August 1999
ECG515/0899

Prepared by:
Internet and E-Commerce
Solution Business Unit

Enterprise Solutions Division

Compaq Computer Corporation

Contents

Point to Point Tunneling Protocol (PPTP) Virtual Private Network (VPN)

Abstract: With the increasing need for remote access and telecommuting, the cost of telephone lines and maintenance is growing. Also, the expansion of businesses into geographically diverse areas and the accelerating need for secure communication are driving the need to use the Internet in a secure manner to accomplish business goals in a cost-effective way.

A Virtual Private Network (VPN) is a secure connection over a public network, usually the Internet, or a connection created by using encrypted dedicated lines between facilities. Because VPNs can reduce the cost of connecting dispersed locations significantly without compromising security, they are fast becoming an important feature of the corporate information infrastructure. This guide describes one VPN solution – Microsoft's PPTP VPN.

Notice

Point to Point Tunneling Protocol (PPTP) Virtual Private Network (VPN)
Technical Guide prepared by Internet and E-Commerce Solutions Business Unit

First Edition (August 1999)
Document Number ECG515/0899

Introduction

Virtual Private Networks (VPNs) are fast becoming an important feature of the information infrastructure for corporations. With the increasing need for remote access and telecommuting, the cost of telephone lines and maintenance is growing substantially. Also, the expansion of businesses into geographically diverse areas and the accelerating need to communicate securely with partners, customers, and vendors are driving the need to use the Internet in a secure manner to accomplish business goals in a cost-effective way.

VPNs are critical for enabling eBusiness/E-Commerce. It is becoming essential to have a VPN in place to efficiently and securely exchange information between a company and its suppliers, partners, and customers in a timely fashion, and to accomplish a company's electronic business.

Both dial-up and dedicated communication lines are expensive, particularly outside the United States. In many cases, VPNs and an Internet connection can reduce this cost significantly. Maintenance and support of modem pools can also be expensive compared to using the Internet, where the local ISP bears the cost of modems and their support. However, the Internet itself is not considered secure, so one of the key features of VPNs is the ability to protect sensitive information from intruders. This is done by a combination of built-in security services such as encryption and authentication.

VPN technology is still in an early adopter phase, so many of the popular solutions do not inter-operate completely, but that is expected to change by the end of 1999. The safest and easiest way to implement a solution for installing a new VPN is to use software and hardware from the same vendor. This may be relatively easy in one company, but it is difficult when you want to interface with several companies in an Extranet. Therefore, most of the VPN implementations today have been employed for remote access users and telecommuters.

There are many companies in the marketplace offering VPN solutions. These include ISPs offering "Global Internet Roaming" services, server manufacturers, software companies, and dedicated hardware companies, to name a few.

There are several types of VPNs that can be implemented depending on your requirements and the available architectures. There are also many types of protocols and security policies to choose from. Because of this complexity, it is recommended that appropriately experienced personnel or consultants be assigned to design and implement a VPN solution.

There are two basic definitions of a VPN. The original definition, made by phone network providers, stated that a VPN is the establishment of a "private" network to be used only by one company. These are sometimes called Private (or Permanent) Virtual Circuits (PVC). This "private" network was typically a dedicated leased line from a telephone company. The company that was leasing them would be the only one using these leased lines. A corporation using these lines accepts the risk (generally considered small) that unauthorized personnel would tap the line to "listen" in at any point, including the physical lines to company facilities, or at any of the switching locations. Encryption and authentication are not typically implemented in this scenario, although they could be.

The second definition, which is more common today, is that a VPN is a secure connection over a public network, usually the Internet. Depending on the need, a VPN may also be created by using encrypted dedicated lines between facilities. Security services for these connections establish:

- privacy/confidentiality
- authentication
- integrity
- access control and
- replay protection

for the information flowing over them. You have a choice of which of the above five services to implement for a VPN, depending on your requirement.

The rest of this paper will focus on the second definition of a VPN, as implemented through a secure connection over the public Internet using the Internet Protocol (IP). VPNs are called tunnels by some vendors. However, a tunnel is just an encapsulation of one protocol into another (for example IPX into IP), not necessarily involving any security services. A VPN creates encrypted and/or authenticated tunnels when in operation.

Types of VPNs

There are basically three types of VPNs. These are:

- Remote Access/Telecommuter VPNs: These VPNs are used for remote access by traveling employees or employees working from home (telecommuters).
- Secure Intranet VPNs: These VPNs connect different geographic locations of a corporation through a VPN on the Internet.
- Secure Extranet VPNs: These VPNs connect a corporation's sites with its business partners, vendors, and customers through the Internet. This is a primary enabler for business to business E-Commerce.

Note: This paper will briefly describe the most popular high-level VPN protocols and concentrate on the implementation of VPNs using the Point to Point Tunneling Protocol (PPTP) implemented by Microsoft.

Overview of VPN Protocols

Several protocols can be used for VPNs. The protocols discussed in this section are the most often used high -level protocols used in VPNs. The non -PPTP and lower level algorithms used for encryption, hashing and signatures are discussed in more detail in a VPN Primer paper available on http://www.compaq.com/activeanswers . This section will give a high level overview of the four most commonly used VPN protocols: IPSec, L2F, L2TP, and PPTP. Subsequent sections will describe PPTP in more detail.

Internet Protocol Security (IPSec)

Internet Protocol Security (IPSec) is one of the most popular protocols for VPN implementations. The Internet Engineering Task Force (IETF) has been working on a standard for IPSec and has developed a robust protocol that is being implemented by many vendors. It is considered essential to implement this protocol to ensure interoperability amongst VPNs from different vendors, particularly for secure Extranets.

IPSec will become part of Internet Protocol Version 6 (IPv6) in the future and is available today as an add-on to Internet Protocol Version 4 (IPv4). It is used only on IP networks, as other protocols can be encapsulated and tunneled.

An IPSec packet is similar to any other type of IP packet. It has been given a specific IP packet type number, and is placed immediately after the IP header. To protect data transmitted over a VPN, IPSec defines two main transformation types: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH and ESP can be used together. ESP is the most popular implementation today, since it provides privacy for information that AH does not.

When an IPSec VPN session is started, both ends negotiate all parameters through the Internet Key Exchange (IKE) protocol. Upon agreement, a Security Association (SA) is created that specifies the parameters for each VPN tunnel. There may be several tunnels active at any point in time on a server, each one with a different SA. A random parameter called a Security Parameter Index (SPI) is set up to uniquely identify the particular VPN tunnel. An SA specifies the following:

- the authentication algorithm
- the encryption algorithm for ESP
- the encryption and authentication keys
- the lifetime of the encryption keys
- the lifetime of the SA
- the replay prevention sequence number

The AH provides authentication, integrity and replay protection for all packets. However, it does not provide for privacy/confidentiality protection.

The AH provides its features by using a keyed hash (or MAC) for each packet created, which can then be validated at the receiving end.

The ESP provides data confidentiality, authentication, integrity, replay protection and limited traffic flow confidentiality. This is accomplished by encrypting and hashing data as specified by the SA.

Several draft standards associated with IPSec implementations are available at http://www.ietf.org.

L2F – Layer Two Forwarding

The L2F protocol is from CISCO. It is specified in RFC 2341. It is not specifically a VPN protocol, because it does not provide any encryption services. However, it is a tunneling protocol and is used as a base for the L2TP protocol described below.

L2TP – Layer Two Tunneling Protocol

The L2TP protocol (currently an Internet Draft) is a combination of L2F and Microsoft's PPTP. It can support multiple, simultaneous tunnels for a single client. It is anticipated that this protocol, while not implemented on a wide basis today, will replace PPTP and L2F, and will be supported by Microsoft in Windows 2000, as well as by CISCO, 3COM, and several other remote access vendors. The advantages and disadvantages of this protocol are essentially the same as PPTP. It is planned that the encryption features of IPSec will be used in L2TP implementations.

PPTP

The PPTP protocol has been implemented by Microsoft and is embedded in Windows NT 4.0 Routing and Remote Access Service, and is available for use with Windows 95 and Windows 98. It resides in the datalink layer in the protocol stack (in reference to the OSI Reference Model), and encapsulates encrypted IP packets within Point to Point Protocol (PPP) packets. These, in turn, are encapsulated by an ISP server in IP packets for routing to a destination.

The latter process of encapsulating other protocols in IP packets for transmission is called tunneling. Microsoft's implementation of the PPTP protocol uses clear text passwords, hashed passwords, or Challenge Handshake Authentication Protocol (CHAP) for authentication (using Microsoft's domain controls) and Microsoft Point-to-Point Encryption (MPPE--Microsoft's implementation of the RC4 encryption algorithm) with 40 or 128-bit key lengths for data encryption. Other algorithms are not supported presently.

This protocol is typically used for Remote Access VPNs, since it is available on a wide number of machines and is free once you have a Microsoft Windows operating system. It can be used for secure Intranets, but this is not usually done. A typical usage of this protocol for remote access is to dial into a local ISP and establish a PPP session. Then a second dial-up session is initiated with a target specified by an IP address. This IP address is the address of a PPTP server within your company. Once this connection is established, all information flowing through this connection will be encrypted.

The rest of this paper concentrates on a more detailed explanation of PPTP, implementation examples and some PPTP advantages and limitations.

A Typical PPTP Scenario

The PPTP protocol is included with Microsoft Windows NT® Server version 4.0 and Microsoft Windows NT Workstation version 4.0 operating systems, and is also available for Microsoft Windows 95 and 98. Computers running these operating systems can use the PPTP protocol to securely connect to a private network as a remote access client by using a public data network such as the Internet. In addition, PPTP can also be used by computers connected to a Local Area Network (LAN) to create a virtual private network across the LAN.

Generally, there are three computers involved in every PPTP deployment:

- a PPTP client
- a network access server
- a PPTP server

To connect to a PPTP server on a LAN, you do not need the network access server to create a PPTP tunnel, if the PPTP client is connected to the same LAN.

The following section describes a typical PPTP scenario using these computers and explains how they relate to each other and then fully defines each of these components.

A typical deployment of PPTP starts with a remote or mobile PPTP client that needs access to a private enterprise LAN by using a local Internet Service Provider (ISP). Clients using computers running Microsoft Windows NT Server or Microsoft Workstation version 4.0 or Microsoft Windows 95 or 98 use dial-up Networking and the remote access protocol PPP to connect to an ISP.

The client connects to a network access server (NAS) at the ISP facility dial-in or point-of-presence (POP) servers. Once connected, the client can send and receive packets over the Internet. The network access server uses the Transport Control Protocol/Internet Protocol (TCP/IP) protocol for all traffic to the Internet.

After the client has made the initial PPP connection to the ISP, a second Dial-Up Networking "call" (the "call" specifies the IP address of the PPTP Server) is made over the existing PPP connection. Data sent using this second connection is in the form of IP datagrams that contain PPP packets, referred to as encapsulated PPP packets.

The second call creates the virtual private networking (VPN) tunnel connection to a PPTP server that resides on the private enterprise LAN. Generally, users will have two phonebook icons on their desktops to accomplish these two connections.

The PPTP Protocol - Details

Protocol Definition

The Point to Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks, normally using an ISP. PPTP supports on-demand, multi-protocol, virtual private networking over public networks such as the Internet.

PPTP is an extension of the remote access Point-to-Point protocol defined by the Internet Engineering Task Force (IETF) RFC 1171, entitled *The Point-to-Point Protocol for the Transmission of Multi-Protocol Datagrams over Point-to-Point Links.*

PPTP is a network protocol that encapsulates PPP packets into IP datagrams for transmission over the Internet or other public TCP/IP-based networks. PPTP can also be used in private LAN-to-LAN networking. The PPTP extension of PPP is explained in detail in the IETF draft: *draft-ietf-pppext-pptp-10.txt*.

PPTP Architecture Overview

The secure communication created using the PPTP protocol typically involves three processes, each of which requires successful completion of the previous process. This section explains these three processes and how they work.

PPP Connection and Communication

A PPTP client uses PPP to connect to an ISP by using a standard telephone line or Integrated Services Digital Network (ISDN) line. This connection uses the PPP protocol to establish the connection and encrypt data packets. PPTP itself does not encrypt information--it relies on the PPP defined encryption process.

PPTP Control Connection

Using the connection to the Internet established by the PPP protocol, the PPTP protocol creates a control connection, using TCP Port 1723, from the PPTP client to a PPTP server normally inside a company's boundary and connected to the Internet (please see the architecture discussion later). This connection uses TCP to establish the connection and is a called a PPTP tunnel.

PPTP Data Tunneling

Finally, the PPTP protocol creates IP datagrams containing encrypted PPP packets that are then sent through the PPTP tunnel to the PPTP server. The PPTP server disassembles the IP datagrams, decrypts the PPP packets, and then routes the decrypted packets to the private network.

The PPTP protocol specifies a series of control messages sent between the PPTP-enabled client and the PPTP server. The control messages establish, maintain and end the PPTP tunnel. There are 8 basic messages used to start, maintain, reply, configure, report errors and end a session. These are defined in the PPTP document mentioned above.

PPP Protocol

PPP is a remote access protocol used by PPTP to send multi-protocol data across TCP/IP-based networks. PPP encapsulates IP, IPX (Internetwork Packet Exchange), and NetBEUI (NetBIOS Extended User Interface) and other types of packets into PPP frames. PPP then sends the encapsulated packets by creating a point-to-point link between the sending and receiving computers.

The PPP protocol is used to create the dial-up connection between the client and network access server and performs the following three basic functions:

Physical Connection

Establishes and ends the physical connection. The PPP protocol uses a sequence defined in RFC 1661 to establish and maintain connections between remote computers.

