

# Configure Windows XP Pro as a remote access server



By [Deb Shinder](#) in [Networking](#) on May 28, 2003, 12:00 AM PST

Configure Windows XP Pro to function as a dial-up or VPN server using remote access

You don't have to buy a Microsoft server product if you want to be able to "call home" and connect to your LAN when you're on the road. Although it only supports one incoming connection at a time per connection type (dial-up, VPN, or direct), XP Pro can function as a remote access server too. And in many circumstances, one connection is all you need. This feature can be handy if you want to access your home computer from work, even if your home system isn't connected to an always-on Internet connection. In this Daily Drill Down, I will look at the differences between a dial-up remote access server and a VPN server, the benefits of setting up your XP Pro machine for remote access, how to configure XP to accept incoming connections, troubleshooting, and security concerns.

### Why do you need a remote access server?

A remote access server is a computer that is attached to a modem or the Internet and is set up to answer incoming calls and grant access to its own resources and those on the local network to which it is attached. A remote access server is often thought of as being a machine running a Windows server product and the Routing and Remote Access Service (RRAS), often with many incoming phone lines and a bank of modems. While this describes the typical corporate RAS server, Windows XP Pro and a single modem can put you in business as a limited remote access server and make it easy, when you're away, to retrieve information from your home computer or home LAN or even (with your employer's approval) from your modem-equipped workstation at the office.

### What you can do via remote access

When you attach to the network over the phone lines or through a VPN, you can do anything that you would be able to do from an on-site computer that is cabled to the LAN, as long as your permissions are configured to allow it. The big difference between a remote access connection and an on-site one is speed; at the physical level, the phone lines are a much slower means of transmission than the Ethernet used to connect computers on-site.

If the computer from which you're connecting (the remote access client) has the Windows Terminal Services client or the Remote Desktop Client software installed, after you dial in or make a virtual connect, you can run the applications that are on the remote access server as well as accessing its files.

---

#### Tip

Although you need an XP Pro computer to be a remote desktop server, XP Home also comes with the RDC client program, and it can be downloaded from the [Microsoft Web site](#) and installed on any computer running Windows 95 or later.

---

#### Dial-up remote access server vs. VPN server

There are two different types of incoming remote access connections supported by Windows XP: dial-up and virtual private networking (VPN). There are advantages and disadvantages to each. To accept incoming dial-up connections, you need a modem and phone line attached to the remote access server computer. The client that is dialing in will also need a modem and phone line. To accept incoming VPN connections, the remote access server computer must be connected to an always-on Internet connection (such as DSL, cable, T-carrier, or dedicated ISDN).

---

#### Tip

If the XP computer you want to act as a VPN server is behind a firewall or NAT device, you may need to use a technique called VPN pass-through to access it via VPN from outside the LAN. This is a method of "tunneling within a tunnel," using another VPN server that is located in the DMZ or perimeter network to reach the internal VPN server.

