Technical Paper

Private Use of Public Networks for Service Providers

New Standards-Based Virtual Private Networks Offer Business Opportunities and Improved Return on Assets

Private Use of Public Networks for Service Providers

New Standards-Based Virtual Private Networks Offer Business Opportunities and Improved Return on Assets

Contents

Private Use of Public Networks for Service Providers

New Standards-Based Virtual Private Networks Offer Business Opportunities and Improved Return on Assets

Virtual private networks (VPNs) offer solutions to some of today's most critical networking challenges. Many Internet service providers (ISPs) are looking to shift the focus of their business from commodity-priced access to higher-margin value-added services for corporations. Serving the needs of corporate clients, however, may require expanding capacity and geographic coverage. VPNs are an opportunity to add new services and expand reach while avoiding major capital investments and facilities negotiations.

Some larger ISPs as well as other types of network service providers (NSPs) already own significant infrastructure and are continuing to invest in it. VPNs offer them the opportunity to improve asset utilization and return on investment by leasing available capacity to other providers. These facility-owning service providers can generate new streams of revenue that can help justify expansion costs. For those companies whose business plans call for expansion of both infrastructure and services, leased facilities can be a means of accelerating coverage, broadening services, and generating revenues to support new service development.

This paper describes how VPNs based on industry-standard secure tunneling are providing solutions for growth and improved return on investment. It describes and diagrams some of the most popular VPN applications. It explains VPN technology, including tunnel components and industry standards for tunneling and tunnel-based security. It introduces tunnel switching and the advantages it offers for more flexible NSP service-level handling of tunneled traffic as well as mutually beneficial partnerships between service providers. The paper closes by discussing 3Com VPN solutions and their advantages.

Why VPNs Mean Opportunity

VPNs enable ISPs and NSPs to use the Internet or their own IP backbones to provide enterprises with remote access and branch connectivity services. The benefits to enterprises include dramatically lower costs, reduced management and end user support requirements, and increased strategic flexibility. The benefits to service providers include opportunities to grow the business by offering a variety of value-added services, to grow customer base and geographic range, and to increase return on assets.

The VPN market is growing rapidly. Infonetics Research[1] predicts that the market will increase at an annual rate of over 100 percent 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, 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 a VPN-enabled access concentrator at an ISP point of presence (POP). It could also be started by a VPN-enabled access router on an enterprise branch or home office

1. "Virtual Private Networks," Infonetics Research, 1997.

Acronyms and Abbreviations

CHAP
Challenge Handshake Authentication Protocol

CPE
customer premises equipment

DES
Data Encryption Standard

IPsec
Secure IP

ISAKMP
Internet Security Association Key Managment 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

LAN, or 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). A tunnel could be ended by a VPN gateway on an ISP's or NSP's network access router or by a tunnel terminator or switch on an enterprise network.

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.

Service-Focused ISPs: Moving Toward More Profitable Business Models

ISPs face fierce competition in a low-margin business based on flat-rate retail pricing models. To stay in business, increase profitability, and grow, many providers are trying to rise above the commodity market by offering higher-margin value-added services to enterprises.

Since the connectivity needs of corporations are rarely confined to local areas, this strategy usually means expanding geographic reach. Faced with the cost of building out their networks and the need to move quickly, ISPs are looking for ways to expand services and reach without adding to infrastructure.

VPNs provide answers to these growth issues. They allow ISPs to differentiate themselves in a crowded marketplace by focusing on the service side of the business, capitalizing on their knowledge of customer needs.

- **Value-added services.** VPNs open up a myriad of possibilities for offering new Internet-based services that can help to relieve margin pressures. By using their existing infrastructure to provide not only Internet access but remote access outsourcing and branch office connectivity, ISPs can generate new revenue streams and improve returns on their facilities investments.

  VPN technology also enables ISPs to differentiate traffic from various customers and even to differentiate traffic from various users within a customer account, making it possible to apply a prenegotiated Quality of Service (QoS) agreement. High-priority traffic, for example, could be directed over the NSP's own backbone, where it can guarantee speed and reliability, instead of onto its Internet gateway. And ISPs can also

Acronyms and Abbreviations

PPTP
Point-to-Point Tunneling Protocol

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

VLL
virtual leased line

VPN
virtual private network

VPOP
virtual point of presence

VTP
Virtual Tunneling Protocol

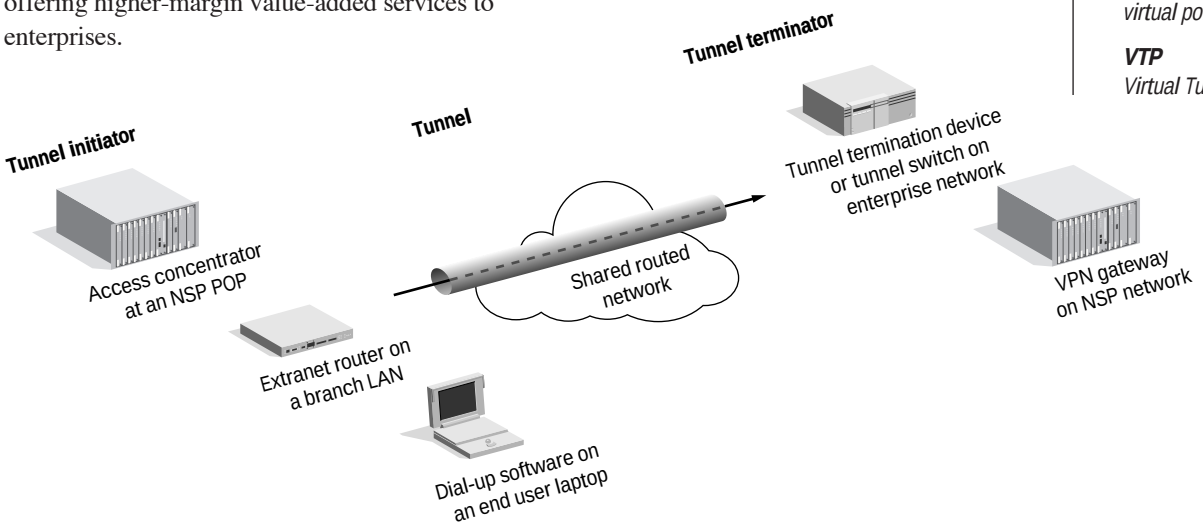

Figure 1. *VPN Components*

capture tunnel user information for input into their itemized billing systems.

- **Geographic expansion without capital investment.** Tunneling enables ISPs to expand geographic coverage on an as-needed basis by establishing virtual points of presence (VPOPs). VPOPs can be set up by purchasing VPN services from dial access outsourcers or other ISPs with available capacity. This arrangement is entirely transparent to customers, who connect to their NSP in the normal way. VPN-based accounting mechanisms enable ISPs to provide accurate end-to-end billing even though part of the route is over someone else's network.

VPNs offer service-focused ISPs and NSPs the opportunity to provide value-added services and economical geographic expansion by deploying three applications of VPNs: dial access outsourcing, virtual leased lines, and/or virtual points of presence.

