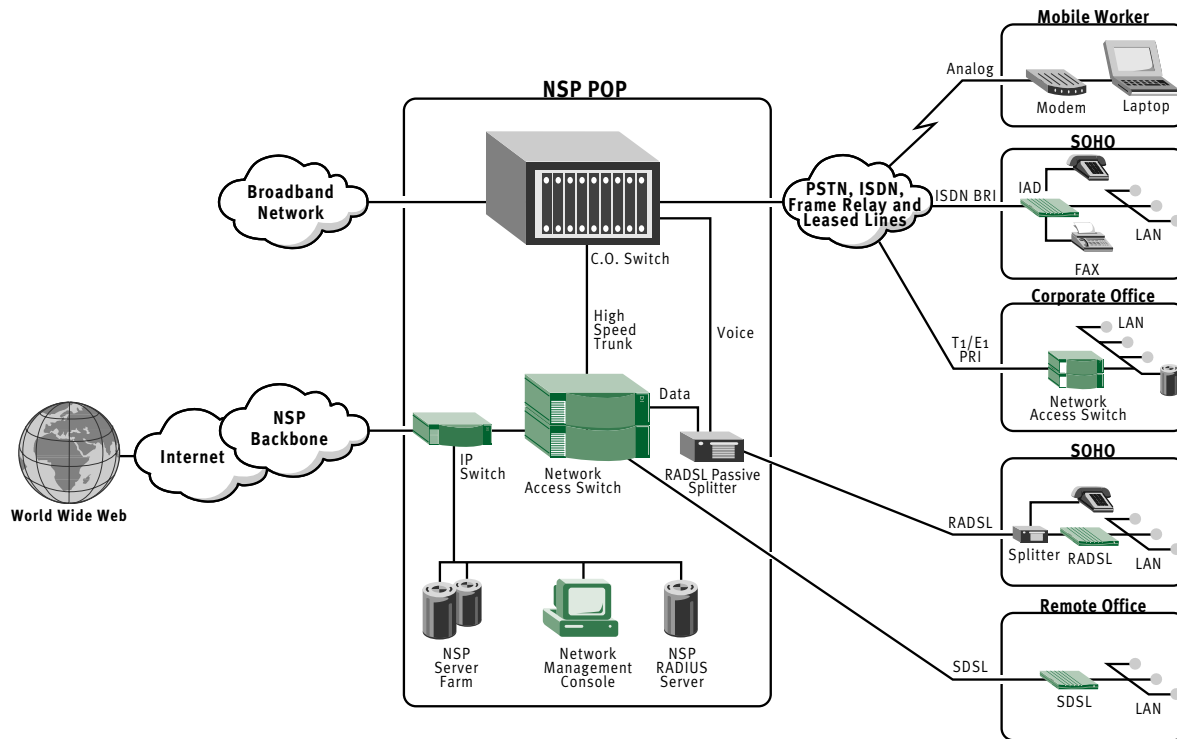


Figure 23 – Various tools are needed to manage the entire VPN infrastructure.

**Management** of VPNs to and through public networks requires a WAN-oriented approach, rather than the traditional device-oriented techniques associated with LANs. In other words, VPN environments require visibility and control of all equipment and links from one end to another, including everything in between. This higher level perspective allows the network to be viewed logically in its entirety, as well as physically in its detail.

Management of VPNs is normally a shared responsibility between the service provider and the organization (the subscriber). The subscriber must be able to manage its own equipment and its virtually private portion of provider's network, including all system resources and links. Specific tasks involve installing, configuring, monitoring and troubleshooting the network equipment and all interconnections. Such Customer Network Management (CNM) features needed to manage hybrid public/private VPNs include:

- 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, as well as traffic conditions, with fault alert/alarm generation based on user-defined thresholds
- Monitoring also offers a way to assess actual throughput on WAN lines, and helps control delivery of contracted Quality of Service (QoS) levels
- 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 bill-back 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
- Support for industry standards, like the Simple Network Management Protocol (SNMP)