Authentication

Authenticates users. PPTP clients are authenticated using the PPP protocol. Clear text passwords using the Password Authentication Protocol (PAP), Challenge Handshake authentication, or a Microsoft modified Challenge Handshake Protocol (CHAP) authentication can be used by the PPP protocol, as implemented in Microsoft's PPTP. PPP Authentication Protocols are described in RFC 1334. RFC 1994 describes the CHAP requirements. RFC 2284, *PPP Extensible Authentication Protocol (EAP)* defines an enhancement to the basic authentication protocols used by PPP. It allows a variety of authentication mechanisms to be negotiated as part of the PPP Link setup. This is currently not implemented in Microsoft's PPTP, but could be used in the future releases to support Smart Cards and other robust authentication methods.

- Password Authentication Protocol

  Password Authentication Protocol provides a simple method for the peer to establish its identity using a 2-way handshake. This is done only upon initial link establishment. After the Link Establishment phase is complete, the peer repeatedly sends an ID/Password pair to the authenticator until authentication is acknowledged or the connection is terminated. PAP is not a strong authentication method. Passwords are sent over the circuit "in the clear", and there is no protection from playback.

- Challenge-Handshake Authentication Protocol

  The Challenge-Handshake Authentication Protocol (CHAP) is used to periodically verify the identity of the peer using a 3-way handshake. This is done upon initial link establishment, and may be repeated anytime after the link has been established.

  After the Link Establishment phase is complete, the authenticator sends a "challenge" message to the peer. The peer responds with a value calculated using a "one-way hash" (for example MD4) function. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise the connection should be terminated.

  CHAP provides protection against playback attack through the use of an incrementally changing identifier and a variable challenge value. The use of repeated challenges is intended to limit the time of exposure to any single attack. The authenticator is in control of the frequency and timing of the challenges.

This authentication method depends upon a "secret" known only to the authenticator and that peer. The secret is not sent over the link. This method is most likely used where the same secret is easily accessed from both ends of the link. Microsoft provides for a modified CHAP that utilizes the user's account password as the base for its authentication.

Creates Datagrams

Creates PPP datagrams that contain encrypted IPX, NetBEUI, or TCP/IP packets. PPP creates datagrams that contain one or more encrypted TCP/IP, IPX, or NetBEUI data packets. Because the network packets are encrypted, all traffic between a PPP client and a network access server is secure.

PPP Protocol Components

The PPP protocol itself has three main components:

1. A method for encapsulating datagrams over serial links.
2. A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
3. A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

PPP Encapsulation

The PPP encapsulation is used to identify multiple types of protocol datagrams. This encapsulation requires framing to indicate the beginning and end of the encapsulation. Methods of providing framing are specified in IETF PPP documents.

A summary of the PPP encapsulation is shown below. The fields are transmitted from left to right.

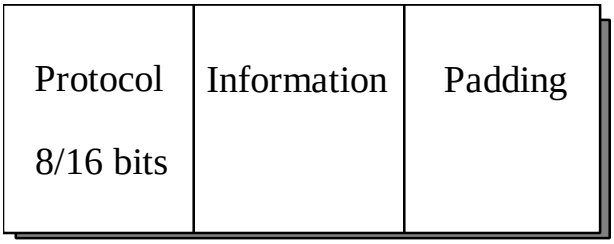


Figure 1. PPP Encapsulation

Protocol Field

The Protocol field is one or two octets, and its value identifies the datagram encapsulated in the Information field of the packet. The field is transmitted and received with the most significant octet first.

In order to establish communications over a point-to-point link, each end of the PPP link must first send Link Configuration Protocol (LCP) packets to configure the data link during Link Establishment phase. There are three classes of LCP packets:

1. Link Configuration packets used to establish and configure a link (Configure-Request, Configure-Ack, Configure-Nak and Configure-Reject). The authentication method is designated within these types of packets.
2. Link Termination packets used to terminate a link (Terminate-Request and Terminate-Ack).
3. Link Maintenance packets used to manage and debug a link (Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply, and Discard-Request).

After the link has been established, PPP provides for an optional authentication phase before proceeding to the network-layer protocol phase.

By default, authentication is not mandatory. If authentication of the link is desired, an implementation must specify the Authentication-Protocol Configuration Option during the Link Establishment phase. These authentication protocols are intended for use primarily by hosts and routers that connect to a PPP network server through switched circuits or dial-up lines, but might be applied to dedicated links as well. The server can use the identification of the connecting host or router in the selection of options for network layer negotiations. Microsoft uses MS-CHAPv1 or MS-CHAPv2 for its authentication protocol.

NCP packets are then used to choose and configure one or more network-layer protocols. For Internet usage, the Internet Protocol Control Protocol (IPCP) is used to establish that IP is being used within the PPP link. Once each of the chosen network-layer protocols has been configured, datagrams from each network-layer protocol can be sent over the link.

One of the NCPs is the PPP Compression Control Protocol (RFC 1962). It describes the compression protocol for compression of data packets before being sent.

Microsoft's implementation of PPTP makes use of the Compression Control Protocol (CCP) packet to define the "Microsoft Point to Point Compression Control Protocol (CCP)," RFC 2118, and the "Microsoft Point to Point Encryption (MPPE) Protocol" in IETF draft document *draft-ietf-pppext-mppe-03.txt*. MPPE is Microsoft's encryption protocol that uses RC4 for the actual encryption.

The MPPE-defined CCP packets are used at tunnel start up time to negotiate the key strength that will be used during the PPTP sessions. There are two options today--40 and 128-bit strength.

The link will remain configured for communications until explicit LCP or NCP packets close the link down, or until some external event occurs, such as the expiration of an inactivity timer or the intervention of a network administrator.

PPTP Data Transmission

After the PPTP tunnel is established, user data is transmitted between the client and the PPTP server. Data is transmitted in IP datagrams containing PPP packets. The IP datagrams are created using a modified version of the Internet Generic Routing Encapsulation (GRE) protocol. (GRE is defined in RFCs 1701 and 1702.) Figure 2 represents the datagram created by PPTP, with each level representing an encapsulation within the previous layer:

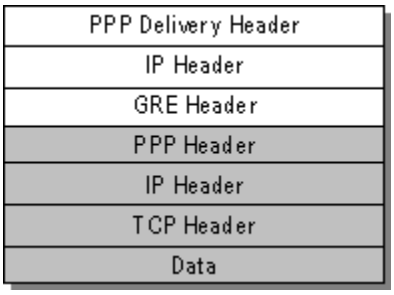


Figure 2. The PPTP datagram

Note: The grayed in area on the above hierarchy indicates the encrypted information. The encrypted IP packet could also be an IPX, NetBEUI, or some other form of packet.

The IP delivery header provides the information necessary for the datagram to traverse the Internet. The GRE header is used to encapsulate the PPP packet within the IP datagram. The PPP packet was created by the remote access service on the client or server. Note that the PPP packet is just one unintelligible block because it is encrypted. Even if the IP datagram were intercepted, it would be difficult to decrypt the data.

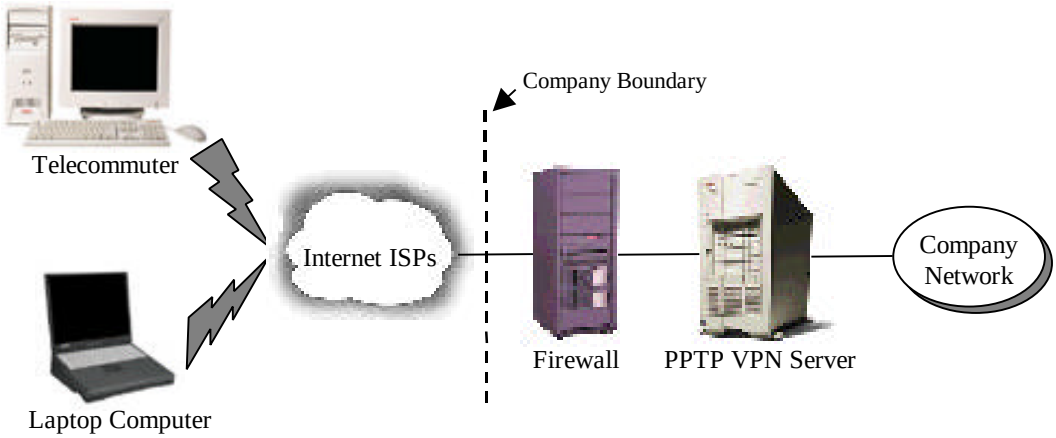
Packet Processing Description

Listed below are the basics steps client data will go through once a VPN is created between itself and the server, through an ISP (IP is used as an example).

1. An IP packet is generated on the client, containing the client's packet data to be communicated. It may contain Transport Control Protocol/Hypertext Transport Protocol (TCP/HTTP) or Transport Control Protocol/ File Transport Protocol (TCP/FTP) or other types of TCP packets. This packet indicates the final destination address for the packet.
2. A PPP header is added to the packet.
3. The PPP header, along with the IP packet, is encrypted with an algorithm previously negotiated.
4. A GRE header is added to the encrypted packet to encapsulate it.
5. An IP header is added that specifies the PPTP server's address inside a company as its destination.
6. The entire accumulated packet is enclosed in a PPP header and the PPP packet is sent to the ISP.
7. The ISP PPP server strips off the PPP header and routes the remaining IP packet to its destination through the normal Internet routing mechanisms.
8. The PPTP Server receives the packet, decrypts the encrypted portions, processes the PPP header, and then routes the packet to the final destination as determined by the IP address of the embedded IP packet.

PPTP Architectures

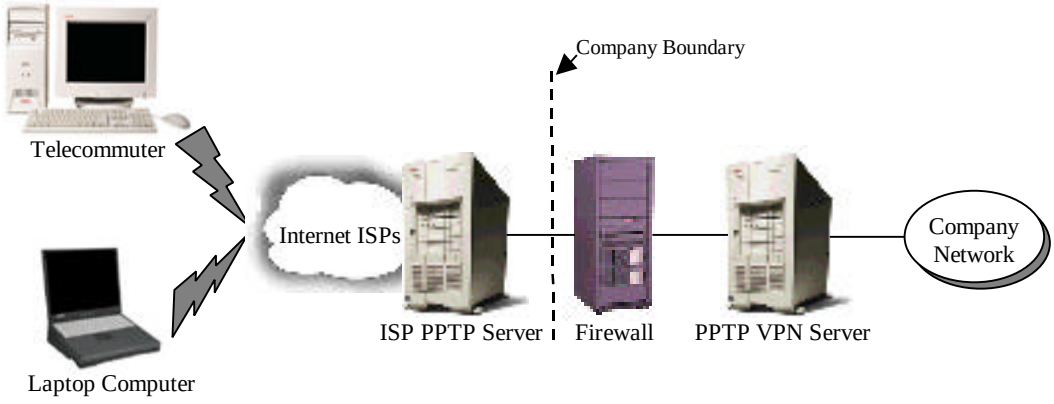
PPTP solutions are used in two basic modes: Remote Access and Site to Site. Remote Access is by far the most popular implementation of PPTP and other types of VPNs today. Figure 3 is a representation of a typical Remote Access architecture.



Data secure from end user to Company PPTP server. Each link is a VPN.

Figure 3. PPTP Remote Access Architecture

For Remote Access, this is the most secure architecture. It requires each client to enable the PPTP client software. (Please see the appendices for configuration instructions.) Based on the support needs of the client PPTP setup, some companies may decide that it is acceptable, from the reduced security standpoint, to have the ISP maintain a PPTP server, instead of having each client use PPTP. See Figure 4 for an example of this architecture.



Data secure from ISP to Company PPTP server. Not secure on dial-up to ISP and at ISP.

Figure 4. Architecture for PPTP Server at ISP

This reduces the level of security available, since the company's information is not protected (encrypted) over the phone line from the user to the ISP. This may not be a significant issue with Plain Old Telephone Service (POTS), but is significant with a cable modem connection. In addition, a company's information is available in clear text to ISP personnel. However, it will be encrypted as it flows over the Internet.

Another possibility with PPTP is a site-to-site or business-to-business scenario to support eBusiness requirements. This architecture is only feasible in a homogeneous network. Since Microsoft's PPTP is not compatible with other VPNs using IPSec or other protocols, both ends of the connection must be using PPTP. This can become an issue if the site-to-site connection is with a partner, supplier or customer who may presently be using or may decide to use different solutions. Figure 5 is an example of the architecture for the site-to-site solution.

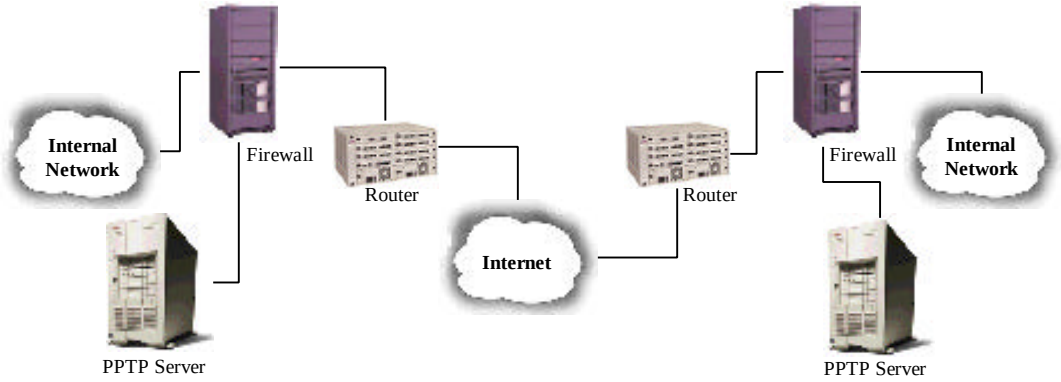


Figure 5. Site to Site PPTP Architecture

Architectural Issues

For both the remote access scenario and the site-to-site scenario, all communications must go through a firewall before reaching the PPTP Server. This requires modification of the firewall rules. PPTP traffic uses TCP port 1723, and the IP Protocol ID is 47 (GRE type). Therefore, these must be specified in the firewall rule set to allow communication. Opening a passage in the firewall should not adversely degrade security, since the packets that the PPTP server expects are all encrypted (except control packets for the PPTP connection itself). However, passing encrypted packets through a firewall to be decrypted and then onto an internal network defeats some of the purpose of a firewall, which can screen the packets for unwanted port numbers, IP addresses, viruses, and more.

