

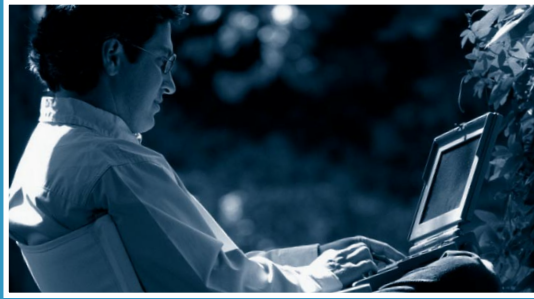
mightywords™

technical

briefings

Glenn Weadock

Mobile Computing and Windows 2000 Professional



MightyWords Technical Briefings: Mobile Computing and Windows 2000 Professional

By Glenn Weadock

Copyright © Glenn Weadock 2001
All rights reserved

Published by MightyWords, Inc.
2550 Walsh Avenue
Santa Clara, CA 95051
www.mightywords.com

ISBN 0-7173-0390-X

Executive Summary

Windows 2000 Professional is quickly catching on as the serious computer user's "road warrior" Operating System (OS) of choice. One big reason is that this latest version of Windows includes a number of notebook-friendly features, including communications tools for dial-up networking.

Why use Windows 2000's built-in communications software? Cost and consistency are the two big benefits. Although many Internet Service Providers (ISPs) offer dozens of megabytes of add-on software to configure PCs for dial-up access, Windows 2000 Professional contains everything most users need. Adding third-party communications software increases cost and reduces consistency of setup because different employees may use different ISPs. Also, training is less expensive if all dial-up communications use the features provided with Windows 2000.

Despite these benefits, setting up the operating system to dial into a corporate network, Virtual Private Network (VPN) or even an Internet service provider isn't necessarily simple. This article explains the key steps to setting up these three types of dial-up accounts and includes troubleshooting tips for frequently encountered problems. The article also discusses the steps for installing, testing, and configuring a modem on a portable Windows 2000 machine, in case one is not already set up (or set up properly).

Table of Contents

Chapter 1: Modem Installation	1
1. Installing a Modem Driver	1
2. Testing Your Modem	2
Chapter 2: Modem Configuration	4
1. Setting Buffers	4
2. Compression Options	6
3. Speed Settings	7
4. Flow and Error Control	8
5. Dialing Locations	10
6. Multilink Setups	11
Chapter 3: Connecting to a Private Network	13
1. How to Create a Dial-Up Link	13
2. Choosing Network Components	17
3. Configuring TCP/IP	21
4. Configuring the Modem	23
Chapter 4: Connecting to a Virtual Private Network	25
1. The VPN Concept	25
2. How to Create a VPN Link	25
3. VPN Encryption	27
Chapter 5: Connecting to an Internet Service Provider	28
1. How to Create an ISP Link	28
2. Choosing Network Components	29
3. Configuring TCP/IP	32
4. Configuring the Modem	33
Chapter 6: Troubleshooting Dial-Up Connections	35

1. Enabling Modem Logging	35
2. Event Log Messages	36
3. Using IPCONFIG	36
4. Troubleshooting Authentication Failures	38
5. Things to Try When the Problem Isn't Obvious	39
About the Author	40

Chapter 1

Modem Installation

Modem installation consists of two phases: The first is installing the driver (the software component that lets the operating system communicate with the hardware), and the second is testing the driver-modem combination.

1. Installing a Modem Driver

How It Should Happen

Generally, installing a modem driver onto a Windows 2000 Professional computer is just a matter of plugging in the hardware (generally into a PC Card slot) and restarting the operating system (Start→Shut Down→Restart). Windows 2000 will autodetect the new modem via Plug and Play and install the appropriate device driver. If the driver isn't a common one (and therefore not present in the DRIVER.CAB archive on your hard drive), Windows will ask you to supply the Windows 2000 CD-ROM so the operating system can get the driver from the CD.

Plug and Play makes adding, configuring, and removing devices easier and more automatic—at least when it works. Plug and Play's goal is to let such users plug and unplug devices as they need to without having to worry about installing or uninstalling device drivers, manually resetting resource assignments (interrupts, memory addresses, etc.), or restarting their computers.

What Can Go Wrong

Plenty of things can go wrong. Plug and Play requires support at all levels—computer hardware, BIOS (Basic Input/Output System), bus, operating system, device driver, and device. Windows 2000 looks at the first two items at setup time and installs the appropriate Hardware Abstraction Layer (HAL).

The biggest factor is that Windows 2000 Plug and Play works best with PCs that support the Advanced Configuration and Power Interface (ACPI) standard. Older

computers that support Advanced Power Management (APM) aren't as compatible with Plug and Play and may not work well with Windows 2000. You can tell what kind of PC you have by clicking on the + sign next to the computer icon at the top of the Device Manager hardware tree (right-click My Computer, choose Properties, click on the Hardware tab and click on the Device Manager button, then expand the System Devices icon).

You usually can't do anything to change an APM machine into an ACPI machine, but sometimes updating the BIOS has this effect. You'll need to reinstall Windows 2000 for the change to take effect. Check with your hardware vendor to see if a BIOS upgrade can make your system appear to be ACPI-compliant to Windows 2000.

Removing and reinstalling a Plug and Play driver may be necessary if you chose the wrong driver file when you originally installed the device. Uninstall the driver using Device Manager, then restart the system and let Windows 2000 autodetect the device again. At that time, you can provide the proper driver files (i.e., on a CD supplied by the modem maker).

Note: Plug and Play can normally install devices even if you're not logged on as an Administrator, as long as the computer doesn't have to ask you for the location of a device driver. In that case, you must be an Administrator. You always have to log on as Administrator to install devices via the Add/Remove Hardware wizard in the Control Panel.

ACPI machines support dynamic reconfiguration of PC Card devices, meaning you can plug in and unplug these devices without having to reboot. PC Card modems often require you to install a COM port driver before you can install the modem driver itself.

2. Testing Your Modem

Once you have the driver installed, you're well advised to take your modem for a spin before putting it to the test. Windows 2000 includes a little-known diagnostics utility in the Phone and Modem Options control panel.

1. Choose Start → Settings → Control Panel → Phone and Modem Options.
2. Click on the Modems tab.
3. Click on the modem of interest and click on the Properties button.
4. In the properties window, click on the Diagnostics tab.
5. Click on the Query Modem button.

After a few moments, you should see a series of commands and responses as shown in **Figure 1**. If you don't see them, Windows isn't communicating with your modem, which means you haven't past square one yet. Check the Device Manager window to see if a yellow exclamation point or red "X" appears next to the modem. If so, you have a conflict with another device.

Tip: The details in the command/response window may tell you the firmware version of your modem. Occasionally modem manufacturers provide user-installable firmware updates (check the modem manufacturer's Web site). This window could save you from installing a firmware "update" that is the same as the one you already have.

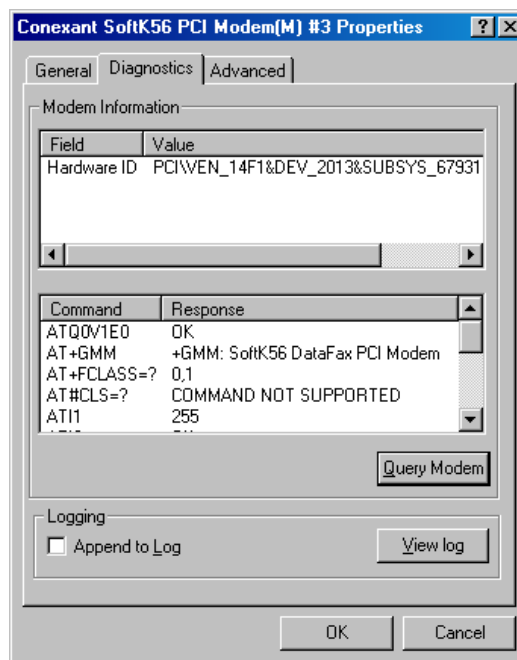


Figure 1: Diagnostic tab

Chapter 2

Modem Configuration

Once you have installed your modem's hardware and driver correctly in Windows 2000, you can set various configuration options that can determine how well—or even whether—you can connect to the desired remote computers.

Note: While you should set these options in the Phone and Modem Options control panel, you can also modify many of them on a per-connection basis. You can do so by modifying the properties sheets for individual connection icons that you create with the Make New Connection wizard in the Network and Dial-Up Connections folder. (Later sections provide details on how to make such connection icons.)