## The Network Access Switch Building Block

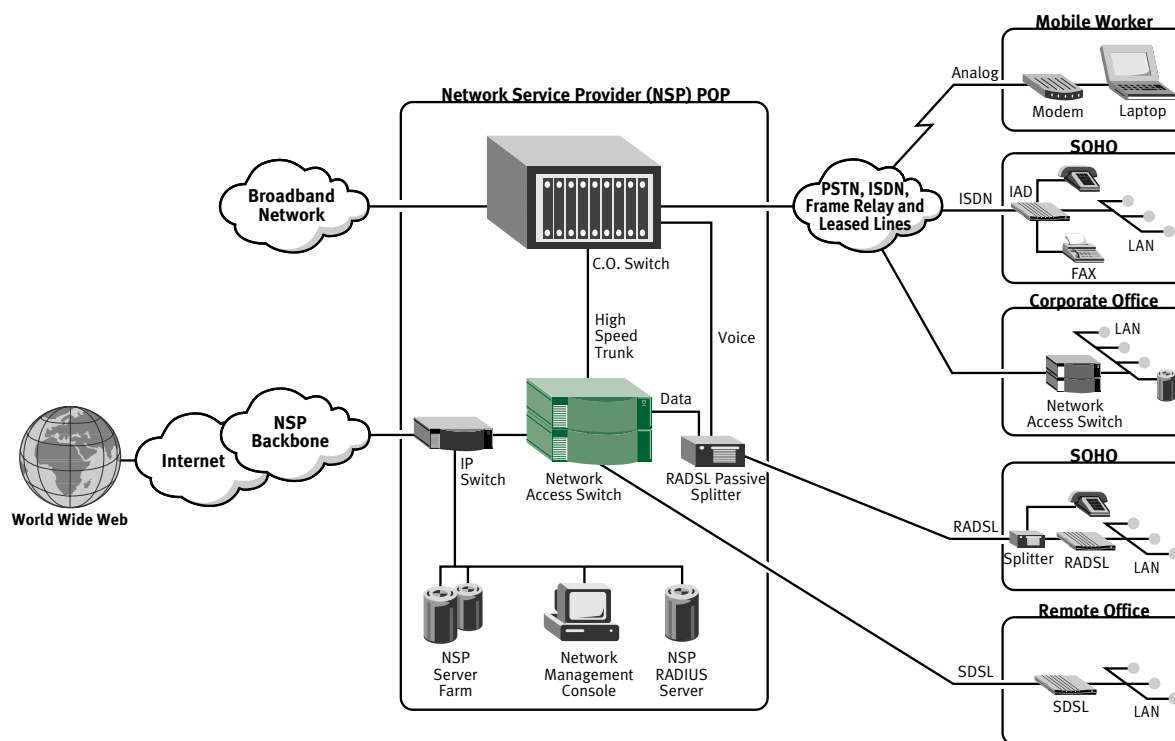


Figure 24 – The network access switch at the NSP’s POP is the core component of the complete end-to-end Virtual Private Network.

The **Network Access Switch** is the heart of the NSP point of presence (POP). Make sure your NSP has a capable, carrier-class network access switch with the following features:

- Variety of local WAN access options, including T1/E1, ISDN PRI/BRI, xDSL, DS-3, analog modems, cellular and X.25
- Ability to interface directly using Frame Relay or ATM
- Digital modem technology for better performance and compatibility with a broad assortment of analog modems, including new asymmetric 56 Kbps modems
- Adequate security provisions, including IPSec encryption and authentication
- Support for L2TP, ATMP and PPTP tunneling
- Support for IP Direct and Frame Relay Direct to channel tunneled packets through a virtual circuit within the NSP's IP or Frame Relay backbone, rather than route traffic unnecessarily onto the Internet itself
- Built-in compression to maximize throughput
- Dynamic bandwidth management for maximum performance at minimal cost
- Ability to accommodate IP multicast and Voice over IP, Frame Relay or ATM
- Software upgradable to conform with emerging tunneling and security standards
- Proxy RADIUS database support for administering security
- Resiliency with dual power supplies and hot-swappable interface cards for reliable operation
- Certification for operation with local carriers

