Microsoft®

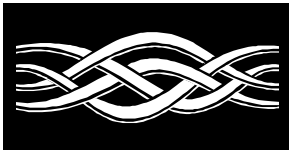# Microsoft®
Windows NT® Server

Server Operating System

White Paper

Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet

Microsoft®
Windows NT® Server

Virtual Private Networking

Microsoft Virtual Private Networking (VPN) technology is based upon the open standard Point-to-Point Tunneling Protocol (PPTP). PPTP is a new networking technology that supports multiprotocol VPNs. Using PPTP, remote users can employ the Microsoft® Windows® 95 and Windows NT® Workstation operating systems and other point-to-point protocol (PPP)-enabled client systems to dial into a local Internet service provider to connect securely to their corporate network via the Internet. Remote users dial into the local number of an Internet service provider, and securely tunnel into their corporate network. VPN technology gives users an economical and easy-to-implement solution for creating secure and encrypted communication across the Internet.

CONTENTS

Employees on business trips need to stay current with their electronic mail. Sales representatives in the field must be able to access corporate databases. Branch offices must be part of the corporate network. Telecommuting workers, including those just working after hours and weekends from home, have to transfer files and open applications. These are just some of the everyday forces that are driving the ever greater demand for remote access to a company's computer network.

For network administrators, the need to provide remote access has been a double challenge. There is the high cost of supportive infrastructure with modem pools and dedicated phone lines (or expensive long-distance costs), along with the threat to a network's security that can result if unauthorized users gained entry.

Paralleling the rising demand for remote access has been the need to provide workers with Internet connectivity, often causing duplicate connectivity investments and soaring costs. Although the Internet provides a natural, and inexpensive path for linking remote users, security concerns have made network administrators reluctant to open their systems to remote access via the Internet.

Microsoft Virtual Private Network (VPN) technology, is specifically designed to solve the problem of providing secure and economical remote access. Based upon the open-standard Point-to-Point Tunneling Protocol (PPTP), VPN allows corporations and individuals to take advantage of the vast Internet infrastructure (or other public carriers) to provide secure connectivity between remote clients and private networks. Remote users just dial into the local number of an Internet service provider, and securely tunnel into their corporate network.

Additionally, PPTP can be used with dense and integrated communications solutions to support V.34 and ISDN dial-up. And corporations can use a PPTP-enabled VPN over IP backbones to outsource dial-up access to their corporate networks in a manner that is cost-effective, hassle-free, protocol-independent, secure, and that requires no changes to their existing network addressing.

Microsoft is working with the PPTP Forum to support PPTP as an open industry standard. This group of leading companies includes Ascend Communications, 3Com/Primary Access, ECI/Telematics, and US Robotics. PPTP is also attracting extensive third-party support.

Emerging as a Standard

At the June 1996 IETF meeting in Montreal, the PPTP Forum companies presented PPTP to the IETF's PPP Extensions working group as an Internet Draft standard. The working group agreed to the proposal, which includes converging PPTP and Cisco's Layer 2 Forwarding approach to tunneling in the months ahead. The PPTP technical specification is now updated and available as an IETF Internet Draft. Sample source code is also available via the World Wide Web so vendors and businesses can implement PPTP solutions on a variety of operating systems and hardware platforms.

This is good news for the industry as a variety of proprietary tunneling methods were available in the past, but no standard. Movement toward this standard

signals an opportunity for remote access system vendors, Internet Service Providers, and firewall vendors to provide great value-added benefits for their customers. PPTP-enabled systems can now be deployed with the confidence that Microsoft will ensure compatibility with the PPTP standard as it evolves through the IETF and into the future.

Providing Economic Benefits

Microsoft Virtual Private Networking (VPN) will be integrated into the Windows NT 4.0 operating system, providing the tunneling solution for remote access at no extra cost. Microsoft also plans to provide PPTP support for Windows 95 by the end of the year.

Significant cost-savings can be achieved by using Microsoft VPN to turn the vast reach of the Internet into your own virtual private network. In addition to saving the costs of leased lines and long distance dialing, businesses can escape the cost of purchasing and managing redundant banks of modems, and specialized software. VPN allows the same equipment used for Internet access to be used for providing remote access.

The transition for remote users is as simple as a few clicks of the mouse, as VPN is smoothly integrated into the same Windows dialup commands they may already be using.

