3Com Technical Papers

Private Use of Public Networks for Enterprise Customers

New Standards-Based
Virtual Private Networks
Offer Cost Savings and
Business Opportunities

Private Use of Public Networks for Enterprise Customers

New Standards-Based Virtual Private Networks Offer Cost Savings and Business Opportunities

Contents

Private Use of Public Networks for Enterprise Customers

New Standards-Based Virtual Private Networks Offer Cost Savings and Business Opportunities

Virtual private networks (VPNs) offer cost-effective solutions to some of today's most critical networking challenges. Enterprises need a more affordable, scalable way to meet the demands of a growing community of remote users and to manage branch office connectivity. They need to be able to accommodate the pace and unpredictability of business by linking customers and partners into extranets on an ad-hoc basis. And they need to be able to provide all of this access to networked resources, including legacy systems and enterprise protocols, without compromising security.

The benefits of VPNs include the opportunity to save 50 percent or more in the cost of remote access and branch office connectivity. VPNs also offer tremendously increased strategic flexibility, which can lead to additional cost savings and potentially important business advantages.

This paper describes how VPNs cut costs and increase strategic flexibility. It describes and diagrams some of the most popular VPN applications. It explains the underlying tunneling technology, including system components and industry standards for tunneling and tunnel-based security. It introduces tunnel switching and the advantages it offers for increased enterprise network security, more flexible access to network resources behind firewalls, and more flexible service-level handling of tunneled traffic. The paper closes by discussing 3Com VPN solutions and their advantages.

Why Enterprises Need VPNs

Industry analysts predict that by 1999, 80 percent of corporate workers will have at least one mobile computing device.[1] IT organizations everywhere are struggling to meet this ballooning demand for remote connectivity and to deal with the resulting increases in network complexity and end-user support costs.

At the same time, IT must support growing branch office connectivity. Particularly in organizations growing through acquisition or merger, the ability to rapidly integrate separate and frequently incompatible infrastructures can be critical to the success of business relationships. In addition, there is the emerging requirement to deploy extranets that support unpredictable relationships with customers and business partners. IT also has to cope with the plethora of management and security issues these connections entail.

Virtual private networks (VPNs) offer solutions to these dilemmas. They provide enterprises with a number of ways to achieve substantial and immediate remote access and branch connectivity cost reductions by taking advantage of the networking infrastructures and services of Internet service providers (ISPs) and other network service providers (NSPs). VPNs offer a cost-effective, scalable, flexible, manageable, and secure means of handling network growth, of linking in newly acquired business units, and of supporting ad-hoc business relationships. Companies can get all these benefits while retaining central control over security and management of adds, moves, and changes.

Enterprises deploying VPNs will have an increasing range of VPN-based services to chose from. Infonetics Research[2] predicts that the VPN market will grow at more than 100 percent per year through 2001, when it will reach nearly $12 billion. They report that 92 percent of large ISPs and 60 percent of all ISPs plan to offer value-added VPN services by mid-1998.

What Is a VPN?

A VPN is a connection that has the appearance and many of the advantages of a dedicated link but occurs over a shared network. Using a technique called "tunneling," data packets are transmitted across a public routed network,

Acronyms and Abbreviations

AAL
ATM adaptation layer

CHAP
Challenge Handshake Authentication Protocol

IPsec
Secure IP

ISAKMP
Internet Security Association Key Management Protocol

ISDN
Integrated Services Digital Network

ISP
Internet service provider

L2F
Layer 2 Forwarding

L2TP
Layer 2 Tunneling Protocol

MPPE
Microsoft Point-to-Point Encryption

NSP
network service provider

POP
point of presence

PPP
Point-to-Point Protocol

PPTP
Point-to-Point Tunneling Protocol

[1] "Internet Remote Access," Network Strategy Service, *The Forrester Report,* vol. 10, no. 8, July 1996.

[2] "Virtual Private Networks," Infonetics Research, 1997.

such as the Internet or other commercially available network, in a private “tunnel” that simulates a point-to-point connection. This approach enables network traffic from many sources to travel via separate tunnels across the same infrastructure. It allows network protocols to traverse incompatible infrastructures. It also enables traffic from many sources to be differentiated, so that it can be directed to specific destinations and receive specific levels of service.

The basic components of a tunnel are:

- A tunnel initiator (TI)
- A routed network
- An optional tunnel switch
- One or more tunnel terminators (TT)

Tunnel initiation and termination can be performed by a variety of network devices and software (Figure 1). A tunnel could be started, for example, by an end user’s laptop equipped with an analog PC modem card and VPN-enabled dial-up software (basic tunneling and security capabilities are bundled into Windows 95 and Windows NT 4.0). It could also be started by a VPN-enabled extranet router on an enterprise branch or home office LAN, or by a VPN-enabled access concentrator at a network service provider point of presence (POP). A tunnel could be ended by a tunnel terminator or switch on an enterprise network or by a VPN gateway on an NSP’s network extranet router.

In addition, there will usually be one or more security servers. Along with the conventional application of firewalls and address translation, VPNs can provide for data encryption, authentication, and authorization. Tunneling devices perform these functions by communicating with security servers. Such servers also usually provide information on bandwidth, tunnel end points, and, in some cases, network policy information and service levels.

VPN capabilities can be added to existing networking equipment through a software or board-level upgrade. Once installed, the capability can be used for multiple VPN applications, each delivering substantial cost and/or revenue benefits.

VPN Benefits

Cost Savings

VPNs offer cost savings in the areas of communications charges, remote user support, and equipment.

- **Communications costs (leased line tariffs, long-distance charges).** Connecting two computers over long distances using the Internet can yield substantial savings over today’s dedicated leased lines and Frame Relay networks. The Internet is also less expensive than long-distance direct modem or ISDN calls. VPNs are money-savers because they enable remote users to make local calls to an ISP, which are then tunneled to a VPN device on the destination network.

Acronyms and Abbreviations

PSTN
public switched telephone network

QoS
Quality of Service

RADIUS
Remote Authorization Dial-In User Service

SMDS
Switched Multimegabit Data Service

TI
tunnel initiator

TT
tunnel terminator

VLAN
virtual LAN

VLL
virtual leased line

VPN
virtual private network

VTP
Virtual Tunneling Protocol

xDSL
digital subscriber line

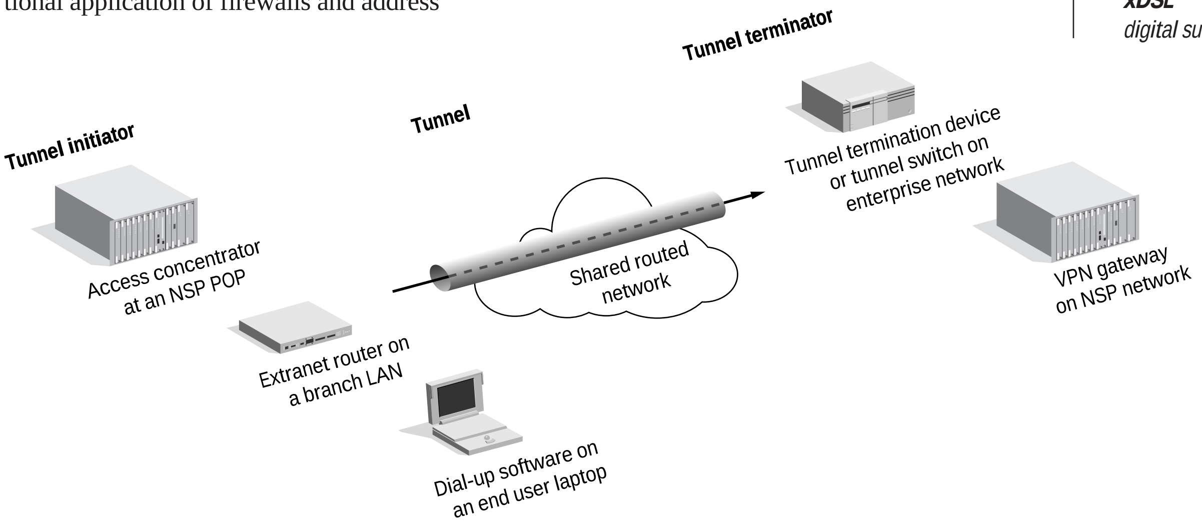
Tunnel terminator
Tunnel
Tunnel initiator
Tunnel termination device or tunnel switch on enterprise network
Access concentrator at an NSP POP
Shared routed network
VPN gateway on NSP network
Extranet router on a branch LAN
Dial-up software on an end user laptop

Figure 1. *VPN Components*

Users have the same experience as if they had dialed directly into the network—typically at half the cost of the most economical 800 number.

Branch offices can use VPNs to replace dedicated leased lines to company headquarters or to other branches. The branch LAN is connected to a business class NSP, which tunnels traffic from LAN users over the Internet or over its own network backbone to a LAN in another part of the user's enterprise. Branch users are still able to access the corporate network in the usual way, and the company saves money. The savings come not only from taking advantage of a shared network for long-distance transport but also because one WAN interface can be used for branch access to both the enterprise network and the Internet.