## The NSP Backbone/Internet Building Block

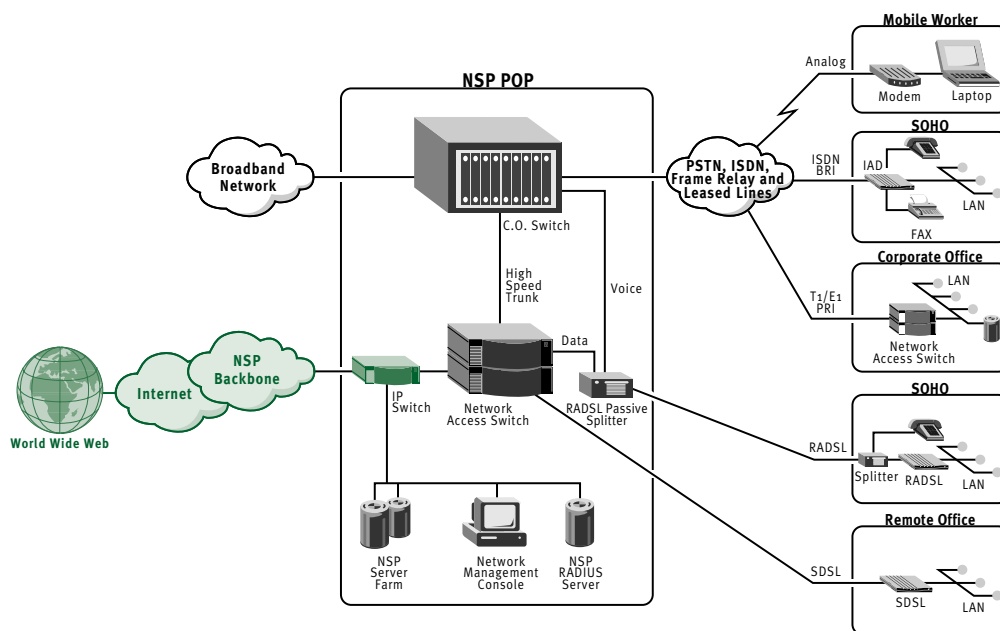


Figure 25 – The NSP's backbone and the Internet itself provide the "long distance" communications for the Virtual Private Network.

The Internet and/or NSP Backbone becomes the wide area network for the VPN. The volume of traffic flow requires high-performance switches and routers. Because the conventional router architecture is no longer able to accommodate the Internet's growth, causing both worldwide congestion and local service outages, switching technologies are now the preferred choice. Your NSP's backbone should have IP, Frame Relay and ATM switching with the following features:

- Virtual IP Routing capability with private IP route tables, closed user groups and interoperability with multiprotocol tunneling
- Virtual Private Trunking to provide high availability Frame Relay and ATM Services
- Compatibility with existing network infrastructures, including interoperability with conventional routers and LAN switches
- Support for IP multicast and Voice over IP, Frame Relay and/or ATM
- Full compliance with industry routing standards, such as RIP1/2, BGP4, EGP, OSPF, IS-IS and IP multicast to eliminate any need for proprietary gateways or special client software
- Next-hop address lookup fast enough to take advantage of the switching engine's low latency and high throughput
- Sufficient tunnel and route table capacity to keep pace with anticipated VPN and Internet growth
- Linear scalability with no performance degradation
- Overall capacity to support a sufficient number of LAN/WAN ports
- Wire-speed performance for all LAN/WAN ports with sustainable throughput that is independent of traffic characteristics, such as flows and cache hits
- Built-in resiliency, including dual power supplies and hot-swappable interface cards



High performance switches will solve one of the biggest paradoxes in the Internet. Today, with the limited performance of traditional IP routers, the only way to grow the Internet's overall capacity is to add more and more routers in parallel. But the proliferation of parallel routers causes next-hop route tables to grow exponentially. Updating these enormous route tables consumes Internet capacity; processing them brings many routers to a grinding halt. The solution is a streamlined infrastructure that adds capacity through better performance, rather than through more boxes.