Therefore, it is recommended for optimum security that a PPTP server be established in the Demilitarized Zone (DMZ) of a company's architecture. In addition, all packets decrypted must be routed through a firewall for the appropriate screening. This can be accomplished with the original firewall the encrypted packet came through, but is more secure if it is accomplished by a secondary firewall, before entry of the packets into the company LAN.

Performance is another architectural issue to address. Encryption of information is computationally intensive, and can degrade performance up to 75 percent depending on the algorithms used. For this reason, it is recommended that the PPTP server be run as a standalone server.

PPTP Security Features

PPTP extends the authentication and encryption security available to computers running Remote Access Service (RAS) under Microsoft Windows NT Server version 4.0 and Microsoft Windows NT Workstation version 4.0 to PPTP clients on the Internet. PPTP also can protect the PPTP server and private network by ignoring all but PPTP traffic. This section addresses the following security features of PPTP:

- authentication
- access control
- data encryption
- PPTP packet filtering
- firewall usage

Authentication

An ISP network access server may require initial dial-in authentication. If this authentication is required, it is strictly needed to log on to the ISP network access server, and is not related to Microsoft Windows NT-based authentication. Check with your ISP for their authentication requirements. Apply these requirements in the Dial-Up Networking entry for that ISP.

On the other hand, if the Windows NT Server version 4.0 is configured as a PPTP server, it controls all access to your private network. That is, the PPTP server is a gateway to your private network. The PPTP server requires a standard Windows NT-based logon. All PPTP clients must supply a user name and password. Therefore, remote access logon using a computer running under Windows NT Server version 4.0 or Windows NT Workstation version 4.0 is as secure as logging on from a Windows NT-based computer connected to the local LAN.

Authentication of remote PPTP clients is done by using the same PPP authentication methods used for any RAS client dialing directly to a RAS server. Microsoft's implementation of the Remote Access Service (RAS) supports the Challenge Handshake Authentication Protocol (CHAP), the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) versions 1 and 2, and the Password Authentication Protocol (PAP) authentication schemes.

Note: MS-CHAPv1 authentication supports the MD4 hash as well as the earlier authentication scheme used in Microsoft LAN Manager.

As with all user accounts, the user accounts of remote users reside in the Microsoft Windows NT Server version 4.0 directory service and are administered through User Manager for Domains. This provides centralized administration that is integrated with the private network's existing user accounts. Only accounts that have been granted specific access to the network through a trusted domain are permitted. Careful user account management is necessary to reduce security risks.

Having a secure password model in place is critical to successful deployment of PPTP, because Internet connections are more susceptible to sniffers and password guessing programs, which can literally crunch through thousands of password and username combinations in a short amount of time.

The only way to minimize this type of attack is to implement secure password policies. Passwords should be difficult to guess. For example, you can require passwords to contain upper case letters, lower case letters, numbers, and special characters. It is recommended you require at least three different types of characters to ensure password uniqueness, and that they be at least eight characters long. For NT Domains with Service Pack 2 or above, good password creation can be enforced by the operating system.

Access Control

After authentication, all access to a private LAN continues to use the Windows NT-based security model. Access to resources on NTFS drives, or to other network resources requires the proper permissions. It is recommended that the NTFS file system be used for file resources that are accessed by PPTP clients.

For more information about using security on NTFS drives or other network resources, see your product documentation or the Microsoft Windows NT Workstation version 4.0 and Microsoft Windows NT Server version 4.0 Resource Kits.

Data Encryption

For data encryption, PPTP uses the RAS "shared-secret" encryption process. It is referred to as a shared-secret because both ends of the connection share the encryption key. Under the Microsoft implementation of RAS, the shared secret is the user password. (Other encryption methods base the encryption on some key available in public. This second method of encryption is known as public key encryption.)

PPTP uses the PPP encryption and PPP compression schemes. The Compression Control Protocol (CCP) used by PPP is used to negotiate encryption.

The user name and password of the PPTP client is available to the PPTP server and supplied by the PPTP client. An encryption key is derived from the hashed password stored on both the client and server. The RSA RC4 standard is used to create this 40-bit session key based on the client password. This key is used to encrypt all data that is passed over the Internet, keeping the remote connection private and secure.

Note: Users in the United States and Canada can obtain a 128-bit session key through a cryptography pack upgrade for use inside the US and Canada.

PPTP Packet Filtering

Enabling PPTP filtering on the PPTP server can enhance network security from malicious activity. When PPTP filtering is enabled, the PPTP server on the private network accepts and routes only PPTP packets from authenticated users. This prevents **all** other packets from entering the PPTP server and private network. In conjunction with PPP encryption, this ensures that only authorized encrypted data enters or leaves the private LAN.

PPTP filtering is enabled on the PPTP server using the Protocols tab in the Network option of Control Panel.

Using PPTP with Firewalls and Routers

PPTP traffic uses TCP port 1723, and IP protocol uses ID 47, as assigned by the Internet Assigned Numbers Authority (IANA). PPTP can be used with most firewalls and routers by enabling traffic destined for port 1723 to be routed through the firewall or router.

Firewalls ensure corporate network security by strictly regulating data that comes into the private network from the Internet. An organization can deploy a PPTP server running Microsoft Windows NT Server version 4.0 behind its firewall. The PPTP server accepts PPTP packets passed to the private network from the firewall and extracts the PPP packet from the IP datagram, decrypts the packet, and forwards the packet to the computer on the private network.

Encryption Issues

The United States government and other governments place restrictions on the export of encryption based products. Some countries also place restrictions on the import of encryption products. Therefore, when planning a VPN implementation, it is essential to understand the appropriate export and import restrictions if any connections will be made outside the originating country. The export office of a company should be consulted to obtain the latest information on the regulations.

Until recently, the US government allowed mass market export of encryption with 40-bit keys (not very secure), and they required a license for the export of above 40-bit key-length products. This license was not typically hard to get, but could take several weeks to obtain. Recently the US government has relaxed its policy to allow a mass market of 56-bit key encryption products to be exported with a general license. Some industries such as banks, health care, etc. are able to export 128-bit encryption implementations with a minimal review. In addition, a personal license can be issued to an international traveler with encryption products on a laptop with minimal effort.

As mentioned above, obtaining an export license does not mean that a company can import the encryption code into other countries. Several countries impose import restrictions on encryption products. These restrictions vary from a simple registering of the product, to a prohibition against importing encryption code without a specific license, which may take months to obtain. This also applies to encryption code embedded on a laptop. It may not be obvious to employees using their company's laptop when traveling that there is encryption code embedded in an application on the laptop. Therefore, it is important that the company's export/import office keep up to date on the rapidly changing laws and communicate the appropriate information and processes to the company's employees.

Note: For some algorithms the decryption key is slightly different, but it can be easily derived from the encryption key. For most popular and secure symmetric algorithms, the length of the key in bits is considered the most important factor in determining the security of an algorithm. 40-bit algorithms have been easily exportable, while only recently 56-bit algorithms have been exportable through the mass market to most countries. Most cryptographers feel that a 128-bit key and a strong algorithm are needed to adequately secure information over the long term. An algorithm using a 40-bit key can be "cracked" in two days on a home computer by exhaustive search. A 56-bit key algorithm can be "cracked" in three days using specialized hardware built for the task (costing approximately $250,000).

PPTP Advantages

PPTP has some advantages over other current implementations of VPNs. The key ones are listed below:

- PPTP is relatively simple to implement by users and system administrators. A company must have relatively modest VPN needs and all of the systems that require a VPN must be running on current Microsoft operating systems.
- PPTP is less complicated to implement than most other forms of VPNs, and is fairly transparent to end users. PPTP uses packet filtering that makes use of existing routers.
- Microsoft provides PPTP free.
- PPTP supports non-IP protocols such as IPX, NetBEUI and AppleTalk.

PPTP Limitations

PPTP has some limitations that a user should be aware of before deciding on a VPN approach.

- Only Microsoft has implemented PPTP in a significant fashion, so users must employ current Microsoft operating systems at both ends of the tunneled communication. This may be feasible within a company that can control the operating systems that its employees use and have standardized on Microsoft systems. However, this may be much more difficult when trying to establish secure Extranets with partners, suppliers and customers who may have different implementations already in place.
- Currently PPTP and L2TP only support a maximum of 255 concurrent tunnels. This may be enough for small and medium companies, but may be inadequate for larger implementations.
- The current selection of encryption and authentication algorithms available with PPTP is fairly limited. Only RC4 with 40 and 128-bit keys are available as encryption algorithms. While the RC4 algorithm is widely used, DES and 3-DES are government standards, so any VPN that needs to be interoperable with other companies or the government must have an option of using these algorithms. In addition, the 40-bit key length is short and can be broken in 3 days on a home computer, and therefore isn't very secure. The 128-bit implementation is not exportable from the USA through the mass market, and requires an export license specific for the implementation. This export restriction is not unique to PPTP implementations, but applies to all high security encryption algorithms.
- Each PPTP packet does not have a separate authentication calculation similar to IPSec. In addition, it does not support replay protection.
- For MS-CHAPv1, the encryption keys are changed every 256 packets. For MS-CHAPv2, they are changed for every packet. In both cases, the keys are a function of the user's initial password, so it is critical that this password is robust. Due to issues of password entropy, for an equivalent 128-bit key the password must be 22 random characters. A standard 8-character password chosen from an English dictionary is equivalent to about a 10.4-bit key. This can lead to problems where higher level security is required, since a password may be a dictionary word, stolen by an attacker or not changed often enough by the user. This is in contrast to other VPN implementations, which can use a dynamic key exchange process to change keys frequently and easily.

- Integrity features do not protect the initial negotiation of encryption key strength.
- The MS-CHAPv1 protocol is subject to several cryptographic attacks. The MS-CHAPv2 protocol is much more secure and is recommended. MS-CHAPv2 is only available in Microsoft's Dial-up Networking (DUN), version 1.3 or above. The version of CHAP used in a VPN is negotiated when the VPN is set up. It starts negotiation at the highest level, but if one end has not upgraded then the level negotiated is a lower and less secure level. Therefore, if one end is using DUN 1.2 or lower, a less secure VPN will result.

PPTP Server Configuration

Remote Access PPTP Server Configuration

A PPTP Server can be set up to handle remote access clients or in a site-to-site mode. The remote access situation is the most popular and is described in detail below. Remote Access is normally dial-in through phone lines to an ISP, but could also be a client connected directly to the Internet. (For example, some hotels have Ethernet connections directly to the Internet.) PPTP Configuration is relatively easy. The following information shows how to configure PPTP support on a RAS Server.

PPTP is installed on top of a RAS server, so ensure that RAS has been installed on the Windows NT server that will be used for PPTP. Remote Access Service (RAS) has been offered with Microsoft Windows NT Server since the product was introduced. A RAS server is usually connected to a Public Switched Telephone Network (PSTN), ISDN, or X.25 line, allowing remote users to access a various network servers. For detailed information on RAS, see the *Microsoft Windows NT Server 4.0 Networking Supplement:*

- Chapter 5, "Understanding Remote Access Service"
- Chapter 6, "Installing and Configuring Remote Access Service"
- Chapter 7, "RAS Security"

To Install PPTP:

1. Click Start, point to Settings, and click Control Panel.
2. Double-click Network.
3. Click the Protocols tab.
4. Click Point to Point Tunneling Protocol, and then click Add.

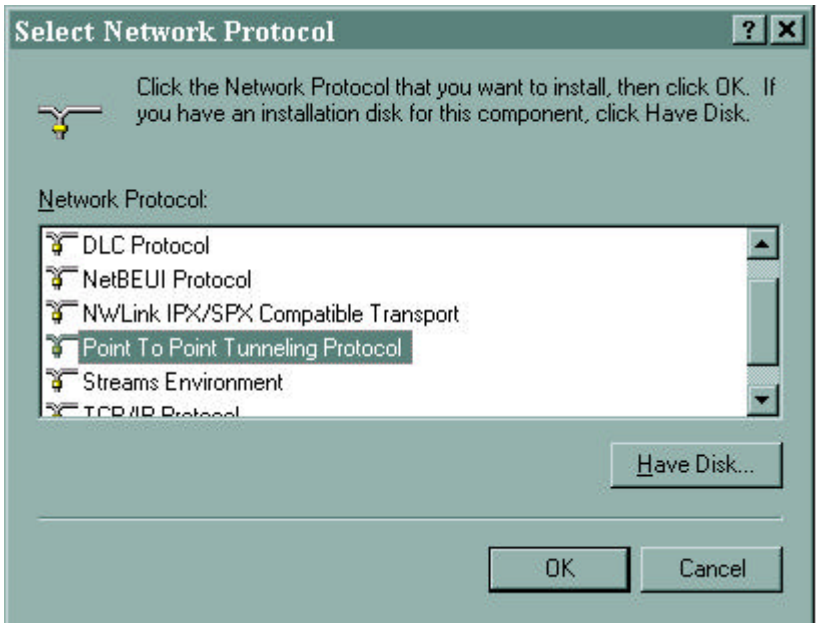


Figure 6. PPTP Protocol Selection

5. Click Have Disk if loading the software from disks or a CD. Or click OK if loading from the network.
6. When prompted, type the full path to the Windows NT Server PPTP files, and then click OK.
7. Enter the number of connections you want available to PPTP (that is, the number of Virtual Private Networks).

