Microsoft® Windows®95 Dial-Up Networking 1.3 Upgrade Release Notes

1. Introduction

The Dial-Up Networking 1.3 Upgrade (DUN 1.3) provides additional features for the Dial-Up Networking components that were first introduced in Windows 95. DUN 1.3 includes all of the features of the 1.2 release, and all of the features of the earlier ISDN 1.1 release. These features include support for internal ISDN adapters, multilink support for two ISDN channels, connection-time scripting to automate non-standard login connections, and PPTP client support.

1.1 Performance Features Added in the DUN 1.3 Release

- A new historyless mode for encryption & compression over PPTP connections has been enabled in this update. This new mode solves performance problems encountered using PPTP in high latency networks or networks that experience significant packet loss. This upgrade is fully compatible with legacy PPTP systems. However, in order to negotiate historyless mode, both the PPTP client and server must support this new mode. If either side refuses the new mode, normal MPPE compression and encryption will be negotiated
- The IP Packet size for dial-up connections is now automatically adjusted based on connection speed. The setting toggles between “Small” (576) for Dial-Up connections of 128kbps and below and “Large” (1500) for faster Dial-Up connections or LAN connections. In addition, the PPTP frame size is adjusted based on the Maximum Transit Unit (MTU) in order to avoid fragmentation. One can manually set both the dial-up and PPTP MTU sizes to a specific size. These are configurable under the advanced properties for the Dial-Up Adapter.
- The default PPTP receive window size was increased to 16.

1.2 Security Features in the DUN 1.3 Release

- A new version of MSCHAP (MSCHAP V2) has been implemented, providing mutual authentication, stronger initial data encryption keys, and different encryption keys for the transmit and receive paths. To minimize the risk of password compromise during MSCHAP exchanges, MSCHAP V2 drops support for the MSCHAP password change V1, and will not transmit the LMHASH encoding of the password.
- A new registry variable, SecureVPN, has been provided which forces the Windows 95 PC to use MSCHAP V2 and to require encryption for all VPN (PPTP) connections.
- There is a new per-connection setting to "Require data encryption".
- A new registry variable, ForceStrongEncryption, has been provided to allow the client to require strong encryption.
- Data encryption can be negotiated independently from software compression.

1.3 Other Features in the DUN 1.3 Release

- With this release, limited server functionality for a dialup Point to Point IP connection is enabled.
- There are new options shown in the connection status display. You can click "Details" after getting connected and see what type of authentication was negotiated and whether data encryption, software compression, or multilink was negotiated.
- You can turn on an improved PPP logging option on a per connection basis. Results are logged to PPPLOG.TXT in your Windows directory.
- The details section of the connection status display has been modified to identify the specific form of CHAP that was used in the connection.

1.4 Features Included from the DUN 1.2b Release

- A fix for a multicast problem was included. This is documented at http://support.microsoft.com/support/kb/articles/q174/0/95.asp.
- This update can now be installed on Windows 95 OEM Service Release 2.1 and Release 2.5

- A setup error was corrected that reported missing files during the installation of the Direct Cable Connection feature.

1.5 Installation Notes

Execute the MSDUN13.exe file and follow the instructions. The installation process will require you to reboot the machine, and may ask for your Windows 95 installation disk (if you originally installed Windows 95 from a CD). If you encounter a "do you want to keep a newer file" dialog, always keep the newer file.

Once the installation is complete, you will be able to remove the Dial-Up Networking 1.3 Upgrade by using the install/uninstall tab of the "Add/Remove Programs" icon in the setup folder. This will remove all of Dial-Up Networking from your system. After this, you can add the original Windows 95 version of Dial-Up Networking by using the windows setup tab of the "Add/Remove Programs" icon. Alternately, you can re-install the 1.3 upgrade by executing the MSDUN13.exe file.

> *Note: An uninstall of the Dial-Up Networking 1.3 Upgrade will completely remove Dial-Up Networking from your system, including any features that depend on it. For example, an uninstall would remove Direct Cable Connection and Virtual Private Networking in addition to the ability to dial out over modems or ISDN devices. If you have installed an ISDN device, removing Dial-Up Networking will logically remove the device and any information that you entered for it. This information will not be restored when you re-install Dial-Up Networking.*

Always use the “Add/Remove Programs” icon in the setup folder in order to add or delete Dial-Up Networking from your system. Do not add or remove individual Dial-Up Adapter or Virtual Private Networking Adapter components via the Network Control Panel applet or from the Device Manager tab of the System applet.