All of this makes Microsoft's multiprotocol VPN the easiest way for businesses to securely and economically extend their private networks across the Internet to remote users.
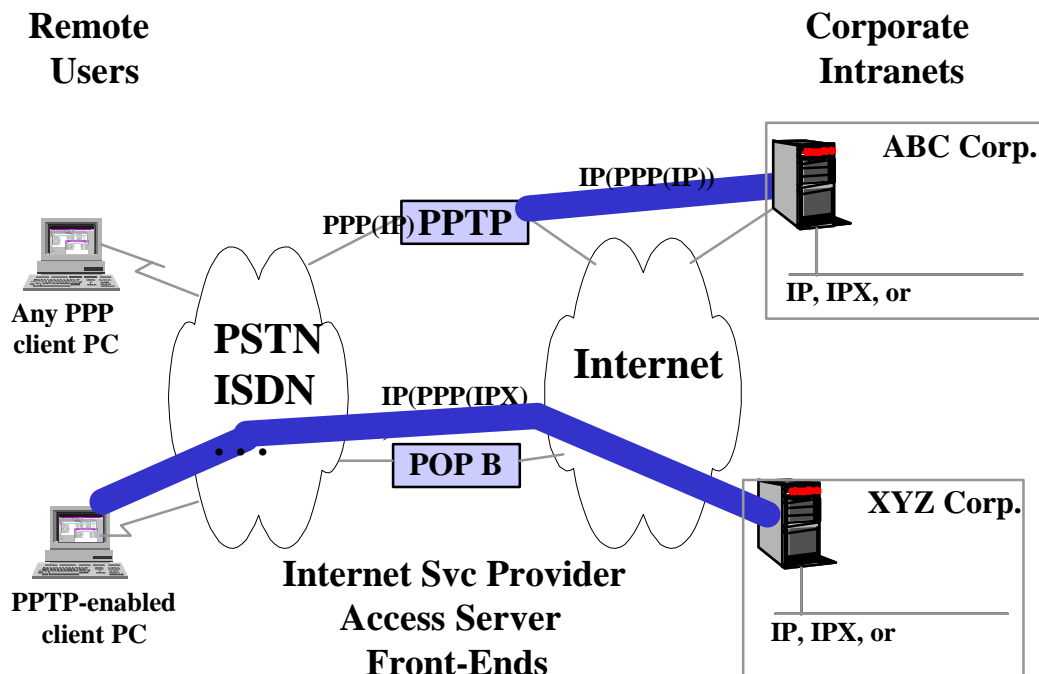
VPN Defined

A Virtual Private Network can be described as the ability to "tunnel" through the Internet or other public network in a manner that provides the same security and other features formerly only available on private networks. It allows a user working at home or on the road to connect to a remote corporate server using the bandwidth provided by the public network. VPN allows a corporation to connect with branch offices, or with other companies, while maintaining a secure PPTP connection.

From the user's perspective, the nature of the physical network being tunneled through is irrelevant because it appears as if the information is being sent over a dedicated private network.

From a more technical perspective, a VPN tunnel encapsulates data within IP packets to transport information that does not otherwise conform to Internet addressing standards. The result is that remote users become virtual nodes on the network into which they have tunneled.

A user on a Remote Access Service (RAS) client machine with a PPTP driver as its WAN driver will be able to access resources across the Internet on a remote LAN through a Windows NT RAS server, via tunneled and encrypted PPP packets. (RAS supports bulk data encryption using RSA RC4 and a 40 bit session key negotiated at PPP connect time between the RAS client and the Windows NT RAS server.)

Remote Users

Corporate Intranets

ABC Corp.

IP(PPP(IP))

PPP(IP) **PPTP**

Any PPP client PC

IP, IPX, or

PSTN ISDN

Internet

IP(PPP(IPX)

POP B

XYZ Corp.

PPTP-enabled client PC

IP, IPX, or

Internet Svc Provider Access Server Front-Ends

A conceptual model of a VPN. Remote clients connecting to IP-, IPX- or NetBEUI-based corporate networks via the Internet.

The PPTP-based solution will also enable the Internet to become a backbone for carrying IPX as well as NetBEUI remote access traffic, so a solution is not tied to IP LANs only.

Providing for Easy Implementation

Microsoft Virtual Private Networks have been designed to make their implementation easy for network administrators. Benefits of using a VPN include the following:

- Enables installation of PPTP on either the client or ISP
- Supports all major network protocols
- Allows existing network addresses to be used
- Allows existing communications equipment to be used
- Provides flow control
- Uses open industry standards
- Ships with Windows NT Server and Windows NT Workstation
- Upgrades for Windows 95 will be ready for downloading by end of year
- Provides value-added opportunity for ISPs

All of this combines to make Microsoft VPN the economical, easy-to-implement, and secure way to use the vast Internet infrastructure in creating your own virtual private networks.

Enables Installation of PPTP on Either the Client or ISP

Once PPTP is installed on the Microsoft Windows NT Server-end, tunneling access is achieved either through a PPTP-enabled client, or through a PPTP-enabled Internet service provider (ISP) point-of-presence (POP) server.

This flexibility means that a person with a PPTP-enabled laptop or home computer can make secure tunneled connection with their company's NT Server network, even when using an ISP that is not PPTP enabled.