## VPNs for Extranets

*Incorporating "outside members" into a VPN, such as customers, suppliers or business partners, is becoming an increasingly common requirement. Note that VPN membership involves access to private internal resources above and beyond those already available to the public on the World Wide Web. For example, customers may want to check order status, suppliers may need access to the master production schedule, and business partners may be on internal teams that use groupware for project management. If it makes sense to give outsiders access to internal resources – a business decision only the organization can make – then it makes sense to use an Internet-based VPN.*

*Outside members of the VPN are likely to be equivalent to either a remote office or an individual user. Even though these parties are not part of the organization, they are handled just like all other members of the VPN: with RADIUS profiles to specify "home" networks, passwords and access privileges. The only difference is that outsider access privileges are likely to be quite restrictive.*

*Defining RADIUS profiles for a limited number of suppliers and business partners is a manageable task, but the effort could become burdensome when a multitude of customers is involved. One way to simplify the job is to define a "generic" customer profile for use by all customers. A customer that requests access to the order processing database, for example, is given the generic user name and password. The access in this case, of course, should be read-only, which must be enforced on the server itself.*

*About the only special requirement with outsiders is network interoperability. The obvious, easiest, least expensive and best way to provide this interoperability is to use Internet addresses and IP applications. And the best application by far is the Web's powerful server/browser combination. Making an internal application or a subset of its information available on a Web server is likely to be a whole lot easier than getting numerous other organizations to convert to the native application, that might be on a mainframe or midrange system, or on a non-IP server. In effect, such an arrangement is similar to an intranet and has, therefore, been dubbed an extranet.*

*Some might ask, "Is an extranet really a Virtual Private Network?" The answer: If it uses the Internet it is! The same application could run on a private IP network constructed with leased lines or switched WAN services to establish connections with all business partners. But as a major computer vendor's sales force always asks, rhetorically, "Why would you want to do that?" Indeed, with the affordability, capability, dependability, flexibility and security of a VPN, why would any organization ever want a purely private network again?*

## Putting It All Together

All five building blocks come together to establish a potentially enterprise-wide Virtual Private Network. The VPN can involve numerous sites, NSP POPs and third party locations, which results in a single solution for access to private, semi-private and public information resources.

### VPN Benefits for the Enterprise

VPNs offer several major benefits to the enterprise:

- Lower costs – from 30 to 80%, according to industry analysts – for data networking and voice/video/fax telecommunications
- Extend reach and gain ubiquitous access to enterprise sites, other organizations and information worldwide
- Build new, secure communication relationships with buyers and suppliers
- Leverage enhanced and expanded services that are unavailable in the PSTN, such as multicast and ubiquitous interoperability
- Increase flexibility and simplify operations with a single per-site connection to the enterprise network, an extranet and the Internet
- Achieve high reliability through the carrier-class redundancy and resiliency of the public network infrastructure
- Gain greater control end-to-end with genuine Customer Network Management

## An Enterprise-Wide Virtual Private Network

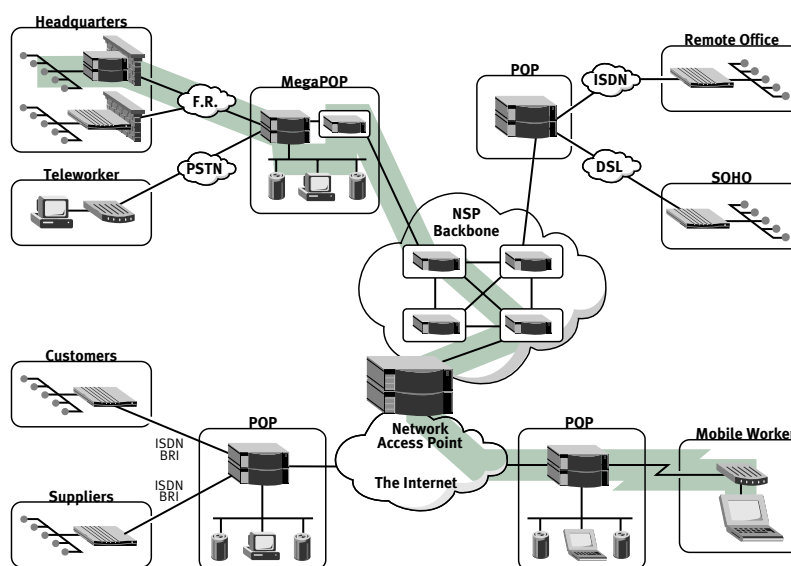


Figure 26 – An Internet-based Virtual Private Network holds the potential to connect the entire organization, along with its many customers and suppliers.