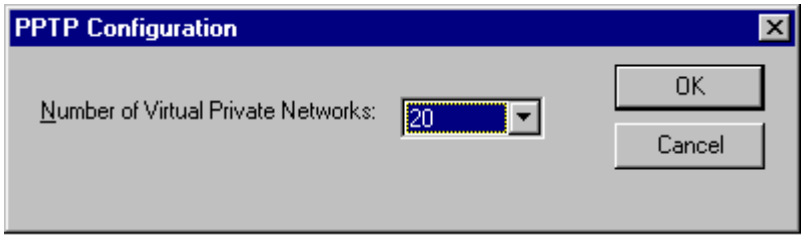


Figure 7. Number of VPNs

8. Next, the RAS Set Up utility is started. This is where the virtual ports that support the VPNs are added.
9. Choose Add to open the RAS Device dialog box.). Figure 8 shows the virtual ports established by Step 7. Select an entry (for example, VPN1-RASPPTPM) and click OK.

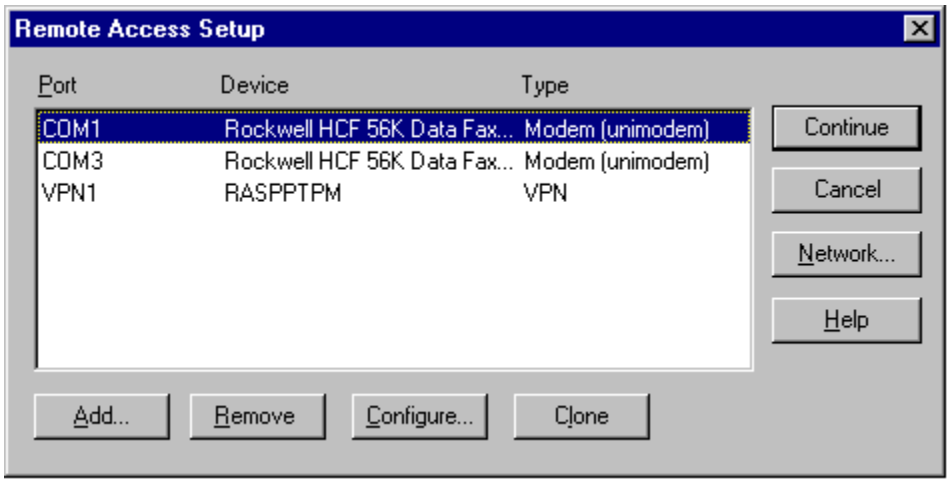


Figure 8. RAS Setup after configuration with one VPN shown

10. In the Remote Access Setup dialog box, select each new entry and choose Configure to open the Configure Port Usage. Select one of the dial-in or dial-out options. At least one port must be configured for dial-in. Repeat this and the previous step for each VPN device to be added. Figure 9 shows the RAS Setup after the VPNs are configured.

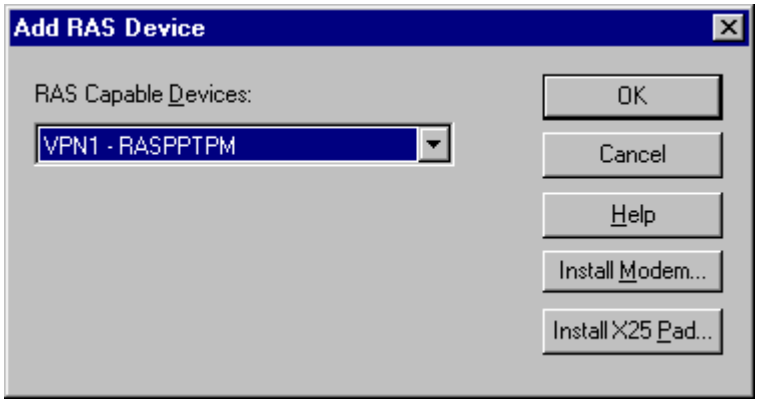


Figure 9. Add RAS Device

11. After all virtual devices have been added, choose Continue.
12. When you are returned to the Protocols tab, choose Close.
13. You must restart your computer to complete the installation.

Ensure the Network configuration (click the Network box), for each VPN has the appropriate check boxes marked for indicating Microsoft Authentication and Data Encryption.

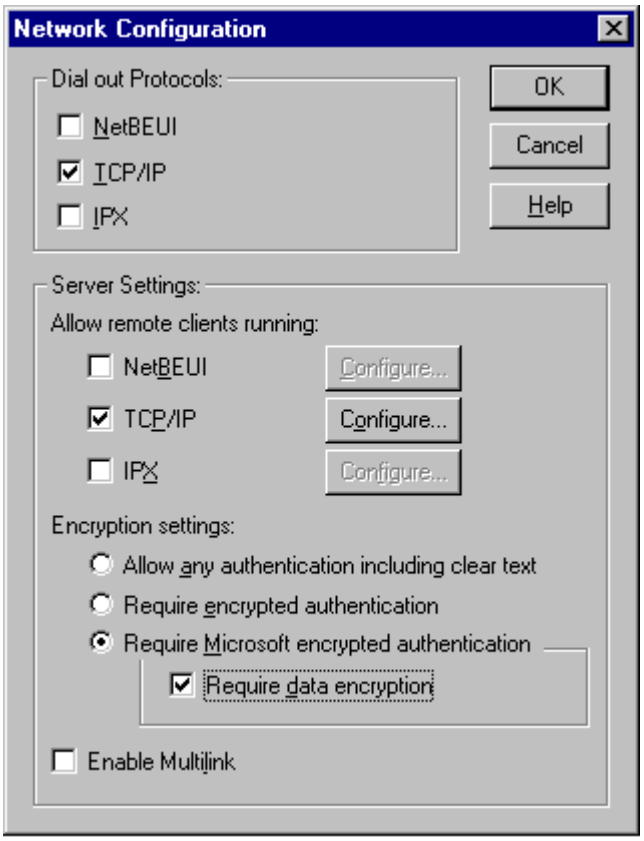


Figure 10. Microsoft Authentication and Data Encryption

After PPTP is installed, the RAS Server will support both PPTP and non-PPTP connections, which is a potential security hole. PPTP filtering can be enabled, disabling support through any ports and for any traffic except PPTP ports and traffic. It is recommended that this option for connections to the Internet be used to enhance the security of the network.

To install PPTP filtering for protection:

1. Click Start, point to Settings, and click Control Panel.
2. Double-click Network.
3. Click the Protocols tab.
4. Click TCP/IP Protocol.
5. Click Properties.
6. Click the IP Address tab, if necessary, and then click Advanced.
7. In Adapter, click the network adapter for which you want to specify PPTP filtering. The PPTP filtering settings in this dialog box are defined only for the selected network adapter.
8. To enable PPTP filtering, click Enable PPTP Filtering.

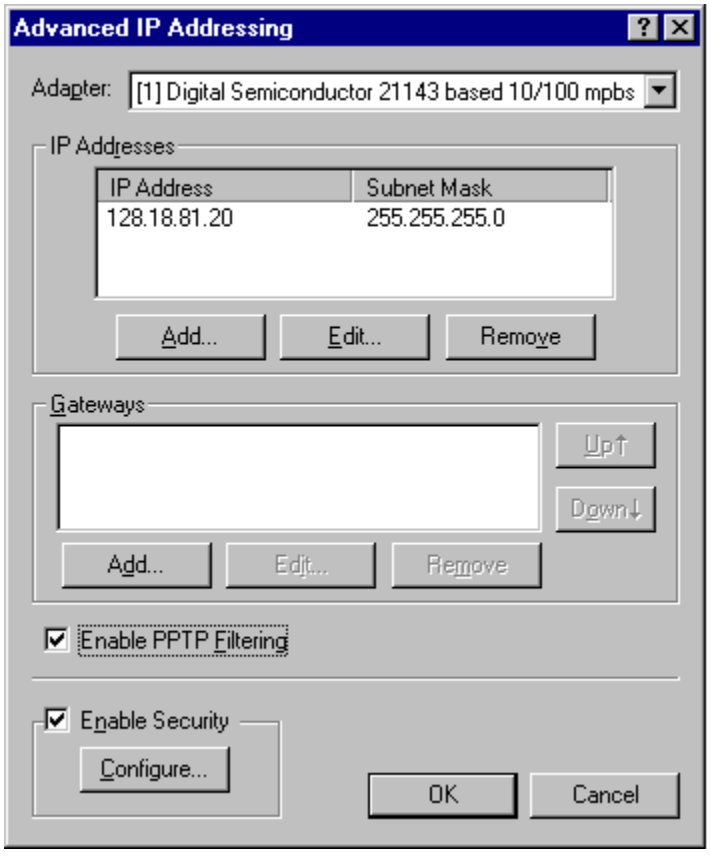


Figure 11. Enable PPTP filtering

Monitoring Server PPTP Support

The PPTP ports in the RAS Server Admin utility can be monitored by choosing the Communication Ports command in the Server menu. Ports appear if they are configured to receive calls. Dial-out ports are not listed.

PPTP Server Site-to-Site Configuration

A PPTP site-to-site implementation can be set up by establishing a PPTP Server at both ends of the connection, setting the appropriate parameters at both ends (as described earlier) and establishing a connection between the two. The initial dial-up connection necessary for remote access is not necessary, and the connection can be set up using an icon (connectoid) on the Dial-up networking screen at both ends. Once connected, the VPN itself could remain active for many days/weeks with no maintenance needed. This would require the communication line to be active at all times.

Remote Access Client Configuration

Appendices 1, 2 and 3 specify the typical processes for setting up a remote access client to use PPTP for Windows 95, Windows 98 and Windows NT.

Summary

VPNs are fast becoming an important factor in a company's information networking strategy. The continued globalization of corporations has increased the need to communicate with branch offices, traveling employees, and telecommuters. Data must be interchanged on a timely basis with vendors, partners, and customers. It is essential that companies put a secure network in place to accomplish this. The Internet is becoming the accepted way to accomplish this while keeping costs under control.

VPN technology is still in the early adopter phase, although it is moving rapidly into the mainstream (particularly with remote access). Interoperability of VPNs from different vendors is still an issue. The best solution is to obtain all pieces of a VPN solution from one vendor. It is anticipated that this issue will be addressed by the end of 1999, leading to more flexibility and the ability to create secure Extranets in a cost-effective manner. The VPN vendors, the IETF in finalizing the IPSec and IKE standards, and companies/trading partners such as the Automotive Network Exchange (ANX) are addressing the issue of interoperability of VPNs.

The methods of implementing VPNs and the protocols involved are still in flux, so a corporation's information technology managers must choose their options to be as flexible as possible. In addition, export and import issues must be considered for those companies that wish to interchange data with others in more than one country.

PPTP as implemented by Microsoft is one method of implementing a VPN, and works best in a homogeneous environment where all computer systems that need to participate in the VPN are Microsoft operating system based. In addition, users must be comfortable with the limited options for security parameters.

Appendix 1 – Windows 95 Client Installation

The following steps are necessary to configure a remote access client to use PPTP for Microsoft Windows 95.

System Requirements:

The client requires the following components:

1. Microsoft Windows 95 with the latest service patch installed
2. Connectivity to the Internet and an ISP account
3. Dial-Up Networking 1.1 installed
4. Dial-Up Networking Upgrade 1.3 software (MSDUN13.exe)
5. Windows Socket 2 (Winsock) Upgrade (W95WS2setup.exe)
6. Microsoft Windows 95 CD/Diskettes or CAB files on hard drive
7. An account with any Internet Service Provider (ISP)
8. 128-bit encryption upgrade--**USA and CANADA only**

Determining Current System Configuration

To determine what version of Dial-Up Networking (DUN) is installed, perform the following tasks:

1. Select the Start button from the Desktop task bar
2. Select Settings
3. Select Control Panel
4. Open (Double Click with the left mouse button) Add/Remove Programs
5. If there is no entry in Add/Remove Programs like the one shown in Figure 12, and you **do not** have a Dial-Up Networking icon in My Computer then you do not have any DUN installed. Go to the section to install DUN 1.1.

   If there is no entry in Add/Remove Programs, like the one shown in Figure 12, and you **do** have a Dial-Up Networking icon in My Computer, then DUN 1.1 is installed. Go to the section to install MSDUN 1.3.

6. If there is an entry in Add/Remove Programs like the one shown in Figure 12, you have DUN 1.2b installed. Go to the section to install MSDUN 1.3.