1. Setting Buffers

The various Advanced Port Settings appear when you click on the Advanced tab of the modem's properties sheet in the Phone and Modem Options control panel and click on the Advanced Port Settings button (see **Figure 2**).

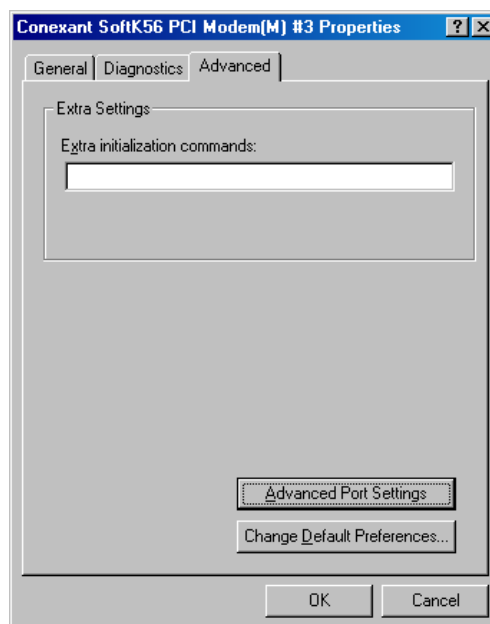


Figure 2: Advanced tab

However, if you have a modem that connects to a separate serial port, you won't see the Advanced Port Settings button in this location. In this case, you must open Device Manager (Start→Settings→Control Panel→System, click on the Hardware tab, then click on the Device Manager button), expand the Ports branch, right-click the COM port that your modem uses, and choose Properties. Choose the Port Settings tab, and there's the Advanced button (see **Figure 3**).

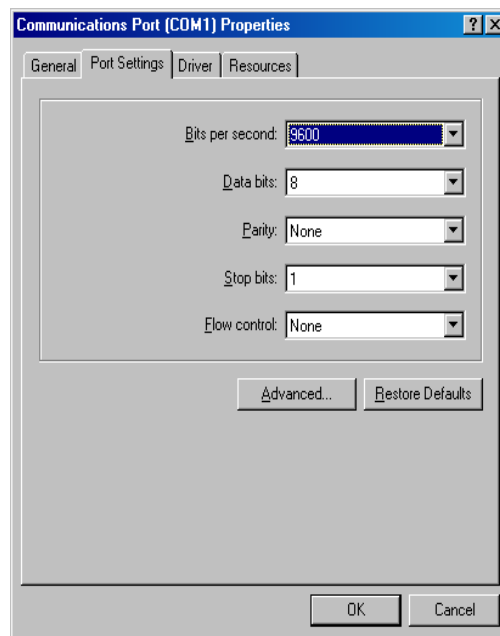


Figure 3: Port Settings tab

However you get there, the dialog box looks like the one in **Figure 4**.

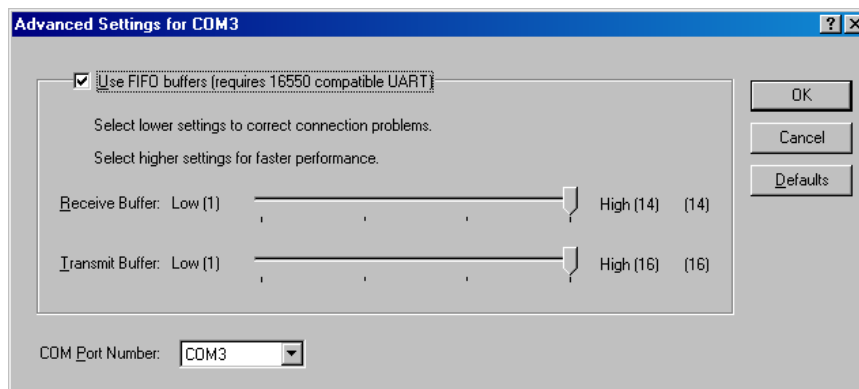


Figure 4: Advanced Settings Dialog box

These settings are as follows:

- **Use FIFO buffers (requires 16550 compatible UART).** This setting should almost always be checked. As long as your PC was manufactured after, say, 1994, it is almost certain to use a “16550 compatible UART,” which is just a fancy way of saying “quick serial port chip.” If you have a really, really old modem or PC, you may have to disable this check box; let your modem installation manual be your guide.
- **Receive Buffer and Transmit Buffer.** I always peg these sliders to the maximum setting unless I have connection problems, in which case I back off the receive buffer one notch. I’ve never seen a situation in which it was necessary to back off the receive buffer more than that.

2. Compression Options

Compression settings are made on the properties page of an individual connection icon rather than in the Phone and Modem Options control panel. The reason for this is that the appropriate compression setting may vary depending on the type of communications server you’re dialing into.

Open the modem configuration dialog box by taking the following steps:

1. Choose Start→Settings→Network and Dial-Up Connections.
2. Right-click the connection icon for which you want to set error control.
3. Choose Properties.
4. Click on the General tab (it should appear by default).
5. Click on the modem of interest and click on the Configure button.

You should see a dialog box like the one in **Figure 5**.

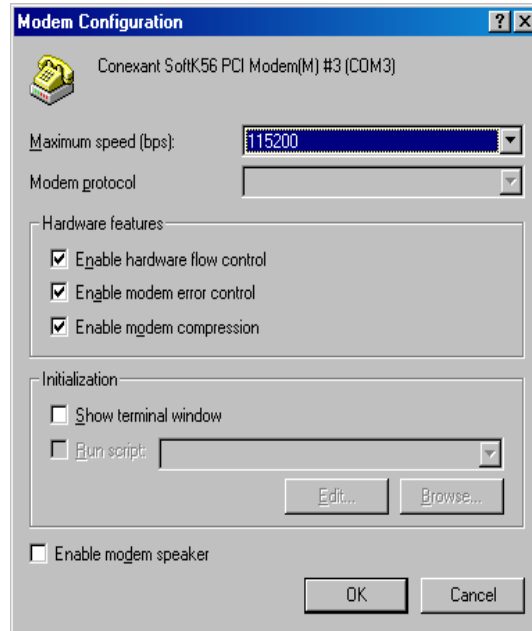


Figure 5: Modem Configuration tab

The last checkbox under Hardware Features, *Enable modem compression*, turns the feature on when checked. I usually recommend that you leave this setting off (cleared) if you normally upload or download pre-compressed files, such as ZIP archives. If your remote computing sessions don't involve file uploading or downloading, you may experiment with activating this setting to improve performance somewhat. However, hardware compression has been known to make connecting to remote computers less reliable under Windows 2000 and earlier versions of Windows.

Note: This setting refers to hardware compression only; that is, software compression may very well be used between two systems even if hardware compression is off. (Typically software compression is set using the Point-to-Point Protocol (PPP) properties page, which you access via the Networking tab of the connection's properties page.)

3. Speed Settings

The *Maximum Port Speed* setting appears on the General tab of the modem's properties sheet in the Phone and Modem Options control panel (see **Figure 6**). This

setting defines the speed—in bits per second (bps)—at which your computer communicates with the modem (the *Data Terminal Equipment* (DTE) speed) as distinct from the speed at which your computer communicates with the remote modem (the *Data Communications Equipment* (DCE) speed).

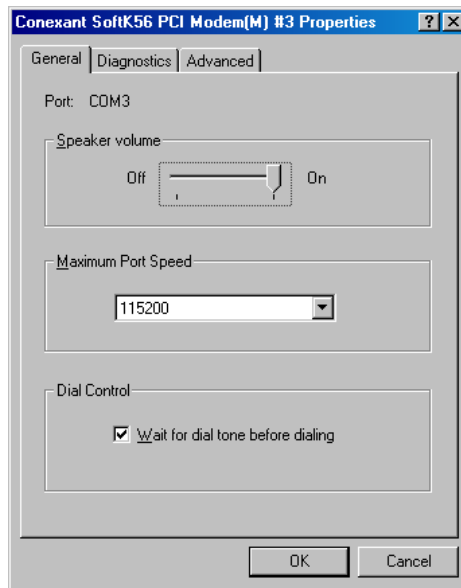


Figure 6: Maximum Port Speed Setting

I generally recommend leaving this at the default setting of 115,200 bps for a V.90, K56 or x2 modem. Having said that, some ISPs have advised me that changing this setting to 57,600 may result in more reliable connections. Put this advice under the category of “things to try if nothing else seems to work.”