The diagram shows a VPN that connects the enterprise headquarters with remote locations and individual workers. Select customers and suppliers are also members of the VPN. Note that traffic can traverse the NSP's backbone alone, or both the Internet and the NSP backbone. A world-wide VPN is also likely to involve other NSPs, especially for access by mobile workers and customers. And therein lies the power of a Virtual Private Network: wherever your employees locate or travel, your very own VPN is just a local phone call away.

## APPENDIX

### VPN Case Study

#### Kinko's Unified Network for Customer and Business Access

**How Ascend helped Kinko's, a major provider of business services, bring Internet access to their customers and build one of the world's largest Virtual Private Networks.**

Leading corporations around the world rely on Ascend's systems and services to solve their networking challenges. This case study demonstrates how Kinko's is using Ascend solutions, particularly the Pipeline product family, to meet its current needs and plans for future growth. Because different Pipeline systems share similar features, other models might be more suitable for your particular needs. Ascend, or its NSPs and resellers, can help identify the right Pipeline model for your specific application and budget, and can assist in designing and implementing your Virtual Private Network.

Kinko's offers consumers photocopying, rental PC access and leading-edge business services from its worldwide chain of 850 retail stores. The company needed a cost-effective way to add Internet access for its PC rental service. Because customers pay by the hour for this service, it was important that Internet access be fast and reliable.

Kinko's also needed a robust and secure way to link its many locations to the headquarters and, as required, to each other. Cost analyses indicated that a private network would be prohibitively expensive to build and maintain, so Kinko's decided to create a VPN that used the Internet as a WAN backbone for its private business-related activities. This solution was particularly attractive because it allowed the same network serving Kinko's PC rental customers to be used by Kinko's 23,000 employees for accessing sales reports, company policies and procedures, credit information, and other business data. But such an arrangement could become a liability if it failed to include iron-clad security for the private information. Discovering that only Pipeline routers could provide that level of security while meeting other important criteria, Kinko's looked to Ascend for a solution.

#### Kinko's Needs

- *Provide fast Internet access to in-store PC rental customers for Web surfing, file transfer, e-mail and multimedia applications*
- *Connect over 850 stores with each other and to corporate headquarters in Ventura, California while providing for future growth*
- *Perform configuration and maintenance activities from a central location for convenience and consistency*
- *Save money on both PC management and monthly ISP service fees*
- *Establish tunneled and encrypted connections to keep public access isolated from corporate data*

## The Ascend Solution

Working closely with Ascend and Lucent Technologies' NetCare services, Kinko's installed an expandable network based on the Pipeline 130 router. Each location accesses a local Internet point of presence through a dial-up ISDN or Frame Relay link. The choice allows each store to select the more cost-effective WAN option, depending on usage levels, and local ISDN and Frame Relay tariffs.

Ascend's Pipeline 130 gives Kinko's a single, cost-effective solution to Internet access for its customers and VPN access for its internal communications.

To simplify and centralize management of every Pipeline 130 on the network, Kinko's uses Ascend's Navis network management software. Navis gives network administrators a bird's-eye view of the entire network, helping to maximize throughput and uptime because any bottlenecks or problems are quickly isolated and resolved.

The Pipeline 130's Network Address Translation (NAT) feature allows the many devices on each retail outlet's LAN to share the Internet connection and the router's IP address. This reduces monthly Internet access charges by eliminating the wasteful and expensive practice of assigning dedicated IP addresses to each and every device. The Dynamic Host Configuration Protocol (DHCP) feature enables each device on the LAN to learn its assigned IP address from the Pipeline 130 automatically, which eliminates the need for a network administrator to configure each device separately.