Dial Access Outsourcing

By offering enterprises an easy way to respond to growing demand for remote access, ISPs can build a high-margin business in value-added service while increasing the return on owned or leased network facilities. The market for this service is likely to grow rapidly as companies realize that outsourcing enables them to achieve a scalable, manageable solution while reducing line charges and equipment costs, and eliminating the need to devote their own technical staff to supporting remote users.

In this type of VPN, an access concentrator at the ISP's POP is the tunnel initiator. The tunnel terminator can vary depending on customer needs. Where the enterprise customer is using a VPN-enabled router to connect to the ISP, the tunnel can extend to the enterprise network (Figure 2). A customer premises tunnel termination device or tunnel switch ends the tunnel. Because tunnels carry with them information about the end user, the enterprise has the opportunity to control user authentication and network access. Most companies will choose to do so. The advantage to ISPs is that their job is simply delivering tunnels, and they don't have to be involved in network access issues.

Some customers will want to continue using their existing Frame Relay connection without a VPN upgrade (Figure 3). In this case, the tunnel termination device is a Frame Relay gateway at the edge of an NSP's network. The gateway extracts packets from the tunnel and sends them over the Frame Relay circuit to the enterprise. Because tunnel termination is the last point where remote user information is available, the NSP must handle user authentication on behalf of the enterprise.

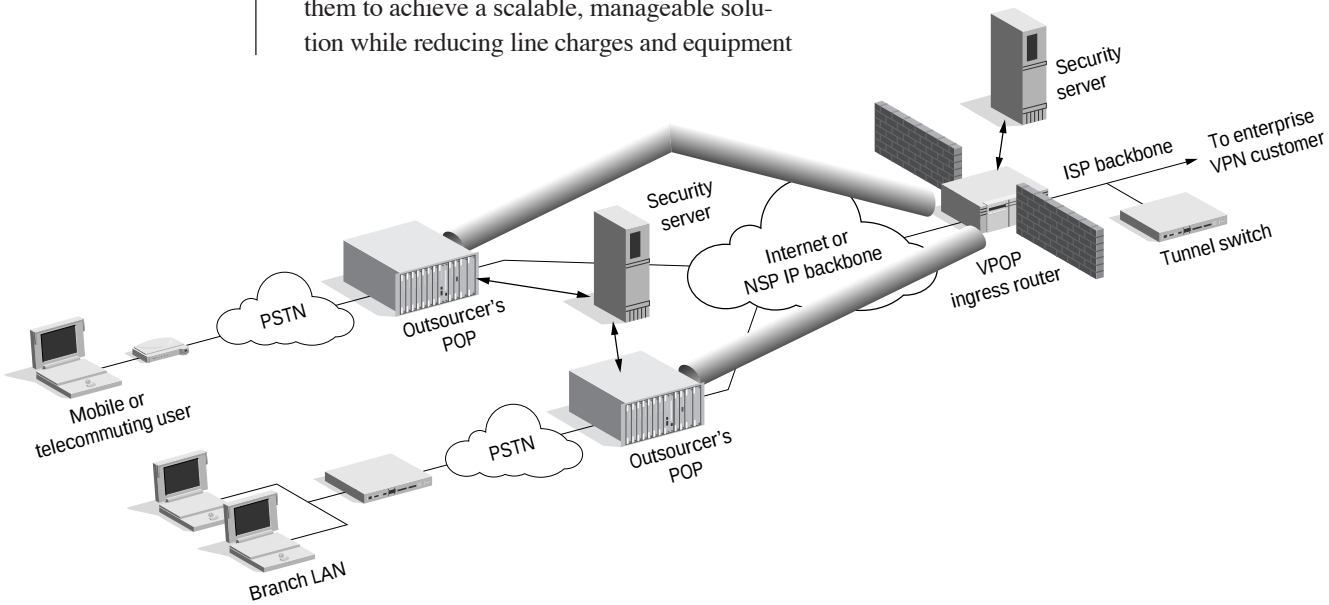

Figure 2. *Dial Access Outsourcing for NSPs*

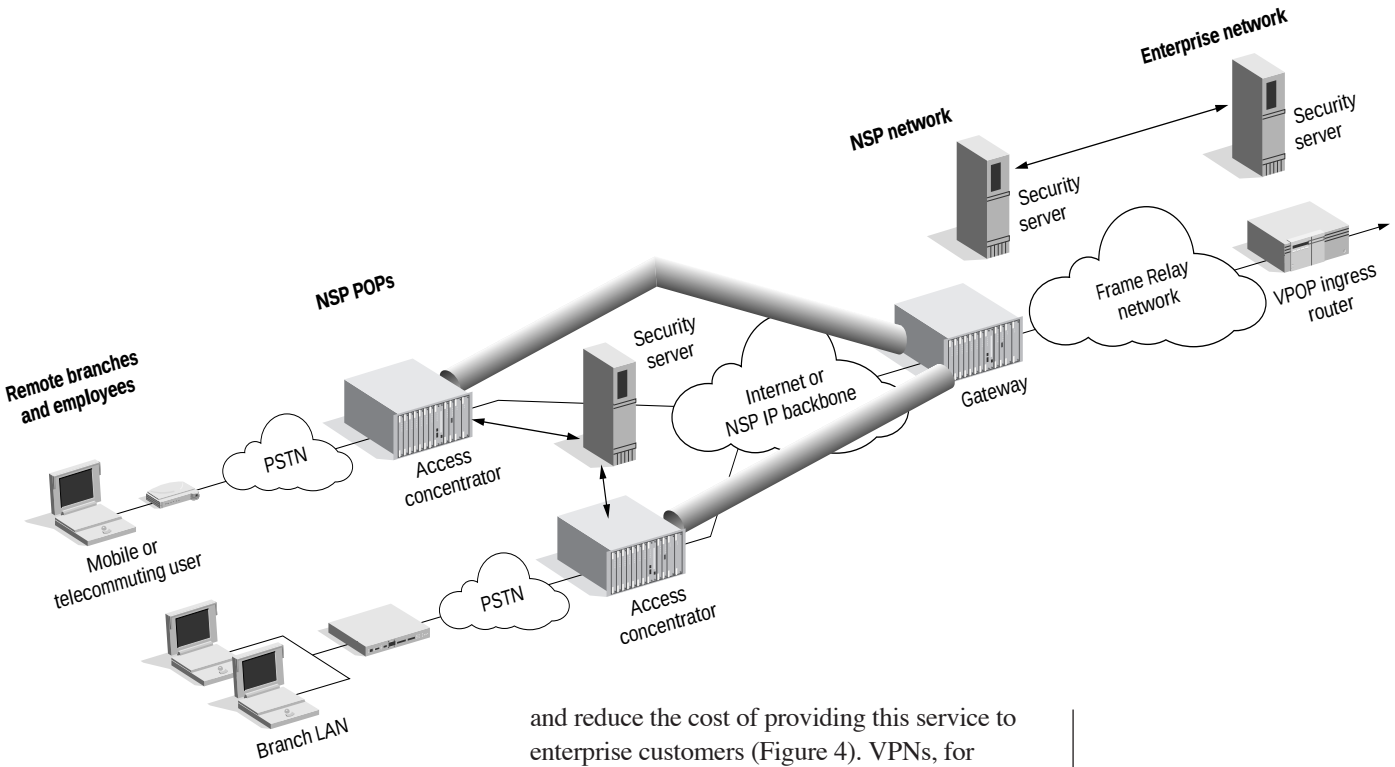

Figure 3. *Dial Access Outsourcing Using a VPN Gateway*

Typically, the NSP's tunnel termination device will perform this service by interfacing with the customer's security server.