4. Flow and Error Control

Error control settings are made on the properties page of an individual connection icon rather than in the Phone and Modem Options control panel. The reason for this is that the appropriate error control setting may vary depending on the type of communications server you’re dialing into.

Open the modem configuration dialog box by taking the following steps:

1. Choose Start → Settings → Network and Dial-Up Connections.

2. Right-click the connection icon for which you want to set error control.
3. Choose Properties.
4. Click on the General tab (it should appear by default).
5. Click on the modem of interest and click on the Configure button.

You should see a dialog box like the one in **Figure 7**.

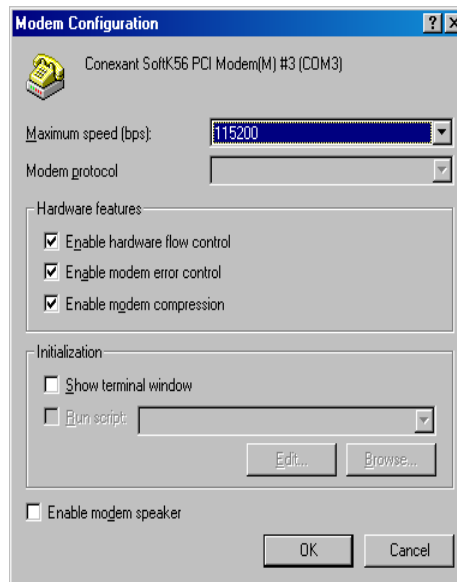


Figure 7: Modem Configuration Dialog box

The relevant settings for flow and error control are as follows:

- **Enable hardware flow control:** Another way of saying, “use hardware handshaking.” This means that the computer uses a dedicated wire (or circuit trace, with an internal modem) to prevent overflow conditions—that is, data coming into the modem faster than the modem can handle it. You want this box enabled (checked) unless the modem manufacturer, ISP, or network manager of the network you’re dialing into specifically advises against it.

Note: You may need to turn this feature off if you’re using an external modem and you don’t have a serial cable that wires all pins straight through. Normally, with a proper modem cable, you always want hardware flow control to be activated.

- **Enable modem error control:** Specifies that you want your modem to perform its own error-checking of the data stream. While this setting generally increases the connection's reliability, it can also slow performance somewhat, so I recommend leaving it cleared (off) unless you encounter problems.

The error correction protocols Windows 2000 Professional supports are MNP2, MNP3, MNP4, and V.42. Normally Windows 2000 negotiates with the remote computer to support the highest-performing error control protocol supported by both modems.

5. Dialing Locations

Configuring Windows 2000 for your dialing location (or locations) is a task you normally perform when adding a modem driver via the Modems control panel or the Add New Hardware wizard. However, you may need to change these settings if your dialing properties change or if you want to add one or more new dialing locations.

Dialing rules are available to all Windows applications that support Telephony Application Program Interface (TAPI). Other TAPI-compliant programs are Microsoft Outlook Express and Microsoft Network (MSN). Also, dialing rules are *global*. If you change the location in the Phone and Modem Options control panel, the dialing rules change for all dial-up connections you have created.

Modify dialing rules as follows: Open Phone and Modem Options in the Control Panel and click on the Dialing Rules tab. Click on the location of interest (only one may appear) and click on the Edit button. A dialog box similar to **Figure 8** below will appear.

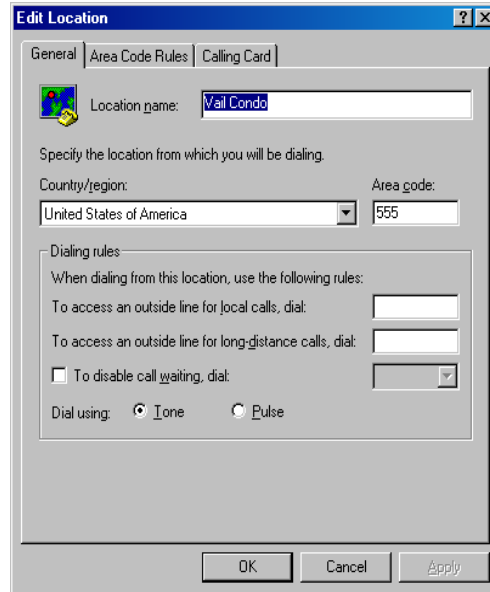


Figure 8: Edit Location Dialog box

Change dialing rules whenever you move your PC to a new location that has different ones (i.e., a different area code). You can specify for each dialing location whether Windows 2000 needs to dial an area code for local calls—which is becoming increasingly more common—with the Area Code Rules tab. You can also specify calling card information via the Calling Card tab. This information is location-specific, as well.

6. Multilink Setups

If you have more than one communication device, you can specify more than one hardware device for a given connection. You could use two modems to create a *multilink* connection by checking both of them on the General tab in the properties sheet for a given connection icon (see **Figure 9**). (Other multilink settings live on the Options tab, for some odd reason.)

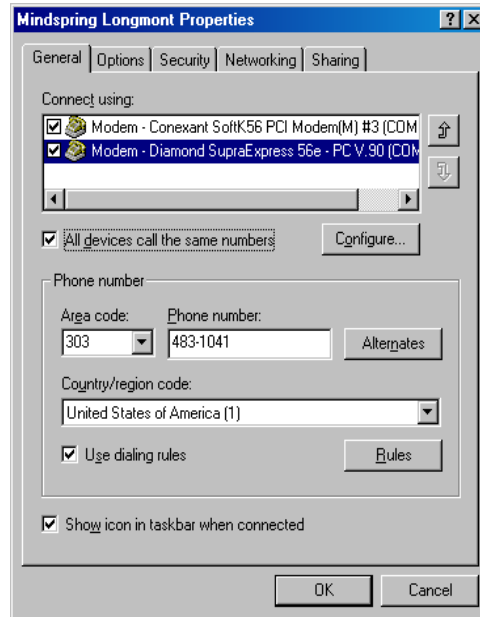


Figure 9: General tab

If both modems should call the same phone number, click on the *All devices call the same numbers* checkbox. Otherwise, clear the checkbox and enter the appropriate phone number for each modem by highlighting the modem and filling in the Phone Number fields as necessary.

For multilink setups to work, they must be supported on both ends of the connection. That is, if you're dialing into an ISP, the ISP must support multilink (unfortunately, many don't). If you're dialing into a private corporate network that uses Windows 2000 Server as a communications server, you can use multilink.

Chapter 3

Connecting to a Private Network

This section discusses how to create a connection to a private network, such as a corporate headquarters Local Area Network (LAN), from your mobile Windows 2000 Professional computer.

1. How to Create a Dial-Up Link

Windows 2000 lumps all connections—local and remote, regardless of media—into a single folder, Network and Dial-up Connections. Get there faster by right-clicking My Network Places and choosing Properties. You'll see a window that looks something like the one in **Figure 10** below. All connection settings are here in one place—no need to bounce around between a Dial-up Networking folder and a Network control panel as in earlier versions of Windows.

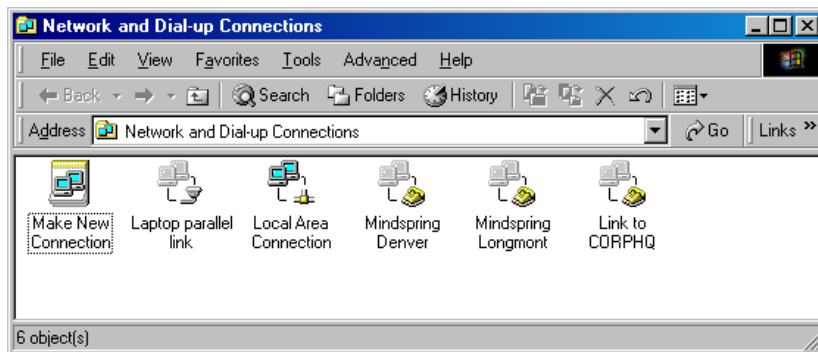


Figure 10: Network and Dial-up Connections Dialog box

Note: This folder is where you configure both inbound and outbound connections, for Windows 2000 Professional can host incoming sessions as well as dial out to other networks. Most mobile computer users are primarily concerned with outbound connections, so that's what this article will focus on.