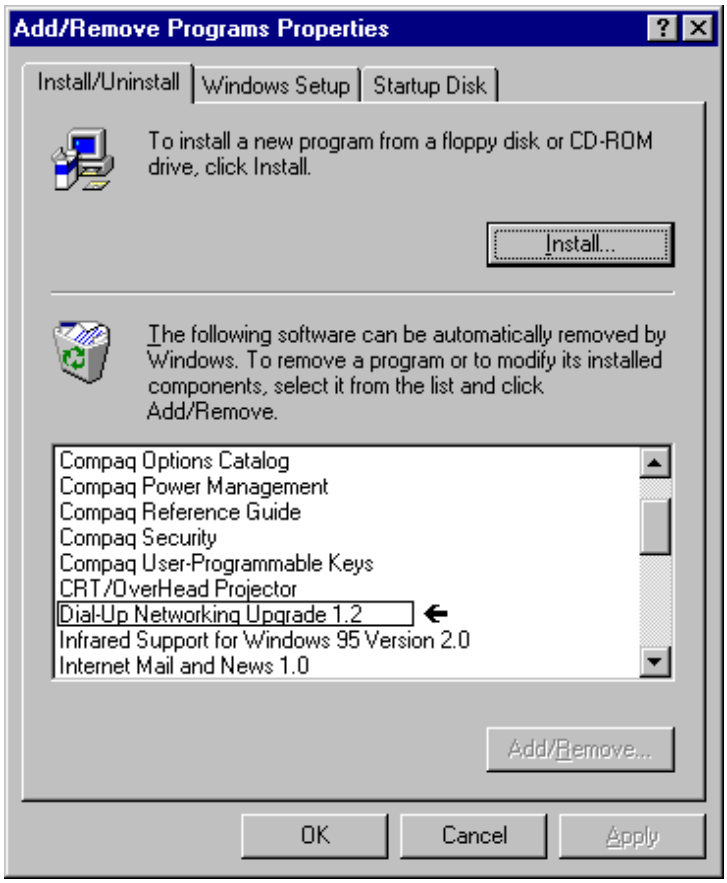


Figure 12. Dial-Up Networking Version

Where to get Components:

1. Microsoft DUN - (MSDUN13.exe)
   - http://www.microsoft.com/windows95/downloads/contents/wurecommended/s_wunetworking/dun13win95/default.asp?site=95

2. Microsoft Winsock v2 - (W95WS2setup.exe)
   - http://www.microsoft.com/windows95/downloads/contents/wuadmintools/s_wunetworkingtools/w95sockets2/default.asp?site=95

3. Win95 Dial-Up Networking 1.3 Utility to enable 128-bit Encryption (8/98) – (MSNT128.exe)
   - http://support.microsoft.com/Support/NTServer/128Downloads.asp

Note: After agreeing to the license agreement, follow the appropriate links to the Windows 95 files.

Installing DUN 1.1

To install DUN 1.1:

1. Go to Start/Control Panel
2. Open Add/Remove Programs
3. Go to the Windows Setup Tab
4. Double click on the Communications entry
5. Click on the Dial-Up Networking entry to place a check in its associated box
6. Select OK
7. Select OK
8. If prompted to keep any files, always select **Yes**
9. Reboot as prompted

IMPORTANT: Always use the Add/Remove Programs object to add or delete.

Installing DUN 1.3

After you have copied DUN 1.3 and the Winsock upgrade files to your hard drive, perform these steps to install the upgrades to your computer:

1. Select Start from the task bar
2. Select RUN from the Pop-Up menu
3. Enter C:*Location of File*\MSDUN13.exe and select OK
4. Select Yes when prompted to install the MS Dial-Up Networking 1.3 for Windows 95
5. Select Yes if you agree with the terms of the End-User License agreement
6. Select Yes when prompted to reboot
7. After rebooting, you may be prompted to insert the Windows 95 C D-ROM. If so:
   - Select OK at the 'Please insert the disk…' enter the location of the CD-ROM or CAB files
8. Select OK if prompted to restart your computer
9. Select Start from the task bar
10. Select RUN from the Pop-Up menu
11. Enter C:*Location of File*\W95ws2setup.exe (*Location of file* is where the files were copied to your hard drive)
12. Select OK
13. Select Yes if prompted to update the Windows 95 Socket API. The files will automatically install.

14. Select Yes if prompted to Restart
15. Select Start from the task bar (128-bit encryption upgrade only)
16. Select RUN from the Pop-Up menu
17. Enter c:\Location of File\msnt128.exe

Configuring DUN 1.3

After Dial-Up Networking 1.3 and the Winsock upgrade are installed and have been setup and enabled, do the following:

Note: The symbol ** denotes a shortcut.

1. Establish a connection with your ISP
2. Run WINIPCFG /ALL from a DOS prompt or from the Start/Run box (WINIPCFG is all one word)
3. Record the complete Host Name and Domain Name (for example, yourname.companyname.com)
   - yourname is the Host name
   - companyname.com is the Domain Name
4. From the IP Configuration dialog box that appears, write down the addresses listed in the DNS Servers box. It is the second box from the top. (Please see Figure 13.)
5. Click on the box just to the right of the DNS Servers (if you have it). It has three Periods (…) in it. This will cycle through the DNS Server addresses. Record all of the addresses, but there are only two you will need (for example, 204.x.x.x.).
   _____ Address #1
   _____ Address #2

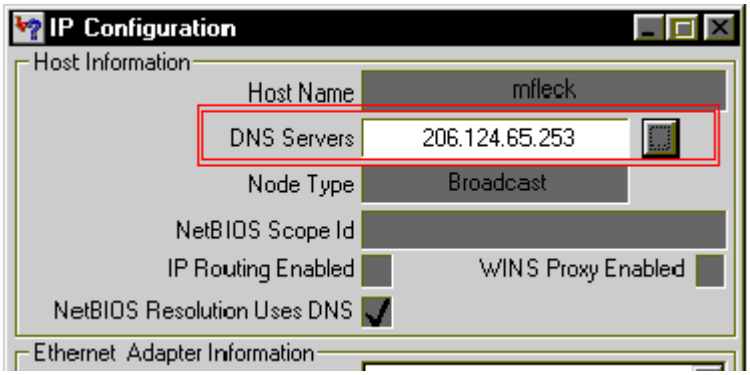


Figure 13. IP Configuration – DNS Servers

6. Now with these numbers, go to Start/Settings/Control Panel and open the Network Applet. (Right Click on Network Neighborhood, then select properties from the pop-up menu.)
7. The Network dialog box should be open. In the "The following network components are installed" box, scroll down until you see the entry TCP/IP->Dial-Up Adapter #2 (VPN Support) and double click on it.

8. Click on the DNS Configuration tab.

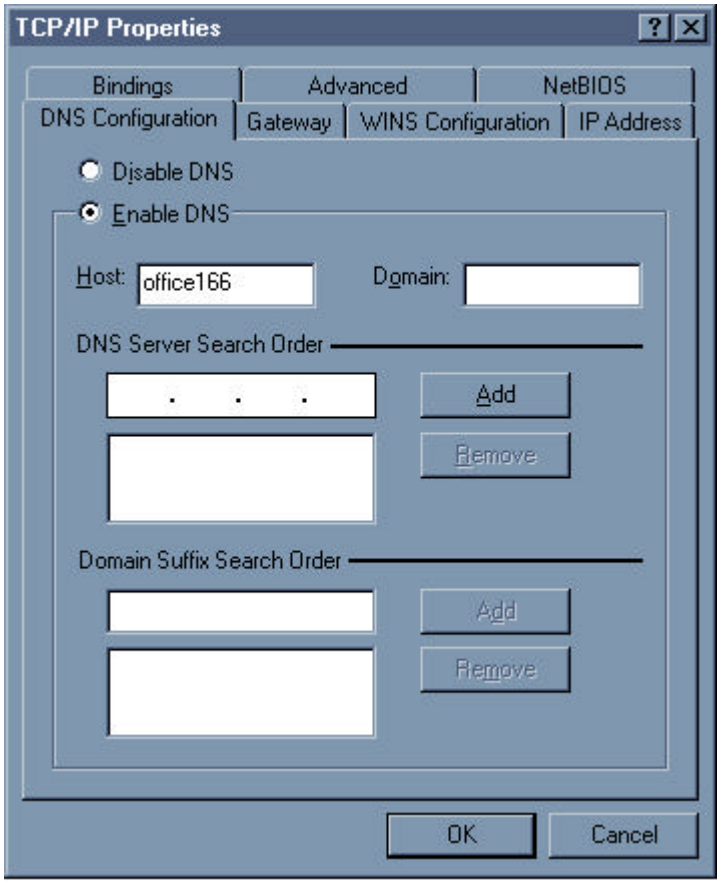


Figure 14. Network Dialog Box –DNS Configuration

9. Make the following changes:
   - Enable DNS
   - Host Name is the name issued to you
   - Domain is left blank
   - DNS Server Search Order. Enter the IP Addresses you collected in Step #3 above
   - Domain Suffix Search Order
     - companyname.com
     - your domain as issued by your ISP
10. Select OK
11. Select OK again. Files will be copied and updated.
12. If prompted to keep **any** file, select YES
13. Select Yes to reboot.

Note: When your system comes back up, start your browser to verify Internet communication.

14. Create a new DUN connectoid. (Make a new connection icon)
    - Open the My Computer object on the desktop
    - Open the Dial-Up Networking Object
    - Open the Make New Connection Object
    - Enter the following information:
        - Name for the computer you are calling = PPTP
        - Select a device = Microsoft VPN Adapter
        - Select Next>
        - Host Name or IP address = IP Address of your PPTP Server
        - Select Next>
        - Select Finish

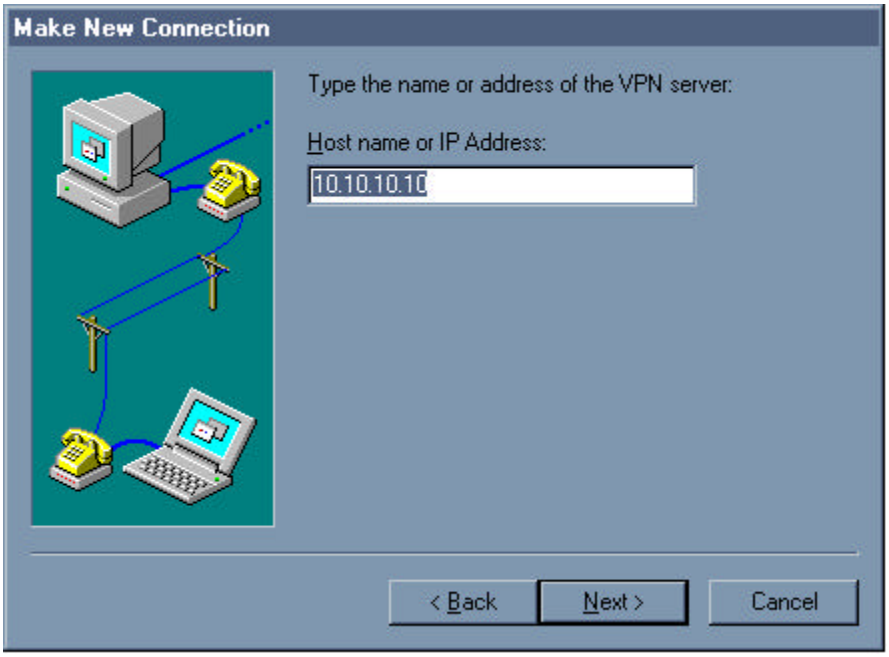


Figure 15. PPTP DUN Connectoid Setup – PPTP Server Address

15. Edit the properties on the new connectoid:
    - Select the connection you just created (Click once)
    - Select File, Properties from the Command Bar (Right Click on PPTP connectoid)
    - Select the Server Types tab
    - PPP (Default. Not changeable)

- Check the following boxes:
  - Log onto network
  - Enable Software Compression
  - Require Encrypted Password
  - Require Data Encryption
  - Allowed Network Protocols: Only TCP/IP should be selected

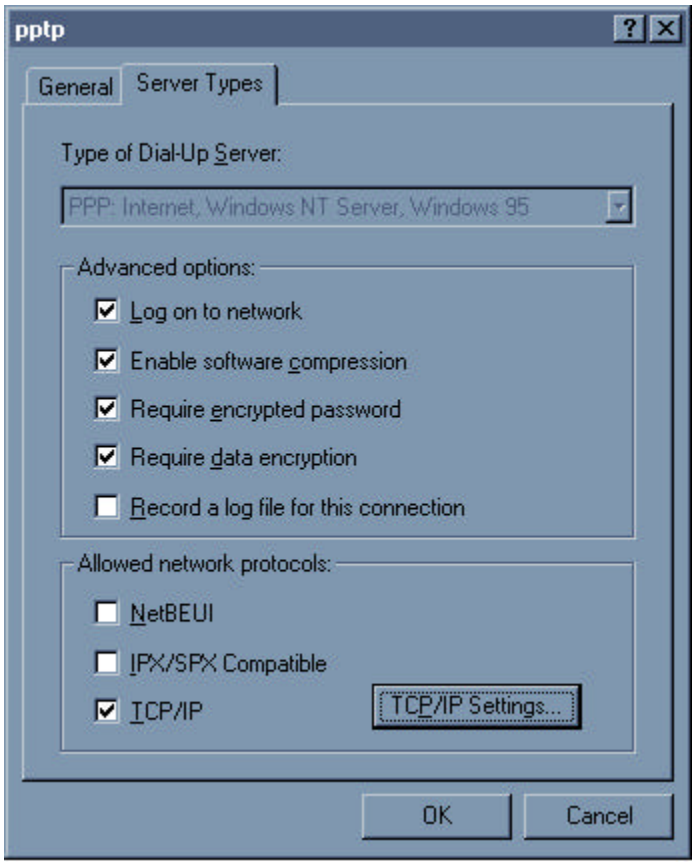


Figure 16. PPTP Settings

- TCP/IP Settings: Check the following TCP/IP Settings
  - Server Assigned IP Address
  - Server Assigned Name Server Addresses
  - Use IP header compression
  - Use default gateway on remote network.
- Select OK

16. Select OK

Tunneling into the Intranet

After establishing a connection to your ISP, establish a second connection by starting the PPTP connection created in this document. You will be prompted for logon information. Use your NT User ID, password, and domain (if required). The settings specified in this document will ensure that your login and subsequent data are encrypted.