A separate utility (DUN128) is available which will modify an MSDUN 1.3 installation to enable use of 128-bit encryption. This utility can be obtained from the web site below.
http://mssecure.www.conxion.com/cgi-bin/ntitar.pl.
This utility places an entry in the “Add/Remove Programs” control panel applet in order to allow you to remove the 128-bit encryption (leaving the original 40-bit encryption in place).

> *NOTE: The Dial-Up Networking 1.3 Upgrade relies on features in the most recent version of the Microsoft TCP/IP stack. For that reason, installation of the upgrade will replace your current TCP/IP protocol stack (or add the stack if you do not already have it installed.) If you have applications that rely on a third party stack, you may want to discontinue this upgrade. If you choose to perform the upgrade, and certain applications stop working, you will have to reload these applications.*

1.6 Server Updates

This upgrade is fully compatible with legacy PPTP systems. However, in order to negotiate historyless mode, both the PPTP client and server must support this new mode. Server support for historyless mode and for MSCHAPV2 will be included in Windows NT 4.0 Service Pack 4. For installations which require these features before general availability of Service Pack 4, a hotfix for Service Pack 3 has been created. This can be found on the Microsoft FTP site at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/pptp3-fix. Servers running the Routing and Remote Access Upgrade should apply the above, and then apply rras30-fix from the same location.

> *NOTE: RAS and PPTP servers must be maintained to current Windows NT Service Pack levels. A Windows 95 client machine that has been upgraded to DUN 1.3 will no longer connect to a Windows NT Server that has not been updated to Service Pack 3 or above.*

Front End Processors (FEPs) are dial-up access servers which are capable of creating PPTP tunnels on behalf of dial-up PPP clients. Servers which terminate such “compulsory” tunnels from FEPs must disable the historyless mode.

2. Feature Overview

2.1 ISDN Support

MSDUN includes the support for internal ISDN adapters that was previously delivered in the ISDN 1.1 Accelerator Pack. To assist in the setup process, an ISDN Configuration Wizard is automatically installed in the Start menu under Start>Programs>Accessories>ISDN Tools.

2.2 Multilink Support

Multilink support enables your computer to use two communications ports as if they were a single port of twice the bandwidth. The feature is most useful to ISDN users, since it allows them to use both sides of an ISDN line for an aggregate bandwidth of 128Kbps. The feature is also available to modem users, but on most systems, the serial port overhead eliminates much of the benefit that could be gained from simultaneous use of two modem calls. Multilink is enabled from the Properties page of any connection icon in the Dial-Up Networking folder.

2.3 Scripting

Some Internet Service Providers require a terminal interaction with the user at the start of a dial-up connection. The Scripting feature included in this Dial-Up Networking upgrade allows you to automate this interaction. Scripting is enabled from the Properties page of any connection icon in the Dial-Up Networking folder. The scripting language is described in the file "script.doc" in your windows directory.

2.4 PPTP Client

MSDUN includes the ability to create a PPTP tunneling client. Tunneling is a networking term describing the encapsulation of one protocol within another protocol. Tunneling is typically done to join two networks using an intermediate network that uses an incompatible protocol or which is under the administrative control of a third party.

2.4.1 PPTP Tunneling

The Point to Point Tunneling Protocol (PPTP) is a tunneling protocol defined by the PPTP Forum whose specifications is publicly available and supported by a variety of Networking vendors. PPTP allows PPP packets to be encapsulated within Internet Protocol (IP) packets and forwarded over any IP network, including the Internet itself. In order to run the Windows 95 PPTP client; you must be able to establish an IP connection with a tunnel server such as the Windows NT® Server 4.0 Remote Access Server (RAS).