Ascend's Secure Access Firewall – integral to the Pipeline 130 – lets Kinko's use a single network connection, simultaneously, for both its rental PC Internet access service and its own internal VPN. The firewall protects the network from hackers by opening ports only as necessary and closing them at the end of each session. The firewall also contains an IPSec encryption option, which renders data unreadable to all but the intended recipients. IPSec's support of single or triple Data Encryption Standard (DES/3DES) cryptography ensures that even the most sensitive corporate data is kept safe from prying eyes.

By distinguishing rental PC traffic from corporate business traffic and creating secure VPN tunnels to transfer sensitive corporate data, the Ascend Pipeline 130 helps Kinko's use the Internet as a conduit for corporate communications, as well as for a fast and reliable information resource for customers.

### Solution Benefits

- *High speed ISDN and Frame Relay interfaces give in-store PC rental users fast, reliable Internet access*
- *IPSec-encrypted tunnels allow the Internet to be used as a Virtual Private Network for internal communication among all stores and the headquarters*
- *Navis network management and Secure Access Firewall software provide complete control of administrative and security provisions*
- *Built-in intelligence for IP address assignment saves money on monthly Internet access fees and address administration*

## Ascend MultiVPN Product Information

Ascend is making enterprise-wide VPNs a worldwide reality today with next-generation platforms and technologies. This appendix offers a high-level introduction to Ascend's MultiVPN product line. Details on these and other products are available at Ascend's Web site ([www.ascend.com](http://www.ascend.com)).

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 POTS (Plain Old Telephone Service) 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. The Pipeline 15 provide a less expensive alternative for individuals with less demanding needs.

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, Ascend's MAX WAN Access Switch affords the capability, scalability and flexibility enterprises need migrating from private to virtual private networks. MAX systems comes in a variety of models to fit any need – from two to over 2,000 concurrent sessions – all with support for L2TP, ATMP and PPTP tunneling. Available WAN options include T1/E1, ISDN PRI/BRI, xDSL, DS-3, Frame Relay, ATM, analog modems, cellular and X.25. For mission-critical facilities, the MAX offers both primary and backup/overflow bandwidth, as well as resiliency with dual power supplies and hot-swappable interface cards. Bandwidth on demand, Quality of Service (QoS) and Voice over IP (VoIP) features empower the MAX to meet the most demanding of applications.

Security for VPNs is the primary responsibility of Ascend's SecureConnect architecture, which includes the Secure Connect family of products and Ascend Access Control. Secure Access combines an ICSA-certified dynamic firewall with IPsec's packet encryption (DES/3DES) and authentication (MD-5/SHA-1). Secure Access is an integrated option for Ascend's Pipeline and MAX systems, and is also available in a software-only Personal Edition 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. CNM gives the enterprise a window into the infrastructure to view, monitor, reconfigure, trouble-shoot and otherwise manage its entire VPN, including its private portion of the public network.

## VPN Implementation Checklist

Proper and comprehensive planning is essential to a successful VPN. The following checklist provides a framework for planning your VPN.

### 1. First Steps to Implementing Your VPN

- ☐ Understand your requirements – what's the vision for your corporate communications
- ☐ Plan for the evolution/expansion of the network
- ☐ Define a pilot project
- ☐ Designate a project leader
- ☐ Develop a VPN architecture
- ☐ Select possible Outsourcing partner

### 2. Success Factors – consider the following when planning your VPN:

- ☐ Short and long-term scalability
- ☐ Outsourcing partners and services
- ☐ Project Management
- ☐ Line Provisioning including dial, ISDN or leased lines
- ☐ Configuration and shipment of VPN equipment
- ☐ Contingency planning (emergency upgrades, etc.)
- ☐ Management of outside partners
- ☐ Consider the impact on others (departments etc.)
- ☐ Help desk requirements
- ☐ Success measurements

### 3. VPN Technology Research

As you prepare for your VPN, you will need to research the following issues:

#### Compatibility

- ☐ How does equipment interoperate both from a hardware and software perspective
- ☐ Small vendors often have good technology and price, but you need to consider the company's viability
- ☐ Does your existing user authentication systems communicate to each other?