- **Remote user support.** In many companies, while a minority of network users are remote, they consume a majority of network support time. IT must support dial-in users with varying technical abilities and with equipment ranging from analog modems and ISDN terminal adapters to new cable modems and digital subscriber line (xDSL) connections. In addition, technical staff must either be located at branches or provide support remotely. Many companies can achieve substantial cost savings by shifting these support responsibilities from overburdened IT groups to the dedicated help desks of NSPs.
- **Equipment installation, maintenance, and obsolescence.** VPNs enable enterprises to save WAN equipment installation and maintenance costs, since a single WAN interface can serve multiple purposes. Companies can eliminate or reduce modem pools in favor of receiving dial-up traffic over an existing or augmented Internet connection. The same Internet connection can also support LAN-to-LAN branch internetworking as well as business-to-business links with customers and partners. And with less capital equipment, companies also lower their exposure to obsolescence.

Easy Scalability

VPNs offer immediate scalability with minimal effort. Enterprises can expand the capacity and reach of their network simply by setting up an account with a new NSP or expanding their agreement with an existing provider. In addition, installing VPN capabilities in remote offices is typically a simple task that does not require a technical specialist on site. A few simple commands should configure an extranet router for both Internet and VPN connectivity, and workstations can get their configuration automatically from the router.

Easy scalability allows agile responses to organizational change and market demands. A company completing an acquisition, for example, could link a dozen new branches into its network and add support for thousands of mobile users within just days, compared to the weeks or even months it could take to get leased lines or Frame Relay circuits installed. In addition, VPNs allow companies to link international locations into the network affordably while avoiding the complexities and delays associated with setting up Frame Relay circuits across borders.

Support for Ad-Hoc Business Relationships

Partnering is essential in many markets today, and the ability to move rapidly to mobilize combined forces can determine success. With VPNs, partners can implement new business relationships immediately. There's no need to delay collaboration while counterparts in the two IT organizations negotiate setup of leased lines or Frame Relay circuits. Connections can be made on an ad-hoc basis with any company that is on the Internet.

Full control

VPNs allow corporations to leverage the facilities and services of NSPs while continuing to exercise full control over their network. For example, companies can outsource dial access while retaining responsibility for user authentication, access privileges, network addressing, security, and management of network changes.

Enterprise VPN Applications

There are numerous ways in which enterprises can gain efficiency, cost, and security benefits. Following are three examples.

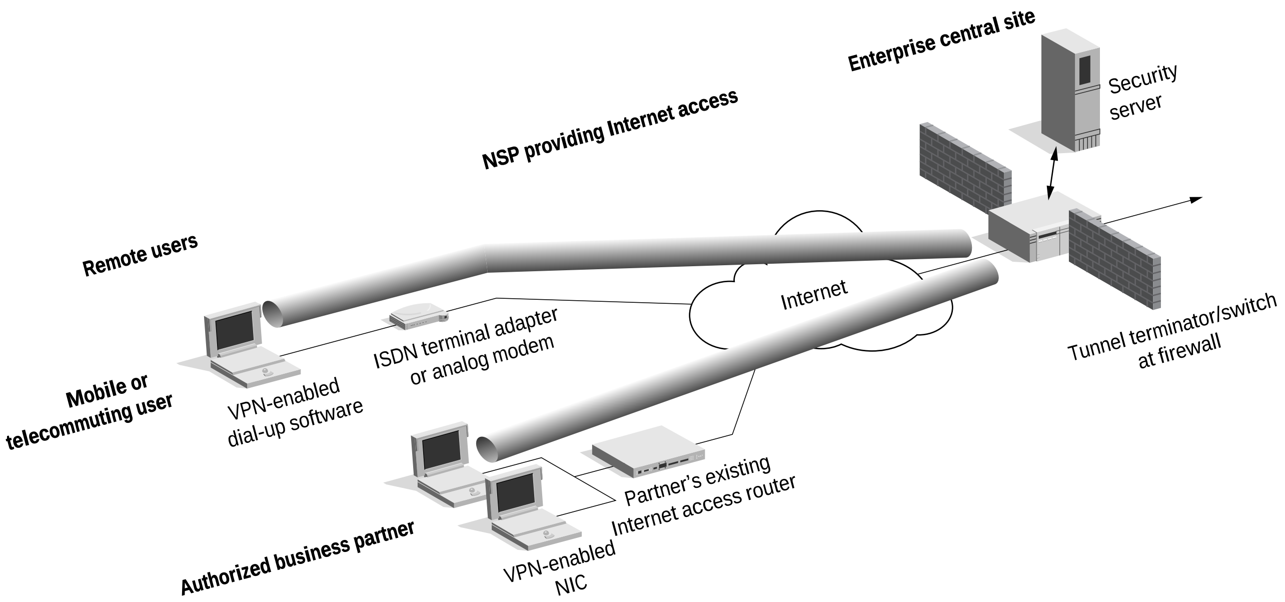
Enterprise central site
Security server
NSP providing Internet access
Remote users
Internet
ISDN terminal adapter or analog modem
Tunnel terminator/switch at firewall
Mobile or telecommuting user
VPN-enabled dial-up software
Partner's existing Internet access router
Authorized business partner
VPN-enabled NIC

Figure 2. *Global Internet Access*

Global Internet Access

Enterprises that use VPNs to replace or augment dedicated dial-up facilities with Internet-based dial-up (see Figure 2) can reduce both line charges and equipment costs. In fact, total operating cost savings can reach 60 percent or better.

VPNs enable remote users to access the corporate network by making a local, normally unmetered call to an NSP. The traffic is then tunneled over the NSP's network to the enterprise's Internet gateway and onto the corporate network. The NSP is not aware that the data is being tunneled and doesn't perform tunnel management tasks. Built-in security features (see page 12) work with the enterprise firewall to ensure user authentication, privacy, and data integrity.

Enterprises can use VPNs to offer traveling employees "global local access." By choosing an NSP with a global presence or setting up corporate accounts with several NSPs, companies can ensure that wherever their people travel, they can get onto the corporate network by making a local call.

Global Internet access can also be used to provide customers and business partners with secure access to extranet resources. In most cases, since users in these organizations will already be connected to the Internet, giving them the VPN capability necessary to access the extranet simply involves upgrading desktop networking software or activating features in existing software.

In this type of VPN, tunnels can be started by a LAN-based or dial-up VPN client using the VPN capabilities in Windows 95 or Windows NT Dial-Up Networking or special VPN software or modem card. A tunnel termination device or tunnel switch at the firewall at headquarters or another central location ends the tunnel. The company can control user authorization and other security functions from the central location.

The remote user is virtually plugged into the corporate network at the point where the tunnel terminates. The exact location will vary depending on the type of firewall being used. In the case of a single firewall configuration, the "plug-in" point will be the enterprise Internet access router where the firewall is deployed. In the case of a double firewall configuration, the plug-in point will usually be the "demilitarized zone" (DMZ), which is the network segment between external and internal firewalls. In either case, the remote user will have access only to those network resources that have points of connection at the network edge.

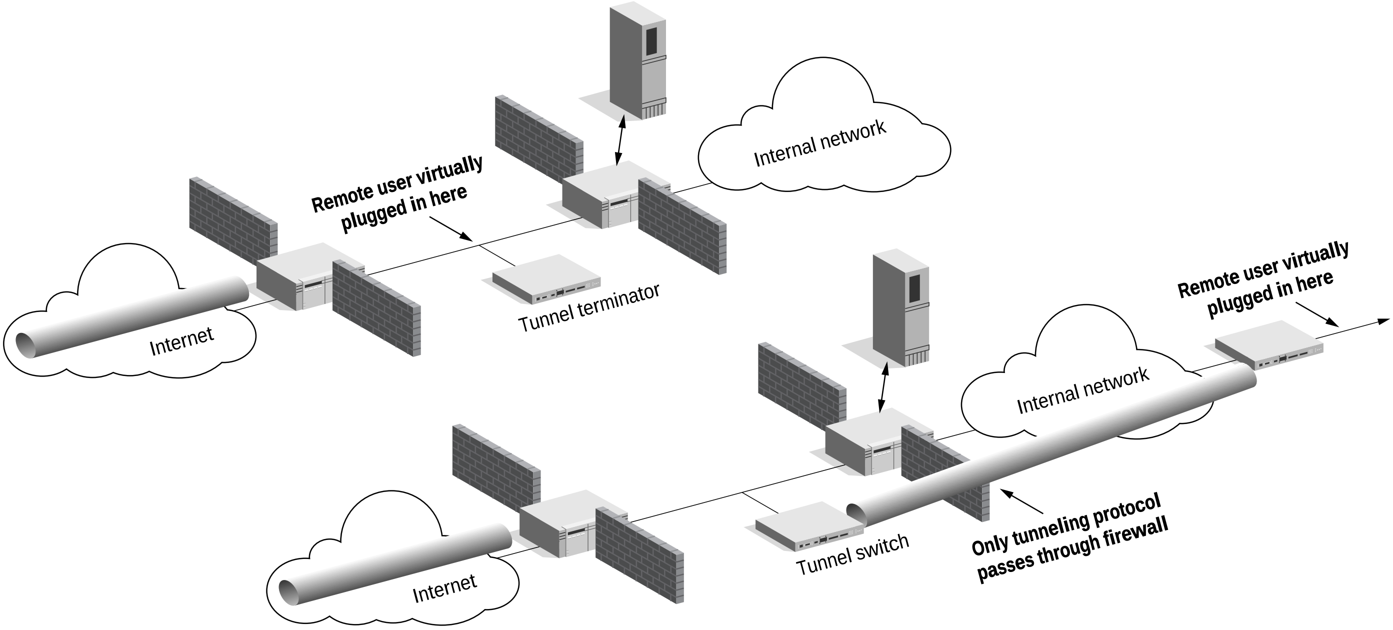
Internal network
Remote user virtually plugged in here
Tunnel terminator
Internet
Remote user virtually plugged in here
Internal network
Tunnel switch
Only tunneling protocol passes through firewall
Internet