Each connection you create has its own communications settings (with a few exceptions, such as dialing rules). That is, one connection can have a different set of DNS server addresses on its Transmission Control Protocol/Internet Protocol (TCP/IP) property sheet than another connection. Generally, if a given setting isn't connection-specific but instead is global, the relevant property sheet will advise you accordingly.

Creating the Connection Icon

Microsoft has provided a Make New Connection wizard that gets you through most of the initial configuration. Here's the procedure for creating a dial-up connection icon to connect to a private network, such as a corporate office (see **Figure 11**).

1. Right-click My Network Places and choose Properties.
2. Double-click the Make New Connection icon.
3. Click on Next to get past the verbiage.

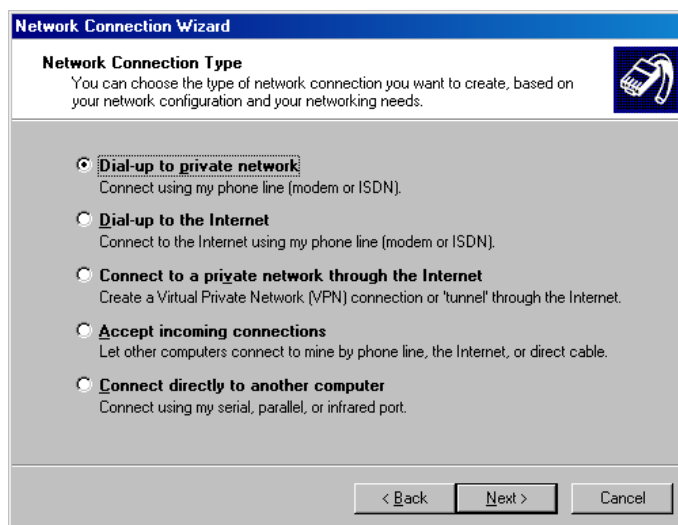


Figure 11: Network Connection Wizard box

4. Click on the *Dial-up to private network* button and click on Next.
5. If you have more than one dial-up device, choose the one you want for this connection and click on Next.

6. Enter a phone number to dial and click on the checkbox if you want this connection to follow the dialing rules you set in the Phone and Modem Options control panel. Click on Next.
7. Specify whether you want all users of this PC to have access to the connection or only you. Click on Next.
8. Type a name for the new connection. Check the checkbox if you want Windows to add a shortcut icon to your desktop.
9. Click on Finish, and Windows will create a new icon in the Network and Dial-up Connections folder.

At this point your connection exists, but you still need to configure various options as well as your network protocol settings.

Setting Connection Options

Right-click the connection icon you created and choose Properties to configure connection options, which appear on the Options tab (see **Figure 12**).



Figure 12: Options tab

If you clear the *Prompt for name and password, certificate, etc.* checkbox, Windows won't give you the chance to enter a username or password the next time you run it (see **Figure 13** below, which shows the default behavior with the box checked). Windows will just use the previous settings you used or pull your authentication data from a Smart Card reader if you have one. Check this option if you want to ensure maximum security in case of theft.

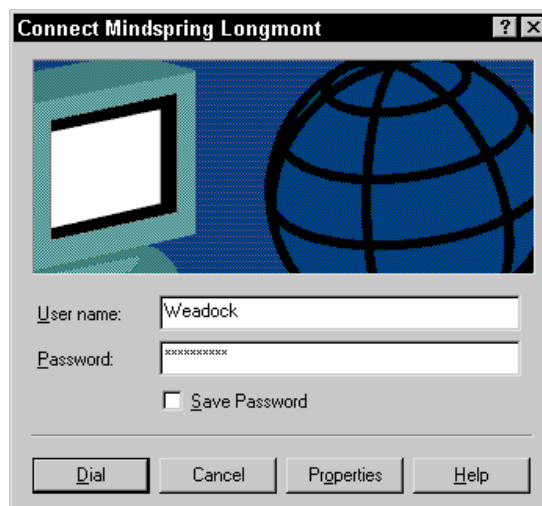


Figure 13: Default Connect Mindspring Longmont Dialog box

Because you're dialing into a private network, you may want to check the *Include Windows logon domain* box. This option lets you choose a domain if you're also prompting for username and password. Use this if you're dialing into a Microsoft network and you want users to be able to choose different domains into which to log on.

The *Prompt for phone number* option is convenient for notebook users because it lets them choose a different phone number and/or dialing location before making the connection.

As for the redial options, just be aware that Internet Explorer overrides the connection's redial settings with its own redial settings, which you reach via the Internet Options control panel.

2. Choosing Network Components

Your Windows 2000 Professional computer can communicate over the modem in exactly the same ways that it communicates over a network interface card—by sending and receiving TCP/IP packets, NetBIOS Extended User Interface (NetBEUI) packets, Internetwork Packet Exchange Protocol/Sequencing Packet Exchange Protocol (IPX/SPX) packets, etc. Your network link is just a communications device that connects to a cable. Therefore, you must configure a dial-up connection to find out which network components it should use. Do this on the Networking tab of the connection’s properties page (see **Figure 14**).

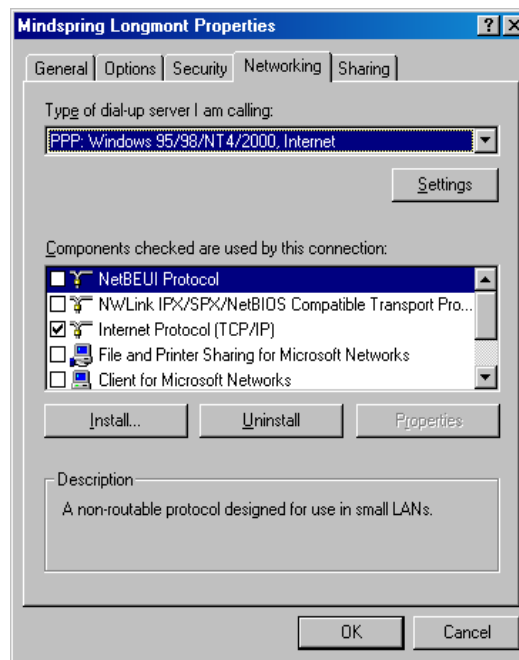


Figure 14: Networking tab

Specifying Server Type

The *Type of dial-up server I am calling* setting at the top of the Networking tab is the place where you specify the connection protocol, or communications protocol. This is a protocol you need for dial-up lines but don’t need for hardwired LAN links. The choice you make here is determined by the kind of computer (server) you’re dialing into such as:

- **Point-to-Point Protocol (PPP):** This is the default choice for dial-up connections because it's the most reliable, secure and efficient. Unlike SLIP, PPP supports error checking. It works with NetBEUI, IPX/SPX and TCP/IP network protocols.
- **Serial Line Interface Protocol (SLIP):** Use this if you have a UNIX server running. SLIP is old, slow and a bad choice unless you're calling up an old, slow UNIX server that doesn't work with PPP. SLIP offers no error correction, no encrypted passwords and no automatic IP address assignment.

Installing and Activating Components

If you want to connect to a corporate network, you need a *transport protocol* (the same as your corporate network uses—i.e., TCP/IP) plus a *networking client* (again, the same as the corporate network uses—i.e., *Client for Microsoft Networks*).

The procedure for installing these components, if they're not already present, is to right-click the connection icon, choose Properties, click on the Networking tab and click on the Install button. Follow the prompts to install the module you need.

If the components are already present but their checkboxes are clear, that means the software is present but not activated for that particular connection. Simply check the box to activate the component.

If you want to share resources with the computer or computers you're connecting to, you need the File and Printer Sharing for Microsoft Networks service. This installs the same way you'd install a transport protocol or networking client, except you'd choose *Service* instead of *Client* or *Protocol*.

Note: A good way to improve a connection's log on speed is to uncheck the protocols, clients and services you know you won't use over a given connection. You should almost always activate only one network protocol for any given connection icon.

Configuring Logon

The Security tab lets you specify how Windows 2000 should handle the authentication, or logon, phase of the connection (see **Figure 15**).