Windows Dial-Up Networking uses the Internet standard Point-to-Point Protocol (PPP) to provide a secure, optimized multiple-protocol network connection over dialed telephone lines. PPTP adds the ability to treat the Internet as point-to-point Dial-Up Networking connection. All data sent over this connection can be encrypted and compressed, and multiple network level protocols (TCP/IP, NetBEUI, and IPX) can be run concurrently. Windows NT Domain Login level security is preserved even across the Internet. PPTP can also be used to connect to an Intranet that is otherwise isolated from the Internet, even if this same Intranet has Internet address space conflicts.

PPTP appears as new modem type (Virtual Private Networking Adapter) that can be selected when setting up a connection in the Dial-Up Networking folder. The VPN Adapter type does not appear elsewhere in the system. Since PPTP encapsulates its data stream in the PPP protocol, the VPN requires a second dial-up adapter. This second dial-up adapter for VPN is added during the installation phase of the Upgrade in addition to the first dial-up adapter that provides PPP support for the analog or ISDN modem.

2.4.2 PPTP Connections

The "Make a New Connection" wizard (in the Dial-Up Networking folder) will guide you through the steps needed to create connection icons for either normal dial-up (modem) calls or PPTP (virtual private network) calls. You indicate use of PPTP by selecting VPN rather than a modem as your device type.

2.4.2.1 Dial-up PPTP Connections

The most typical application for PPTP involves a dial-up PPP connection to the Internet followed by a separate PPTP connection to a remote tunnel server. This "two call" sequence requires two connection icons in the Dial-Up Networking folder, and two "dialing" actions by the user. The results of a successful tunnel over the Internet are two network connections on your PC: one to the Internet, and one to the target network served by the tunnel server. To understand the behavior of your PC in this configuration, see the discussion below regarding *Default Routing to Remote TCP/IP Networks*.

2.4.2.2 LAN-based PPTP Connections

A second application for PPTP involves a tunnel over a LAN to which your PC is already attached. In this case, only a single connection icon is required, and only a single "dialing" action by the user in order to initiate the tunnel. Under this scenario, it is not necessary to have a Dial-Up Networking connection to the Internet to support PPTP. The ability to route packets correctly to the PPTP tunnel server over an IP network is the only requirement for a PPTP connection. Again, see the discussion below *Default Routing to Remote TCP/IP Networks* or the more detailed discussion in the file *About PPTP and Dial-Up Networking 1.3.doc* in your Windows directory.

2.5 Per-Connection Encryption Settings

In most installations, the server's settings will determine the level of encryption on a dial-up or PPTP connection. The Windows NT 4.0 server can be set to require encryption for all connections (in which case it will offer 40-bit encryption), or to require strong encryption (in which case it will offer 128-bit encryption). The Windows 95 Dial-Up Networking client will normally accept the server's encryption request.

The DUN 1.3 upgrade adds the ability to require encryption for a specific connection. In the DUN 1.3 upgrade, a checkbox on the S*erver* tab of the connection's property page has been added, allowing you to require encryption for a successful connection. A new registry variable, ForceStrongEncryption, has been provided to allow the client to require strong encryption. If the server proposes 40-bit encryption, such a client would respond by requesting 128-bit encryption. A 128-bit capable server would accept the client's request. Note that a server which is capable of only 40-bit encryption would not be able to accept a client request for 128-bit encryption. A connection request of this type would fail.

The registry flag which forces strong encryption is defined below. By default, the flag is absent. The value of this flag is checked just before a connection is attempted.

```
HKLM\System\CurrentControlSet\Services\RemoteAccess

DWORD: ForceStrongEncryption
Default: 0x00000000

0x00000000 = No effect; does not force strong encryption
0x00000001 = Requires 128-bit encryption for any connection which already requires encryption
```

Note that data encryption is negotiated during the CCP (Compression Control Protocol) phase of the connection. Consequently, the properties sheet for a connection must enable either compression or *encryption (below) in order for the encryption negotiation to succeed. This is rarely an issue since compression is enabled by default.*

2.6 Modem Pool Access

PPTP can be also used as a method for a LAN-based PC to make a dial-up connection to a remote computer or network through a modem pool on an appropriately configured access server.

If PPTP connections are established to your network by a PPTP-enabled access server (sometimes called a FEP, or Front End Processor), and if your system administrator has configured the access server with several modems set aside for outbound calls, your PPTP client can cause these modems to initiate a PPP dial-out connection between your client and another computer or network.