Figure 3. *Tunnel Switching*

Optional tunnel switching can be used with global Internet access to increase security and flexibility (Figure 3). In this case, a tunnel switch at the enterprise extranet router or in the DMZ ends the incoming tunnel and starts a new tunnel to a tunnel termination device on the internal network. The remote user is thus virtually plugged into the network inside of the firewall, where more network resources are available (Figure 4). There are several advantages:

- **Multiple applications can be supported without having to open up multiple holes through the firewall.** Tunnel switching can eliminate the need to put special application servers in the DMZ between the external and internal firewalls. Tunnels can carry network traffic for a wide variety of IP applications (FTP, Telnet, etc.) safely across the firewall to internal servers. Since the protocols for these applications are encapsulated, a hole needs to be opened in the firewall only for the tunneling protocol.
- **Traffic from partners and customers can be segregated from remote employee traffic.** Tunnel switching enables tunnels coming in from different types of users over the same Internet interface to be terminated at different locations where different security policies can be applied. Network managers can easily view and control extranet activity and rapidly make adds and changes to accommodate new business relationships.
- **Remote users can access legacy network protocols and systems.** Tunnel switching can provide safe Internet-based access to networks, such as SNA, Novell NetWare, and AppleTalk, and the applications running over them. Frequently these protocols are not available in the DMZ.
- **Organizational divisions can share an Internet interface while controlling their own user authorization and access policies.** In a large organization that has various divisions (state government for example), these divisions can enjoy economies of scale from sharing one high-speed Internet connection, without relinquishing control over their own piece of the network. A tunnel switch can create tunnels that direct traffic to separate tunnel termination devices on each division’s LAN. Remote users are virtually plugged into these network segments, and the division can control network access privileges in its own way.

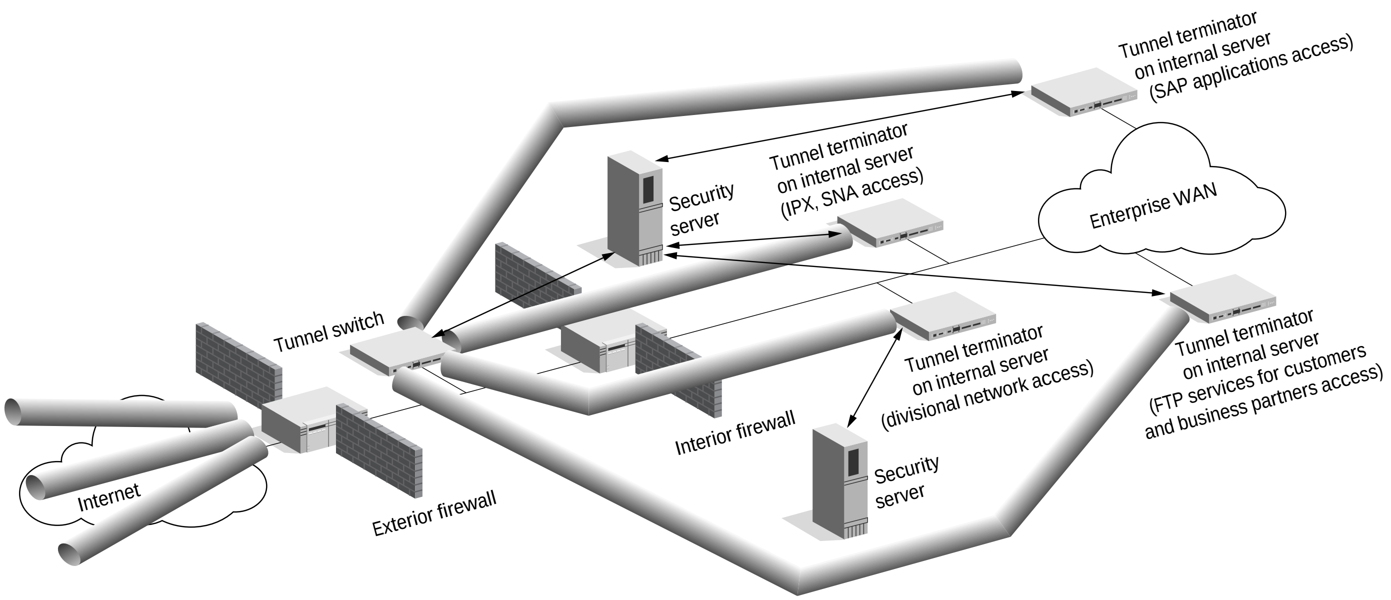

Figure 4. *Enterprise Tunnel Switching Application*

- **Companies can make optimal use of IP address space.** Tunnel switching enables VPN traffic to be terminated inside the network, where more address space is available than is usually the case in the DMZ. Companies can use their own internal addressing schemes for tunnel end points, and these addresses are invisible to the NSP providing the Internet VPN service, further increasing security.
- **Remote users can function as members of virtual LANs (VLANs).** VLANs improve network efficiency by directing traffic only to where it needs to go and they simplify user moves and changes. But where VPNs are used without tunnel switching, all incoming traffic has to be assigned to the same VLAN. This is because VLAN assignment is usually based on the hub port the user is plugged into. With VPNs, remote users accessing the network through a tunnel are virtually plugged into the same port as whatever device is terminating the tunnel. With tunnel switching, however, tunnel traffic can be forwarded to TTs at different locations, enabling users to be virtually plugged into the network through different ports and thus to be members of different VLANs.

Benefits: Global Internet Access

- Cut long-distance charges in half and overall remote access costs by even more
- Reduce capital and maintenance costs by replacing modem banks with a single Internet connection
- Enable remote employees to access the corporate network over their existing Internet connection
- Offer traveling employees worldwide local dial access to the corporate network
- Rapidly establish secure extranet connections for ad-hoc business relationships
- Retain central control of security, firewalling, IP address management, and service offerings

Additional Benefits with Tunnel Switching

- Increase access to network applications and resources without compromising the security perimeter
- Differentiate and manage various types of tunneled traffic coming in over the same Internet connection
- Increase network scalability
- Allow organizational divisions to share the same WAN interface while enforcing separate network access policies
- Increase addressing flexibility
- Combine the advantages of VPNs and VLANs

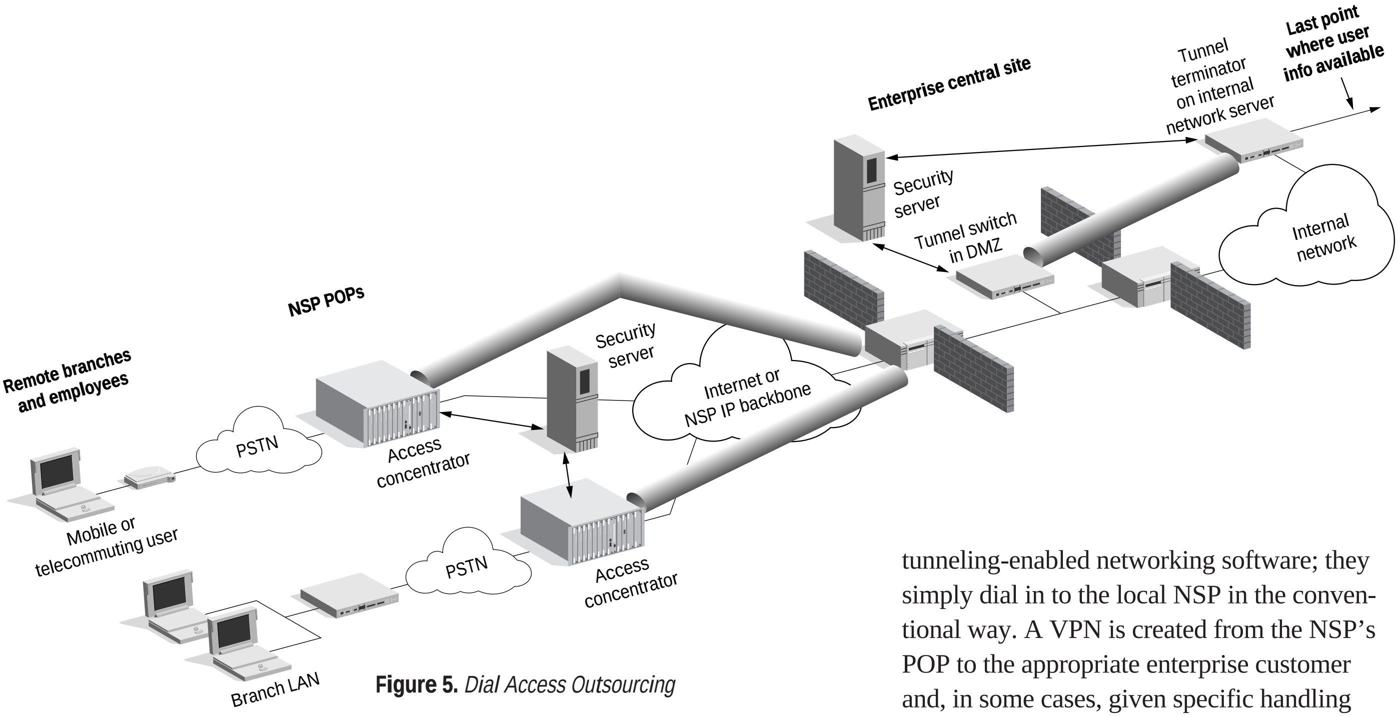
Last point where user info available
Tunnel terminator on internal network server
Enterprise central site
Security server
Tunnel switch in DMZ
Internal network
NSP POPs
Security server
Internet or NSP IP backbone
Remote branches and employees
PSTN
Access concentrator
Mobile or telecommuting user
PSTN
Access concentrator
Branch LAN

Figure 5. *Dial Access Outsourcing*

Dial Access Outsourcing

Companies that outsource remote access to an NSP can reduce not only communications charges (tariffs, long-distance charges, etc.) and equipment costs, but end-user support costs as well (Figure 5). They can let their NSP take on those responsibilities as part of a package of VPN services.