Virtual Leased Lines

NSPs that currently offer branch connectivity over their own value-added IP networks can use VPNs to simplify network management and reduce the cost of providing this service to enterprise customers (Figure 4). VPNs, for example, eliminate the need to segregate each enterprise customer's traffic and manage loads on that portion of the network. Traffic from all enterprise customers can travel the same network in separate tunnels. NSPs, as a result, can leverage their IP networks across a growing customer base without creating a corresponding increase in network complexity.

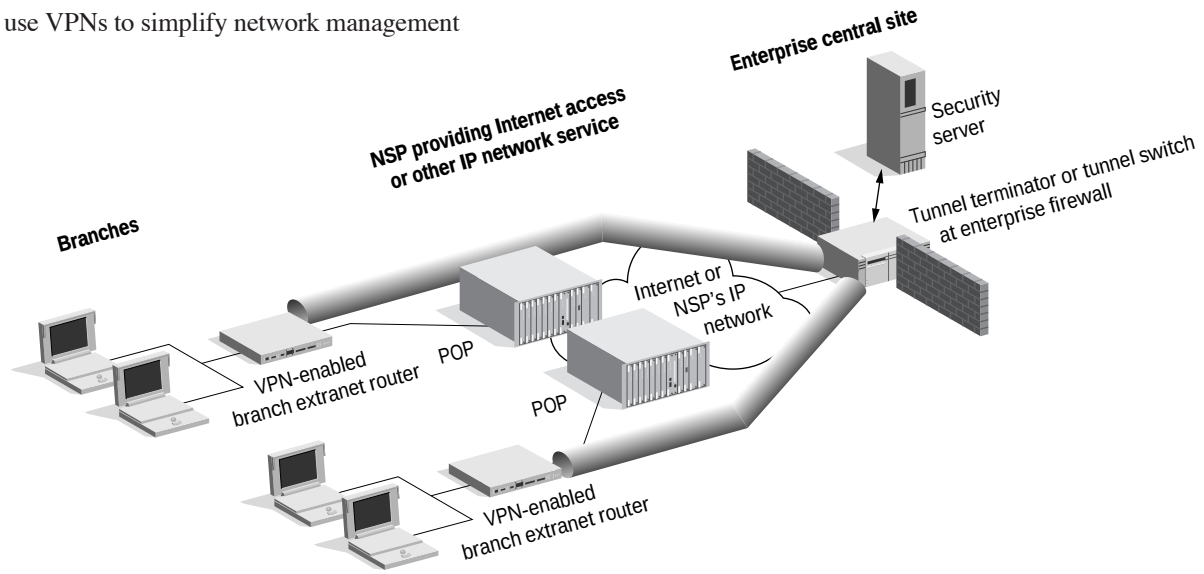

Figure 4. *Virtual Leased Lines*

Benefits: Remote Access Outsourcing

- Shift focus of business to higher-margin value-added services
- Increase rate of return on existing network facilities
- Provide service through customers' existing WAN interfaces as well as through tunneling-enabled upgraded devices
- Offer turnkey solution option, including CPE provisioning and management

Benefits: Virtual Leased Lines

- Leverage existing IP network over larger customer base while keeping management simple and costs low
- Offer Internet-based branch connectivity
- Expand value-added service offerings
- Provide turnkey solutions, including CPE installation and management

They also have the option of expanding their service tier structure by offering branch connectivity over the Internet to customers with less demanding requirements for network performance and guarantee of service.

ISPs as well as NSPs that do not currently offer branch connectivity services can now enter the market without having to make the capital investment to build out their own IP network. The service provider simply tunnels traffic between customers' branch offices over the Internet.

In virtual leased lines (VLLs), tunnels are initiated and terminated by VPN-enabled routers at the customer premises. The service provider can be responsible for just the bandwidth or it can offer a turnkey VLL package, including the installation and management of customer premises equipment (CPE).

Virtual POPs

ISPs with business plans that call for investment in services rather than infrastructure can still expand their geographic reach by leasing VPOPs. Dial access outsourcers can receive calls at their POPs and then, based on user information, forward the traffic over a VPN to the ISP (Figure 5). Users never know this is happening; as far as they're concerned, they've dialed into the ISP's POP.

The combination of VPOPs and VPNs means that even small ISPs have the opportunity to participate on a national and even international scale in the growing markets for remote access outsourcing and branch interconnectivity. As shown in the next section, even ISPs that don't have tunneling-enabled equipment can take advantage of VPOPs to expand their customer base for Internet access only.

In this type of VPN application, an access concentrator at the dial access outsourcer's POP starts the tunnel. Where the tunnel ends and what type of device performs the termination determine how wide a range of services the