To cause such a connection, simply establish a PPTP connection whose tunnel address is specified as "AccessServer<space>PhoneNumber". AccessServer is the DNS name or IP address of the PPTP-enabled access server; PhoneNumber is the set of digits to be dialed to reach the other site. The access server will bring up a dial-up PPP connection to the digits supplied. On connection, your PC will behave as if it had dialed directly into the remote site. Authentication will be performed by the remote site. Again, see the discussion below regarding *Default Routing to Remote TCP/IP Networks* or the more detailed discussion in the file *About PPTP and Dial-Up Networking 1.3.doc*.

Note: This feature is only supported by access servers which support "compulsory tunneling". These are servers which receive an ordinary dial-up PPP call, then create a tunnel on the caller's behalf, and then insert the PPP traffic into the tunnel. Windows NT RAS does not presently support this feature.

3. Product Limitations and Related Issues

There are network routing issues and product limitations that affect network behavior when you are using Windows 95 Dial-Up Networking. Network routing issues are discussed in the *Default Routing to Remote TCP/IP Networks* section below. Product limitations and related issues are discussed in this section.

3.1 Name Resolution Issues

The original release of Windows 95 Dial-Up Networking had limited support for WINS and DNS name resolution when a PC was connected to multiple networks. The Dial-Up Networking 1.3 Upgrade resolves all of the WINS limitations, and applies a Winsock upgrade to resolve the remaining DNS limitations. This Winsock upgrade represents a minor change over the Winsock that was originally delivered with Windows 95.

Microsoft has also released Winsock2, a complete redesign of the Winsock architecture. Winsock2 is fully compatible with the Dial-Up Networking 1.3 Upgrade. If Winsock2 has already been installed, the Dial-Up Networking 1.3 Upgrade will not overwrite it. If you wish to install it, Winsock2 is available from the Microsoft web site at http://www.microsoft.com/windows95/info/system-updates.htm

3.2 Static IP Address, WINS, and DNS Settings

In almost all cases, you should allow the network to define your PC's IP address and to provide WINS and DNS server addresses automatically. This occurs when you boot your machine on a LAN, or when you successfully establish a PPP or PPTP connection to a remote network. In the rare cases where an ISP or systems administrator requires you to set an IP address or to define addresses for WINS and/or DNS servers, you should do this in the appropriate connection icon. (Use the TCP/IP Settings button on the Server Type tab of the Properties page for the icon.)

Generally, you should not set TCP/IP properties for dial-up adapters or LAN adapters from the Network icon in the control panel. Values set via the control panel are global settings that override the settings in individual connection icons, and may override any dynamic information established during a dial-up or

PPTP connection. In particular, setting a static WINS address on a LAN adapter will prevent dynamic WINS assignments on dial-up or PPTP connections. Setting a static DNS address on the LAN adapter does not have this effect. So additional DNS addresses will be obtained on a successful connection to a remote network. (However a bug in the winipcfg utility may prevent these DNS addresses from being displayed.)

> *NOTE: There have been cases where cable modem installation instructions required the user or installer to use the network control panel applet to define a DNS server and to define a DNS domain suffix search order for the LAN card serving the cable modem. (This information is on the TCP/IP properties sheet for the affected LAN card.) Defining a DNS suffix search order will cause timeout delays when a tunnel is used to reach another network, unless the suffix for that network is included at the top of the list.*

3.3 Remote Access after Physical Disconnection from a LAN

An addressing problem can occur when a computer that has been directly connected to a private TCP/IP network is physically disconnected and then attempts a dial-up or PPTP connection. (This can happen, for example, when a laptop user disconnects an Ethernet connection from the corporate network and then tries to dial in from home.) If the network card is still installed, TCP/IP may be configured so that the computers that could be reached through the netcard, still appear reachable through the netcard. Even after a modem Dial-Up Networking connection or a PPTP connection is established back to the same network, TCP/IP will continue to send all traffic for computers on the local network out the netcard.

The workaround, if the computer originally booted from DHCP, is to run the *winipcfg* utility and select the *Release* option. If this does not fix the problem, the netcard may have been manually configured through the control panel, and will have to be disabled through the control panel.