The advantage to mobile users and telecommuters is that they don't need to have tunneling-enabled networking software; they simply dial in to the local NSP in the conventional way. A VPN is created from the NSP's POP to the appropriate enterprise customer and, in some cases, given specific handling based on a service level agreement.

In this type of VPN, an access concentrator at the NSP's POP starts the tunnel. A tunnel termination device or tunnel switch at the enterprise DMZ ends the tunnel. Tunnel switching can be used in any of the ways described above under "Global Internet Access" to achieve additional benefits, including secure access to multiple applications and protocols across the firewall and the ability to differentiate and apply appropriate security to

Benefits: Dial Access Outsourcing

- Cut long-distance charges in half and overall remote access costs by even more
- Replace modem banks with a single Internet connection
- Reduce end-user support costs
- Enable remote employees to access the corporate network over their existing Internet connection without the need for special networking software
- Offer traveling employees worldwide local dial access to corporate network and superior performance (bandwidth, throughput, speed)
- Rapidly establish secure extranet connections for ad-hoc business relationships
- Retain central control of security, firewalling, IP address management, and service offerings

Additional Benefits with Tunnel Switching

- Increase access to network applications and resources without compromising the firewall
- Differentiate and manage various types of tunneled traffic coming in over the same Internet connection
- Increase network scalability
- Allow organizational divisions to share the same WAN interface while enforcing separate network access policies
- Increase addressing flexibility
- Combine the advantages of VPNs and VLANs

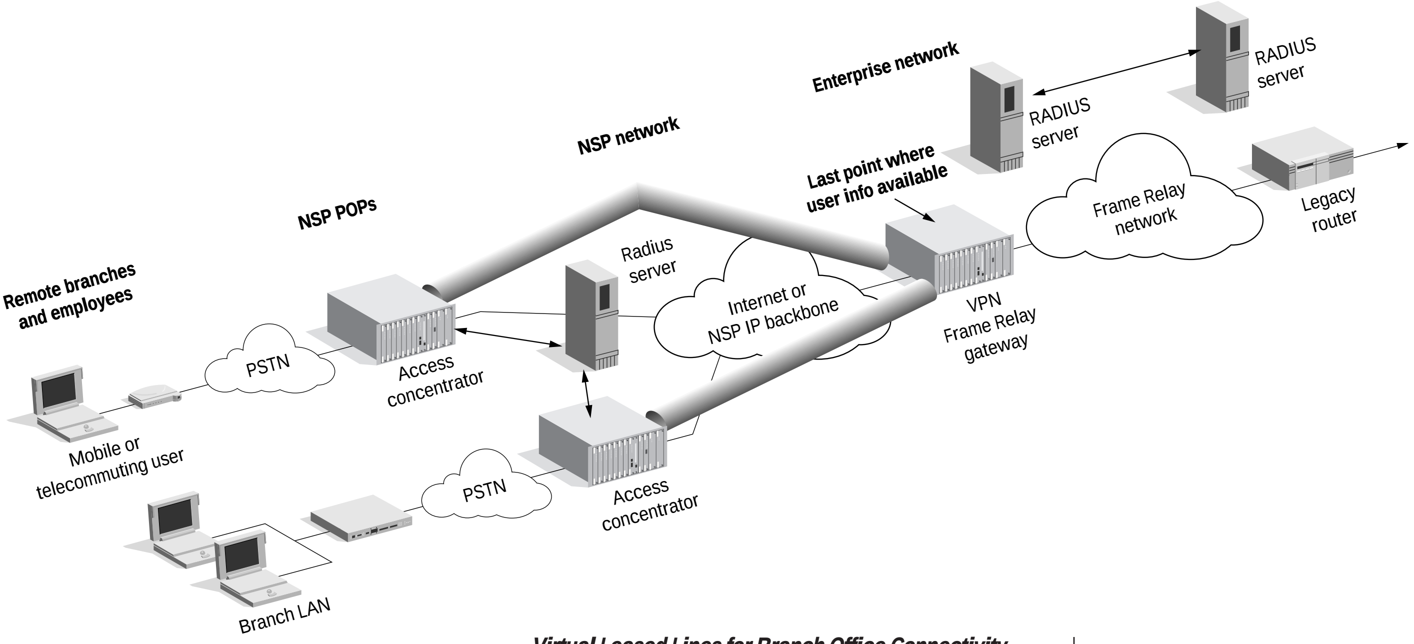

Figure 6. *Dial Access Outsourcing with VPN Frame Gateway*

tunneled traffic coming in over the same Internet interface from employees, customers, and partners.

Whether or not switches are used, because the tunnel is being terminated at the enterprise network, the corporation can continue to control user authorization and other security functions independently of the NSP. (Tunnel termination is the last point where information about the end user, necessary for performing authorization and applying privileges and policies, is available.)

Even companies that are not using a VPN-enabled device to connect to their NSP can take advantage of VPN services (Figure 6). A gateway at the edge of the NSP's network terminates the tunnel and forwards the traffic over a Frame Relay circuit to the enterprise network. In this case, the NSP needs to be able to access or mirror the corporation's network policy server since its tunnel termination device (the last point where user information is available) must perform authorization functions. The enterprise, of course, continues to control network access for all users at the firewall.

Virtual Leased Lines for Branch Office Connectivity

Companies that connect branches with virtual leased lines (VLLs) can typically save 50 to 75 percent over the cost of dedicated lines (see Figure 7 on page 10) while gaining the strategic advantage of enabling companies to link in new branches without delay. VLLs reduce communications charges by replacing long-distance links with a connection to a local NSP. Equipment and administration costs are also reduced since a single connection to a local NSP can provide access to both the corporate network and the Internet. As a result of these cost savings, VLLs make a fully meshed network, with its performance and redundancy advantages, affordable for most companies. And, like a leased-line mesh network, a VLL mesh network can incorporate preprogrammed alternative routing paths around busy or out-of-service routers.

Companies can purchase VLLs as a turnkey service from an NSP or they can install and maintain their own equipment, using the NSP only for transport. For companies that decide to do it on their own, the installation process is still very simple; it involves setting up an account with an NSP and performing mostly automated remote configuration tasks on the router.

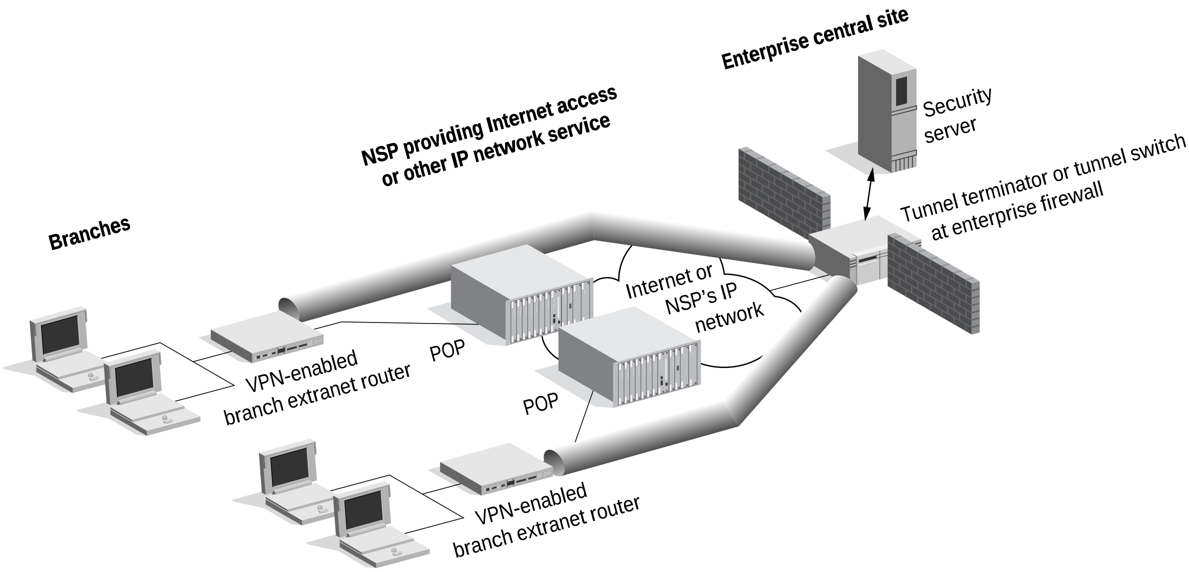
Enterprise central site
Security server
NSP providing Internet access or other IP network service
Tunnel terminator or tunnel switch at enterprise firewall
Branches
Internet or NSP's IP network
POP
VPN-enabled branch extranet router
POP
VPN-enabled branch extranet router

Figure 7. *Virtual Leased Lines*

In this type of VPN, an access router at the branch office starts the tunnel. A tunnel terminator device or tunnel switch at a central enterprise DMZ ends the tunnel. The connection used at the branch can be any permanent or dial-on-demand link that meets the bandwidth requirements of that location. In this respect, VLLs offer much more flexibility than direct Frame Relay or ISDN connections, which require all end points to be the same.