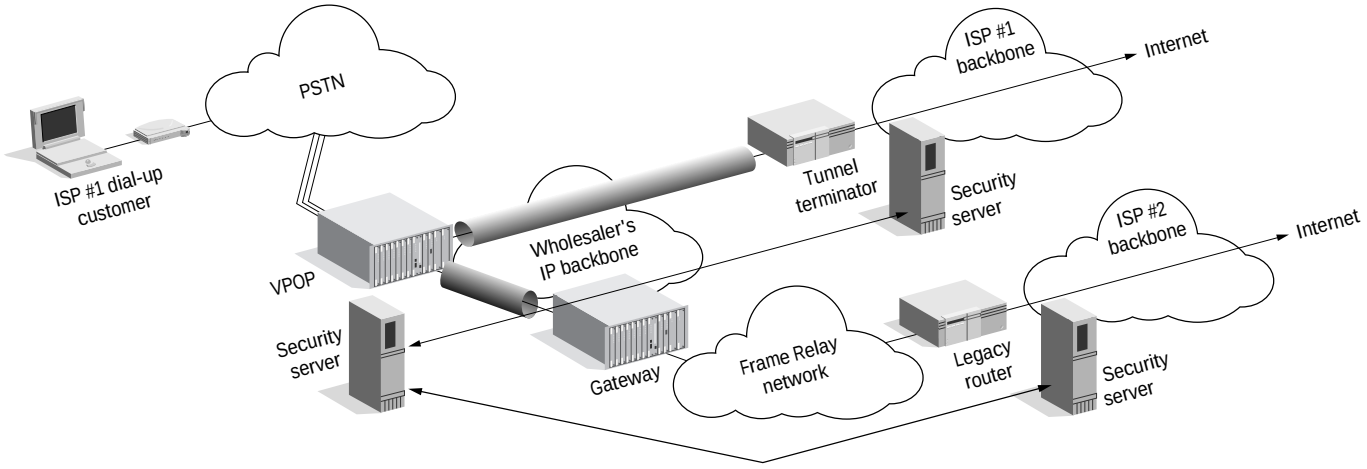

Figure 5. *Virtual POP*

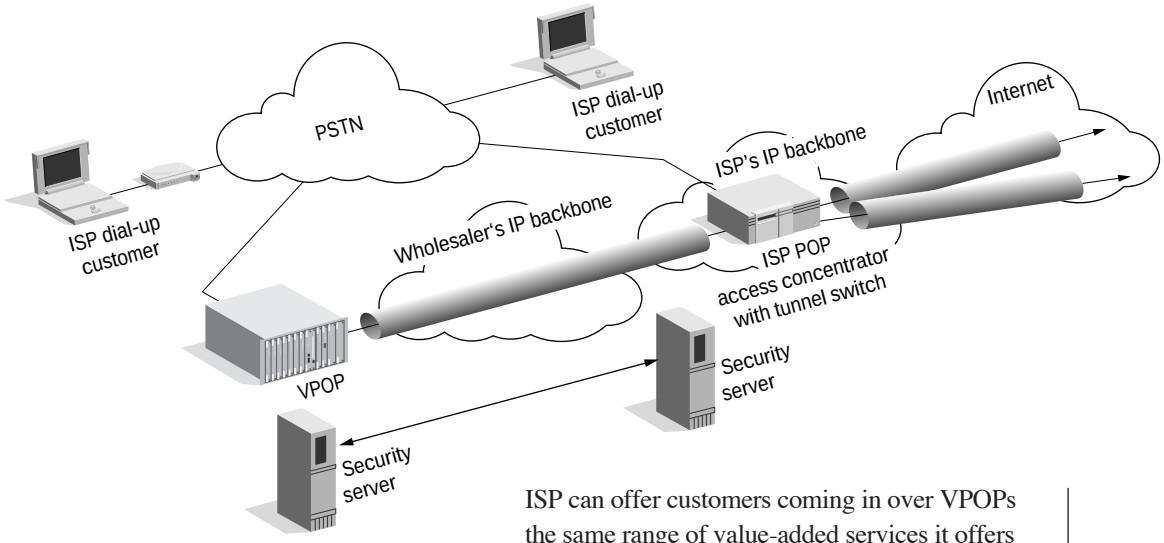

Figure 6. *Virtual POP with Tunnel Switching*

ISP can provide to traffic coming in over VPOPs.

If the ISP is not using VPN-enabled equipment to connect to its dial access outsourcer, the VPN must end at the edge of the outsourcer's network. The outsourcer's gateway terminates the tunnel and forwards the packets over a Frame Relay circuit to the ISP's network. The ISP can then direct the packets onto the Internet.

If the ISP is using VPN-enabled equipment to connect to its dial access outsourcer, the VPN can extend to the ISP's network. In that case, a tunnel termination device or tunnel switch ends the tunnel, removes the packets, and directs them onto the Internet.

If the device that terminates the tunnel coming in from the outsourcer is a tunnel switch, the ISP gains even more advantages (Figure 6). The tunnel switch can not only end the incoming tunnel but can create a new tunnel to direct the traffic over the Internet to a particular enterprise customer. As a result, the ISP can offer customers coming in over VPOPs the same range of value-added services it offers to customers coming in over its own POPs.

Service providers can deploy any number of these VPN applications over a single network infrastructure, increasing return on their owned and leased facilities. For technical information about how VPNs work, please turn to page 9.

Capital-Intensive NSPs: Improving Return on Investment While Expanding Business

NSPs that have built large network infrastructures have made costly investments. VPNs offer these providers the means to increase return on their investments by selling wholesale access to other NSPs, by providing value-added services to enterprises, or by a combination of these strategies.

Dial Access Outsourcing

VPNs create a market for leasing network capacity, enabling NSPs with available infrastructure capacity to improve asset utilization and leverage investments across the traffic flows of other service providers (Figure 7 on page 8). Depending on their business focus, providers can launch dial access outsourcing

Benefits: Virtual POPs

- Rapidly expand geographic reach without capital investment
- Meet the demands of corporate customers for national or international coverage
- Ensure total transparency to customer base

Additional Benefits with Tunnel Switching

- Offer customers coming in over virtual POPs a full range of value-added services

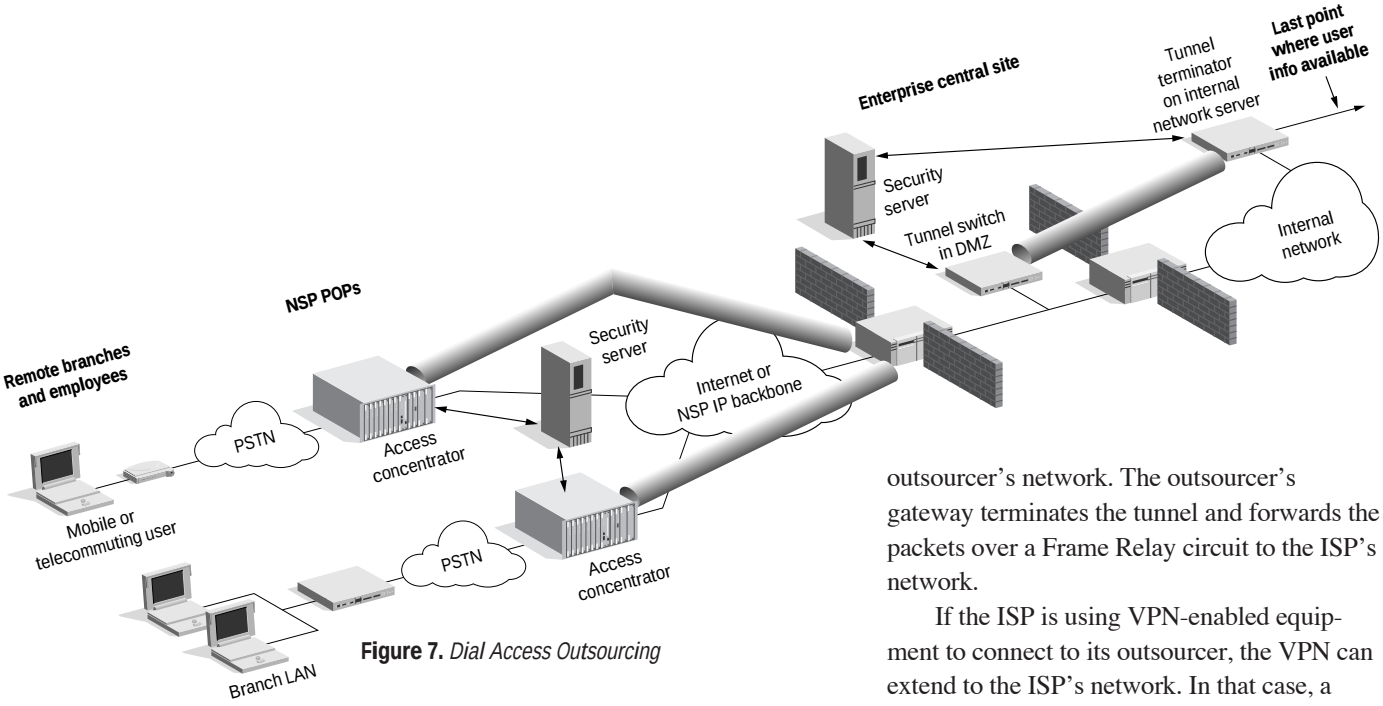

Figure 7. *Dial Access Outsourcing*

businesses or remain primarily in retail access and service while helping to finance expansion by occasionally leasing access to selected business partners. In either case, outsourcers can offer VPN services to multiple ISPs while keeping traffic for each ISP independent from the others and from traffic generated by the outsourcer's own enterprise customers.