---

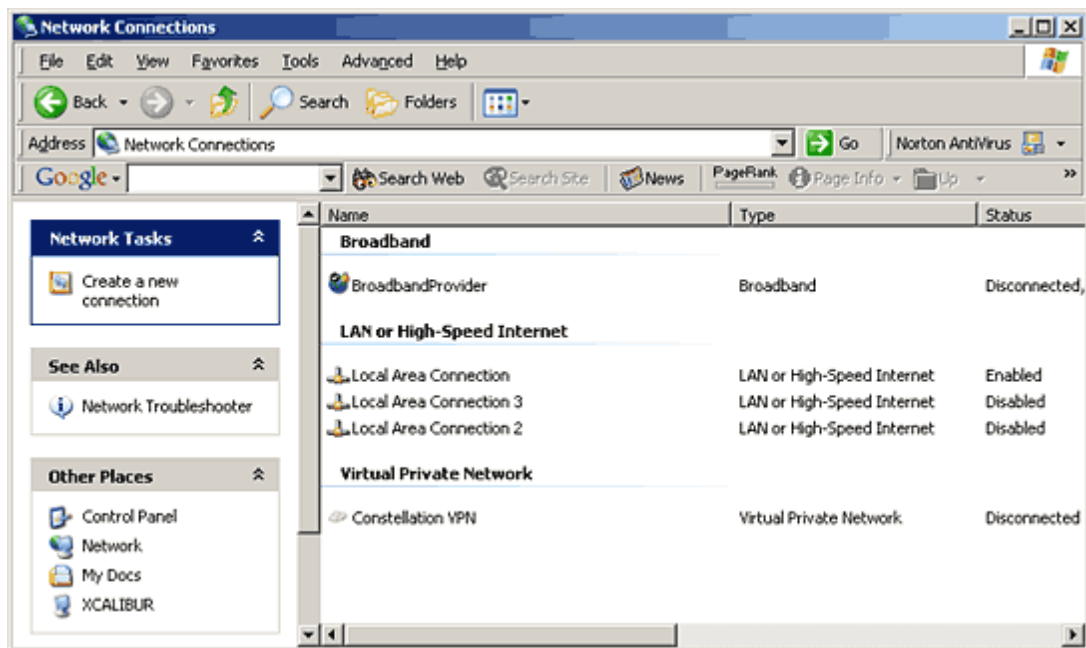
If the client and server are in different dialing areas so that a modem call would incur long distance charges, and the server has an always-on Internet connection, VPN is the most economical choice. If the server does not have an always-on Internet connection, dial-up remote access is the obvious choice.

A VPN connection over a broadband Internet connection will be faster than using a modem to dial up a remote access server. XP Pro does, however, support multilink, which lets you configure more than one modem or ISDN adapter to be used with incoming dial-up connections. This increases the effective bandwidth but requires multiple lines on both ends.

## Configuring XP Pro to accept incoming connections

Setting up XP Pro as a remote access server is pretty straightforward, but there are a few issues that aren't obvious from the configuration dialog boxes. First, log on as a member of the Administrators group. Whether you want to allow incoming dial-up connections, VPN connections, or both, you start by accessing Network Connections from the Control Panel. Select Create A New Connection from the left pane under Network Tasks, as shown in **Figure A**.

Figure A



Use the Network Connections applet to create a new incoming connection.

---

### Tip

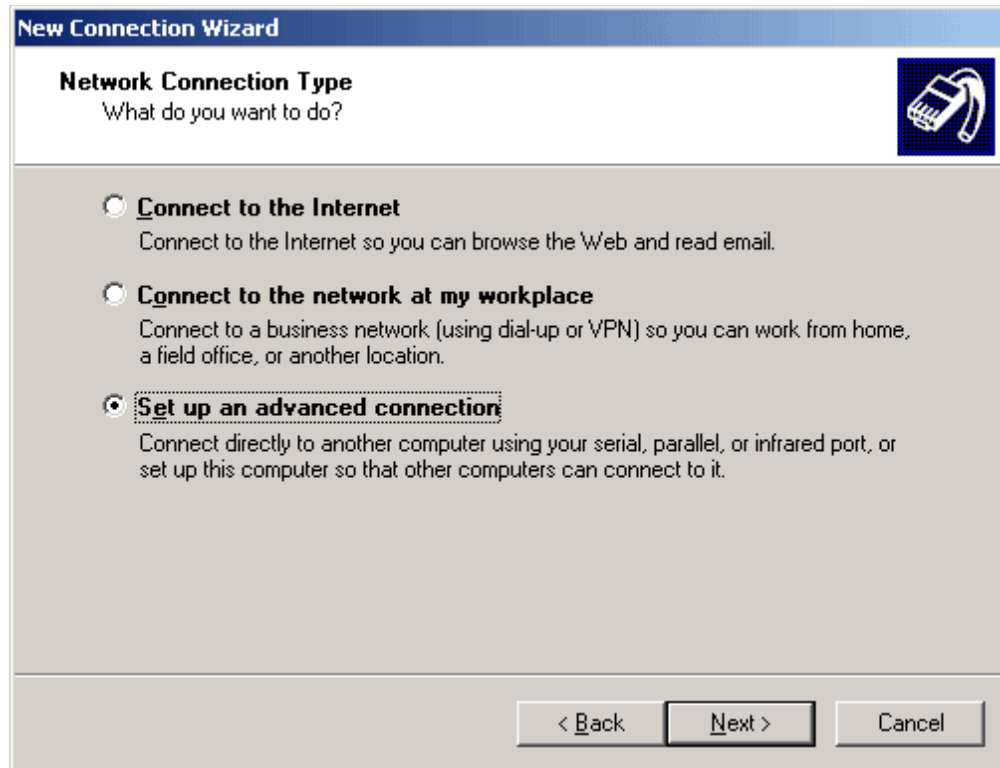
Note that the VPN connection(s) shown under Virtual Private Network in the right pane refers to outgoing VPN connections, not incoming connections such as you will be setting up for a remote access server.