Similarly, a user without a PPTP-enabled computer can make a secure tunneled connection if their ISP has upgraded its network to support PPTP on its servers.

This gives ISPs the ability to provide value-added services to users who want to take advantage of PPTP communication, but haven't installed it on their own computers.

PPTP can also be used for a remote client using a non-telephone connection such as an Ethernet card connected to a Frame relay service with a direct connection into an Internet carrier. As long as both the remote client PC and the server are upgraded to support PPTP, the user can benefit from secure PPTP connections.

Upgrading is Easy

Internet Service Providers can provide their customers full multiprotocol VPN capability with an easy software upgrade for their existing remote access servers. Ascend, 3Com, ECI Telematics, and US Robotics are including PPTP support in their existing products as a software upgrade.

Again, end users can install PPTP on their PCs and use essentially any Internet Service Provider. A software upgrade to the client PC and organization's server will enable the secure tunnel through any Internet POP, even if the ISP has not upgraded its infrastructure to support PPTP.

Supports All Major Network Protocols

VPN supports all major networks including TCP/IP, IPX/SPX, and NetBEUI. Multiprotocol VPN enables remote users to access heterogeneous networks across the Internet.

Microsoft VPN allows a user to dial in with an analog modem, an ISDN connection, an X.25 device, or other connection, through a POP, which would ideally be local to avoid long distance telephone charges. VPN can go through any type of network, including Windows NT Remote Access Server, IPX-based Novell, and NetBEUI environments. Because VPN supports multiprotocols, users can retain the benefits of PPTP when on different networks.

Allows Existing Network Addresses To Be Used

VPN requires no change to existing network addressing schemes. This is helpful to companies deploying internal networks with an arbitrary device-numbering scheme that doesn't conform to the standard Internet Assigned Numbers Authority (IANA) approach. Once a user registers their domain name, the DNS can resolve the common name used in the address.

This ability to handle nonconforming addresses can be a huge benefit for LAN administrators, saving them from having to re-address each device on their network just to enable remote access. Because PPTP uses encapsulation,

which hides nonstandard addresses, VPNs allow companies to use non-standard IP and IPX addresses.

Allows Reuse of Communications Gear

Microsoft VPN allows companies to leverage their existing communication links and services. Rather than add an entire bank of new modem gear or other equipment to allow remote access to their networks, a company can use their existing links to the Internet. By eliminating the need for custom hardware and software, Microsoft VPN also saves companies in staffing and training costs that are otherwise needed to support custom proprietary solutions.

Provides Flow Control

Microsoft has included a new flow control protocol as part of PPTP. Flow control sits between the client and the server on the data path. Without flow control, a client can continue sending packets to an overloaded server that cannot handle them. Performance will be slowed as packets are sent several times before they pass through. Flow control allows the server to tell the client to stop, and to start again when resources are available. Flow control also reduces network congestion, by eliminating the need to re-send packets.

Uses Open Industry Standards

Microsoft VPN is based upon PPTP (a protocol introduced by the PPTP Forum) and is now an IETF Internet Draft Standard. PPTP is an extension of two important Internet foundations for routing and security: IP and PPP. PPTP enjoys broad and growing industry support, and has been embraced by leading remote access vendors, ISPs, and vendors of other related products.

Because PPTP is an open standard, it isn't specific to Windows-based systems and can be deployed throughout a heterogeneous environment. Any PPP client computer (including UNIX and Macintosh), server type, or other remote access system can make use of PPTP.

Microsoft has published sample source code to facilitate PPTP implementation on other platforms. You can download it from the Web at ftp://ftp.microsoft.com/developer/drg/pptp/src.

Ships with Windows NT and Windows 95

Microsoft VPN was shipped as part of Windows NT 4.0, and an upgrade will be supplied for Windows 95. Open APIs will be provided toward the end of 1996 so that other companies can create Windows 3.1 or other client implementations of PPTP. Third-party companies are also creating products that support PPTP for other operating systems.

Because it is based upon Windows NT Server, Microsoft VPN provides all of the benefits of Windows NT. Windows NT is open, reliable and robust; supports multithreading and multitasking; is secure and scalable; and is completely integrated with the Microsoft BackOffice™ family of server applications for the Internet and intranet. These attributes make Windows NT an excellent platform for value-added development of communications applications, such as routing and telephony, in addition to remote access.

Provides value-added opportunity for ISPs

Internet service providers can use Microsoft VPN to offer secure, tunneled connections for subscribers, allowing them to tap into their own virtual private networks. ISPs can use this important value-added feature to distinguish their services in an increasingly competitive market.

Making PPTP Easy to Use

Microsoft's Multiprotocol VPN, enabled by the Point-to-Point Tunneling Protocol (PPTP), is the easiest way for businesses to securely and economically extend their private networks across the Internet to remote users. Ease of use has been built into VPN from its inception for both the server and client personal computer. For network administrators faced with rolling out new technologies, ease of use means rapid and effective adoption.