3.4 Accessing Network Shares Across Private Networks

In the special case where two networks are under Windows NT domain login security and they are in different, non-trusted domains, it is not possible to tunnel across one network to reach hosts or servers on the second network. Windows 95 logs into the first domain and cannot log in to a second domain. The workaround is to skip the initial domain login (*Cancel*) and log into the second network when the PPTP connection is established.

Note that since the Internet does not employ domain login security, this problem will not occur when tunneling across the Internet.

3.5 Multi-homed IPX Support in Microsoft Client for Networks

A PC which uses the Client for Microsoft Networks may have problems communicating with a remote IPX network over PPTP if IPX is simultaneously bound to a LAN adapter. These problems do not occur in an ordinary dial-up connection. These problems do not occur in a PC which is running the Client for NetWare Networks.

3.6 Suspend Mode for Laptop PCs

You can suspend operation of a laptop PC by selecting *Suspend* from the Start menu. Many machines offer a hardware Suspend button, but some of these do not provide adequate time for the software components of Windows 95 to safely stop operation. On some platforms, use of the Suspend feature will result in a disabled machine on Resume. You should always use the Start menu to suspend execution on any laptop.

3.7 ISDN1.0 Accelerator Pack Drivers

Windows 95 now supports ISDN NDISWAN drivers that are binary compatible with Windows NT. This has been the case since the release of the ISDN Accelerator Pack 1.1, which required the use of Windows

NT-compatible ISDN 1.1 drivers. Consequently, most ISDN vendors supply ISDN 1.1 drivers with their hardware. Drivers compatible with the Windows 95 ISDN Accelerator Pack 1.0 no longer work.

See http://www.microsoft.com/windows/getisdn for a list of known vendor drivers.

3.8 ISDN Driver Installation

Many vendors bundle the old ISDN1.1 Accelerator Pack with their own device drivers on their installation diskette to simplify the installation process. As a result, if a vendor's install procedure is run on a system that has been upgraded to 1.3, the install procedure may overwrite some of the upgraded files and leave various portions of the system unusable. Typically, the vendor install will ask you if it is OK to install ISDN 1.0 or ISDN 1.1. You should say "no".

If you think that the vendor's install has overwritten Dial-Up Networking, you should immediately re-run the Dial-Up Networking 1.3 Upgrade installation routine MSDUN13.exe.

As a general note regarding ISDN driver installation, make sure you know the ISDN switch type, SPIDs, and phone numbers. This information is available from your telephone company. You should have it before you proceed.

3.9 Multilink Operation

After your additional devices are configured using the procedure outlined in the previous section, you are ready to dial your Multilink connection. When you dial the connection, Dial-Up Networking dials the primary number of the primary device specified for the connection. Once the first connection is established, Dial-Up Networking will then dial the other devices specified in the Additional Devices list.

Once the connections are established, you can view status information about the link by double clicking on the "communicating computers" icon displayed in the taskbar, or you may disconnect the connection. The status information includes the number of bytes sent and received, the network protocols negotiated for use on the connection and a list box showing each of the additional devices. As you highlight a device in the list box, a "Suspend" or "Resume" button is displayed. If a Suspend button is displayed, then the device is now in use and "bundled" into the Multilink connection. Clicking on the "Suspend" button disconnects that line and removes the line from the bundled connections. If the "Resume" button is displayed, then click on "Resume" to dial that connection and add that line to the bundle. You may suspend and resume individual links without dropping the connection.

3.10 Limited IP-IP Dial-in Server

Previously, Windows 95 could only act as a dial up server for IPX and NetBEUI traffic. This new feature lets a Windows 95 machine answer a dial up call for machine to machine applications such as Microsoft NetMeeting (which supports application sharing, chat, video conferencing, and IP based telephony). The Dial-Up client is always assigned 192.168.55.2, and the server is always 192.168.55.1. The Point to Point IP Server is enabled by default, and can be enabled/disabled in the advanced properties for the Dial-Up Adapter.