---

Clicking Create A New Connection invokes the New Connection Wizard, which you can use to create both outgoing and incoming connections. Click Next on the welcome page.

On the Network Connection Type page, shown in **Figure B**, select the third choice, Set Up An Advanced Connection, and click Next.

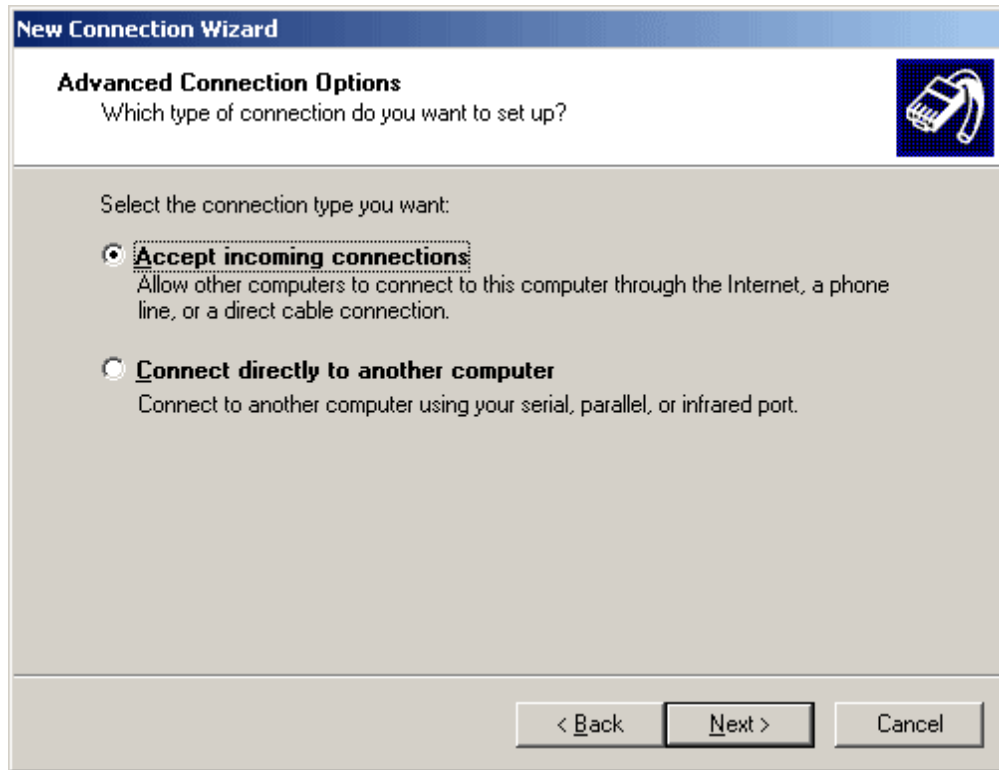
Figure B



To configure incoming connections, select Set Up An Advanced Connection.