If the incoming Internet tunnel is terminated with a tunnel switch, a new secure tunnel can be established to a tunnel terminator on the internal network (Figure 8). Tunnel switches enable VLLs to support traffic between legacy LANs without having to put support for protocols such as IPX on the portion of the network that connects to the public Internet. (They shift the virtual LAN-to-LAN connection point inside the firewall.) Tunnel switching can also facilitate branch access to applications that are available only over legacy network protocols as well as to those for which restrictions are being enforced at the firewall. In addition, switches enable employees transferred to or working temporarily at branch offices to remain members of VLANs.

Benefits: Virtual Leased Lines

- Reduce branch office connection costs by more than half
- Enable branches to access corporate network and Internet from a single connection to a local NSP
- Connect new branches rapidly by purchasing a turnkey service or by self-installation (non-expert)
- Enable branches to choose network access devices that meet their particular bandwidth requirements
- Support multiprotocol LAN-to-LAN connections
- Selectively retain central control of security, firewalling, IP address management, and service offerings OR outsource to NSP
- Provide enterprise IT managers with self-provisioning VPN tools

Additional Benefits with Tunnel Switching

- Support multiprotocol connections, including legacy protocols, without putting interfaces on the part of the network that connects to the Internet
- Increase branch access to network applications without compromising the firewall

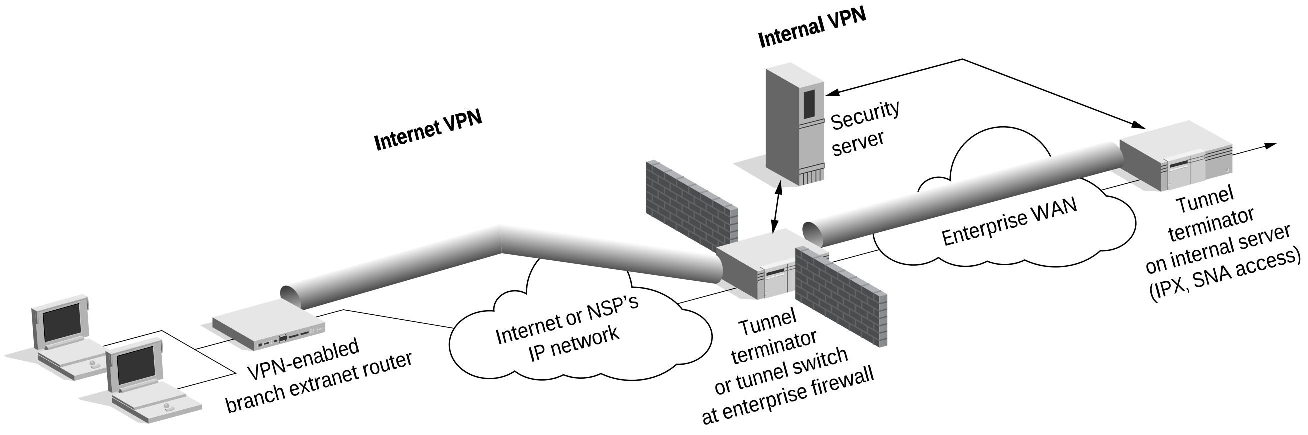
Internal VPN
Security server
Internet VPN
Enterprise WAN
Tunnel terminator on internal server (IPX, SNA access)
Internet or NSP's IP network
VPN-enabled branch extranet router
Tunnel terminator or tunnel switch at enterprise firewall

Figure 8. *Virtual Leased Lines with Tunnel Switching*

Enterprises can take advantage of any number of these VPN applications through a single WAN connection. In many cases, all that is required is a simple upgrade to existing network access devices.

How VPNs Work

There is nothing exotic about VPNs. They are based on familiar networking technology and protocols (Figure 9).

In the case of a remote access VPN, for example, the remote access client is still sending a stream of Point-to-Point Protocol (PPP) packets to a remote access server. Similarly, in the case of LAN-to-LAN virtual leased lines, a router on one LAN is still sending PPP packets to a router on another LAN. What is new is that in each case instead of going across a dedicated line, the PPP packets are going across a tunnel over a shared network.

The effect of VPNs is like that of pulling a

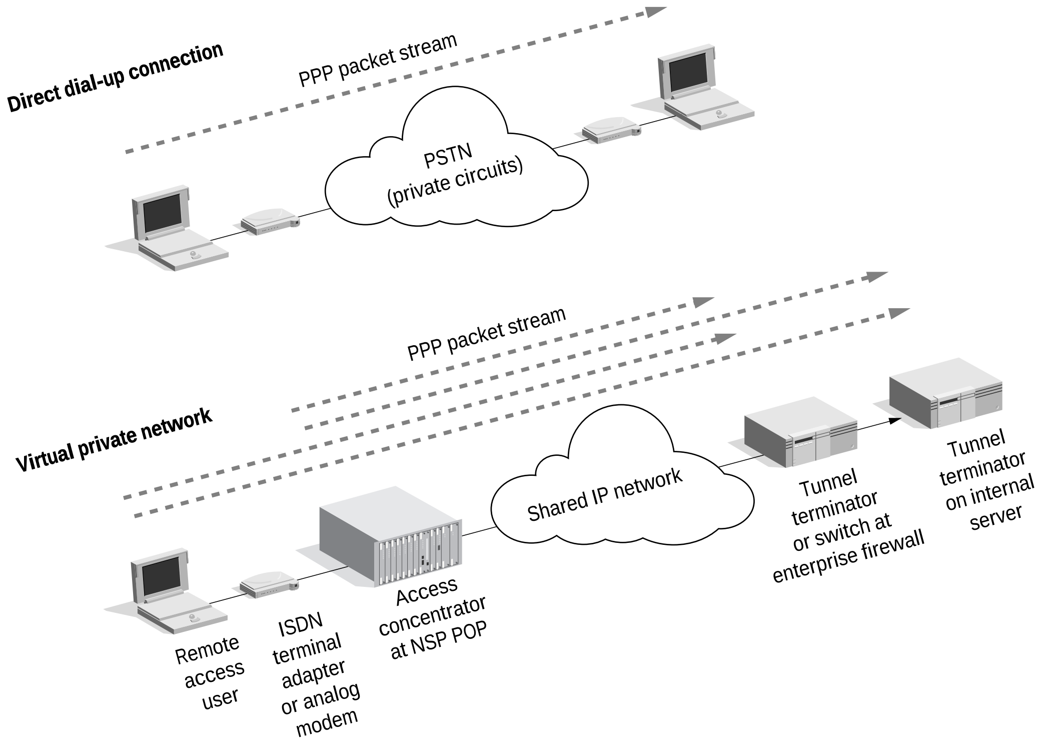
Direct dial-up connection
PPP packet stream
PSTN (private circuits)
PPP packet stream
Virtual private network
Shared IP network
Tunnel terminator or switch at enterprise firewall
Tunnel terminator on internal server
Remote access user
ISDN terminal adapter or analog modem
Access concentrator at NSP POP

Figure 9. *VPNs Are Based on Familiar Technology*

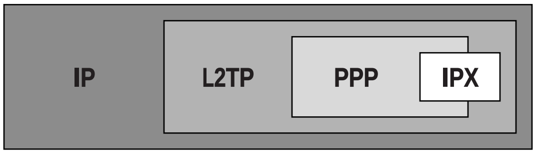

Figure 10. *Layer 2 Tunneling Protocol Encapsulation*

serial cable across a WAN cloud. PPP protocol negotiations set up a direct connection from the remote user to the tunnel termination device.

The most widely accepted method of creating industry-standard VPN tunnels is by encapsulating network protocols (IP, IPX, AppleTalk, etc.) inside the PPP and then encapsulating the entire package inside a tunneling protocol, which is typically IP but could also be ATM or Frame Relay. This approach is called "Layer 2 tunneling" since the passenger is a Layer 2 protocol (Figure 10).

Alternatively, network protocols can be encapsulated directly into a tunneling protocol such as 3Com's Virtual Tunneling Protocol (VTP). This approach is called "Layer 3 tunneling" since the passenger is a Layer 3 protocol (Figure 11).

VPN Protocols

Currently, Microsoft's Point-to-Point Tunneling Protocol (PPTP), which is bundled with Windows 95 and Windows NT 4.0, is the most widely used protocol for VPNs. (PPTP was developed by 3Com and Microsoft.) In the near future, however, most VPNs will be based on the emerging Layer 2 Tunneling Protocol (L2TP).