On the Server

Setting up VPN on Windows NT Server 4.0 is easy. VPN can be considered just a special case or use of RAS, an important feature set already built into Windows NT. As a result, setting up a VPN using PPTP involves many of the same steps an IS administrator takes when setting up a server to accept dial-up networking connections via RAS.

After setting up the Wide Area Networking (WAN) card, the IS administrator then selects the protocol or protocols to be used with RAS—IP, IPX, and/or NetBEUI. PPTP is now another protocol that can be selected and installed in the same way these other protocols are enabled. IS administrators who are familiar with RAS set-up will find the few screens and dialog boxes used to set up and use PPTP quite similar.
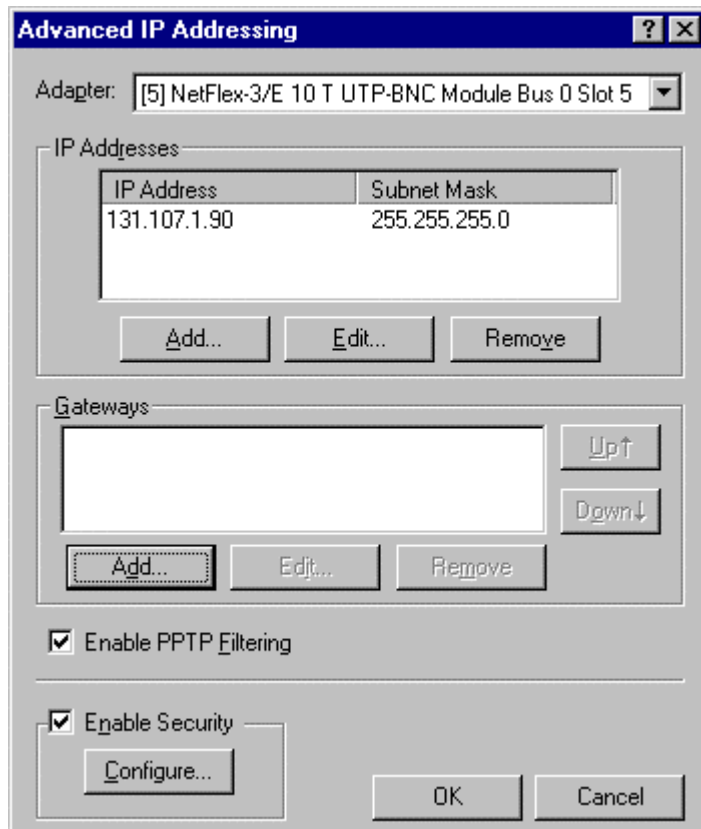
The IS administrator can set-up the server to accept only PPTP-based users as an added measure of security.

The IS administrator retains control of who gets access to the corporate network with Microsoft's VPN, even if the company has outsourced its VPN service to a third party. That's because user profiles are retained on the Windows NT Server so they can be quickly updated by the IS administrator to reflect employee changes, and so on.

As an added security measure when using VPN, the IS manager can have the server apply a filter that gives access to the corporate network only to PPTP-based users . This is shown in the preceding figure.
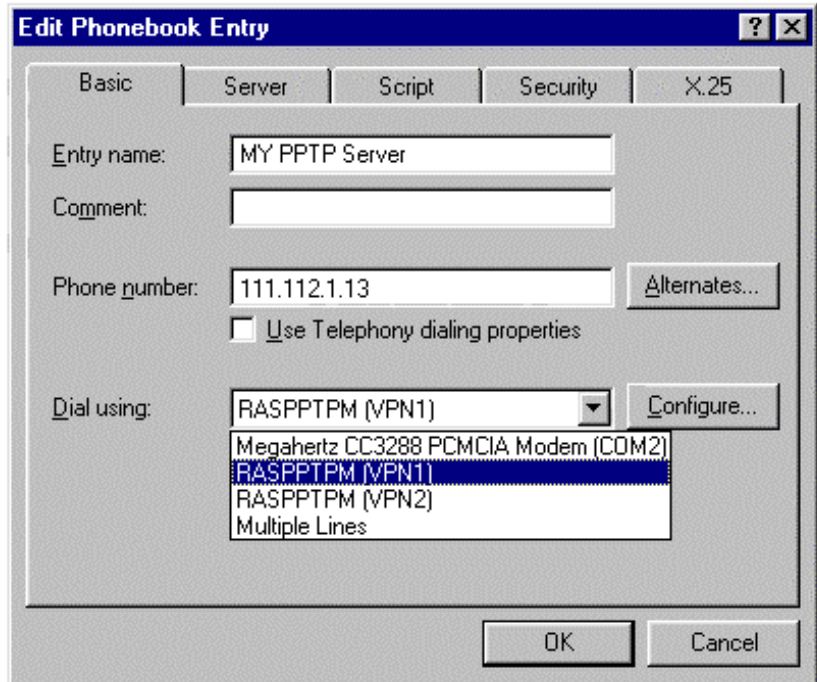
On the Client