In this type of VPN, tunnels are started by an access concentrator at the dial access outsourcer's POP. The outsourcer provides each ISP customer with one or more telephone numbers. When calls come into the POP, based on the number the user dialed or other user identification information, the TI creates a tunnel to the appropriate ISP.

If the ISP is not using VPN-enabled equipment to connect to the dial access outsourcer, the VPN must end at the edge of the outsourcer's network. The outsourcer's gateway terminates the tunnel and forwards the packets over a Frame Relay circuit to the ISP's network.

If the ISP is using VPN-enabled equipment to connect to its outsourcer, the VPN can extend to the ISP's network. In that case, a tunnel termination device or tunnel switch on the ISP's network ends the tunnel.

Access and Value-Added Service Mix

VPNs are a potentially huge business opportunity (Figure 8). Capital-intensive NSPs can use them to generate multiple revenue streams—access wholesaling, retail Internet access, value-added services such as remote access outsourcing and branch connectivity—over a single network infrastructure. In most cases, adding VPN capability requires only software or board-level upgrades to existing devices on the edges of the NSP's network.

Where multiple services are being offered to both enterprise and ISP customers, there will be a mix of equipment initiating and terminating tunnels. Tunnels can be started by access concentrators on the NSP's network as well as by end-user workstations or laptops at

Benefits: Wholesale Access

- Generate incremental revenue from fixed assets
- Accelerate return on investment
- Improve utilization of excess-capacity facilities
- Finance expansion and development of new service offerings

Benefits: Access and Value-Added Service Mix

- Accelerate return on network facilities investments by leveraging them across multiple wholesale and retail revenue streams
- Improve margins by offering value-added VPN services
- Offer turnkey solution options, including CPE provisioning and management

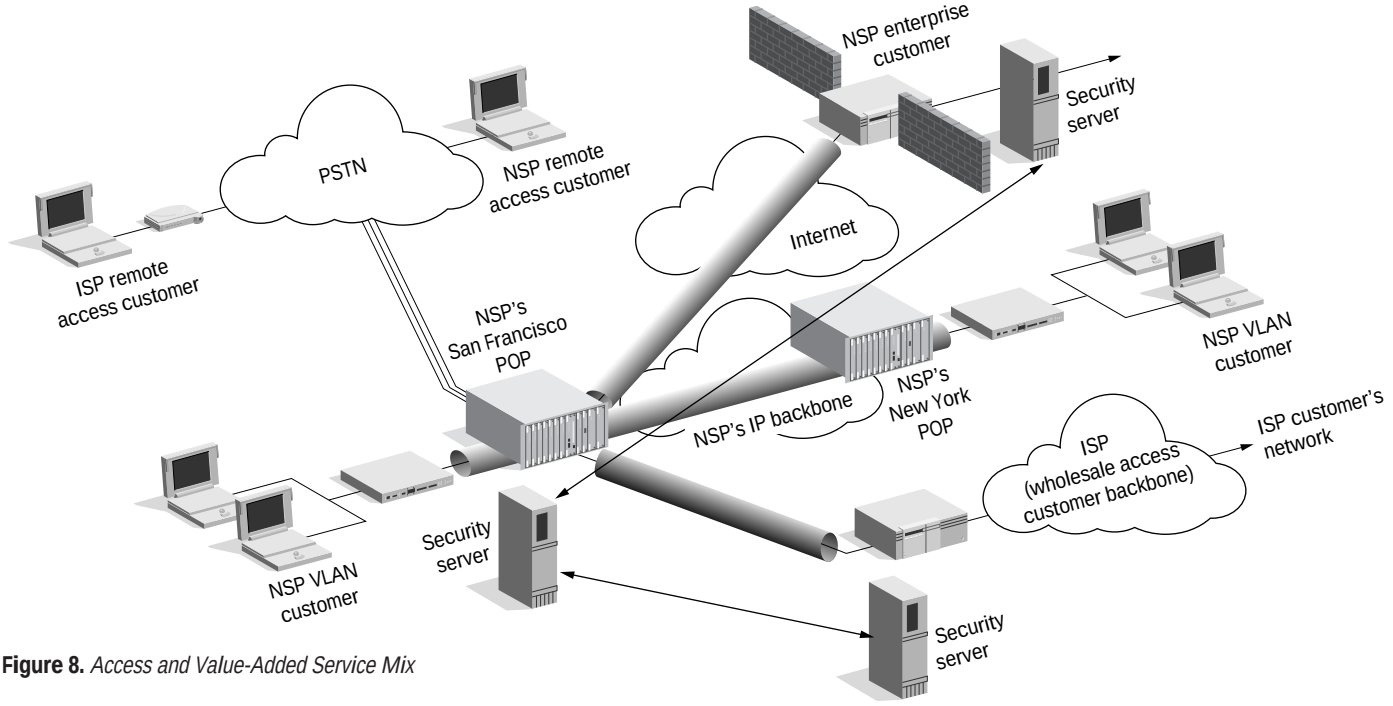

Figure 8. *Access and Value-Added Service Mix*

enterprise customer locations. Tunnels can be ended by a tunnel termination device or tunnel switch at an enterprise customer's premises or on the network of an ISP dial access outsourcing customer. They can also be ended by a Frame Relay gateway either on the network of the outsourcer or the network of the ISP leasing the access.

NSPs can deploy any number of these VPN applications as customer demands and market opportunities develop. The next section provides technical information about how VPNs work.

How VPNs Work

There is nothing exotic about VPNs. They are based on familiar networking technology and protocols (Figure 9 on page 10). 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 VLLs, 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 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 on page 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 on page 10).

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).