The L2TP standard represents a merging of PPTP and the Layer 2 Forwarding (L2F) protocol, both of which operate at Layer 2. The emerging standard offers the best features of these protocols as well as additional features. One such enhancement is multipoint tunneling. It will enable users to initiate multiple VPNs in order, for example, to access both the Internet and the corporate network at the same time.

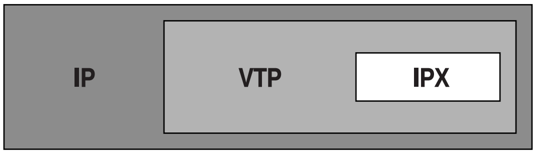

Figure 11. *Layer 3 Tunneling Protocol Encapsulation*

Both L2TP and PPTP offer additional capabilities that aren't available with Layer 3 tunneling protocols:

- They allow enterprises to choose whether to manage their own user authorization, access permissions, and network addressing, or to have their NSP do it. By receiving tunneled PPP packets, enterprise network servers have access to information about remote users, necessary for performing these tasks.
- They support tunnel switching. User information is necessary for tunnel switching, which is the ability to terminate a tunnel and initiate a new tunnel to one of a number of subsequent tunnel terminators. Tunnel switching extends the PPP connection to a further end point.
- They enable enterprises to apply fine-grained access policies at the firewall and at internal servers. Because tunnel terminators at the enterprise firewall are receiving PPP packets that contain user information, they can apply specific security policies to traffic from different sources. (With Layer 3 tunneling, in contrast, there is no way to differentiate packets coming in from the NSP, so the same set of filters has to be applied across the board.) In addition, if a tunnel switch is used, it can initiate a subsequent Layer 2 tunnel to direct traffic from specific users to the appropriate internal servers, where additional levels of access control can be applied.

VPN Security

Secure VPNs apply specific security protocols to tunnels or to the packets they carry. These protocols enable hosts to negotiate encryption and digital signature techniques that ensure data confidentiality, data integrity, and authentication of the sending and receiving sources.

Microsoft Point-to-Point Encryption (MPPE)

MPPE adds integrated data privacy (encryption) into standard Microsoft Dial-Up Networking (Figure 12). A 40-bit version is bundled with PPTP into Windows 95 and Windows NT Dial-Up Networking; a 128-bit version is also available.

3Com Offers More Flexible VPN Choices

3Com provides VPN products that enable both ISP/NSP-terminated tunnels and enterprise-terminated tunnels. 3Com also supports both L2TP and PPTP tunneling protocols, and is the only company currently offering tunnel switching.

MPPE encrypts PPP packets on the client workstation before they go into a PPTP tunnel. When the client workstation negotiates PPP with the ultimate tunnel terminator, an encryption session is initiated. (Interim tunnel switches do not have the ability to decrypt PPP packets.)

MPPE provides data privacy and uses an enhanced Challenge Handshake Protocol (MS-CHAP) for strong user authentication.

Secure IP (IPsec)

IPsec is an emerging standard for VPN security. In cases where IP is used to transmit tunneled traffic, IPsec will enable tunnel initiating and tunnel terminating products from multiple vendors to interoperate.

The standard, which was written by Internet Engineering Task Force (IETF) committees, consists of a set of IP-level protocols for setting up an agreement between two IP stations about the encryption and digital signature methods that will be used. IPsec is recommended for use with L2TP and will be mandatory for IPv6 compliance.

More robust than MPPE, IPsec encompasses user authentication, privacy, and data integrity (Figure 13 on page 14). It can also be extended beyond the tunnel terminator to the destination host workstation.

Another advantage of IPsec is that its security mechanisms for authentication and security are loosely coupled with its key management systems. While Internet Security Association Key Management Protocol (ISAKMP)/Oakley and manual management are the two key systems currently mandated in IETF draft standards, this loose coupling will allow for future systems to be used without requiring modification of security mechanisms.

IPsec Example 1: Remote Access with ISP VPN Initiation. In this example, remote access is achieved when the ISP initiates the VPN. This example describes the steps followed in the security process. In the example that follows, the client initiates the VPN, and the ISP's access concentrator acts as a router.

1. **User authentication.** The remote user dials up her ISP. The networking software on her

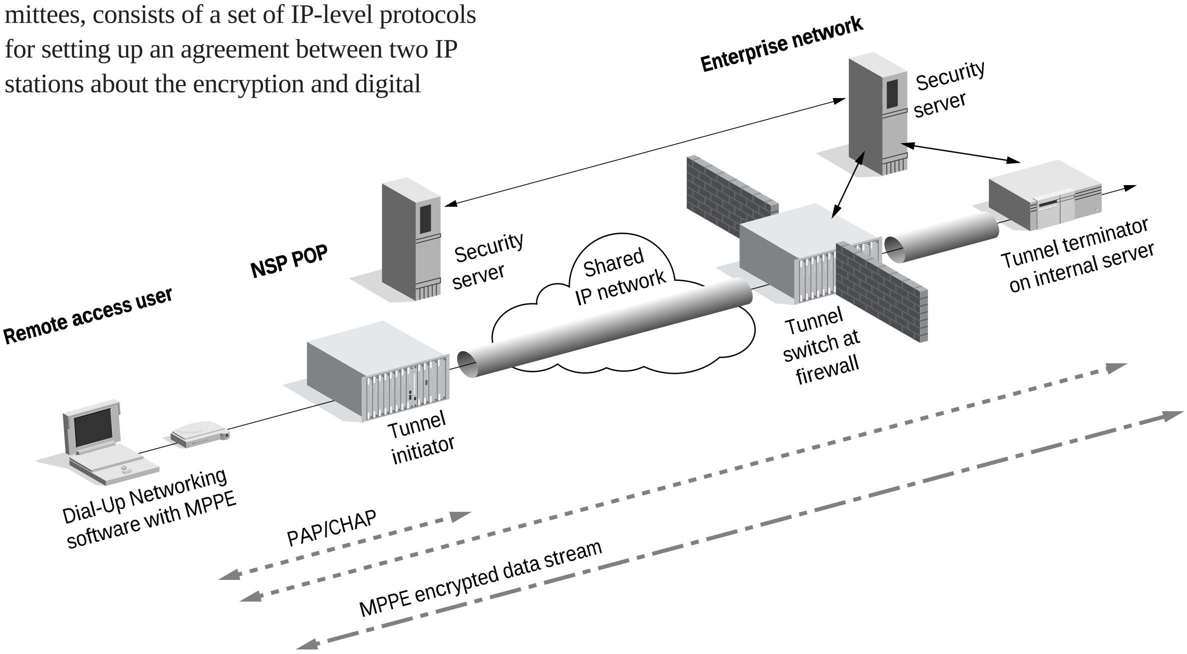
Enterprise network
Security server
NSP POP
Security server
Shared IP network
Remote access user
Tunnel switch at firewall
Tunnel terminator on internal server
Tunnel initiator
Dial-Up Networking software with MPPE
PAP/CHAP
MPPE encrypted data stream

Figure 12. *MPPE with CHAP*

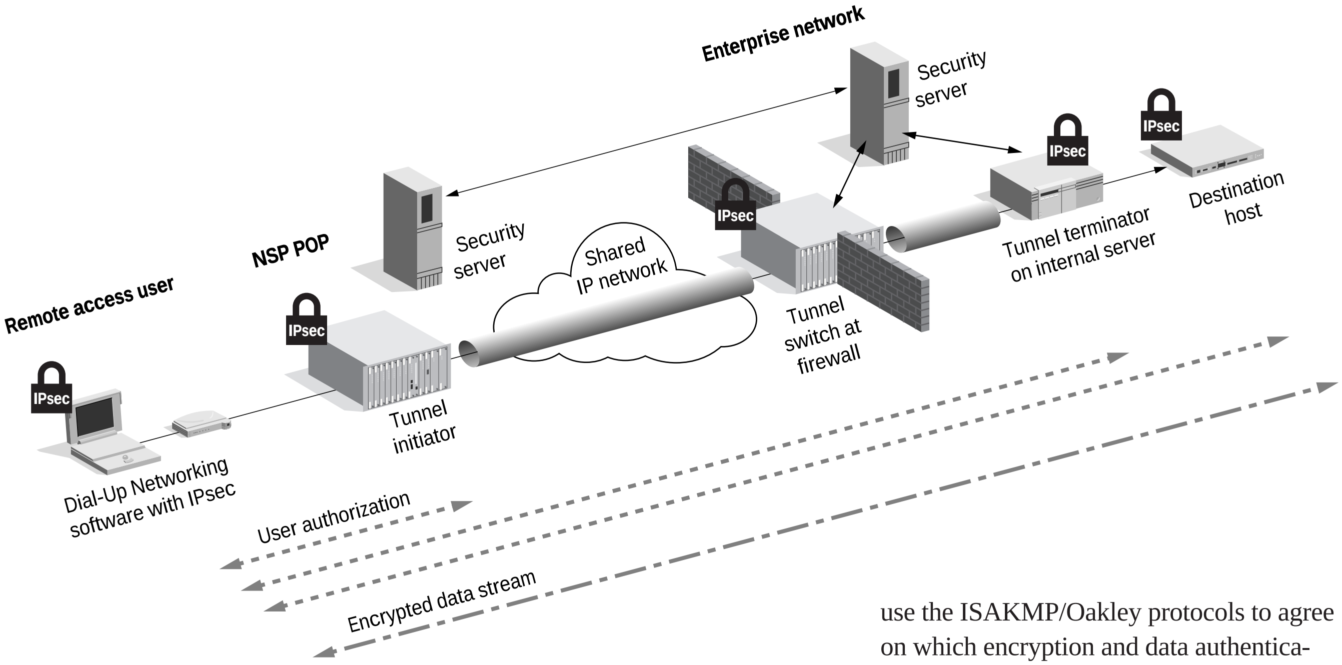

Figure 13. *IPsec*

laptop sends a CHAP message with the user's name and password to the access concentrator at the ISP's POP. The access concentrator transmits the name and password to a security server (for example, Remote Authorization Dial-In User Service, or RADIUS) for user authentication. When it receives a response from the server, it converts the response back into CHAP and transmits it to the remote user's laptop.