Common Issues

Q¾ No VPN device in the Select Device box when creating the connectoid

All of the necessary components were not installed. Go to Control Panel and open the network Applet. Verify that the following components are installed:

- Dial-Up adapter
- Dial-Up Adapter #2
- Microsoft Virtual Private Networking adapter
- NDISWAN -> for Microsoft Virtual Private Networking Adapter
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> Dial-Up Adapter #2 (VPN Support)

Win 95 and 98 have a 5-adapter limitation. If there are already 5 adapters installed, identify and remove any unused adapters and then select Add, Protocol
–or–
Adapter, depending on which needs to be installed. If the TCP/IP -> Dial-Up Adapter #2 (VPN Support) is missing, select ADD, Protocol, Microsoft, TCP/IP. This will add the Dial-Up Adapter #2 if there is room.

Q¾ Receive Error 629

You are probably not getting to the Tunnel server. Verify connectivity to your ISP. Bring up your Internet Browser, Internet Explorer or Netscape (remember to uncheck the proxy setting), and connect to www.lycos.com or www.yahoo.com. If you are unable to reach either of these sites, contact your ISP.

Perform a trace route to your Gateway from a DOS prompt, for example C:\Tracert 10.10.10.10. If you do not receive a valid response, you are not getting across the Internet to the server. Contact your system administrator.

Q¾ When tunneled in, can't browse the Internet

Open Internet Explorer (IE). Select View from the command bar, Select Internet Options, select Connection tab. Click on the " Access the Internet using a Proxy" server box. Whenever you are tunneled in, this box will need to be checked. When you are not tunneled and connected to your ISP, this box needs to be unchecked. IE 5 will resolve this issue.

Q¾ Tunnel connections drop or fail to connect

To verify whether the problem is with the tunnel server or a component on the Internet, perform a trace route to your Gateway from a DOS prompt, for example C:\Tracert 10.10.10.10. If you do not see a valid response, then you are not getting across the Internet. In this case check with your ISP. If you do get all the way to your Gateway server, notify your system administrator.

Q¾ Script does not run when tunneling

During the Login process, the Domain Controllers see cached credentials and believe the system has already been logged in or validated by some domain. For this reason you should follow these steps:

Win 95 Systems:

1. When you first power on your system, cancel or Escape out of the Network Login screen if it appears.
2. Login to your ISP.
3. Tunnel into your Company.

Creating a Dial-Up Profile

If the computer is going to be dialing in through an Internet Service Provider (ISP) over Analog or ISDN and has a network adapter installed, the network adapter driver has to be disabled from the Hardware profile for correct dial-up operation. The following document from Microsoft explains how to create and configure a new hardware profile on you computer.

Note: This is not necessary for ADSL or Cable Modem users.

Windows 95 uses hardware profiles to determine which drivers to load when the system hardware changes. When you start Windows 95, Windows 95 runs detection to see if any hardware on the computer has changed. If the hardware has changed significantly, Windows 95 creates a new hardware profile and prompts you for a name. If you move the computer to a new site and use a different configuration, Windows 95 notices it when you start the computer, and loads the appropriate drivers.

The only time Windows 95 prompts you for the name of a hardware profile is when two profiles are so similar that Windows 95 can't differentiate between them. If this happens, Windows 95 displays a Hardware Profile menu from which you can choose the correct one.

Hardware profiles are an especially important feature for portable computers that can be docked. Windows 95 uses one hardware profile to load drivers when the portable is docked, and another profile when the portable is undocked, for example, at a customer site that has a different monitor than at the office.

Note: It is not necessary to use a different hardware profile for a Plug and Play portable computer, because the computer automatically knows when it is docked or undocked.

Creating a Hardware Profile

1. In the System option in Control Panel, click the Hardware Profiles tab.
2. Click the name of the hardware profile you want to base the new hardware profile on, and then click Copy.
3. Type a name for the hardware profile you are creating.
4. Change which hardware is enabled or disabled in this profile by using the Device Manager, as described in the following procedure.

Note: If you have a hardware profile with the same name as a Windows 95 Startup Menu item, the corresponding menu item will be run automatically when you use that hardware profile for system startup.

Enabling or Disabling Hardware in a Hardware Profile

1. In Device Manager, click the plus sign (+) next to the hardware type and then double-click the hardware.
2. In the Device Usage box, click to place a check mark next to each hardware profile in which you want to enable the hardware, or clear the check box to disable the hardware for that hardware profile.
3. If you see a message prompting you to restart your computer, click Yes.

Deleting or Renaming a Hardware Profile

1. In the System option in Control Panel, click the Hardware Profiles tab.
2. Click the name of the hardware profile you want to change.
3. If you want to remove this profile, click Delete.
   – or –
   If you want to change the name of the profile, click Rename, and then type a new name.

Configurations are created when Windows 95 queries the BIOS for a dock serial ID and then assigns a name for the docked and undocked configuration. Windows 95 then stores the hardware and software associated with this configuration. Applications access and store information for each of the different hardware configurations used by the mobile user. The Registry support enables applications to adapt gracefully to different hardware configurations.

Note: If you are running Multiconfig, you can name a hardware profile the same as a Multiconfig menu option. In this case, Windows 95 detects a hardware profile and automatically runs the corresponding Multiconfig menu option. You can create this by specifying identical names for the Multiconfig menu option and the hardware profile.

Terms

1. **Applet**. The Icons in the Control Panel
2. **Connectoid**: Icons in Dial-Up networking
3. **DUN:** Dial-Up Networking

Appendix 2 – Windows 98 Client Installation

The following steps are necessary to configure a remote access client to use PPTP for Microsoft Windows 98.

System Requirements

The client requires the following components:

1. Microsoft Windows 98 with the latest service patch installed
2. Analog, ISDN, Cable Modem, ADSL, and connectivity to the Internet
3. Dial-Up Networking installed
4. Dial-Up Networking Upgrade 4.0 software
5. Microsoft Windows 98 CD/Diskettes or CAB files on hard drive
6. An account with any Internet Service Provider (ISP)

Where to get Dial-Up Networking (DUN) 4.0

- **http://support.microsoft.com/download/support/mslfiles/Dun40.exe**

Where to get 128-bit Encryption Upgrade (USA and Canada only)

128-Bit version of the Win98 Dial-Up Networking Security Upgrade (8/98) - (MSNT128.exe)

- **http://support.microsoft.com/Support/NTServer/128Downloads.asp**

Installing DUN

1. Go to Start/Control Panel
2. Open Add/Remove Programs
3. Go to the Windows Setup Tab
4. Double click on the Communications entry
5. Click on the Dial-Up Networking entry to place a check in its associated box
6. Select OK
7. Select OK
8. If prompted to keep any files, always select Yes
9. Reboot as prompted

IMPORTANT: Always use the Add/Remove Programs object to add or delete.

Installing DUN 4.0 Upgrade

After you have copied DUN 4.0 to your hard drive, perform these steps to install the upgrade.

1. Select Start from the task bar.
2. Select RUN from the Pop-Up menu.
3. Enter C:*Location of File*\DUN40.exe and select OK.
4. Select Yes when prompted to install the MS Dial-Up Networking 4.0 for Windows 98.
5. Select Yes if you agree with the terms of the End-User License agreement.
6. Select Yes when prompted to reboot
7. After rebooting, you may be prompted to insert the Windows 98 CR-ROM. If so:
    - Select OK at the 'Please insert the disk…' enter the location of the CD-ROM or CAB files.
8. Select OK if prompted to restart your computer.
9. Select RUN from the Pop-Up menu.
10. Enter C:\Location of File\msnt128.exe (128-bit encryption upgrade only).

Configuring DUN 4.0

After Dial-Up Networking 4.0 is installed and your Internet connectivity is enabled:

Note: The symbol ** denotes a shortcut.

1. Establish a connection with your ISP.
2. Run WINIPCFG /ALL from a DOS prompt or from the Start/Run box. (WINIPCFG is all one word.)
3. Record the Host Name. The format is: Your *System Name*.*Domain Name* (For example, yourname.companyname.com).
4. From the IP Configuration dialog box that appears, write down the addresses listed in the DNS Servers box. It is the second box from the top. (Please see Figure 17.)
5. Click on the box just to the right of the DNS Servers. (If you have it.) It has three Periods (…) in it. This will cycle through the DNS Server addresses. Record all of the addresses, though there are only two you will need (for example, 204.x.x.x).

   _____ Address #1

   _____ Address #2

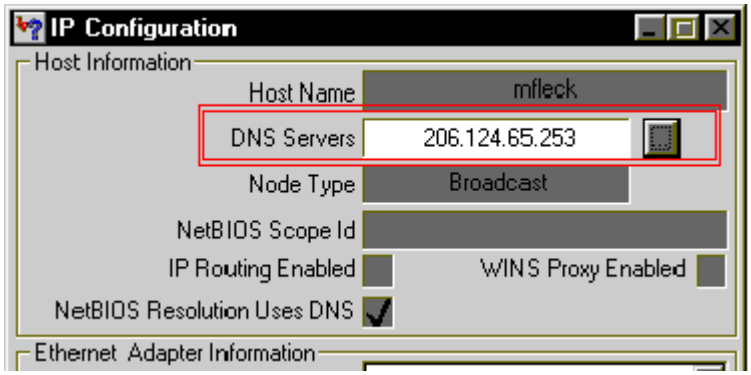


Figure 17. IP Configuration – DNS Servers

6. Now, with these numbers go to Start/Settings/Control Panel and open the Network Applet. ** (Right Click on Network Neighborhood from the desktop then select properties from the pop-up menu.)

   The Network dialog box should be opened. In the "The following network Components are installed" box, scroll down until you see the entry TCP/IP->Dial-Up Adapter #2 (VPN Support) and double click on it.

7. Click on the DNS Configuration tab.

8. Make the following changes:
   - Enable DNS
   - Host name = The System name from above. (i.e. yourname.companyname.com)
   - Domain is left blank
   - DNS Server Search Order. Enter the IP Addresses you collected in Step #3 above
   - Domain Suffix Search Order
     - Your company domain name (i.e. yourcompanyname.com)
     - Your ISP domain name. (i.e. ispname.com)
   - Select OK
9. Select OK again. Files will be copied and updated.
10. If prompted to keep ANY file select YES
11. Select Yes to reboot.

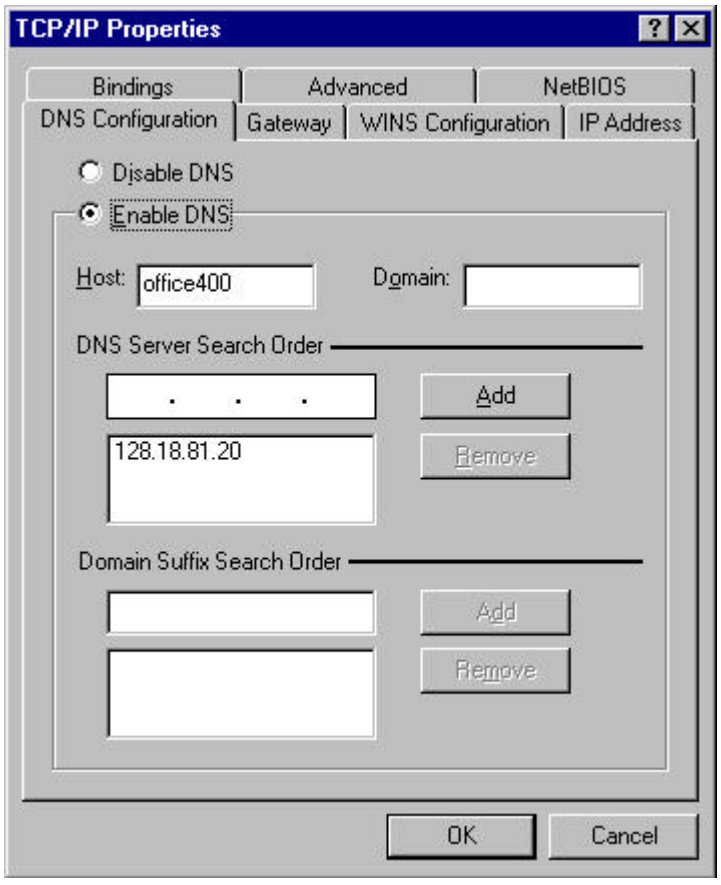


Figure 18. DNS Configuration screen

Note: When your system comes back up, start your browser to verify Internet communication.