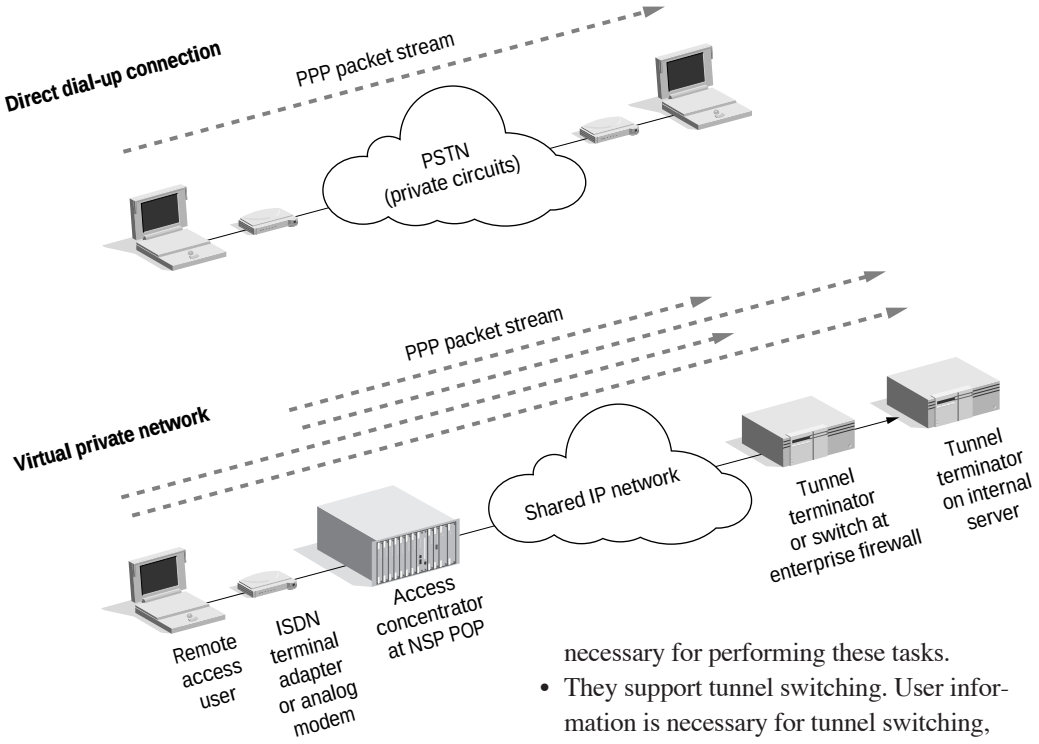

Figure 9. *VPNs Are Based on Familiar Technology*

The L2TP standard represents a merging of PPTP and 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.

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 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.

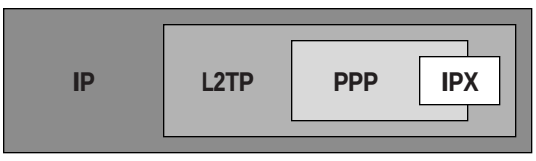

Figure 10. *Layer 2 Tunneling Protocol Encapsulation*

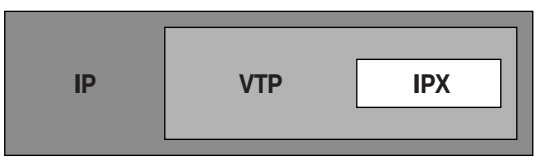

Figure 11. *Layer 3 Tunneling Protocol Encapsulation*

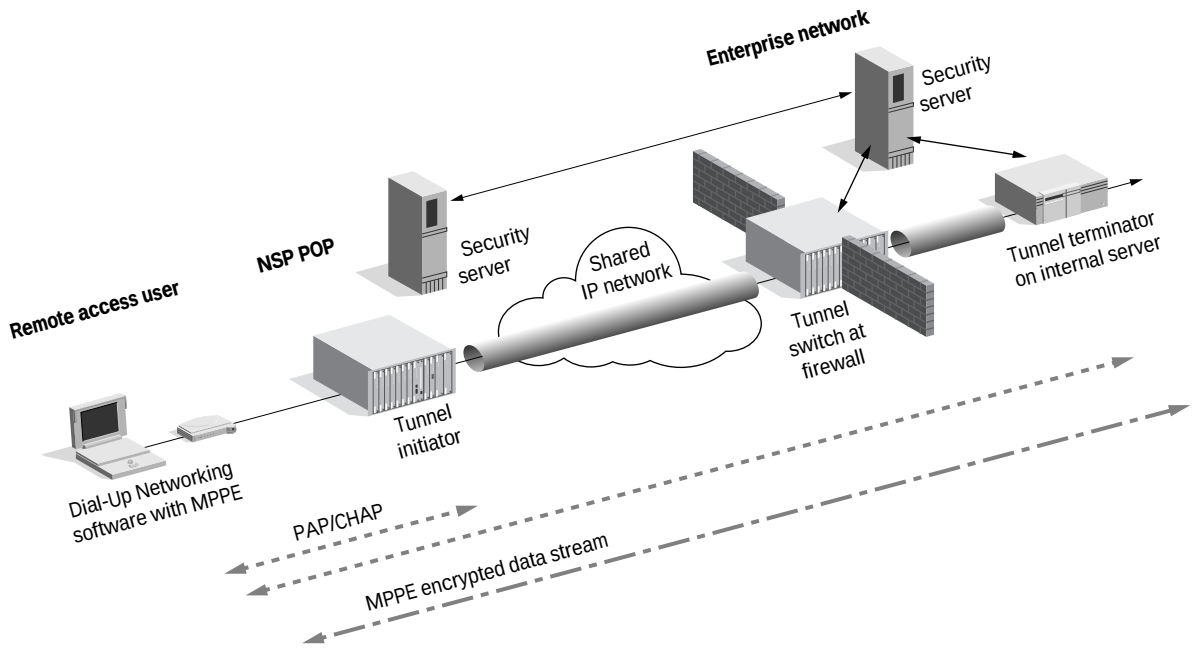

Figure 12. *MPPE with CHAP*

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.

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 12). 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

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.