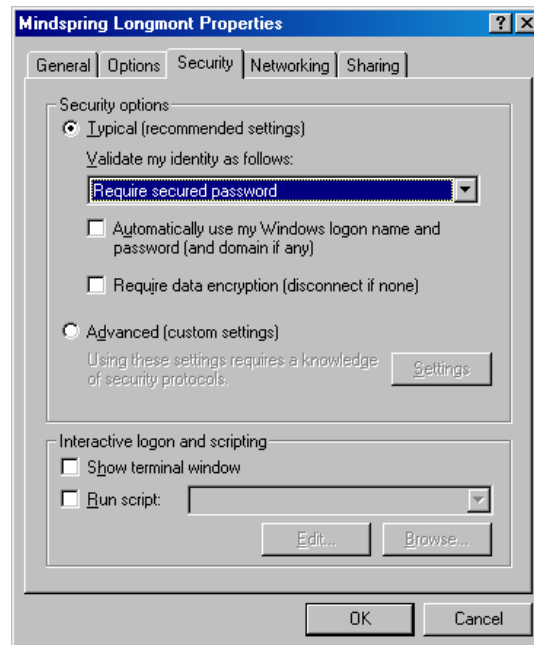


Figure 15: Security tab

Selecting *Allow unsecured password* in the drop-down list within the Security Options part of the dialog box makes the other two settings just below the list box appear grayed-out, as they are then irrelevant. If you choose *Require secured password*, which lets you make a connection only if the remote computer also supports encrypted passwords, you can set both of these settings. If you choose *Use Smart Card*, you can only set the data encryption checkbox.

As you're dialing into a private network, check the box labeled *Automatically use my Windows logon name and password (and domain if any)* if your network is a Microsoft network. Your domain credentials (username and password) authenticate you, as long as you log on to Windows with an account that is known on the remote server.

The *Require data encryption (disconnect if none)* checkbox means that if the remote computer supports *Data Encryption Standard (DES)*, the entire communications session will be encrypted and secure. The protocols that support encryption are MS-CHAP, MS-CHAPv2, and EAP/TLS.

If the network to which you're connecting has very specific security requirements, Windows 2000 lets you get more detailed. Specifically, the *Advanced (custom settings)* radio button leads to the dialog box in **Figure 16**.

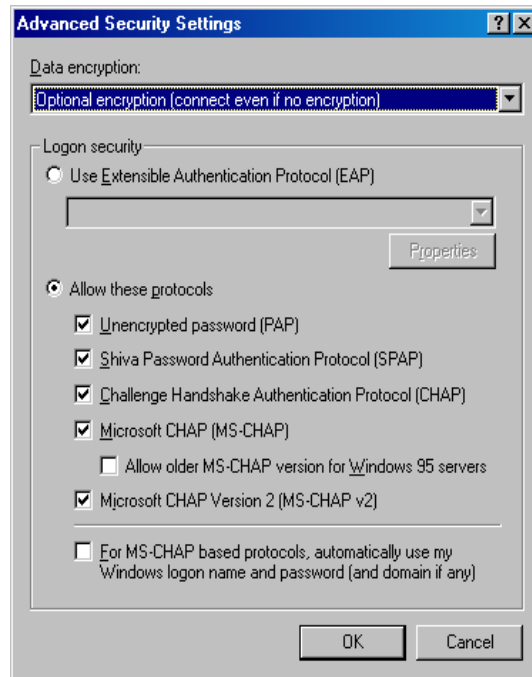


Figure 16: Advanced Security Settings Dialog box

At the top of this dialog box, you can choose one of three DES settings that apply to the entire communications session (i.e., require encryption—use it if it’s available or require that it *not* be used).

Here’s a rundown of the acronyms you will find in the Logon Security area:

- **Extensible Authentication Protocol (EAP):** An extension to PPP; it evolved to support Smart Cards and other related devices. With EAP, client and server negotiate an authentication method—such as Transport Level Security (TLS), a Smart Card authentication standard.
- **Password Authentication Protocol (PAP):** Uses no password encryption and may be required for dialing up non-Windows systems. Passwords cross the wire in “cleartext” (that is, unencrypted), so PAP is a low-security protocol.
- **Shiva Password Authentication Protocol (SPAP):** Used for dialing into and out of Shiva (a brand name) communication products. It doesn’t support data encryption but does perform password encryption. SPAP is a medium-security protocol.

- **Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP):** Works with Windows 9x and NT 4 as well as Windows 2000. It authenticates the client and uses one-way encryption.
- **MS-CHAPv2:** Another Microsoft protocol; this extension of MS-CHAP authenticates both client and server. MSCHAPv2 is required over MSCHAPv1 for encrypted PPP or Point-to-Point Tunneling Protocol (PPTP) connections.

When setting up a Smart Card, choosing EAP on the Advanced Security Settings dialog box forces you to also choose *Smart Card or other certificate* from the drop-down list (that's the TLS component). Also notice that as soon as you choose EAP, the other options—PAP, SPAP, MS-CHAP, etc.—become unavailable.

3. Configuring TCP/IP

One network component that is worth particular mention is the TCP/IP transport protocol—by far the most common network protocol in use today, thanks largely to the Internet. When dialing into a private corporate network using TCP/IP, you have to get various settings right on the Windows 2000 Professional client; otherwise, you may be able to establish a physical connection without actually gaining access to network resources.

If your private network is set up to use *Dynamic Host Control Protocol* (DHCP) to provide IP addresses and DNS server addresses for dial-up connections, all you need to do is double-click the TCP/IP entry in the list on the Networking tab and specify the radio buttons *Obtain an IP address automatically* and *Obtain DNS server address automatically*, as shown in **Figure 17** below.

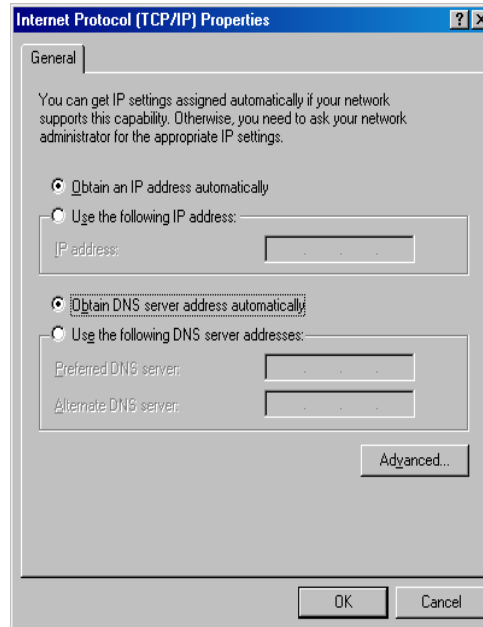


Figure 17: Obtain DNS server address automatically checkbox

You may be dialing into a network that can automatically assign you an IP address but not a DNS server address. In this case, you may need to set the TCP/IP property sheet up to look like the one in **Figure 18**.

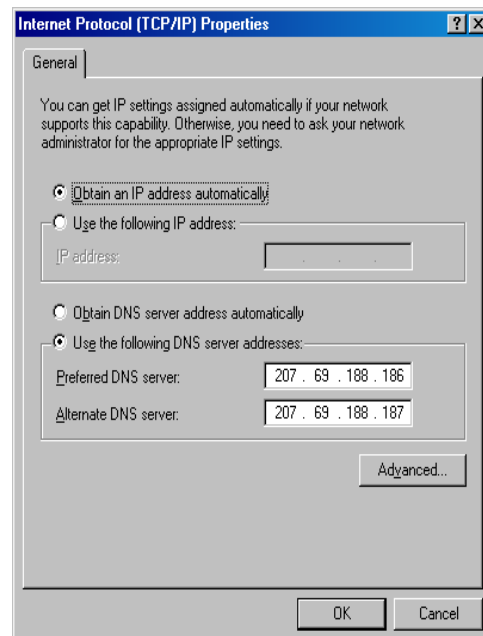


Figure 18: Use the following DNS server addresses checkbox

You may need to use a “static” IP address and subnet mask if your network doesn’t use DHCP to assign such information. In this case, you would need to click on *Use the following IP address* and fill in the information as directed by your network manager.

4. Configuring the Modem

On the General tab of the connection icon’s properties sheet, you can modify several modem settings by clicking on the Configure button as in **Figure 19**. (In a multilink setup with multiple modems, first click on the modem you want, then click on the Configure button.)

The settings you make here are very similar to the ones you set in the Phone and Modem Options control panel, but these settings apply only to the connection icon you’re configuring—they’re local rather than global. You can tailor them to the characteristics of the servers you’re dialing (i.e., one information service may support error correction, while another may not).