VPN set-up and use on the client is also easy. As noted, when PPTP support is provided by an ISP, no change in set-up is required to the client computer. In this situation, VPN support is transparent to the user, as shown in the following figure..
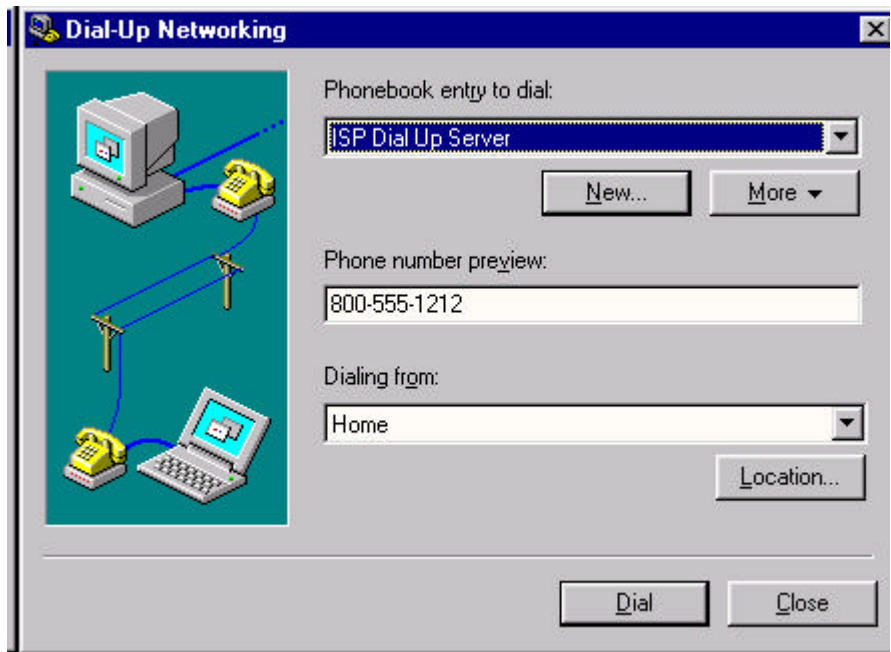
Establishing a VPN connection via an Internet Service Provider that supports PPTP is transparent to the client computer. The remote client computer dial up sequence looks like any other RAS dial-up sequence.

VPN service can also be enabled on the client computer, allowing the user to connect to the corporate network via any ISP—even those ISPs which do not provide PPTP support in their points of presence. In this case, the client computer must have the PPTP protocol installed, in much the same manner as on the server machine. Again, PPTP is treated just like IP, IPX or other selectable protocols.

Once PPTP is installed on the client computer, the user then creates a RAS Phone Book entry for the VPN connection. This entry looks like any other Phone Book entry with two exceptions: an IP address appears in place of a telephone number , and the *Dial Using* pull down list includes a PPTP option. This VPN Phone Book entry is activated after the user has connected to the ISP, so it is a two-step process. To further simplify use, both the ISP connection and the VPN connection can be set up and activated from one easy auto-dial Phone Book entry.

Setting up a client computer to enable it to use VPN service is straightforward, as this screen indicates. PPTP has already been installed on this computer so that when a new RAS Phone Book entry is created, a PPTP option is available in the Dial Using pull down list.

Once this Phone Book entry has been set up, the user can simply double-click on the Phone Book Entry icon to automatically dial into the PPTP-supported server via any ISP, as noted in following figure.
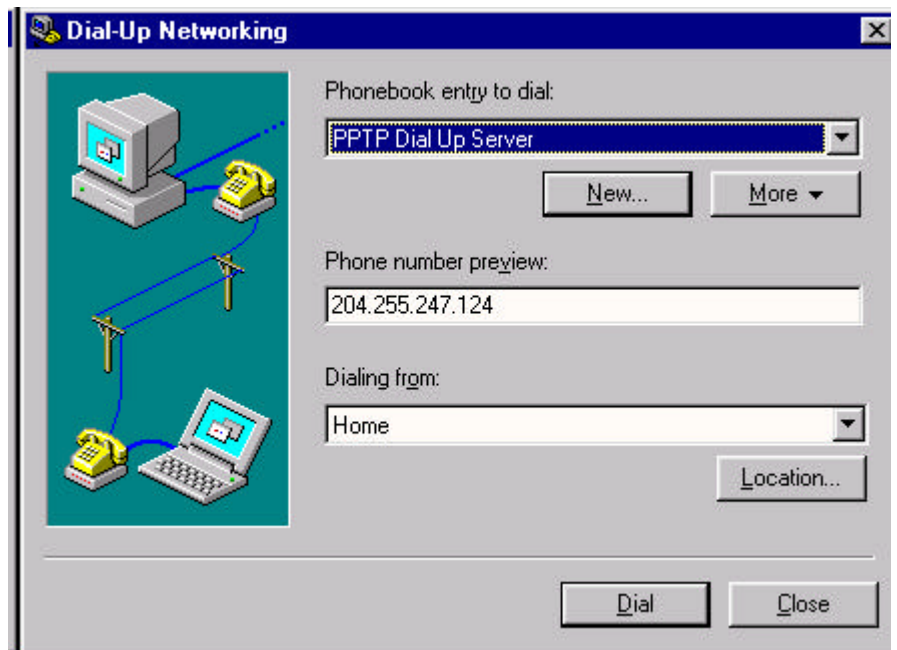
Establishing a VPN connection from a PPTP-enabled client computer lets you use essentially any ISP to connect to the Internet and back to your corporate network.