**Security**

- ☐ What are your security requirements?
- ☐ Is tunneling or encryption enough?
- ☐ Will encryption be required host-to-host, host-to-server, host-to-router, router-to-router etc?
- ☐ Is token-based authentication enough?
- ☐ What about encryption session key management and certificate authorities?
- ☐ How does this all fit together with global roaming? (IPASS etc.)
- ☐ What about Frame Relay and ATM PVCs or SVCs?
- ☐ What about virtual private trunks or private route tables?
- ☐ What about LAN network partition and secured system/departmental logons?

**Availability**

- ☐ What are your bandwidth requirements
- ☐ Define your quality of service requirements?
- ☐ Which service providers provide service level agreements to meet your needs?

**Management**

- ☐ Where is management required?
- ☐ Will you require a proactive network management system?
- ☐ What level of network management is required?
  - device, object, management
  - software and configuration management
- ☐ Define the level of security for the management system?
  - administrative logins - is it clear text or encrypted?
  - protection of the management system itself
- ☐ Consider real-time and long term trending and analysis options
- ☐ Will your service provider give you visibility of your VPN and is it secured?
- ☐ Do you have the resources to manage the network, or is outsourcing an option?

**4. VPN Project planning**

## Phase 1, Proof of VPN concept

- ☐ Determine facilities/location to be utilized for test
- ☐ Order dial, ISDN, frame relay or other lines to be used in test
- ☐ Order IP address space to be used if required
- ☐ Prepare other LAN network infrastructure
- ☐ Determine testing dates or duration upon which success or failure is achieved (include enough time for device, access line and configuration troubleshooting.)

### Phase 2, VPN Implementation

- ☐ Determine your VPN users – which sites are upgraded or effected
  - number of local and remote modem dial users
  - number of mobile workers/roaming sales force
  - number of ISDN TA users
  - number of users with ISDN routers
  - number of remote offices with ISDN, Frame Relay or leased line routers
- ☐ Determine timeframe to implement
- ☐ Incremental, controlled installations if possible
- ☐ Prepare existing locations where cabling, circuits or device movement is required
- ☐ Prepare new locations where cabling and circuits are required.
- ☐ Order equipment

## 5. Define Your Network Architecture

Diagram your existing infrastructure and note the following

- ☐ Names of locations
- ☐ Carriers or NSPs providing services
- ☐ Existing equipment
- ☐ Link speeds
- ☐ Number of users
- ☐ Number of devices
- ☐ Protocols used (IP, IPX, others)
- ☐ Applications accessed
- ☐ Issues to be resolved
- ☐ Person(s) in charge

## 6. Diagram Your New VPN Infrastructure

In addition to the above listed elements, include the following:

- ☐ Existing or new NSP providing VPN services
- ☐ Existing equipment – note those to be replaced, upgraded etc.
- ☐ Link speeds
- ☐ New technologies used (nat/dhcp etc)
- ☐ VPN services used: VPT, VIPR, VPRN (tunnel protocol and/or 40, 56 or 128 bit encryption)
- ☐ Quality of service – service level agreement
- ☐ Person(s) in charge – including contact at service provider



## 7. Testing

### Phase I Testing

- ☐ Configure Phase 1 Test
  - verify all required service provider VPN options are enabled/on
  - verify all required authentication mechanisms(i.e. Proxy RADIUS) are enabled/on
  - connect cabling infrastructure
  - connect devices to be tested
  - configure devices to be tested
  - dial clients
  - routers
  - authentication devices including RADIUS, Token authentication servers etc.
  - verify configuration parameters
  - verify minimal connectivity (ping etc.)
- ☐ Test minimal authentication mechanisms first
- ☐ Manual on remote access server (router?)
- ☐ RADIUS server (verify proxy radius is working at service provider)
- ☐ Token authentication systems
- ☐ Test applications including mapping of remote computer hard drives, ftp, e-mail, www
- ☐ Does solution scale?
  - from a configuration perspective
  - from a management perspective
  - from a compatibility perspective
  - from a performance perspective
  - from a network evolution perspective
- ☐ Reconfigure and test again when/where needed

### Phase II Testing

Extend the Phase I test to include an incremental number of remote locations.