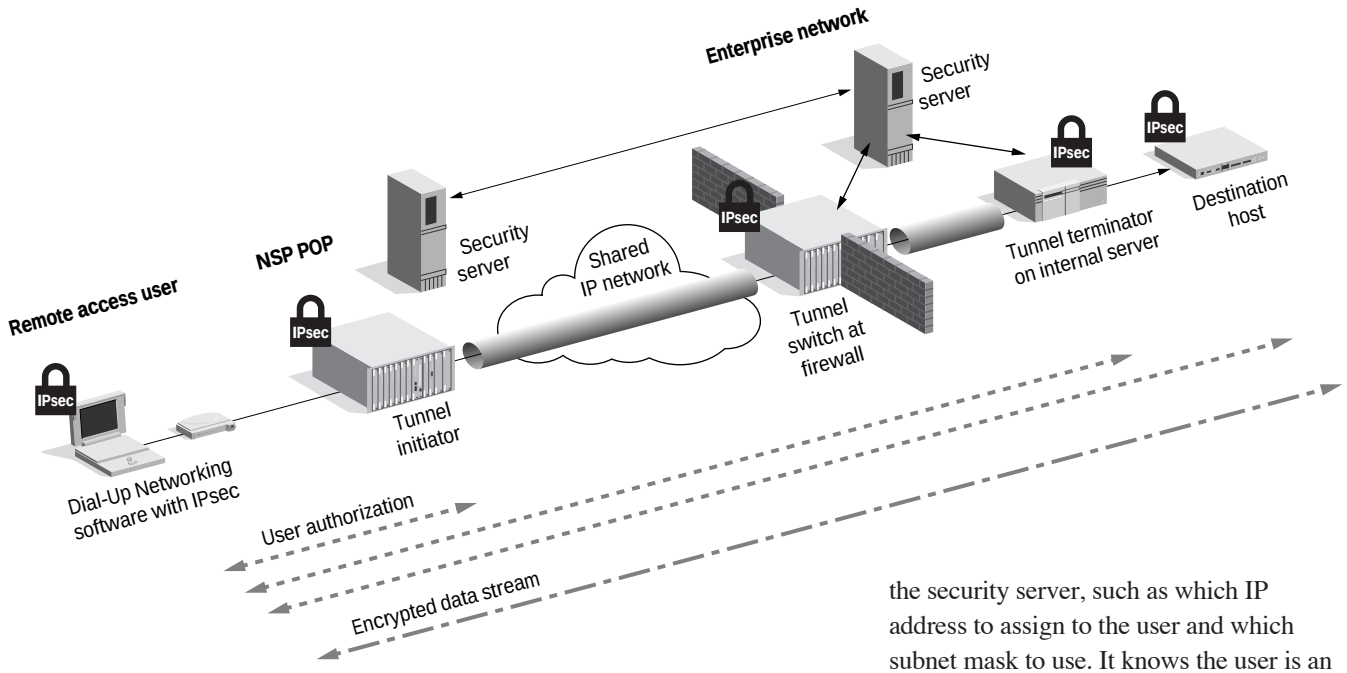

Figure 13. *IPsec*

(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 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

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.

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"

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 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: More Business Models and Service Delivery

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 an 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.

One of the most intriguing aspects of tunnel switching is the opportunities it opens up for mutually beneficial relationships between service providers (Figure14). Tunnel switching is the enabler for the much-needed cooperation between providers that has been missing from conventional "cloud" services such as Frame Relay. It means that any two VPN customers could potentially exchange packets without both having to use the same service provider. Using switching, ISPs and NSPs could hand off packets to each other, with appropriate data capture for separate accounting. And, as a result, even those ISPs that do not have large network infrastructures could offer their customers nationwide and even worldwide coverage.

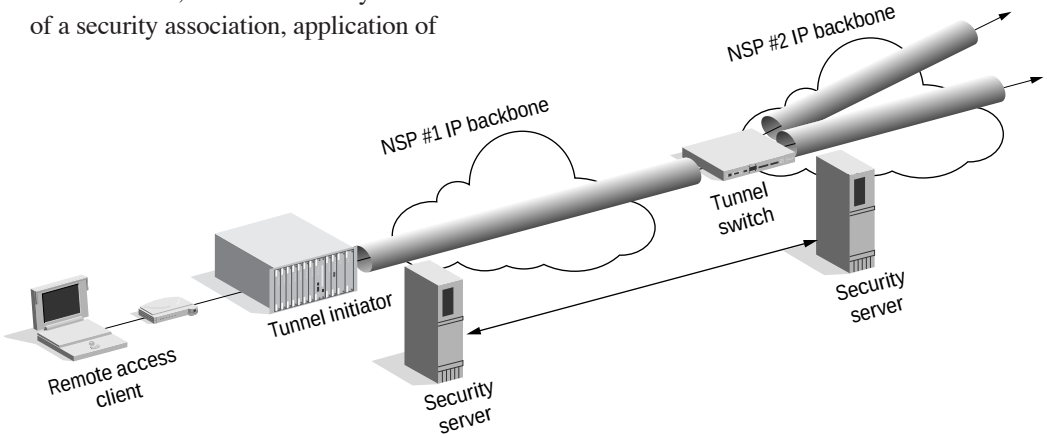

Figure 14. *Tunnel Switching Between Provider Networks*

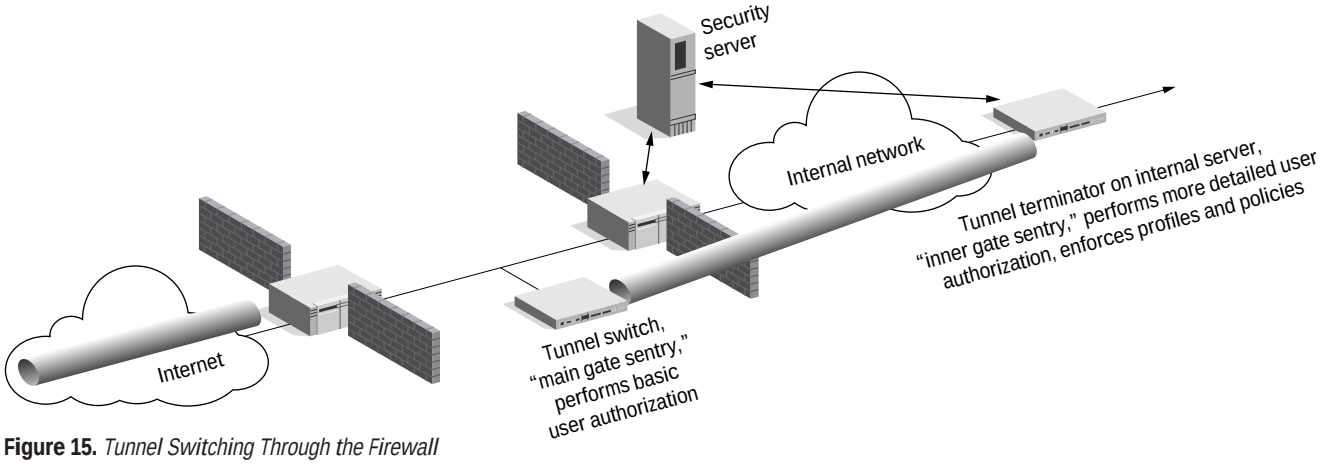

Figure 15. *Tunnel Switching Through the Firewall*

Service providers can also 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.

Tunnel switching can also benefit enterprises. A company, for example, could use tunnel switching to increase security at the firewall while improving its ability to manage remote access to network resources behind the wall (Figure 15). In this case, the tunnel switch would generally be located on the enterprise firewall. Based on a RADIUS lookup on the user name, the switch would initiate a new tunnel through the firewall to a specific internal server. Switching protects the integrity and performance of the firewall while increasing access to networked applications and resources. Other benefits for enterprises include the ability to perform server load balancing for incoming VPN traffic and increased flexibility for IP addressing.

VPN Management

The goal of 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 software, 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 software, 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. Today, 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 one another, 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 VPN Technology Leadership

- First remote access vendor to deliver VPN solutions
- Key member of IETF L2TP working group
- Inventor of patent-pending Tunnel Switching architecture
- Developer of PPTP for Microsoft Windows and Windows NT
- Developer of Virtual Tunneling Protocol (VTP) based on close carrier input

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 3Com VPN solutions 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 NSPs

NSPs can transport and receive tunneled traffic using the 3Com Total Control™ family of hubs. These devices enable NSPs to respond flexibly to market needs by simply adding or exchanging application interface cards. An NSP, for example, currently supporting ISDN and 33.6 Kbps modem dial-up connections, can add Frame Relay by just hot-swapping a card. Adding 56 Kbps modem support simply requires a software download. Total Control hubs provide all connections in a single chassis, relying on the system buses rather than congestion-prone cabling for communications.

Hubs can configure themselves on the fly to support different applications. A single modem can support, for example, dial-up to a mainframe host, remote access to a corporate LAN, and point-of-sale transaction processing—applications that would otherwise require three different modem pools.