Taking a Closer Look at PPTP

Microsoft VPN makes use of existing corporate backbones, SNA backbones and Internet backbones as "virtual WANs." In the case of PSTN, ISDN, and X.25, a remote access client establishes a point-to-point connection with a RAS server over a switched network. Once the connection is established, network packets are sent over the switched connection to the RAS servers for routing to the destination LAN.

Combining PPP and IP

The PPTP protocol is built upon the well-established Internet communications protocol of PPP (Point-to-Point Protocol), and TCP/IP (Transmission Control Protocol/Internet Protocol). PPP is multiprotocol, offers authentication, and also offers methods of privacy and compression of data. IP is routable, and has an Internet infrastructure. PPTP allows a PPP session to be tunneled through an existing IP connection, no matter how it was set up. An existing connection can be treated as if it were a telephone line, so a private network can run over a public one.

Tunneling is achieved because PPTP provides encapsulation by wrapping packets of information (IP, IPX, or NetBEUI) within IP packets for transmission through the Internet. Upon receipt, the external IP packets are stripped away, exposing the original packets for delivery. Encapsulation allows the transport of packets that will not otherwise conform to Internet addressing standards.

A rough analogy is someone in a branch office addressing an interoffice mail envelope to "Bill Smith, Marketing," and then dropping it into the U.S. mail, hoping it would be delivered to Bill Smith in the home office. PPTP encapsulation essentially wraps the interoffice mail envelope into a standardized envelope that carries the home office's exact (DNS) address. Once it arrives at the home office, the standardized envelope is removed, and the original interoffice envelope's addressing is sufficient for final delivery. Of course, PPTP does much more than simply deliver messages. Once a PPTP link has been established, it provides its user with a virtual node on the corporate LAN or WAN.

A typical packet

Media	IP	GRE	PPP	PPP Payload

PPTP uses an enhanced Generic Routing Encapsulation (GRE) protocol in transporting PPP packets.

Encryption is used for encapsulated data. An authentication protocol is used to verify users' identities before granting access.

Coordinating Data Transmission

PPTP tunneling makes use of two basic packet types—data packets and control packets. Control packets are used strictly for status inquiry and signaling information. Control packets are transmitted and received over a TCP connec-

tion. When a link is established between a Windows NT Server and a front-end processor (FEP), they will use a single TCP connection for the control channel. Data packets contain the user data that must be sent to or received from the LAN or WAN. Data packets are PPP packets encapsulated using the Internet Generic Routing Encapsulation Protocol Version 2 (GRE V2).

When two computers want to talk to each other, they ask for permission to send IP traffic, establishing the compression scheme and encapsulation method to be used. This "handshaking" makes sure the computers know how to talk to each other.

During transmission, data can be divided into small IP packets, framed with a PPP header, and sent across the network, with PPP providing serialization to detect if a packet is lost.

Coordination of data transmission is enhanced with the PPTP protocol, which performs the following tasks:

- Queries the status of communications servers
- Provides in-band management
- Allocates channels and places outgoing calls
- Notifies Windows NT Server of incoming calls
- Transmits and receives user data with bidirectional flow control
- Notifies Windows NT Server of disconnected calls
- Assures data integrity, while making most efficient use of network bandwidth by tightly coordinating this packet flow.

Security

Microsoft VPN uses proven Windows NT RAS security. Businesses can ensure secure communication between remote users and the private network using Windows NT RAS encryption and authentication protocols. Windows NT RAS supports Password Authentication Protection (PAP), the more sophisticated Challenge Handshake Authentication Protocol (CHAP), a special Microsoft adaptation called MS-CHAP, as well as RSA RC4, and DES encryption technologies.