Meanwhile, the access concentrator has received additional information from the security server, such as which IP address to assign to the user and which subnet mask to use. It knows the user is an employee of a particular enterprise customer and the specified IP address of the appropriate tunnel termination device for that customer. In most cases, this tunnel terminator will be the enterprise firewall or another device inside the firewall "DMZ" (the network segment between the components of a two-part firewall).

2. **Establishment of a secure channel between the tunnel initiation and termination devices.** The ISP's access concentrator and the tunnel termination device now use the ISAKMP/Oakley protocols to agree on which encryption and data authentication algorithms (such as DES, 3DES) they will use to establish a secure channel. In ISAKMP each participant in an exchange has a pair of keys, one private and one public. The ISP's access concentrator sends the tunnel terminator a message along with a digital signature that it creates using its private key.

To read the digital signature, the tunnel terminator must use the access concentrator's public key. It may already have the key stored; if not, it can get it by contacting a Certificate Authority. This authority might be a commercial organization such as VeriSign or GTE's CyberTrust, or it might be an enterprise server that stores the certificates of companies with which the enterprise does business. (The enterprise Certificate Authority will, in turn, be certified by a commercial or government organization, which may, in turn, be certified by another organization, and on up the hierarchy of trust.)

The tunnel terminator returns a message with a signature created by its private key to the ISP's access concentrator. The access concentrator then uses the tunnel terminator's public key to authenticate the signature.

The Oakley protocols are employed to exchange information that will be used to generate encryption keys. The access concentrator and the tunnel terminator each employ an algorithm called Diffie-Hellman to independently generate another public/ private key set (actually, two half-keys, one of which is kept secret). They then exchange the public half of their keys. The access concentrator takes its own secret half-key and the tunnel terminator's public half-key and runs a mathematical function on them that results in a third secret key. The tunnel terminator performs the function against its secret half-key and the access concentrator's public half-key, coming up with the same third secret key. This process is highly secure because anyone intercepting the exchange will get only the two public half-keys. There is no hardware currently available in the market with the computational power to derive the secrets from the public keys.

3. **Application of organizational security policies.** The next step is for the devices to exchange information on how security will be handled for this particular user. A transmission from the CEO, for example, may need to be sent using stronger message authentication and integrity methods (for example, multiple levels of encryption, hash functions) than one from a sales representative.

   The access concentrator gets policy information about the user from a RADIUS server or other internal source, and then initiates an exchange with the tunnel terminator. This exchange is encrypted using the algorithm already agreed upon during the ISAKMP/Oakley exchange.

   The user's data packets (including the payload and the IP header) are then encrypted and encapsulated in a new IP header. This header has a different set of addresses than the original IP header on the user's packet. Where initially the source address was the user's laptop and the destination address was a host somewhere behind the firewall, in the new IP header, the source is the ISP's access concentrator and the destination is the tunnel terminator. This method is called IPsec "tunneling mode," because during transmission across the public network, the IP addresses of the source and destination hosts are hidden.

To ensure data integrity during transmission, a hash function may be calculated on the user's IP packet before the new IP header is added. Or, for stronger security, it may be calculated on the user's packet and the new header together. When the tunnel termination device receives the packet, it will perform the same hash function on the packet. If it gets the same value, then the packet has not been tampered with.

The tunnel terminator uses the DES key to decrypt the packets as they are received. If the tunnel is being terminated by the ISP, the packets are transmitted to the enterprise via a Frame Relay circuit or other dedicated link. If the tunnel is being terminated by the enterprise, the packets are dropped onto a LAN for transmission to the destination host. If the enterprise is using a tunnel switch to receive

IPsec Tunneling Mode Is Not the Same as a VPN Tunnel

When IPsec-compliant encryption is applied to an entire network protocol packet (IP, IPX, AppleTalk, etc.), and then the encrypted results are encapsulated into another IP packet, the process is called "tunneling mode."

The advantage of using this mode is that a network protocol can travel across a network that does not support it to a tunnel termination device that does. Tunneling mode also protects the identity of networks, subnetworks, and terminating notes. To confuse the picture further, Layer 2 VPNs provide these same benefits, whether or not they incorporate IPsec.

As a result of similarities in terminology and this single overlap in functions, some people assume that all tunneling functions are performed by IPsec tunneling mode. In fact, IPsec provides only a small part of the capabilities needed for virtual private networking.

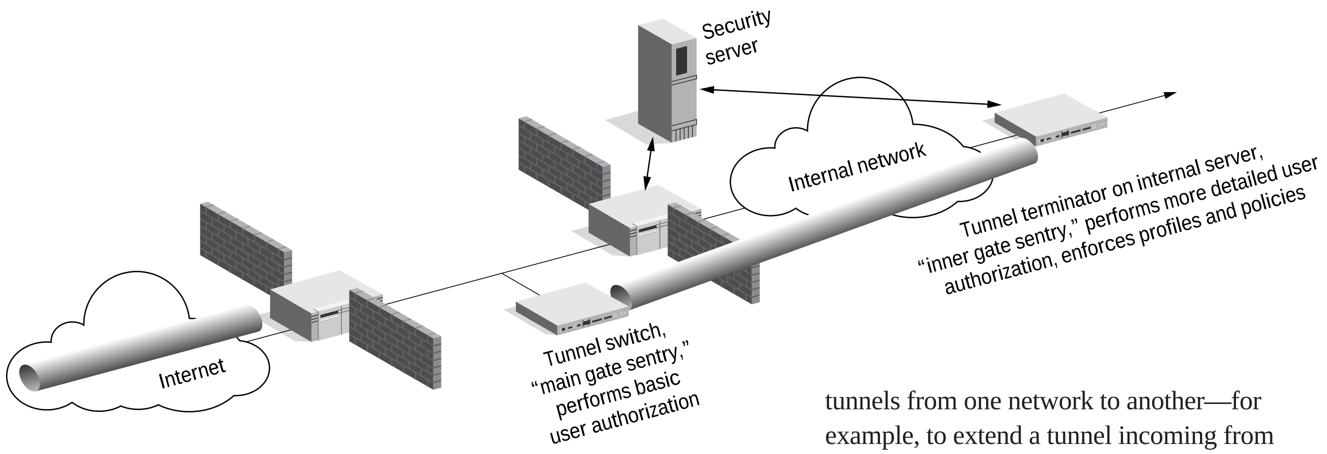
Security server
Internal network
Tunnel terminator on internal server, "inner gate sentry," performs more detailed user authorization, enforces profiles and policies
Internet
Tunnel switch, "main gate sentry," performs basic user authorization

Figure 14. *Tunnel Switching Through the Firewall*

VPN traffic from its ISP or NSP, the switch creates a new tunnel to the destination host. IPsec security can also be applied to this tunnel.

IPsec Example 2: Remote Access with Client VPN Initiation. This process is the same as the one described in the first example, except that all of the exchanges (CHAP user authentication, ISAKMP/Oakley establishment of a security association, application of organizational policy, and encrypted transmission) take place between the remote user's laptop and the tunnel termination device. The ISP's access concentrator simply acts as a router. It is not even aware that a secure VPN has been established.

Tunnel Switching: Improved Security and More Flexible VPN Applications

A tunnel switch is a combination tunnel terminator/tunnel initiator. It can be used to extend tunnels from one network to another—for example, to extend a tunnel incoming from ISP's network to a corporate network. It can also be used to replace a point-to-point connection with a point-to–switched fabric–to-point connection—one that behaves much like a dedicated telephone switched circuit even though it occurs over a routed network.

For More Information

To find out more about security technology, refer to the following documents:

- RFC-1825, "Security Architecture for the Internet Protocol"
- RFC 1827, "Encapsulating Security Payload (ESP)"
- RFC-1851, "The ESP Triple DES Transform"

Tunnel switching offers many business advantages and opens up the possibility of a myriad of tunneling applications. Enterprises, for example, can use tunnel switching to increase security at the firewall while improving their ability to manage remote access to network resources behind the wall (Figure 14). In this case, the tunnel switch is generally located on the enterprise firewall. Based on a RADIUS lookup on the user name, the switch initiates a new tunnel through the firewall to a specific internal server. This approach protects the integrity and performance of the firewall while increasing access to networked applications and resources.

Only a "rifle shot" hole has to be opened up in the firewall for the tunneling protocol to pass through. During the initial tunnel termination, however, the tunnel switch can identify other encapsulated protocols that the IP datagram is carrying with it. It can do a lookup to a firewall RADIUS server and, based on the remote user name and the protocols, retrieve information on the approved destinations of those packets. The switch then initiates new tunnels to carry packets to specific servers behind the firewall. These internal network servers, which do the final tunnel termination, can be equipped with detailed user profiles and privileges, enabling them to make fine-grained decisions about network access.

