Microsoft® Windows®95 Dial-Up Networking 1.2 Upgrade Release Notes

1. Windows95 Dial-Up Networking 1.2 Upgrade

The Windows®95 Dial-Up Networking 1.2 upgrade is a significant enhancement to the Dial-Up Networking features that were originally delivered with Windows95. This upgrade provides client support for a single PPTP connection, support for internal ISDN adapters, multilink capabilities, connection-time scripting to automate non-standard logins, and improved performance and stability. All of the improvements included in the OSR2 release of Windows95 and the ISDN1.1 Accelerator Pack have been included in this package.

The Windows95 Dial-Up Networking 1.2 upgrade replaces all of the Dial Up Networking components, and installs new versions of the TCP/IP stack and the NDIS layer. A new version of Winsock is included as an optional component in order to correct name resolution limitations in the original Windows95 software.

This Dial-Up Networking 1.2 upgrade can be applied to existing Window95 systems, including the retail release and OEM Service Release 2 (OSR2). This package cannot be used to upgrade a Memphis Developer's Release or future Memphis beta releases. (Note that the features provided by this Dial-Up Networking Upgrade are already present in the Memphis Developer's Release.)

1.1 Installation Notes

To install the upgrade, simply execute the MSDUN12.exe file and follow the instructions. The installation process will require you to reboot the machine, and may ask for your Windows95 installation disk (if you originally installed Windows95 from a CD.) If you encounter a "do you want to keep a newer file" dialog, always keep the newer file. After the boot, you will see a DHCP error message asking if you wish to see future DHCP error messages. (Select "yes".)

Beta users can install the Dial-Up Networking 1.2 upgrade over a previous beta version of the upgrade without removing the previous version.

Once the installation is complete, you will be able to remove the Dial-Up Networking 1.2 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 Windows95 version of Dial-Up Networking by using the windows setup tab of the "Add/Remove Programs" icon. Alternately, you can re-install the 1.2 upgrade by executing the MSDUN12.exe file.

Note that an uninstall of the Dial-Up Networking 1.2 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.

2. Feature Overview

2.1 ISDN Support

This release 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 any benefit that could be gained from simultaneous use of two modem calls. Multilink can be 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

This release 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 which uses an incompatible protocol or which is under the administrative control of a third party.

2.4.1 PPTP Tunneling

PPTP is a tunneling protocol defined by the PPTP Forum that 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 Windows95 PPTP client, you must be able to establish an IP connection with a tunnel server such as the WindowsNT® 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, IPX) can be run concurrently. WindowsNT Domain Login level security is preserved even across the Internet. PPTP can be used to connect to an Intranet that is otherwise isolated from the Internet, and may even have 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.

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 *pptpinfo.doc* in your windows directory.

2.5 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 network through a modem pool on the tunnel server.

If your systems administrator has configured the tunnel 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 network. To cause such a connection, simply establish a PPTP connection whose tunnel address is specified as "TunnelServer<space>PhoneNumber". TunnelServer is the DNS name or IP address of the tunnel server; PhoneNumber is the set of digits to be dialed to reach the other network. The tunnel 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 network. Authentication will be performed by the remote network. Again, see the discussion below regarding *Default Routing to Remote TCP/IP Networks* or the more detailed discussion in the file *pptpinfo.doc*.

3. Known Bugs and Limitations

There are a number of network routing issues, known bugs and product limitations that affect network behavior when you are using Windows95 Dial-Up Networking. Network routing issues are discussed in the *Default Routing to Remote TCP/IP Networks* section below. Bugs and product limitations are discussed in this section.

3.1 Name Resolution Issues

The original release of Windows95 Dial-Up Networking had limited support for WINS and DNS name resolution when a PC was connected to multiple networks. The Dial-Up Networking 1.2 Upgrade resolves all of the WINS limitations, and supplies a Winsock upgrade which you can install to resolve the remaining DNS limitations.

A Winsock update installer (ws32upd.exe) has been placed in your windows\msdun directory. Simply execute the installer and it will install a revised Winsock on your system. This is a clean solution for most users. However, there are a few network or internet applications which replace Winsock with their own version, or which use “hooking and chaining” techniques to attach their own features to the Microsoft version of Winsock. You should uninstall such applications before running the Winsock installer, then re-install them when Winsock has been updated. The Winsock Proxy component of Microsoft Proxy Server is an application of this sort. You should uninstall Winsock Proxy before updating Winsock, then re-install it when you are finished.

The Winsock update installs a revised version of Winsock 1.1. This version represents a minor change over the Winsock that was originally delivered with Windows95. Microsoft has also released Winsock2, a complete redesign of the Winsock architecture. Winsock2 is available from the Microsoft web site at www.microsoft.com. It is fully compatible with the Dial-Up Networking 1.2 Upgrade

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 when you successfully establish a PPP or PPTP connection. In the rare cases where an ISP or systems administrator require 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.) You should never set these TCP/IP properties for one of the Dial-up Adapters or your LAN adapter 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 will prevent these DNS addresses from being displayed.)

3.3 Remote Access after Physical Disconnection from a LAN

A 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 which 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 WindowsNT 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. Window95 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 Setting Encryption on Dial-up or PPTP Connection

There is no user control over encryption in the Windows95 Dial-Up Networking client. Encryption is controlled by appropriate settings in the Windows NT Remote Access Server. Due to a bug in the Windows95 client, encryption must be requested with compression. The server will not be able to negotiate encryption without compression. (Note that the server can enable compression without encryption.)

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 Windows95 to safely stop operation. This will result in a crash on Resume. You should always use the Start menu to suspend execution on the laptop.

3.7 Ejecting PCMCIA Net Cards

If you eject a PCMCIA ethernet card from a running laptop, then make a subsequent dial-up connection to a TCP/IP network, you will find that TCP/IP traffic is disabled. No problem occurs if you eject the card while the machine is off, or if you eject the card during a successfully established TCP/IP connection.

3.8 ISDN1.0 Accelerator Pack Drivers

Windows95 now supports ISDN NDISWAN drivers that are binary compatible with WindowsNT. This has been the case since the release of the ISDN Accelerator Pack 1.1, which required the use of WindowsNT-compatible ISDN 1.1 drivers. Consequently, most ISDN vendors supply ISDN 1.1 drivers with their hardware. Drivers compatible with the Windows95 ISDN Accelerator Pack 1.0 will no longer work.

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

3.9 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 1.2, 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 1.2 Upgrade installation routine MSDUN12.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.

3.10 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.

3.11 Dial-in Server Limitations

The Windows 95 Dial In Server supports only IPX and NetBeui clients. There is no support for a dial-in TCP/IP client. Not that the Dial-in Server feature does not support multilink connections.

4. Security Issues

PPTP provides a new level of security by employing 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 which request tunnel connections to the private network. Security can be further enhanced by enabling PPTP filtering on the tunnel server, or by placing the tunnel server behind a firewall. See the *User and Administrator Guide on Installing, Configuring and Using PPTP with Microsoft Clients and Servers* for further information.

4.1 PPTP Filtering

PPTP filtering can be enabled on the 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.

4.2 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 which cannot be configured to accept protocol 47.

4.3 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 tunnel established correctly, but transmits no data, your Internet Service Provider may be screening GRE packets.

4.4 Proxy Incompatibility

It is not possible to pass a PPTP session from a client through a proxy server to a remote tunnel server (or vice versa). However, in many cases, one can achieve the same results by hosting a PPTP Tunnel Server and a Proxy Server on the same hardware server.

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. 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 WindowsNT 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 Windows95 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 Windows95 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 which 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.