Authentication and Encryption

Clients accounts are validated against the Windows NT user database, and only those with valid permissions are allowed to connect. The keys used to encrypt data are derived from the users credentials, and are not transferred on the wire. When authentication is completed, the user's identity is verified, and the authentication key is used for encryption. Windows NT 4.0 uses 40-bit RC-4 encryption. For the United States and Canada, Microsoft will provide an optional add-on pack for 128-bit encryption, which provides security so tight that exporting it elsewhere is prohibited today by U.S. law.

PPTP Filtering

PPTP filtering is an important security feature. An administrator can decide to only allow PPTP-enabled users to connect to the corporate network from the Internet. Filtering out non-PPTP packets avoids the risk of somebody attacking the corporate network through the PPTP gateway server.

Front End Processors

PPTP is designed to allow front-end processors (FEPs) to be connected with Windows NT servers, so clients that call into the FEP have transparent access to the server's network. This means the client won't notice whether it's going straight to the server, or to an FEP which is tunneling through the server. Because Microsoft VPN provides transparent access to a PPP client, it can work with UNIX, Win 16, MS-DOS®, Macintosh, and other clients.

FEPs can be operated by telephone companies because FEPs don't allow access to the data exchange between the client and server. The FEP is just a pass-through that lacks the intelligence to evaluate the information passing through it. From a security standpoint, this means a company will not lose control of who gets access to its network. Data privacy is maintained. This is very important for companies that outsource dial-up access because they need their data to be secure.

Another important point is to keep control of who has access to the server on the server itself, rather than on the FEP. The server authenticates the clients calling in. The FEP only looks at the callers identity and establishes the tunnel to the server. Because it has a passive role, security is tight.

Looking Toward the Future

Microsoft is a leader in developing and implementing encryption and other security technologies. Because security is so crucial to maintaining the integrity of the world's computer networks, research and development at Microsoft and elsewhere is a continuing project. For example, the Internet Protocol Security Protocol Working Group (IPSEC) is developing enhancements for existing IP security, and RSA Data Security is leading a consortium effort to implement the S/WAN initiative, to ensure interoperability among firewall and TCP/IP products. As new security technologies are developed, they will be evaluated for integration with Microsoft VPN.

Taking Advantage of Microsoft VPN

Microsoft VPN provides a new range of opportunities for CIOs, MIS directors, net administrators and third-party developers. VPN will also be vital to Internet service providers, or other public network operators such as telephone companies that are trying to get into the Internet service business.

Outsourced Networks

Many corporations would like to eliminate the cost and overhead of purchasing and managing their own modem pools, and out-source dial-up access to their corporate backbones. This needs to be done in a manner that is cost-effective, hassle-free, protocol-independent, secure, and that requires no changes to existing network addressing. Microsoft VPN provides the solution for telephone companies and ISPs to use in meeting such corporate needs.

PPTP will allow dedicated hardware devices (such as those manufactured by US Robotics and Ascend) deployed by Telcos in Points-of-Presence to act as "front-ends" to Windows NT RAS servers deployed at corporate premises by tunneling PPP packets through Wide Area Networks. An end user would make a local V.34 or ISDN dial-up call into a hardware device (such as a FEP) that is situated in the same city as the user. The FEP would then connect to a Win-

dows NT Server located in a different city via a WAN such as frame relay or X.25. The FEP does this by taking PPP packets from the end-user and tunneling them through the WAN.

Telephone companies can take advantage of many of the Windows NT strengths to provide a dial-up access solution that is scalable, secure and easy to administer from the standpoint of both network addressing and security.

VPN and the robust Windows NT platform will allow service providers to manage server farms for customers, either on a customer's premises or through a POP. This is a significant benefit to companies that don't want to invest in the financial and management overhead required to operate their own data networks. Another major value of VPN and RAS is that because they sit on a Windows NT platform, they provide full integration with Microsoft BackOffice. This enables a service provider to offer a range of value-added services beyond remote access—including server support and application support.

Allowing Dense Communications

Using VPN, dense and integrated communications solutions from companies like US Robotics can be used as front-end processors across a LAN to Windows NT Servers. This would enable easy to handle dense RAS server configurations that are well integrated with the Windows NT - NOS environment.

Internet Communications

As Windows NT Internet support is enhanced by adding routing protocols and demand-dial support, the PPTP protocols of a VPN will enable corporations to connect IP and IPX LANs across the Internet—again in a secure manner. And if the need is only intra-corporate connectivity, these connections can be made without requiring universal addressing of the respective corporate LANs.

In addition to VPN support, PPP tunneling also enables use of dense modem/ISDN front-ends to Windows NT RAS servers, thus enabling access server vendors to easily integrate their solutions from a management perspective (user accounts, logging, etc.) into a Windows NT network.