- ☐ Test applications including
  - mapping of remote computer hard drives, ftp, e-mail, www
- ☐ Does solution scale?
  - from a configuration perspective
  - from a management perspective
  - from a compatibility perspective
  - from a performance perspective
  - from a network evolution perspective
- ☐ Reconfigure and test again when/where needed
- ☐ Note all issues and impact on implementation

## 8. Putting it All Together

- ☐ Plan the VPN working closely with your NSP(s):
- ☐ Make a list of all VPN applications
- ☐ Create a list of all VPN members, both sites and individuals
- ☐ The member list should include the location of and the WAN service option for each site or individual user
- ☐ Determine which sites/users will be “dependent” and which will be “independent”
- ☐ Generate a list of all new equipment needed
- ☐ Prepare for the implementation:
  - Check/test all existing equipment, possibly altering its configuration
  - If any existing systems proves unsuitable for the VPN, add its replacement to the equipment list
  - Order all necessary hardware and software
  - Obtain a sufficient block of IP address (potentially very small when tunneling, DHCP or NAT is used)
- ☐ Implement the pilot or “Phase I” VPN sites:
  - Install new equipment where needed, and configure all systems at all sites
  - Configure the RADIUS server with profiles for all VPN sites/users
  - Reconfigure the internal router internetwork, if necessary
  - Install, configure and test each site’s security provisions
- ☐ Test the pilot or “Phase I” VPN:
  - Check/alter equipment configurations
  - Verify proxy RADIUS operation
  - Assess the performance
  - Deploy the remainder of the network using the steps listed for both implementing and testing the pilot or “Phase I” VPN
- ☐ Perform on-going management responsibilities, which include:
  - Monitoring attempted security violations and taking corrective action
  - Evaluating and tuning end-to-end performance
  - Downloading of any new feature set software to remote sites

## Reference Material

The following materials are available from Ascend Communications:

- The *Corporate Remote Access Guide* discusses various aspects of remote networking, including an overview of the main building blocks.
- Ascend's Web site <http://www.ascend.com> has an extensive glossary along with a technical library that includes numerous white papers and technical briefs on pertinent topics.

The following is a list of Requests for Comments (RFCs) applicable to enterprise networking. RFCs are the way the Internet Engineering Task Force ([www.ietf.org](http://www.ietf.org)) establishes standards for IP and the Internet. Copies of the RFCs are available on the Information Sciences Institute Web site at [info.internet.isi.edu/1/in-notes/rfc](http://info.internet.isi.edu/1/in-notes/rfc)

- RFC 1001: Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods
- RFC 1002: Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications
- RFC 1041: Telnet 3270 Regime Option
- RFC 1205: 5250 Telnet Interface
- RFC 1234: Tunneling IPX Traffic Through IP Networks
- RFC 1490: Multiprotocol Interconnect over Frame Relay
- RFC 1533: DHCP Options and BootP Vendor Extensions
- RFC 1534: Interoperation Between DHCP and BootP
- RFC 1538: Advanced SNA/IP: A Simple SNA Transport Protocol
- RFC 1576: TN3270 Current Practices
- RFC 1597: Address Allocation for Private Internets
- RFC 1631: The IP Network Address Translator
- RFC 1646: TN3270 Extensions for LU Name and Printer Selection
- RFC 1647: TN3270 Enhancements
- RFC 1701: Generic Routing Encapsulation (GRE)
- RFC 1702: GRE Over IPV4 Networks
- RFC 1795: DLSw Switch-to-Switch Protocol (replaces RFC 1434)
- RFC 1853: IP in IP Tunneling
- RFC 2024: Definitions of Managed Objects for DLSw
- RFC 2106: DLSw Remote Access Protocol
- RFC 2114: DLSw Client Access Protocol
- RFC 2131: Dynamic Host Configuration Protocol (Obsoletes 1531 and 1541)
- RFC 2132: DHCP Options and BootP Vendor Extensions

**Notes:**

**Notes:**