One way to think about the impact that tunnel switching can have on security is to imagine a sentry at the main gate of a secure compound. This main gate sentry does not have access to restricted access information such as passwords, but he does have a generalized set of criteria for screening visitors and placing them in categories. This allows the sentry to direct the visitors to a specific guard station at an internal gate. The guards at these internal gates have much more detailed information about access permissions and can demand a password or some other form of authentication.

The benefits of tunnel switching are not limited to security, however. Enterprises can also use tunnel switches to perform server load balancing for incoming VPN traffic and to increase flexibility for IP addressing. NSPs can use tunnel switching to flexibly direct traffic from different customers—and even from different users within a customer account—into tunnels with appropriate end points and Quality of Service (QoS) handling. An NSP, for example, could switch a high-priority customer onto a higher-speed fabric or use tunnel switching to avoid network congestion points.

VPN Management

The goal in VPN management is to make VPNs look like a private network. 3Com VPN solutions incorporate management tools that monitor and provide visibility into VPNs running over provider networks. 3Com Transcend® AccessWatch/VPN, for example, is a Web-based application that enables network administrators to profile the use and performance of VPNs using both real-time and historical data. Using Transcend® AccessWatch/VPN, administrators can perform capacity utilization, QoS, security exception, and tunnel usage analyses. New-generation policy-based management tools will also be deployable across both conventional network links and VPNs.

3Com VPN Solutions

3Com has more experience with VPNs than any other internetworking provider. 3Com was the first remote access vendor to deliver VPN solutions, and now 3Com has more than 50,000 VPN ports currently in use, with more than 2 million VPN-ready ports installed worldwide.

3Com offers end-to-end VPN solutions, including products for enterprises and both service-focused and infrastructure-intensive NSPs. All 3Com VPN solutions adhere to industry standards (including IPsec for security) and are compatible with each other, making it easy for VPN providers and users to establish mutually beneficial business partnerships.

Enterprises and NSPs can choose 3Com VPN products with confidence. VPN capabilities are built into 3Com's proven product lines, including multiprotocol routers equipped with a rich set of management features and market-leading, award-winning access concentrators and the highest-density carrier class solutions on the market. As the market leader in NICs and modems, 3Com also understands the needs of remote users.

3Com is also the first vendor to extend the VPN architecture to incorporate tunnel switching, the key to better security and more flexible VPN applications.

All VPN products ship with TranscendWare™ software, ensuring that 3Com customers will be able to deploy and enforce network policies consistently across both conventional links and VPNs. TranscendWare software allows edge devices to communicate with end devices to enforce network policies. By monitoring VPN tunnels, these devices will be able to better manage dial-up ports, bandwidth allocation, network load and destination, and return policy leases—all critical elements for control in a VPN environment.

3Com Solutions for Enterprises

Enterprises can add VPN network server capability (tunnel termination) to their existing NETBuilder II® or SuperStack® II bridge/router. This single device can provide a connection to an NSP over leased line, Frame Relay, ISDN, SMDS, or Switched 56, and it provides LAN connections over Ethernet, Token Ring, and ATM. The NETBuilder II router supports all major LAN protocols, enabling multiprotocol tunnel traffic to be routed to the appropriate LAN server; and it also supports SNA for access to legacy systems.

NETBuilder® and SuperStack II products offer the unique advantage of Boundary Routing® system architecture. Boundary Routing technology enables companies to simplify remote router installation and configuration, eliminating the need for on-site technical staff, by shifting key router management and overall router management to a central site.

Where NSPs are providing tunnel creation services, branch offices and remote users can continue to use their existing 3Com networking devices (OfficeConnect® routers, 3ComImpact® IQ ISDN terminal adapters, 3Com x2™ or Courier™ modems, 3Com Megahertz® PC modem card) as is. Where remote user devices are to create tunnels, additional software is required. This software is already integrated into 3Com network interface cards and is also bundled into the Windows 95 and Windows NT operating systems.

Conclusion

Industry-standard virtual private networks are ushering in the next generation of network connectivity. Most analysts expect that Internet-based VPNs will eventually replace most leased-line networks. VPNs are being widely adopted because they offer immense cost savings as well as new business opportunities for both enterprises and network service providers. Many of these benefits can be gained by rapidly establishing new types of business relationships that are mutually beneficial to all parties.

3Com has a broader product line of solutions and more experience with VPNs than any other vendor, and is the first vendor to offer the competitive advantage of tunnel switching. 3Com customers can begin exploiting the benefits of VPNs now, with confidence, because 3Com VPN solutions are available (in most cases, through upgrades) on some of the industry’s most highly praised, market-proven networking platforms and products.

3Com Corporation
P.O. Box 58145
5400 Bayfront Plaza
Santa Clara, CA
95052-8145
Phone: 800-NET-3Com
or 408-764-5000
Fax: 408-764-5001
World Wide Web:
http://www.3com.com

3Com ANZA
Sydney, Australia
Phone: 61 2 9937 5000
Fax: 61 2 9956 6247
Melbourne, Australia
Phone: 61 3 9866 8022
Fax: 61 3 9866 8219

3Com Asia Limited
Beijing, China
Phone: 8610 6849 2568
Fax: 8610 6849 2789
Shanghai, China
Phone: 86 21 63501581
Fax: 86 21 63501531
Hong Kong
Phone: 852 2501 1111
Fax: 852 2537 1149
India
Phone: 91 11 644 3974
Fax: 91 11 623 3192
Indonesia
Phone: 6221 572 2088
Fax: 6221 572 2089
Korea
Phone: 82 2 319 4711
Fax: 82 2 319 4710
Malaysia
Phone: 60 3 732 7910
Fax: 60 3 732 7912
Pakistan
Phone: 92 21 5846240
Fax: 92 21 5840727
Philippines
Phone: 632 892 4476
Fax: 632 811 5493
Singapore
Phone: 65 538 9368
Fax: 65 538 9369
Taiwan
Phone: 886 2 377 5850
Fax: 886 2 377 5860
Thailand
Phone: 622 231 8151 5
Fax: 622 231 8158

3Com Belgium
Belgium, Luxembourg
Phone: 32 2 725 0202
Fax: 32 2 720 1211
Netherlands
Phone: 31 30 6029700
Fax: 31 30 6029777

3Com Canada
Calgary
Phone: 403 265 3266
Fax: 403 265 3268
Montreal
Phone: 514 683 3266
Fax: 514 683 5122
Toronto
Phone: 416 498 3266
Fax: 416 498 1262
Vancouver
Phone: 604 434 3266
Fax: 604 434 3264

3Com France
Phone: 33 1 69 86 68 00
Fax: 33 1 69 07 11 54

3Com GmbH
Munich
Phone: 49 89 627 320
Fax: 49 89 627 32 233
Austria
Phone: 43 1 580 17 0
Fax: 43 1 580 17 20
Berlin
Phone: 49 30 34 98790
Fax: 49 30 34 987999
Poland
Phone: 48 22 645 1351
Fax: 48 22 645 1352
Switzerland
Phone: 41 31 996 1414
Fax: 41 31 996 1410

3Com Ireland
Phone: 353 1 820 7077
Fax: 353 1 820 7107

3Com Japan
Phone: 81 3 3345 7251
Fax: 81 3 3345 7261

3Com Latin America
U.S. Headquarters
Phone: 408-326-2093
Fax: 408-764-5730
Argentina
Phone: 541 312 3266
Fax: 541 314 3 3329
Brazil
Phone: 55 11 5181 0869
Fax: 55 11 5182 7399
Chile
Phone: 562 633 9242
Fax: 562 633 8935
Mexico
Phone: 525 520 7841
Fax: 525 520 7837

3Com Northern Latin America
Miami, Florida
Phone: 305-261-3266
Fax: 305-261-4901
Colombia
Phone: 571 629 4110
Fax: 571 629 4503
Venezuela
Phone: 582 953 8122
Fax: 582 953 9686

3Com Mediterraneo
Milano, Italy
Phone: 39 2 253011
Fax: 39 2 27304244
Rome, Italy
Phone: 39 6 5279941
Fax: 39 6 52799423
Spain
Phone: 34 1 509 69 00
Fax: 34 1 307 66 63

3Com Middle East
Phone: 971 4 349049
Fax: 971 4 349803

3Com Nordic AB
Denmark
Phone: 45 39 27 85 00
Fax: 45 39 27 08 44
Finland
Phone: 358 0 435 420 67
Fax: 358 0 455 51 66
Norway
Phone: 47 22 58 47 00
Fax: 47 22 58 47 01
Sweden
Phone: 46 8 632 56 00
Fax: 46 8 632 09 05

3Com Russia
Moscow
Phone: 007 095 258 09 40
Fax: 007 095 258 09 41

3Com South Africa
Phone: 27 11 807 4397
Fax: 27 11 803 7405

3Com UK Ltd.
Marlow
Phone: 44 1628 897000
Fax: 44 1628 897003
Manchester
Phone: 44 161 873 7717
Fax: 44 161 873 8053
Edinburgh
Phone: 44 131 240 2900
Fax: 44 131 240 2903

Printed in U.S.A.

500651-001 2/98