12. Create a new DUN connectoid. (Make a new connection icon.)
    - Open the My Computer object on the desktop
    - Open the Dial-Up Networking Object
    - Open the Make New Connection Object
    - Enter the following information:
        - Name for the computer you are calling = PPTP
        - Select a device = Microsoft VPN Adapter
    - Select Next>
    - Host Name or IP address = IP Address of your PPTP Server
    - Select Next>

- Select Finish

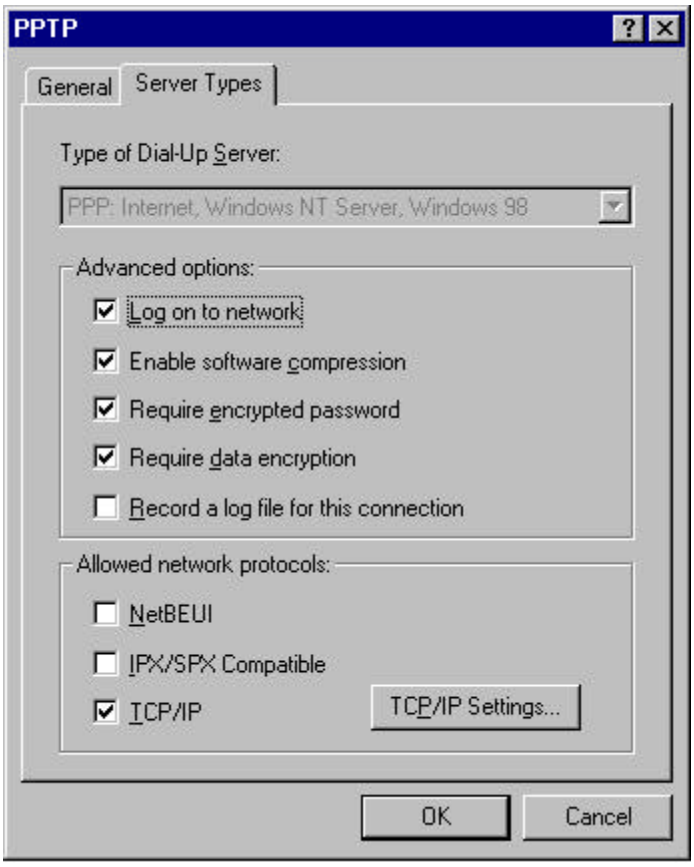


Figure 19. PPTP Server Address

13. Edit the properties on the new connectoid:
    - Select the connection you just created (click once with mouse)
    - Select File, Properties from the Command Bar
      **(Right Click on PPTP connectoid)
    - Select the Server types Tab
    - PPP (Default. Not changeable)
    - Check the following boxes:
      - Log onto network
      - Enable Software Compression
      - Require Encrypted Password
      - Require Data Encryption

- Allowed Network Protocols: Only TCP/IP should be selected

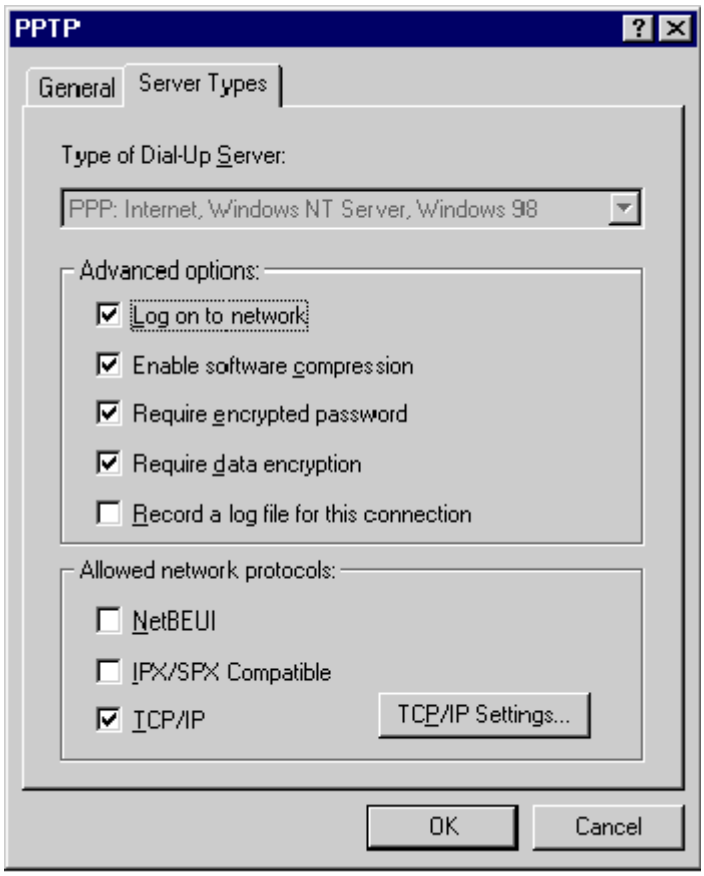


Figure 20. PPTP Server Settings

- TCP/IP Settings: Check the following TCP/IP Settings
  - Server Assigned IP Address
  - Server Assigned Name Server Addresses
  - Use IP header compression
  - Use default gateway on remote network.
- Select OK

14. Select OK

Tunneling Across the Internet

After establishing a connection to your ISP, Establish a second connection by starting the PPTP connection created in this document. You will be prompted for logon information. Use your NT User ID, password, and domain. The settings specified in this document will ensure that your login and subsequent data are encrypted.

Common Issues:

Q¾ No VPN device in the Select Device box when creating the connectoid

All of the necessary components were not installed. Go to Control Panel and open the network applet. Verify that the following components are installed:

1. Dial-Up adapter
2. Dial-Up Adapter #2
3. Microsoft Virtual Private Networking adapter
4. NDISWAN -> for Microsoft Virtual Private Networking Adapter
5. TCP/IP -> Dial-Up Adapter
6. TCP/IP -> Dial-Up Adapter #2 (VPN Support)

Windows 95 and Windows 98 have a 5-adapter limitation. If there are already 5 adapters installed, identify and remove any unused adapters and then select, Add, Protocol or Adapter, depending on which needs to be installed. If the TCP/IP -> Dial-Up Adapter #2 (VPN Support) is missing, select ADD, Protocol, Microsoft, TCP/IP. This will add the Dial-Up Adapter #2 if there is room.

Q¾ Receive Error 629

You are probably not getting to the tunnel server. Verify connectivity to your ISP. Bring up your Internet Browser, Internet Explorer or Netscape (remember to uncheck the proxy setting), and connect to www.lycos.com or www.yahoo.com. If you are unable to reach either of these sites contact your ISP.

Perform a trace route to your Gateway from a DOS prompt, for example C:\Tracert 10.10.10.10. If you do not receive a response then you are not getting across the Internet to the server. Contact your system administrator.

Q¾ When tunneled in, can't browse the Internet

Open IE. Select View from the command bar, Select Internet Options, select Connection tab. Click on the Access the Internet using a Proxy server box. Whenever you are tunneled in, this box will need to be checked. When you are not tunneled and connected to your ISP, this box needs to be unchecked. IE 5 will resolve this issue.

Q¾ Tunnel connections drop or fail to connect

To verify whether the problem is with the tunnel server or a component on the Internet, perform a trace route to your Gateway from a DOS prompt, for example C:\Tracert 10.10.10.10. If you do not see a response then you are not getting across the Internet. In this case check with your ISP. If you do get all the way to the Gateway server, notify your system administrator.

Q¾ Script does not run when tunneling

During the Login process, the Domain Controllers see cached credentials and believe the system has already been logged in or validated by some domain. For this reason you should follow these steps:

Win 98 systems:

1. When you first power on your system, cancel or Escape out of the Network Login screen if it appears.
2. Login to your ISP.
3. Tunnel into your Company.

Creating a Dial-Up Profile

If the computer is going to be dialing in through an Internet Service Provider (ISP) over Analog or ISDN and has a network adapter installed, the network adapter driver has to be disabled from the Hardware profile for correct Dial-Up operation. The following document from Microsoft explains how to create and configure a new hardware profile on you computer.

Note: This is not necessary for ADSL or Cable Modem users.

Windows 98 uses hardware profiles to determine which drivers to load when the system hardware changes. When you start Windows 98, Windows 98 runs detection to see if any hardware on the computer has changed. If the hardware has changed significantly, Windows 98 creates a new hardware profile and prompts you for a name. If you move the computer to a new site and use a different configuration, Windows 98 notices it when you start the computer and loads the appropriate drivers.

The only time Windows 98 prompts you for the name of a hardware profile is when two profiles are so similar that Windows 98 can't differentiate between them. If this happens, Windows 98 displays a Hardware Profile menu from which you can choose the correct one.

Hardware profiles are an especially important feature for portable computers that can be docked. Windows 98 uses one hardware profile to load drivers when the portable is docked, and another profile when the portable is undocked, for example, at a customer site that has a different monitor than at the office.

Note: It is not necessary to use a different hardware profile for a Plug and Play portable computer, because the computer automatically knows when it is docked or undocked.

Create a Hardware Profile

1. In the System option in Control Panel, click the Hardware Profiles tab.
2. Click the name of the hardware profile you want to base the new hardware profile on, and then click Copy.
3. Type a name for the hardware profile you are creating.
4. Change which hardware is enabled or disabled in this profile by using the Device Manager, as described in the following procedure.

Note: If you have a hardware profile with the same name as a Windows 98 Startup Menu item, the corresponding menu item will be run automatically when you use that hardware profile for system startup.

Enabling or Disabling Hardware in a Hardware Profile

1. In Device Manager, click the plus sign next to the hardware type, and then double-click the hardware.
2. In the Device Usage box, click to place a check mark next to each hardware profile in which you want to enable the hardware, or clear the check box to disable the hardware for that hardware profile.
3. If you see a message prompting you to restart your computer, click Yes.

Deleting or Renaming a Hardware Profile

1. In the System option in Control Panel, click the Hardware Profiles tab.
2. Click the name of the hardware profile you want to change.
3. If you want to remove this profile, click Delete
   – or –
   If you want to change the name of the profile, click Rename, and then type a new name.

Configurations are created when Windows 98 queries the BIOS for a dock serial ID and then assigns a name for the docked and undocked configuration. Windows 98 then stores the hardware and software associated with this configuration. Applications access and store information for each of the different hardware configurations used by the mobile user. The Registry support enables applications to adapt gracefully to different hardware configurations.

Tip: If you are running Multiconfig, you can name a hardware profile the same as a Multiconfig menu option. In this case, Windows 98 detects a hardware profile and automatically runs the corresponding Multiconfig menu option. You can create this by specifying identical names for the Multiconfig menu option and the hardware profile.

Terms

1. **Applet**. The Icons in the Control Panel
2. **Connectoid**: Icons in Dial-Up networking
3. **DUN:** Dial-Up Networking

Appendix 3 – Windows NT Client Installation

The following steps are necessary to configure a remote access client to use PPTP for Windows NT 4.0.

System Requirements

The client requires the following components:

1. Windows NT with the SP3 or SP4 installed
2. Internet connectivity
3. Win NT CD/Diskettes or install files on hard drive
4. An account with any Internet Service Provider (ISP)

Determining System Current Configuration

To determine what Operating System level you are at, perform the following:

1. Select Run from the Start button on the task bar.
2. Type in WINMSD.
3. Select the OK button.
4. Windows NT Diagnostics appears. Your Operating system and Service Pack level will be listed on the Version tab page. You will need at least Service Pack level 3 installed. The service pack can be found by going to the Microsoft web page at: http://support.microsoft.com/support/downloads/.

Where to get the Latest PPTP Patch File for 128-bit encryption

1. PPTP Patch file for NT 4.0 – (*PPTPfixi.exe*) ** Only for SP3 and earlier **
   - ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/pptp3-fix/

2. SP3 – PPTP Performance & Security Upgrade for WinNT4.0 (8/98) – x86 – (MSNT128.exe)
   - http://support.microsoft.com/support/ntserver/content/servicepacks/SP3.asp

3. SP4 – Windows NT4.0 SP4 Auto-Install (10/98) – X86
   - http://support.microsoft.com/Support/NTServer/128Downloads.asp

Note: Numbers 2 or 3 above are required to get 128-bit encryption on the tunnel connections. If you have SP3 installed, you only need to copy and install the single MS128nt.exe file from the web location above. If you have SP4 installed, you will need to copy and run the file named in Number 3. This will update some of the SP4 files to enable 128-encryption. It will not install the complete SP4.

Installing and Configuring PPTP and Remote Access Service

The following steps will guide you through the installation and configuration of your NT workstation for PPTP access to the Intranet.

1. In Control Panel, double-click Network.
2. Click the Protocols tab.
3. Click Add, then click Point-to-Point Tunneling Protocol, and click on OK.

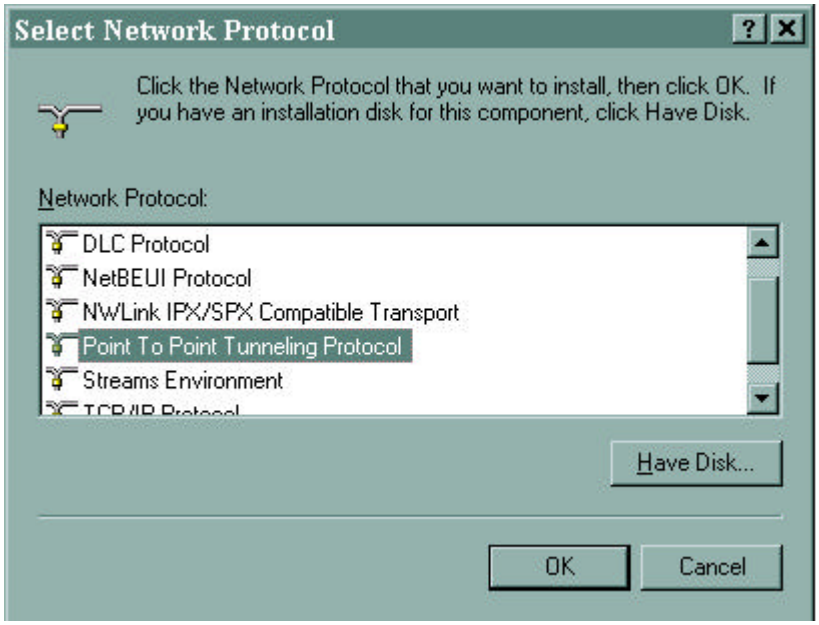


Figure 21. Addition of PPTP Protocol

4. Enter the location of the installation files when prompted and select Continue.
5. When you are prompted for how many Virtual Private Networks (VPN) to enable, click 1.
6. RAS setup will be automatically invoked to configure the PPTP port. Select OK at the Setup message.

7. In RAS Setup, add the new Virtual Private Network (VPN) port by clicking Add and selecting the RASPPTPM device from the Add RAS device menu. Select OK.