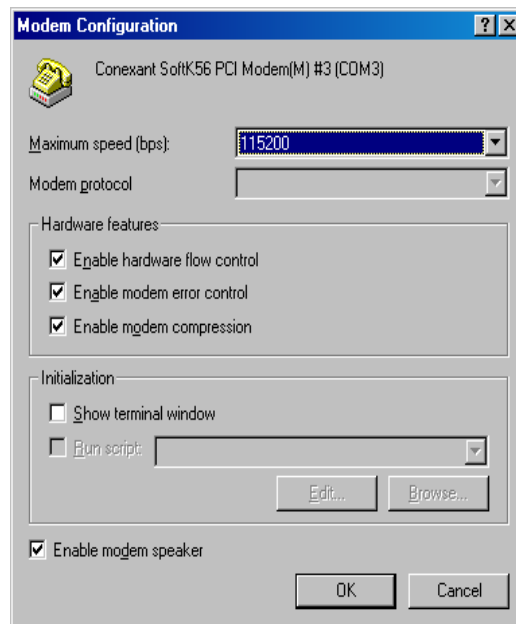


Figure 19: Modem Configuration Dialog box

Note: If you later make a change to the Phone and Modem Options control panel, don't assume that change automatically propagates to your connection icons. Some changes do, but most don't. Verify the change by checking the icon properties, and make the change there again if you need to.

Multilink Note: If you have multiple modems checked on the General tab and you choose *Dial devices only as needed* on the Options tab, you can set your Bandwidth Allocation Protocol (BAP) and Bandwidth Allocation Control Protocol (BACP) options by clicking on the Configure button on the Options tab (which is not the same as the one on the General tab). See **Figure 20**—the dialog box doesn't use these acronyms and BAP and BACP let you save cash if you're paying by the minute.

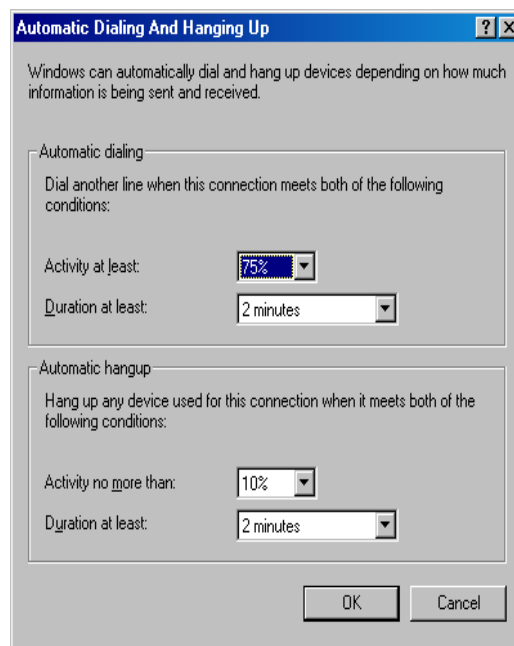


Figure 20: Automatic Dialing and Hanging Up Dialog Box

Chapter 4

Connecting to a Virtual Private Network

1. The VPN Concept

Windows 2000 offers *Virtual Private Networking* (or VPN for short) for those situations when you want to use the Internet to connect to a corporate network in a secure manner.

VPN is a private network link that isn't really private and doesn't use a normal network connection (hence the term *virtual*). VPN creates a secure tunnel through an intermediary network, such as the public Internet, in which two computers can communicate privately and securely. The VPN bundles IP, IPX, or NetBEUI packets inside PPP packets. VPNs differ from "normal" dial-up links in that they provide not only authentication but also encryption and compression.

I like to think of VPN as using the Internet as the communications medium instead of a traditional web of leased lines and Wide Area Network (WAN) carriers. The speed of a VPN is always limited by the speed of the various intervening Internet links, but if that's not a major consideration, a VPN can save an organization some money by obviating the need for more expensive traditional media.

2. How to Create a VPN Link

Nuts and Bolts

You can create a VPN link in Windows 2000 by starting the Make New Connection wizard in the Network and Dial-up Connections folder. Choose the *Connect to a private network through the Internet* option.

To use the Internet to make a VPN connection, you normally use one icon to establish the Internet link and another to establish the VPN tunnel. The first icon may already exist, in which case you should select it and click on *Automatically dial this initial connection* (see **Figure 21**). If you don't need to create an ISP link (i.e., because an always-on link already exists), click on *Do not dial the initial connection*.



Figure 21: Automatically dial this connection button

As you follow the wizard, you'll be asked to specify the domain name or IP address of the VPN server. As usual, you can also specify whether you want the connection all to yourself or if you prefer to share it with other users of that PC. Name the connection to complete the wizard.

To connect via a VPN link, just double-click the connection icon you created. After Windows establishes the link, your PC will behave as if it were logged on to the private network rather than to the public Internet.

VPN Connection Protocols

VPNs use different communications protocols from other types of dial-up connections. The two choices in Windows 2000 are *Point-to-Point Tunneling Protocol* (PPTP) and *Layer 2 Tunneling Protocol* (L2TP). Both PPTP and L2TP work over dial-up lines, local network links, WAN links and public TCP/IP networks (such as the Internet). However, some differences do exist:

- L2TP uses header compression for lower overhead, while PPTP does not.
- PPTP requires an IP network connection. L2TP can work with an IP, ATM, frame relay, or X.25 connection.

- L2TP provides tunneling but not encryption. Therefore you would normally use L2TP in combination with Internet Protocol Security (IPSec), which is a set of security protocols to protect the privacy of IP communications. PPTP provides encryption via PPP.

After the remote access protocol sets up the connection using either L2TP or PPTP, communication between computers takes place with “normal” LAN protocols: NetBEUI, IPX/SPX, or TCP/IP.

3. VPN Encryption

One of the key aspects of virtual private networking is encryption (i.e., the “scrambling” of data inside the VPN tunnel so outside observers can’t understand it).

Windows 2000 makes a determination as to what method to use for data stream encryption based on the setup of the VPN server into which you’re dialing.

- If you connect to a server that’s set up to use the PPTP protocol, Windows 2000 will automatically use *Microsoft Point-to-Point Encryption* (MPPE).
- If you connect to a server that’s set up to use the L2TP protocol, Windows 2000 will automatically use IPSec. Your VPN connection icon must be set up to enable IPSec via the advanced TCP/IP properties page for the connection.

Normally the process of selecting the encryption method is transparent to the user, and you don’t have to make any particular dialog box settings. Note, however, that MSCHAPv2 is required over MSCHAPv1 for encrypted PPTP connections.

Chapter 5

Connecting to an Internet Service Provider

1. How to Create an ISP Link

The procedure for creating a link to an Internet service provider is similar to that described for connecting to a private network, with a few extra dialog boxes thrown in. The steps are as follows:

1. Right-click My Network Places and choose Properties.
2. Double-click the Make New Connection icon.
3. Click on Next to get past the verbiage.
4. Click on the *I want to sign up for a new Internet account* button and click on Next. (At this point, the Make New Connection wizard will hand you off to the Internet Connection Wizard. See **Figure 22.**)



Figure 22: Internet Connect Wizard box

5. In most cases you'll choose the third radio button, which says *I want to set up my Internet connection manually, or I want to connect through a Local Area Network*

(LAN), and click on Next. (Select one of the first two buttons if you want to use Microsoft's referral service to help you find an ISP.)

6. At the *Setting Up Your Internet Connection* dialog box, specify whether you connect through a modem or a LAN. (Portable computer users who sometimes connect to a LAN when in the main office can run the Make New Connection wizard twice, once for each circumstance.) Click on Next.
7. If you chose "modem" in Step 6, Windows may prompt you to specify the modem to use. If so, choose one and click on Next.
8. Tell Windows the phone number for your ISP in the *Internet account connection information* dialog box. Check *Use area code and dialing rules*. Skip the Advanced button for now, and click on Next.
9. At the Internet Account Logon Information screen, enter the username and password your ISP gave you for logging on to its service. (Often, the username is the same as your full e-mail address, but it may be something entirely different.) Click on Next.
10. Give the connection icon a name, and click on Next.
11. If you want to set up an Internet e-mail account in Outlook or Outlook Express, click on Yes in the *Set up your Internet mail account* dialog box. (Usually you'll skip this and set up your e-mail account later.) Click on Next.
12. Click on the Finish button, and Windows will create a new icon in the Network and Dial-Up Connections folder. (Watch out—this connection will become your default Internet connection, even if you've previously defined other dial-up connection icons! You can change this set up in the Internet control panel on the Connection tab.)

Hint: If you want Internet Explorer to use the modem to connect you to the Internet automatically, you can set that via in the Internet control panel's Connection tab. (Outlook Express shares that setting.)