3Com Total Control hubs provide the high reliability NSPs require. They are fault-tolerant and equipped with redundant power supplies. Hot-swappable cards and software downloadable upgrades mean that these systems rarely need to be taken off-line. To avoid a single point of failure, they also incorporate card or port redundancy, with the ability to reroute traffic to hot-standby backup cards if necessary.

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,

3Com VPN Solutions Advantages

- End-to-end compatible VPN solutions
- Built into industry-leading, market-proven products
- Tunnel switching for increased flexibility in service offerings and Quality of Service handling, cooperation with other service providers
- Standards-based (L2TP, IPsec, MPPE, etc.)
- Easy, cost-effective scalability
- Flexibility to add or change communication components with board plug-ins and software downloads
- Low cost of ownership
- Ease of migration/investment protection

Token Ring, and ATM. The NETBuilder II router products support all major LAN protocols, enabling multiprotocol tunnel traffic to be routed to the appropriate LAN server, and they also support 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 using their existing 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 must be used. 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 NSPs. 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 now begin exploiting the benefits of VPNs 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

More connected.™

3Com Corporation enables individuals and organizations worldwide to communicate and share information and resources anytime, anywhere. As one of the world's preeminent suppliers of data, voice, and video communications technology, 3Com has delivered networking solutions to more than 200 million customers worldwide. The company provides large enterprises, small and medium enterprises, carriers and network service providers, and consumers with comprehensive, innovative information access products and system solutions for building intelligent, reliable, and high-performance local and wide area networks.

3Com Corporation
P.O. Box 58145
5400 Bayfront Plaza
Santa Clara, CA
95052-8145
Phone: 1 800 NET 3Com
or 1 408 326 5000
Fax: 1 408 326 5001
World Wide Web:
www.3com.com

Asia Pacific Rim

Sydney, Australia
Phone: 61 2 9937 5000
Fax: 61 2 9956 6247

Melbourne, Australia
Phone: 61 3 9934 8888
Fax: 61 3 9934 8880

Beijing, China
Phone: 86 10 68492 568
Fax: 86 10 68492 789

Shanghai, China
Phone: 86 21 6350 1581
Fax: 86 21 6350 1531

Hong Kong
Phone: 852 2501 1111
Fax: 852 2537 1149

India
Phone: 91 11 644 3974
Fax: 91 11 623 3192

Indonesia
Phone: 62 21 572 2088
Fax: 62 21 572 2089

Osaka, Japan
Phone: 81 6 536 3303
Fax: 81 6 536 3304

Tokyo, Japan
Phone: 81 3 5977 3266
Phone: 0120 313266
(toll free from Japan)
Fax: 81 3 5977 3370

Korea
Phone: 82 2 3455 6300
Fax: 82 2 319 4710

Malaysia
Phone: 60 3 715 1333
Fax: 60 3 715 2333

New Zealand
Phone: 64 9 366 9138
Fax: 64 9 366 9139

Philippines
Phone: 632 892 4476
Fax: 632 811 5493

Singapore
Phone: 65 538 9368
Fax: 65 538 9369

Taiwan
Phone: 886 2 2 377 5850
Fax: 886 2 2 377 5860

Thailand
Phone: 662 231 8151 5
Fax: 662 231 8158

3Com Austria
Phone: 43 1 580 17 0
Fax: 43 1 580 17 20

3Com Benelux B.V.

Belgium
Phone: 32 2 725 0202
Fax: 32 2 720 1211

Netherlands
Phone: 31 346 58 62 11
Fax: 31 346 58 62 22

3Com Canada

Calgary
Phone: 1 403 265 3266
Fax: 1 403 265 3268

Edmonton
Phone: 1 403 423 3266
Fax: 1 403 423 2368

Montreal
Phone: 1 514 683 3266
Fax: 1 514 683 5122

Ottawa
Phone: 1 613 566 7055
Fax: 1 613 233 9527

Toronto
Phone: 1 416 498 3266
Fax: 1 416 498 1262

Vancouver
Phone: 1 604 434 3266
Fax: 1 604 434 3264

3Com Eastern Europe/CIS

Bulgaria
Phone: 359 2 962 5222
Fax: 359 2 962 4322

Czech Republic
Phone: 420 2 21845 800
Fax: 420 2 21845 811

Hungary
Phone: 36 1 250 8341
Fax: 36 1 250 8347

Poland
Phone: 48 22 6451351
Fax: 48 22 6451352

Russia
Phone: 7 095 258 09 40
Fax: 7 095 258 09 41

Slovak Republic
Phone: 421 7 317 850
Fax: 421 7 317 849

3Com France
Phone: 33 1 69 86 68 00
Fax: 33 1 69 07 11 54
Carrier and Client Access
Phone: 33 1 41 97 46 00
Fax: 33 1 49 07 03 43

3Com GmbH

Munich, Germany
Phone: 49 89 627320
Fax: 49 89 62732233

3Com Iberia

Portugal
Phone: 351 1 3404505
Fax: 351 1 3404575

Spain
Phone: 34 1 509 69 00
Fax: 34 1 307 79 82

3Com Latin America

U.S. Headquarters
Phone: 1 408 326 2093
Fax: 1 408 764 5730

Miami, Florida
Phone: 1 305 461 8400
Fax: 1 305 461 8401

Argentina
Phone: 54 1 312 3266
Fax: 54 1 314 3329

Brazil
Phone: 55 11 246 5001
Fax: 55 11 246 3444

Chile (serving Chile, Bolivia, and Peru)
Phone: 562 240 6200
Fax: 562 6240 6231

Colombia
Phone: 57 1 629 4847
Fax: 57 1 629 4503

Mexico
Phone: 52 5 520 7841/7847
Fax: 52 5 520 7837

Peru
Phone: 51 1 221 5399
Fax: 51 1 221 5499

Venezuela
Phone: 58 2 953 8122
Fax: 58 2 953 9686

3Com Mediterraneo

Milan, Italy
Phone: 39 2 253011
Fax: 39 2 27304244

Rome, Italy
Phone: 39 6 5279941
Fax: 39 6 52799423

3Com Middle East
Phone: 971 4 319533
Fax: 971 4 316766

3Com Nordic AB

Denmark
Phone: 45 48 10 50 00
Fax: 45 48 10 50 50

Finland
Phone: 358 9 435 420 67
Fax: 358 9 455 51 66

Norway
Phone: 47 22 58 47 00
Fax: 47 22 58 47 01

Sweden
Phone: 46 8 587 05 600
Fax: 46 8 587 05 601

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

3Com Switzerland
Phone: 41 844 833 933
Fax: 41 844 833 934

3Com UK Ltd.

Edinburgh
Phone: 44 131 240 2900
Fax: 44 131 240 2903

Ireland
Phone: 353 1 823 5000
Fax: 353 1 823 5001

Manchester
Phone: 44 161 873 7717
Fax: 44 161 873 8053

Winnersh
Phone: 44 1189 27 8200
Fax: 44 1189 695555

To learn more about 3Com products and services, visit our World Wide Web site at www.3com.com. 3Com is a publicly traded corporation (Nasdaq: COMS).

Printed in U.S.A. on recycled paper

500649-002 11/98