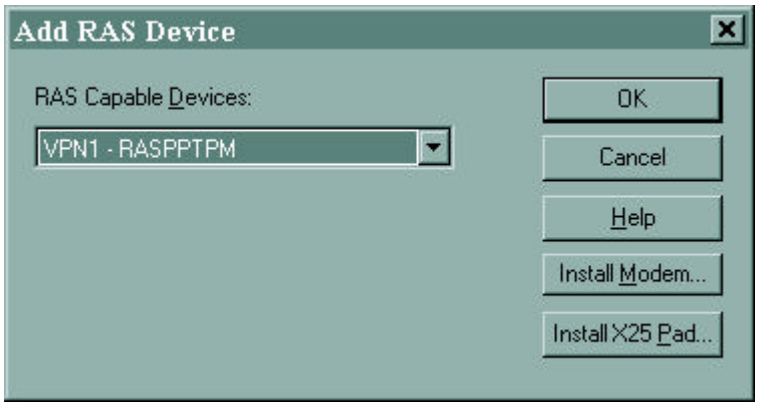


Figure 22. RAS Device Addition

8. Click on the Network button from the Remote Access Setup screen.

9. The following settings should be selected:
   - Dial out Protocols = TCP/IP
   - Server Settings = TCP/IP
   - Encryption settings = Require Microsoft encrypted authentication.
     Require Data encryption.

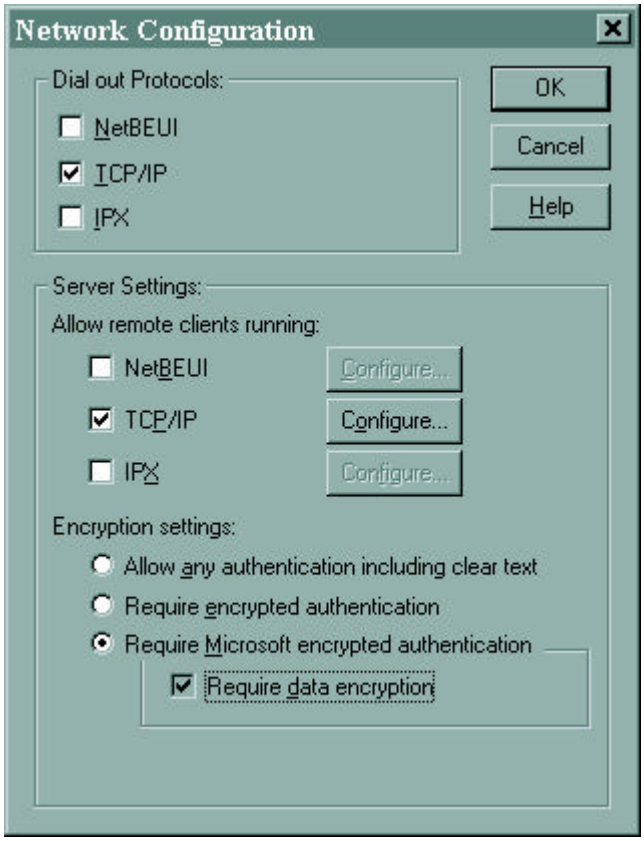


Figure 23. Encryption Settings

10. Click Continue at the Remote Access Setup screen.
11. Click Close at the Network window.
12. When you are prompted to restart the computer, do so.
    Your system is now configured for Remote Access dialing. The following section will configure the Dial-Up Networking phonebook entries for PPTP connectivity.
13. After the system has rebooted, double click on the My Computer icon on your desktop.
14. Double click on the Dial-Up Networking icon.
15. If you have not used the Dial-Up Networking Phonebook before, you will receive a dialog box to add a new entry, Select OK and go to Step 17.
16. If you already have an entry in the phonebook, click on the NEW button on the Dial-Up Networking dialog box and go to Step 17.

17. Enter or select the following information under each tab of the New Phonebook Entry dialog box:

    - Basic:
      Entry Name = PPTP
      Phone Number = IP Address of your PPTP Server
      Dial using = RASPPTPM (VPN1)
    - Server:
      Dial-Up server type = PPP: Windows NT, Windows 95 Plus…
      Network Protocols = TCP/IP (The only protocol that should be selected)
      Script : Accept all defaults
    - Security:
      Authentication and encryption policy = Accept only MS encrypted authentication
      Require data encryption.

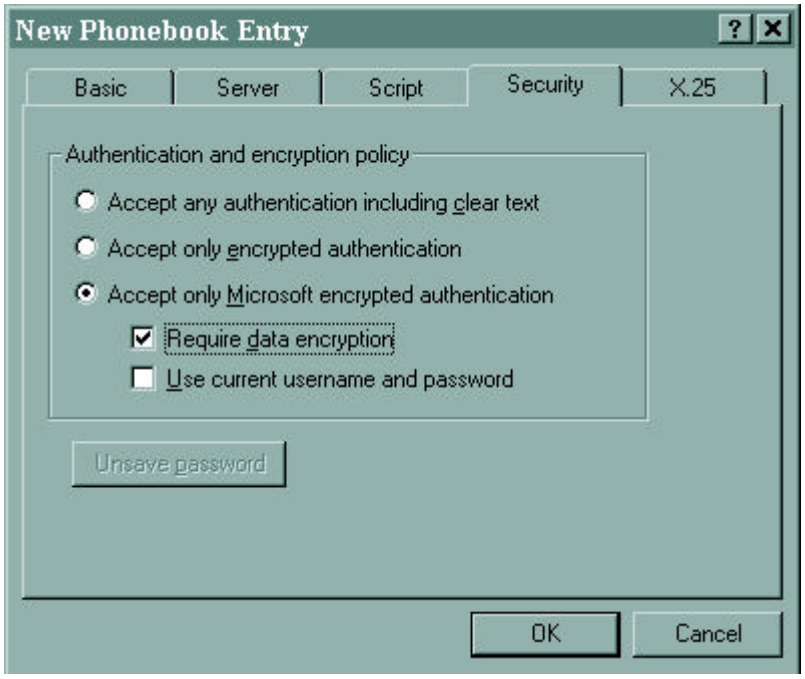


Figure 24. Phonebook Entry Setup

18. Select OK on the New Phonebook Entry Screen.
19. Select the Network Icon from the Control Panel. Select the TCP/IP properties for the appropriate adapter for the PPTP connection.

20. Click on the DNS Configuration tab.
    - Make the following changes: Host name = The System name from above. (i.e. yourname.companyname.com)

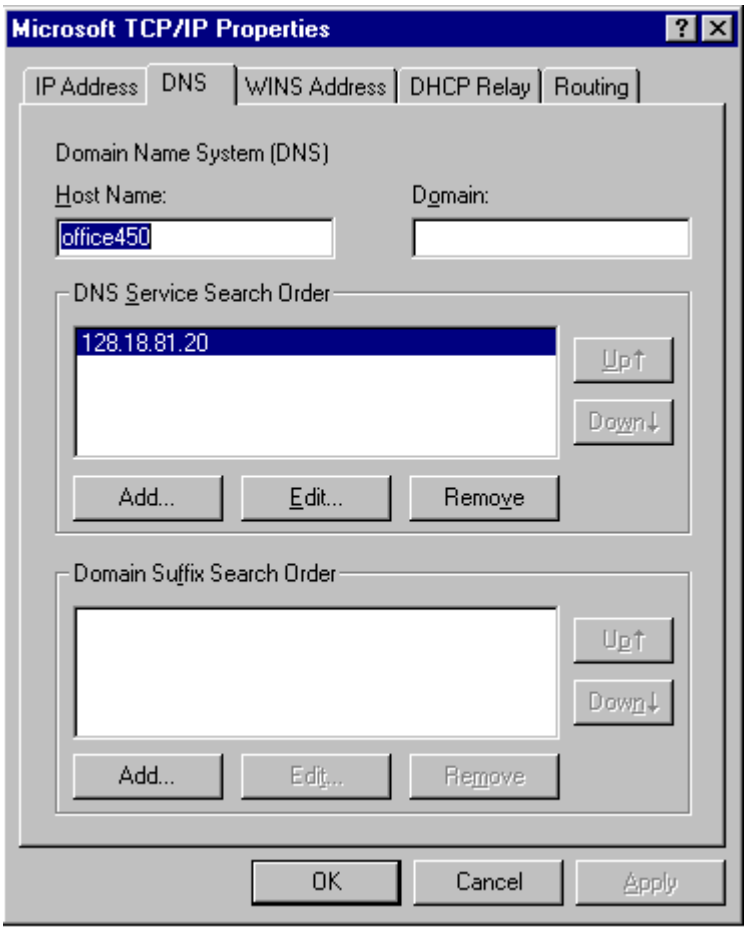


Figure 25. DNS Settings

    - Domain is left blank
    - DNS Server Search Order. Enter the IP Addresses as appropriate
    - Domain Suffix Search Order
    - Your company domain name (i.e. yourcompanyname.com)
    - Your ISP domain name. (i.e. ispname.com)
21. Select OK

Installing PPTP Patch for 128-bit Encryption (US and Canada Only):

If you are running SP3, you will need to copy the file pptpfixi.exe to your local hard drive This is a self-extracting and installing file. A text file is included in the directory that describes the pptpfixi.exe file purpose. Run the file on your local system and then reboot when prompted.

If you are running SP4 systems:

If you have SP4 installed, you can verify if it is the 40-bit or the 128-bit encryption version; Use Windows Explorer and check the following file properties: SChannel.dll. It is located in the WINNT/SYSTEM32 directory.

1. Right click on the file and select properties
2. Select the Version tab. If the Description field states TLS/SSL Security Provider (Export Version), you have the 40-bit version.

Once the correct files have been retrieved as specified earlier than the patch can be installed. This will update just the files necessary to enable 128-bit encryption on your tunnel sessions.

On SP3 Systems:

1. Select Start
2. Select Run
3. In the Open box, enter the path to pptpfixi.exe
4. Select OK
5. Reboot as prompted
6. After the system restarts, logon to the local workstation
7. Select Start
8. Select Run
9. In the Open box, enter the path to MS128nt.exe
10. Select OK

On SP4 Systems:

1. After running the MS128nt.exe file, your system will and automatically update your system

Tunneling across the Internet

Win NT system using Analog or ISDN:

1. Run the Reg_Tunnel.exe file. This will allow you to Logoff your workstation and still maintain a connection to your ISP.
2. Logon to your workstation and connect to your ISP.
3. Logoff your workstation.
4. Logon to your workstation using the Dial-Up Networking Option.
5. Select the VPN phonebook entry and establish a tunnel.

Win NT system using Cable Modem, ADSL, or other direct connect to Internet method:

1. Logon to your workstation using the Dial-Up Networking Option.
2. Select the VPN phonebook entry and establish a tunnel.

To close the tunnel and disconnect from the Intranet, double click on the phone icon in the Task Bar tray (lower right corner of the desktop predominantly) and select disconnect. Your connection to your ISP will be restored as the default connection.

Common Issues:

Q¾ No VPN device in the Select Device box when creating the connectoid

All of the necessary components were not installed. Go to Control Panel and open the network applet. Verify that the following components are installed:

- Dial-Up adapter
- Dial-Up Adapter #2
- Microsoft Virtual Private Networking adapter
- NDISWAN -> for Microsoft Virtual Private Networking Adapter
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> Dial-Up Adapter #2 (VPN Support)

If the TCP/IP -> Dial-Up Adapter #2 (VPN Support) is missing, select ADD, Protocol, Microsoft, TCP/IP. This will add the Dial-Up Adapter #2 if there is room.

Q¾ Receive an Error 629

You are probably not getting to the Tunnel server. Verify connectivity to your ISP. Bring up your Internet Browser, Internet Explorer or Netscape (remember to uncheck the proxy setting), and connect to www.lycos.com or www.yahoo.com. If you are unable to reach either of these sites contact your ISP.

Perform a trace route to the Gateway from a DOS prompt, for example: C:\Tracert 10.10.10.10. If you do not receive a response then, you are not getting across the Internet to the server. Contact your system administrator.

Q¾ When tunneled in, can't browse the Internet

Open Internet Explorer (IE). Select View from the command bar, Select Internet Options, select Connection tab. Click on the Access the Internet using a Proxy server box. Whenever you are tunneled in, this box will need to be checked. When you are not tunneled and connected to your ISP, this box needs to be unchecked. Internet Explorer 5 is expected to resolve this issue.

Q¾ Tunnel connections drop or fail to connect

To verify whether the problem is with the tunnel server or a component on the Internet, perform a trace route to the Gateway from a DOS prompt; e.g. C:\Tracert 10.10.10.10. If you do not see a response then, you are not getting across the Internet. In this case check with your ISP to let them know. If you do get all the way to your gateway server, notify your system administrator.

Q¾ Script does not run when tunneling

During the Login process, the Domain Controllers see cached credentials and believe the system has already been logged in or validated by some domain. For this reason you should follow these steps:

Win NT system using Analog or ISDN:

1. Run the Reg_Tunnel.exe file. This will allow you to Logoff your workstation and still maintain a connection to your ISP.
2. Logon to your workstation and connect to your ISP.
3. Logoff your workstation.
4. Logon to your workstation using the Dial-Up Networking Option.
5. Select the VPN phonebook entry and establish a tunnel Win NT system using Cable Modem, ADSL, or other direct connect to Internet method.
6. Logon to your workstation using the Dial-Up Networking Option.
7. Select the VPN phonebook entry and establish a tunnel.

Terms

1. **Applet**. The Icons in the Control Panel
2. **Connectoid**: Icons in Dial-Up networking
3. **DUN:** Dial-Up Networking