By exploiting the infrastructure that the Internet Domain Name Service (DNS) offers, combined with Windows NT 4.0 feature enhancements (such as autodial support in RAS), it will be possible for Microsoft to significantly enhance business-to-business communications across the Internet in the 1996 time frame.

Looking Beyond the Internet

While the most important focus for VPN is to provide a secure way to extend private network access through the Internet, it can also work in virtually any type of network over which IP packets can be sent, including X.25 and Frame relay networks.

VPN allows the Internet to be treated as if it were a telephone network being used to reach the network that the user wants to be on. Companies taking advantage of VPN will be in a position to offer users what the telephone companies might call IP dial tone, meaning very high-speed PC access from the home. By default the transport mechanism will be IP. So users can make

use of the giant telecommunication networks, tunneling through to get to wherever they want to go. That same tunnel might also go through the Internet, but the pathway would be transparent to the user.

Telephone and Cable Applications

Microsoft is working with telephone and cable companies to create high-speed, dedicated links between home computers and company networks, taking advantage of the existing telephone or cable wiring to the home. Because PPTP isn't bandwidth-constrained, it works with the underlying communications services, whether it be analog POTS, ISDN, or even ADSL and cable modems. That is because PPTP makes use of PPP transport.

Phone companies can use a device called an Asynchronous Digital Subscriber Line (ADSL) modem, which would be installed both at the central office and the customer's home. It would not interfere with regular phone service, but would multiplex data traffic onto the same line. Using an IP connection, caching Internet servers could be installed at the central office, to provide a connection to the Internet, CD-ROM servers, or other system resources. Users could then connect to either the Internet or a private network. PPTP would allow users to tunnel through the service provider's bank of servers and through the different address types. A router at the central office could be connected to the Internet, so that users could reach distant corporate networks. Or the corporate network could be directly attached, permitting direct access.

Providing Compatibility with Cisco L2F

As noted earlier, the PPP Extensions working group agreed to the PPTP Forum proposal at the June 1996 IETF meeting in Montreal. This includes converging PPTP and Cisco's Layer 2 Forwarding approach to tunneling. Microsoft and the other PPTP Forum companies are working to provide mutual compatibility between PPTP and Cisco's Layer 2 Forwarding (L2F) tunneling protocol. This is good news for users because regardless of which tunneling protocol they initially use, the other will be supported.

Windows NT 4.0 RAS Enhancements

The Windows NT platform provides powerful administration tools for LAN managers, ISPs, and other network professionals. For Windows NT 4.0, Microsoft has made several specific enhancements to RAS, including the addition of PPTP support.

WINDOWS NT 4.0 RAS ENHANCEMENTS

In addition to PPTP, other enhancements have been made to RAS that are included in Windows NT 4.0. The following is a brief summary:

- **PPP multilink** Provides the ability to aggregate two or more physical connections to form one larger logical connection, improving bandwidth and throughput for remote connections. Software tools have also been added to facilitate ease of use.
- **Auto dial** Makes it easier and faster for remote users to connect to their corporate networks.
- **Logon dial** If activated, automatically connects the remote user to the corporate Intranet when the computer is turned on.
- **Restartable File Copy (RFC)** Addresses the problem of having to dial in and start over if an interruption occurs while downloading a huge file off a server to a remote computer. RFC allows the transfer to continue where it left off, once the connection has been re-established.
- **RAS API enhancements** Gives third-party companies more options to create their own custom solutions, applications, and utilities based on RAS.

Availability

Microsoft VPN, with its PPTP foundation, shipped with Windows NT Server 4.0 and Windows NT Workstation 4.0. A downloadable PPTP upgrade for Windows 95 is planned for year-end 1996 availability. PPTP support is also made available by a growing number of remote access solution vendors, like those in the PPTP Forum, firewall vendors, and others.

Summary

Microsoft Virtual Private Network (VPN) technology is based upon the industry-standard point-to-point tunneling protocol (PPTP). It allows users to achieve secure connectivity between remote clients and private networks via the Internet or other public carriers. VPN provides businesses with an economical and easy-to-implement strategy for securely using the Internet as an extension of their private network. The security, reliability, ease of use, and speed of PPTP-enabled Windows NT Servers, combined with the DNS infrastructure, provides significantly enhanced business-to-business communications across the Internet.

The movement to the open PPTP protocol standard signals an opportunity for remote access system vendors, Internet Service Providers, and firewall vendors to provide great value-added benefits for their customers. PPTP-enabled systems can be deployed now with the confidence that Microsoft will ensure compatibility with the PPTP standard as it evolves through the IETF and into the future.

For more information

Please refer to Microsoft's network communications and telephony web site for the latest in technology and solution information pertaining to these important topics, including PPTP progress. From the PPTP area, you can find the latest specification, FAQ material, and other information. Here is the address:

http://www.microsoft.com/communications.