2. Choosing Network Components

Your Windows 2000 Professional computer can communicate over the modem in exactly the same ways that it communicates over a network interface card—by

sending and receiving TCP/IP, NetBEUI, or IPX/SPX packets. Your network link is just a communications device that connects to a cable. Therefore, you must configure a dial-up connection to find out which network components it should use. (You can do this via the Networking tab of the connection's properties page. See **Figure 23.**)

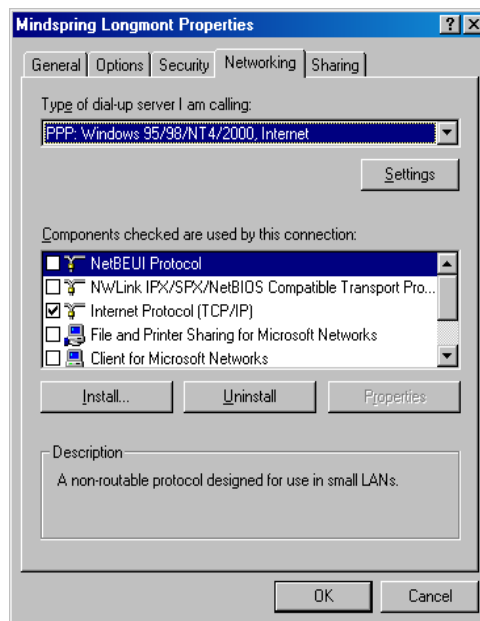


Figure 23: Networking tab

Specifying Server Type

The *Type of dial-up server I am calling* setting at the top of the Networking tab is where you specify the connection (or communications) protocol. It is a protocol you need for dial-up lines but don't need for hardwired LAN links. The choice you make here is determined by the kind of computer (server) you're dialing into as follows:

- **PPP:** The default choice for dial-up connections because it's the most reliable, secure and efficient. Unlike SLIP, PPP supports error checking. It works with NetBEUI, IPX/SPX, and TCP/IP network protocols.
- **SLIP:** Use this with a UNIX server running Serial Line Interface Protocol. SLIP is old, slow and a bad choice unless you're calling up an old, slow UNIX server that doesn't work with PPP. SLIP offers no error correction, no encrypted passwords and no automatic IP address assignment.

Typically, your ISP will tell you what you need to choose here, but PPP is almost always the right choice.

Installing and Activating Components

If you need to connect to the Internet with a Web browser, all you need is the TCP/IP protocol. You don't need a networking client (such as the Client for Microsoft Networks); however, you do need a Web browser. Internet Explorer 5 comes with Windows 2000, and you can also add other browsers to your system.

Configuring Logon

As for the logon process, most ISPs require that you set your system to no authentication protocol (that is, your user ID and password cross the phone lines as unencrypted "cleartext"). This is the default setting for an ISP connection icon created by the Make New Connection wizard, but if you want to double-check it, right-click the icon and choose Properties. Click on the Security tab and make sure the active setting is *Allow unsecured password*, as shown in **Figure 24**.

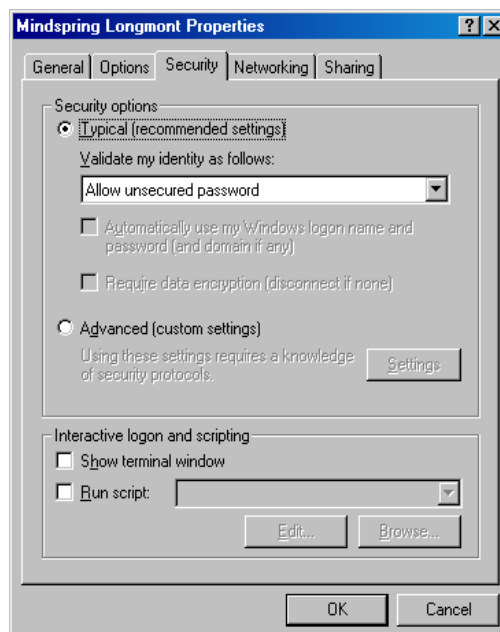


Figure 24: Security tab

3. Configuring TCP/IP

Usually, when you use a PPP connection protocol with an ISP, you choose *Obtain an IP address automatically* and *Obtain DNS server address automatically*, as in **Figure 25** below. (You can get there by opening the connection's properties page, clicking on the Networking tab, and double-clicking the entry for TCP/IP.) Most ISPs and TCP/IP hosts provide this information automatically after you connect. For ISPs that don't, you still have the flexibility to hardcode specific IP addresses for your computer and for one or more DNS servers by clicking on *Obtain an IP address automatically* and/or *Obtain DNS server addresses automatically*.

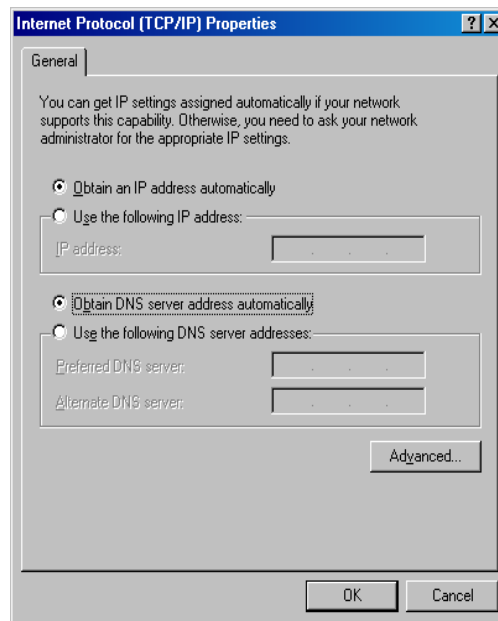


Figure 25: Obtain an IP Address Automatically and Obtain DNS Server Addresses Automatically buttons

Tip: If you're just connecting to the Internet to browse the Web, you use domain names, so you don't need a WINS server.

If you click on the Advanced button on the TCP/IP Properties page, you'll see a dialog box similar to the one in **Figure 26**.

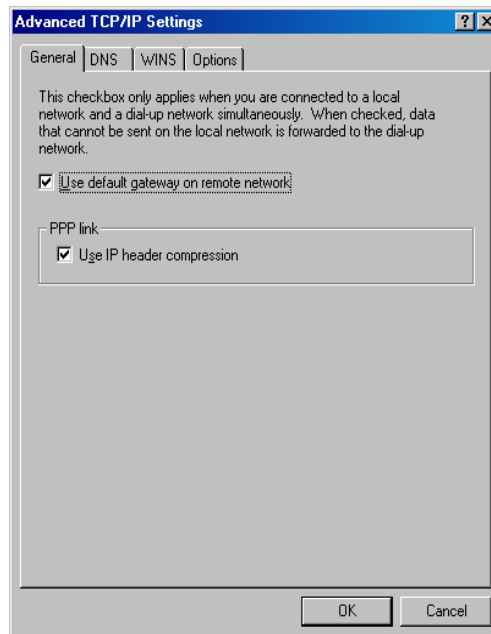


Figure 26: Advanced TCP/IP Setting Dialog box

The checkbox on the General tab of the Advanced TCP/IP settings property sheet, *Use default gateway on remote network*, tells Windows 2000 not to use the default gateway you may have configured on your local TCP/IP LAN if both it and your dial-up connection are live. As with the checkbox *Use IP header compression* (which improves performance as long as your ISP supports the feature), you should normally leave this option checked (activated).

4. Configuring the Modem

On the General tab of the connection icon's properties sheet, you can modify several modem settings by clicking on the Configure button. (In a multilink setup with multiple modems, first click on the modem you want, and then click on the Configure button.)

The settings you make here are very similar to the ones you set in the Phone and Modem Options control panel, except these settings only apply to the connection icon you're configuring—they're local rather than global. You can tailor them to the characteristics of the servers you're dialing (i.e., you can adapt an information service that doesn't support error correction to another that does). The settings are as follows:

- Maximum speed, in bps.
- Hardware flow control (on or off).
- Modem error control (on or off).
- Modem compression (on or off).
- Whether to show a terminal window before making connection.
- Run a script before dialing.
- Modem speaker (on or off).

Note: If you later make a change to the Phone and Modem Options control panel, don't assume that change automatically propagates to your connection icons. Some changes do, but most don't. Verify the change by checking the icon properties, and make the change there again if you need to.