4. Security Related Notes

PPTP employs existing PPP features to enable secure, encrypted access to a private network for selected clients on the Internet without providing access to all of the potential clients on the internet. The PPTP tunnel server controls this access by authenticating connection requests from the clients that request tunnel connections to the private network. Security can be further enhanced by enabling static PPTP filtering on the tunnel server, or by placing the tunnel server behind a firewall, or by enabling IP filtering on a Windows NT4 tunnel server equipped with the Routing and Remote Access service. See the *User and Administrator Guide on Installing, Configuring and Using PPTP with Microsoft Clients and Servers* located at: http://www.microsoft.com/communications/morepptp.htm for further information.

4.1 MSCHAP V2

This release supports a new MSCHAP (MSCHAP V2) which provides the following security features:

- Mutual authentication, based on random challenges from both server and client
- Stronger initial data encryption keys, generated from both the user's password and the random challenges from the server and the client
- Separate initial encryption keys for encrypting the transmit and receive paths
- Drops support for the MSCHAP password change V1
- Drops use of the LMHASH encoding of the password

An updated DUN client will negotiate MSCHAP V2 before negotiating the original MSCHAP. The Windows NT 4.0 server (updated as described below) will also negotiate MSCHAP V2 first, so networks with updated clients and servers will shift entirely to MSCHAP V2 authentication. To ensure that no clients authenticate using MSCHAP, the server can be set to require MSCHAP V2. This will prevent legacy clients from presenting their credentials in an MSCHAP or PAP or CHAP exchange, and is a likely configuration for networks that require the most secure authentication method.

If there are special circumstances in which you wish to ensure that your PC uses only the new MSCHAP V2 for all VPN connection attempts, a new client-side registry flag, *SecureVPN*, can be used to force this behavior. When this flag is set, your PC will only accept MSCHAP V2 authentication for any VPN connections. In addition, this flag will require data encryption for all VPN connections. Dial-up connections are not affected.

> *NOTE: Most users will not need to use the Secure VPN flag. This flag should be used with care because it will affect the behavior of all VPN connections from your machine. In general, the required use of MSCHAP V2 and data encryption can be enforced more easily on the server.*

The registry setting which will force a Windows 95 client to use only the new MSCHAP V2 secure mode and require data encryption for PPTP connections is defined below. By default, this registry variable is absent, meaning "do not force secure mode on PPTP connections". The value of this variable is checked just before a connection is attempted.

HKLM\System\CurrentControlSet\Services\RemoteAccess
Default: 0x00000000

DWORD: SecureVPN
Value: 0x00000001 == Force secure mode (MSCHAP V2 plus data encryption) on all PPTP connections
Value: 0x00000000 == Do not force secure mode on PPTP connections

4.2 LMhash Suppression

This release also provides a new registry variable which prevents the client from sending the LM response to a legacy MSCHAP challenge, as defined below. By default, this variable is absent, meaning that the client should send the LM response (in order to maintain compatibility with legacy servers). The value of this variable is checked just before a connection is attempted.

> *NOTE: Most users will not need to use this registry variable. The new secure mode MSCHAP V2 will not send the LMHash response, so this registry value is most useful when connecting to older access servers which use the original MSCHAP.*

HKLM\System\CurrentControlSet\Services\RemoteAccess

DWORD: UseLmPassword
Default: 0x00000001

0x00000000 = Do not send LM challenge response (send only NT challenge response)
0x00000001 = Send LM challenge response

4.3 PPTP Filtering

Static PPTP filtering can be enabled on a tunnel server, and if enabled, allows only PPTP packets to pass into the tunnel server. This immediately limits Internet access to PPTP clients. When setting up a tunnel server, keep in mind that the ICMP Echo packets used by ping will not pass through this filter and are simply discarded. Consequently, it may be useful to disable PPTP filtering during the shakedown period, and then enable PPTP filtering for production use.

4.4 Firewall Compatibility

PPTP traffic will pass through a properly configured firewall. The PPTP tunnel control channel uses TCP port 1723. Data packets are transmitted over IP using protocol ID 47 (GRE) with a GRE Protocol field of 0x880B. The firewall filters must be properly set to admit this traffic into the private network and to exit from the network. Note that there are a few firewall products that cannot be configured to accept protocol 47. If you need enhanced PPTP filtering capability look at the Routing and Remote Access service which can be downloaded from http://www.microsoft.com/communications .

