# Microsoft® Windows®95 Dial-Up Networking 1.4 Upgrade Release Notes

## 1. Introduction

The Dial-Up Networking 1.4 Upgrade (DUN 1.4) provides additional features for the Dial-Up Networking components that were first introduced in Windows 95. The 1.4 release includes all of the features of all previous DUN releases, as well as those included in the ISDN 1.1 release. DUN 1.4 features include PPTP client support, 128-bit encryption, support for internal ISDN adapters, multilink support, and connection-time scripting to automate non-standard login connections. The DUN 1.4 upgrade can be applied to any version of Windows 95. It will not install on any other version of Windows, such as Windows 98.

## 1.1 New Features in DUN 1.4

1)128-bit encryption supported with the Dial-Up Networking 1.4 Upgrade.

2)The Dial-Up Networking 1.4 Upgrade includes several fixes to improve the stability of PPTP connections.

3)A Year 2000 fix for the DHCP Client has been included in the DUN 1.4 Upgrade

## 1.2 Installation Notes

Execute the MSDUN14.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 1.4 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 1.4 upgrade by executing the MSDUN14.exe file.

> *Note: An uninstall of the Dial-Up Networking 1.4 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.

> *NOTE: The Dial-Up Networking 1.4 Upgrade relies on features in a more 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.*

# 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. 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.

## 2.4 PPTP Client

### 2.4.1 PPTP Tunneling

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 a 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.

#### 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 is used 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.

## 2.5 Per-Connection Encryption Settings

The DUN 1.4 upgrade adds the ability to require encryption for a specific connection. 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. 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.

## 2.6 Other Features in the DUN 1.4 Release

1)Limited server functionality for a dialup Point to Point IP connection is enabled.
2)Additional information is available to 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.
3)You can turn on an improved PPP logging option on a per connection basis. Results are logged to PPPLOG.TXT in your Windows directory.

# 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 1.4 Upgrade resolves all of the WINS limitations, and applies a Winsock upgrade to resolve the remaining DNS limitations.

Microsoft has also released Winsock2, a complete redesign of the Winsock architecture. Winsock2 is fully compatible with the Dial-Up Networking 1.4 Upgrade. If Winsock2 has already been installed, the Dial-Up Networking 1.4 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 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.

> *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 ISDN1.0 Accelerator Pack Drivers

Windows 95 now supports ISDN NDISWAN drivers that are 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.

## 3.7 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 DUN 1.4, 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 1.4 Upgrade installation.

## 3.8 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.

## 3.9 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:

1)Mutual authentication, based on random challenges from both server and client
2)Stronger initial data encryption keys, generated from both the user’s password and the random challenges from the server and the client
3)Separate initial encryption keys for encrypting the transmit and receive paths
4)Drops support for the MSCHAP password change V1
5)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 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.

## 4.2 PPTP Connections Through Firewalls

Some networks utilize GRE messages for internal operations and have set their routers to prevent GRE packets from entering or leaving the network. PPTP traffic uses TCP port 1723 and routing protocol 47. If the PPTP tunnel is configured correctly, but transmits no data, your Internet Service Provider may be screening GRE packets, or the necessary port may be blocked.  Contact your ISP to resolve this issue.

# 5. Network Routing Behavior

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.

# 6.  Additional Information for Advanced Users

## 6.1 LMhash Suppression

This release also provides a 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

## 6.2 The SecureVPN Flag

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

## 6.3 The Force Strong Encryption Flag

A new registry variable, ForceStrongEncryption, has been provided to allow the client to require strong encryption. 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.

## 6.4 PPTP Historyless Mode

A historyless mode for encryption & compression over PPTP connections is available. This mode solves performance problems encountered using PPTP in high latency networks or networks that experience significant packet loss. To negotiate historyless mode, both the PPTP client and server must support the new mode. If either side refuses the new mode, normal MPPE compression and encryption will be negotiated. Be sure that servers supporting historyless clients are running Windows NT 4.0 Service Pack 3 or later, or Windows 2000.

## 6.5 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 computer or network through a modem pool on an appropriately configured access server. To initiate 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

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

## 6.6 Packet Size Adjustment

The IP Packet size for dial-up connections is 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 Windows 95 PPTP client is based on code developed by 3Com Corp.