Chapter 6

Troubleshooting Dial-Up Connections

When a dial-up connection gives you trouble, troubleshooting can be nightmarish considering all the many property sheet settings Microsoft has scattered throughout the operating system's user interface. The following are a few tips that may help.

1. Enabling Modem Logging

Modem logging is on by default in the Windows 2000 Professional OS (it's off by default in Windows 2000 Server). Though you can't turn it off, you can specify whether a new log will be created each time a new connection occurs or the logging information will be appended to the existing log. (This setting is on the modem's property sheet in the Phone and Modem Options control panel.)

The log file itself lives in the C:\WINNT folder and has a name that begins in MODEMLOG and ends in TXT. The precise filename depends on the make and model of your modem.

You may be able to use the modem log (view it in Notepad or any other text editor) to glean some details about what's happening during the dial-and-connect phases. For example, the modem log provides information on the way two computers negotiate flow control, error control and compression, on the speed of connection, whether or not the remote computer is picking up the phone, etc. **Figure 27** shows an excerpt from a typical modem log.

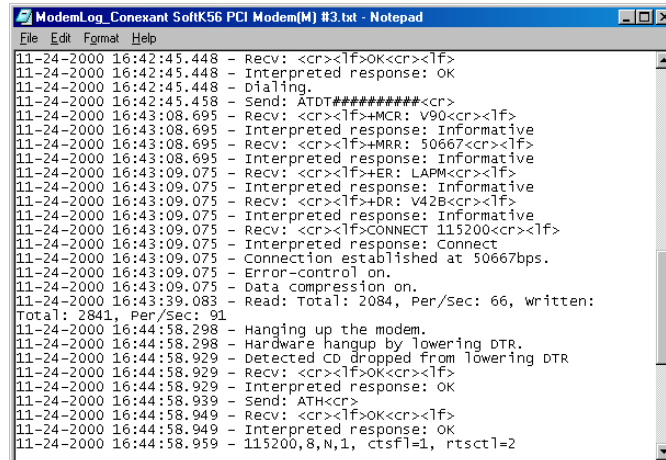


Figure 27: Excerpt from a Typical Modem Log

2. Event Log Messages

You may be able to spot clues about connection problems by using the Event Viewer utility (Start→Settings→Control Panel→Administrative Tools→Event Viewer). Services that fail to start, hardware that does not initialize and other “major” communications problems should generate entries in the event logs. If you’re dialing into a Windows 2000 or Windows NT server computer, the event logs on that server machine could also be a valuable source of information.

3. Using IPCONFIG

The IPCONFIG command-line utility is handy for checking the current IP configuration, if your connection uses the TCP/IP protocol. Unlike Windows 98, Windows 2000 doesn’t come with a graphical utility; so you have to open a command prompt window (choose Start→Run and type *CMD*), and then type *IPCONFIG* at the prompt.

If you want to see all the gory details, type *IPCONFIG /ALL*. The display may be too large to fit in the window, but you can use that handy scroll bar along the command prompt window’s right edge to scroll and view content—or, better yet, resize the command prompt window itself. **Figure 28** shows how this command provides details on the IP address, subnet mask, default gateway and DNS server(s)

for the dial-up connection. Use this information to check against the settings on the connection icon's property sheet.

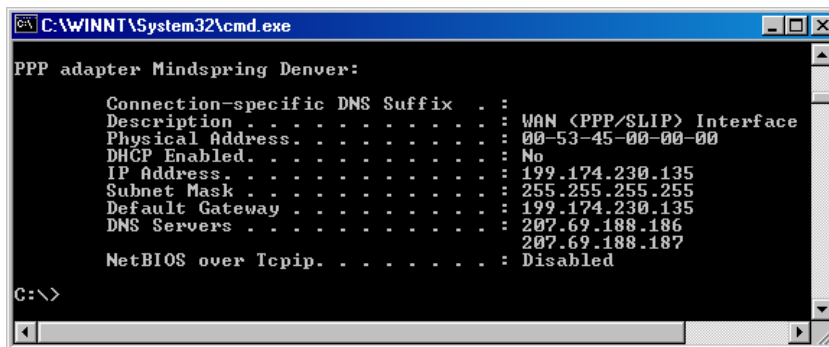


Figure 28: IPCONFIG/ALL

With the help of IPCONFIG, you can troubleshoot TCP/IP problems using the following tips:

- Run IPCONFIG. If IPCONFIG reports that your subnet mask is 0.0.0.0, your computer has a duplicate IP address with another computer on the same network.
- Open a command prompt window and type *PING 127.0.0.1* to confirm that TCP/IP is properly bound to your dial-up network adapter. (The IP address 127.0.0.1 is known as the *loopback address* and refers to the local machine.) A successful result is a “reply from” message repeated four times.
- Ping the default gateway (as reported by IPCONFIG). If you get a successful result here, your computer can “see” the link to computers on remote subnets.
- If you can't connect to network resources using a computer name, you may have an incorrect entry for the address of a WINS server on your connection icon's TCP/IP properties page.
- If you can't connect to network resources using a domain name, you may have an incorrect entry for the address of a DNS server on your connection icon's TCP/IP properties page.

4. Troubleshooting Authentication Failures

When connecting to an ISP, the most common authentication failure occurs when you've specified an authentication protocol on the Security tab of the connection icon's properties sheet. Most ISPs require that the *Typical* radio button be selected and the *Allow unsecured password* option appear in the drop-down list box.

The next most common failure occurs when your Windows 2000 Professional system is configured to use an authentication protocol that the server you're dialing doesn't support. (Remember, not all versions of Windows support all protocols; for example, a Windows 98 dial-up server doesn't support MS-CHAPv2.)

One trick is to set your notebook computer to use no authentication whatsoever—that is, to “Allow unsecured passwords.” Try this and see if you can connect reliably. If so, you can then focus your attention on which authentication protocol or protocols (if any) also permit you to connect, using trial and error. If not, don't waste your time testing authentication protocols because your problem lies somewhere else.

Be aware that if you're dialing into a Windows 2000 Server computer, several factors could result in your not being authenticated to the server:

- Your *dial-in permissions* (set in Active Directory Users and Groups for a domain environment, or in Local Users and Groups for a stand-alone server environment).
- *Remote access policies* that a network manager has set up on the specific server to contain various conditions for permitting a connection.
- *Remote access profiles* that a network manager has set up on the specific server and that determine the type of access the server will grant if a connection is permitted.

Check with the manager of the network into which you're dialing to be sure that none of these factors are causing your account to be denied access.

5. Things to Try When the Problem Isn't Obvious

Getting More Information

Sometimes you can get a hint about what's going on by activating the display of the Taskbar icon for your connection. This can be useful in verifying your connection speed or verifying whether a given link is still "alive." Make sure the *Show icon in Taskbar when connected* checkbox is checked on the General tab of the connection icon's property sheet.

I also like to make sure the *Display progress while connecting* box on the Options tab of the icon's property sheet is checked; that way I can watch the progress as Windows 2000 establishes the communications link.

Miscellaneous Tricks

One of the reasons I like external modems is because you can turn them off and back on again if they get confused (i.e., by misinterpreting something in the data stream as a modem command). Most notebook users have internal modems, but you may be able to affect a "hard reset" by ejecting the modem (if it's a PC Card type) and reinserting it. Otherwise, the only way to force a hard reset of the modem is to perform a restart (Start → Shut Down → Restart).

Turn off any connection settings that may make connecting more difficult. For example, disable hardware compression (see the section entitled *Modem Configuration* for details). You may also want to turn off LCP extensions on the PPP properties page (access it via the Networking tab of the connection's properties page).

Turn on any connection settings that are likely to improve reliability. For example, turn on hardware flow control (again, in the section entitled *Modem Configuration*).

About the Author



Glenn Weadock, MCSE, is president of Independent Software Inc. (www.i-sw.com), a consulting firm he founded in 1982 after graduating from Stanford University's engineering school. One of the country's most popular technical trainers, Glenn has taught Windows to thousands of students in the United States, the United Kingdom and Canada in more than 200 seminars since 1988. Glenn is the author of fifteen published books, including *MCSE Windows 2000 Professional for Dummies* (Hungry Minds, 2000), *Windows 2000 Registry for Dummies* (Hungry Minds, 1999), and *MCSE Windows 2000 Network Infrastructure for Dummies* (Hungry Minds, 2000). He recently served as an expert witness in the Microsoft antitrust trial.