4.5 GRE Packet Filtering

Some networks utilize GRE messages for internal operations and have set their routers to prevent GRE packets from entering or leaving the network. If the PPTP tunnel is configured correctly, but transmits no data, your Internet Service Provider may be screening GRE packets. Contact your ISP to resolve this issue.

4.6 Winsock Proxy Limitations

The Proxy Server and a RAS tunnel server can be co-located on the same server hardware. In this configuration, the Proxy Server supports local users on the LAN who wish to access the Internet in a protected manner, while the RAS tunnel server allows remote users to reach this LAN via the Internet in a secure manner.

The only limitation to this configuration is that a client on the local LAN cannot originate a tunnel to a remote tunnel server while configured to use Winsock Proxy for Internet access. It is not possible to pass a PPTP session from a client running the Microsoft Winsock Proxy through a proxy server to a remote tunnel server. In order to originate a tunnel, the client must have direct routed access to the remote tunnel server, and must disable the Winsock Proxy for the duration of the PPTP session.

5. Network Routing Behavior

When a PPTP connection is established, the client network protocols will see an additional dial-up adapter become active. PPTP itself uses TCP/IP to tunnel network packets, so at least one adapter in the client must be bound to, and running TCP/IP. This adapter can be a NIC, in the case where the client is connecting to a PPTP server on a LAN. The TCP/IP adapter can also be a dial-up adapter, in the case where the client is dialing into a RAS server or ISP, and then connecting to a PPTP server across a private Intranet or the public Internet. The client must also support the network protocol of the target (private) network. The behavior of NBF, IPX and TCP/IP clients are described below

5.1 NBF Clients

It is assumed that the PPTP client is connecting to an NT RAS/PPTP server. NetBIOS Frames (NBF) will work as expected. The PPTP client will be able to see both the original network and the new network concurrently. The client will be visible to computers on both LANs, but the networks will not be joined through the client. The client's ability to see computers on the new network is provided by the Windows NT Server's NetBIOS gateway.

5.2 IPX Clients

Once connected via PPTP, only the target network will be visible with IPX at that time. This is unchanged from current Window95 dial-up IPX connections. Currently, when IPX is selected in a phonebook entry and IPX is active on a NIC, a dialog is presented to the user (at dial time) explaining that NetWare servers on the local LAN will no longer be visible once a connection is established to the remote LAN. Users will see this same dialog when establishing a PPTP connection.

5.3 Default Routing to Remote TCP/IP Networks

All TCP/IP host computers (including your Windows 95 PC) share a routing limitation that will be important for Dial-Up and PPTP users accessing remote TCP/IP networks. Host computers rely on a routing scheme called default gateway routing. This mechanism is simple: to reach any computer not on the local network, and not specified by any other routing table entries, forward the traffic to a specified default gateway router. The gateway router generally knows how to forward the traffic correctly. This approach has the advantage that your Windows 95 computer can connect to millions of other computers without complex routing tables. This approach has the disadvantage that it assumes that there is only a single connection to all of the external networks it may wish to reach.

The default gateway concept works particularly well for a stand-alone PC that is dialing into a remote network. When a dial-up connection is established, a default gateway is assigned to route traffic through that connection.

The concept breaks down when your PC already has a default gateway, and a second default gateway is assigned by Dial-Up Networking to reach a new network. This could happen, for example, if your computer had a default route for its local LAN and then dialed an additional connection into a remote network. It could also happen if your computer dialed into the Internet and then made a second PPTP connection to a remote tunnel server. In both of these cases, the first gateway is replaced by the most recent gateway, and computers that were reachable though the first gateway will no longer be visible. Note that a DNS or WINS name server that may be one of the computers that is hidden. This will result in the inability to resolve computer names on the affected network.

In summary, TCP/IP default gateway routing is designed to work with computers that connect to a single network. A PPTP connection over a Dial-up link, or a Dial-Up connection from a LAN-based PC, result in two network connections.. In each case, the default route will point to the most recent connection. When the PPTP or Dial-Up connection is released, all connectivity to the first network will be restored.

5.3.1 Static Routes

The workaround is to add a route entry to destination network or computer by using the *route* command from a DOS prompt. For matching traffic, TCP/IP will use this route rather than the default gateway.

The following example walks through the case of dialing into an ISP and then establishing a tunnel to a private network. The abbreviated output below shows the default gateway after the dial-up connection has been established. The *ping* command is used to demonstrate that ww.microsoft.com can be reached across the Internet:

```
C:\OSR2>route print

Active Routes:

  Network Address        Netmask     Gateway Address    Interface     Metric
  0.0.0.0                0.0.0.0     206.63.152.32      206.63.152.32     1
```

(other route table entries can be ignored)

```
C:\OSR2>ping www.microsoft.com

Pinging www.microsoft.com [207.68.137.65] with 32 bytes of data:
```

```
Reply from 207.68.137.65: bytes=32 time=149ms TTL=58
Reply from 207.68.137.65: bytes=32 time=144ms TTL=58
Reply from 207.68.137.65: bytes=32 time=133ms TTL=58
Reply from 207.68.137.65: bytes=32 time=135ms TTL=58
```

The default gateway is the entry with the *Network Address* of 0.0.0.0. This is the simple case of being connected to a single network (the Internet). There is only a single default gateway.

The output below shows the assignment of a second default gateway after a PPTP connection has been established to a private network across the Internet. The more current gateway has the lowest *Metric*, and will be used to provide access to the private network. The gateway with the Metric 2 will not be used again until the PPTP connection is released.

```
C:\OSR2>route print

Active Routes:

  Network Address          Netmask  Gateway Address    Interface        Metric
          0.0.0.0          0.0.0.0    206.63.152.32    206.63.152.32       2
          0.0.0.0          0.0.0.0    192.168.70.42    192.168.70.42       1
```

The result of this is that we can no long ping www.microsoft.com:

```
C:\OSR2>ping 207.68.137.65

Pinging 207.68.137.65 with 32 bytes of data:

Request timed out.
```

Adding a static route in this form solves the problem:

```
C:\OSR2>route add 207.68.137.65 206.63.152.32

C:\OSR2>ping 207.68.137.65

Pinging 207.68.137.65 with 32 bytes of data:

Reply from 207.68.137.65: bytes=32 time=164ms TTL=58
Reply from 207.68.137.65: bytes=32 time=160ms TTL=58
Reply from 207.68.137.65: bytes=32 time=157ms TTL=58
Reply from 207.68.137.65: bytes=32 time=144ms TTL=58
```

The first number in the *route add* command is the IP address of the target computer and the second is the default gateway that has the Metric of 2.

Notice that we pinged www.microsoft.com by using the IP address returned from the previous ping, rather than the name www.microsoft.com. Why? The process of converting an Internet computer name to an IP address is called name resolution, and uses a computer on the Internet called a *Domain Name Server* (DNS). The DNS computer IP addresses was entered for this dial-up connection in the phone book entry. Unfortunately, the DNS server itself becomes invisible after the 2nd default gateway becomes active. A ping by name will fail because the DNS server cannot be contacted to resolve the name.

```
C:\OSR2>ping www.microsoft.com
Bad IP address www.microsoft.com.
```

The important thing to notice here is that the ping did not fail. It didn't even get started because the name www.microsoft.com could not be translated into an address for ping to use. Adding a route to the DNS server itself fixes this.

```
C:\OSR2>route add 198.137.231.1 206.63.152.32

C:\OSR2>ping www.microsoft.com
```

```
Pinging www.microsoft.com [207.68.137.65] with 32 bytes of data:

Reply from 207.68.137.65: bytes=32 time=164ms TTL=58
Reply from 207.68.137.65: bytes=32 time=160ms TTL=58
Reply from 207.68.137.65: bytes=32 time=157ms TTL=58
Reply from 207.68.137.65: bytes=32 time=144ms TTL=58
```

Note that some DNS servers resolve the same name to different IP addresses at different times, typically for load-balancing. The only workaround for this is to add *network* route entries for all possible IP addresses. This is beyond the scope this document.

Finally, note that since a static route references the IP address of the dial-up connection, it can only be defined once the dial-up or PPTP connection has been established.

Microsoft Dial-up Networking Upgrade

Information in this document is subject to change without notice and is provided for informational purposes only. The entire risk of the use or results of the use of this document remains with the user, and Microsoft Corporation makes no warranties, either express or implied. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The Windows 95 PPTP client is based on code developed by 3Com Corp.