On the Advanced Connection Options page, shown in **Figure C**, select Accept Incoming Connections, and click Next.

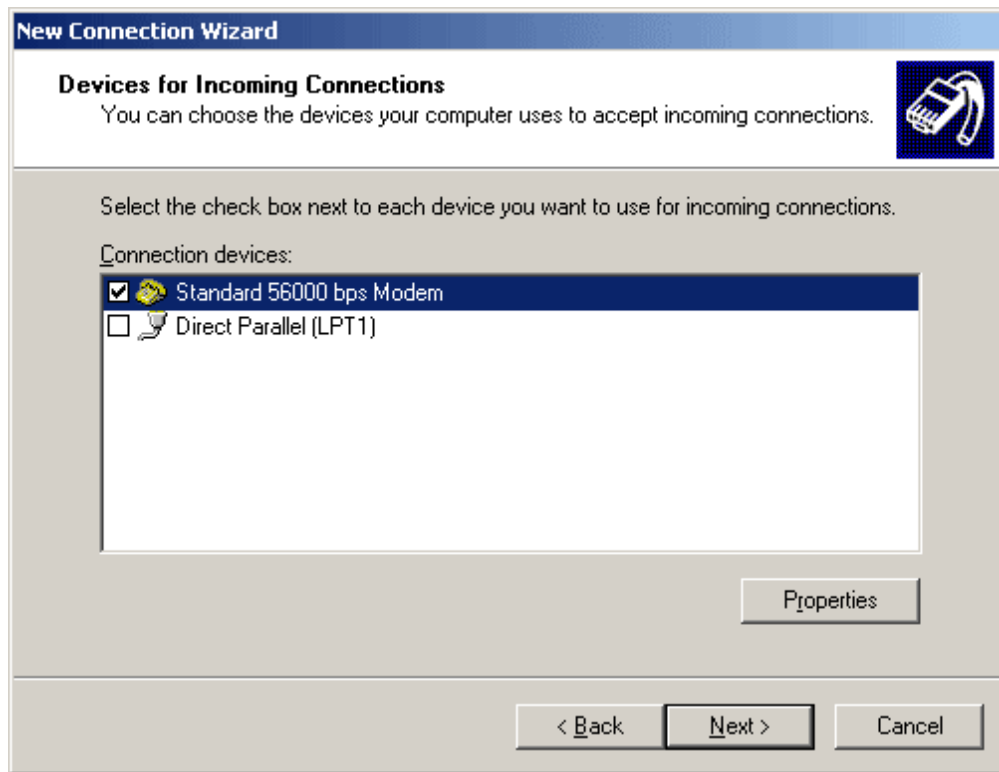
Figure C



Select Accept Incoming Connections so others can connect to this remote access server.

If you have a modem connected to the computer, the Devices For Incoming Connections page will show it in the list of connection devices. If you want to set up the computer to accept incoming dial-up connections, check the checkbox for the modem you want to use, as shown in **Figure D**.

Figure D



Select the modem you want to use for incoming dial-up connections.

If you have more than one modem and phone line connected, you will have the option to enable multilink. If you do not have a modem connected, you may see only one choice: Direct Parallel. Do not check this box unless you want to connect another computer to this one through their parallel ports (this is useful for such tasks as quickly transferring files from a laptop to a desktop machine). The computer's network interfaces don't appear here, so if you will be accepting VPN connections only, just skip this page and click the Next button.

The next page allows you to set the computer up to accept incoming VPN connections. Your computer will need a name or IP address that's known on the Internet to accept VPN connections outside the LAN, unless you use VPN pass-through. Even if your computer is directly connected to the Internet, if you are using a firewall, it will have to be configured to let VPN packets through.

---

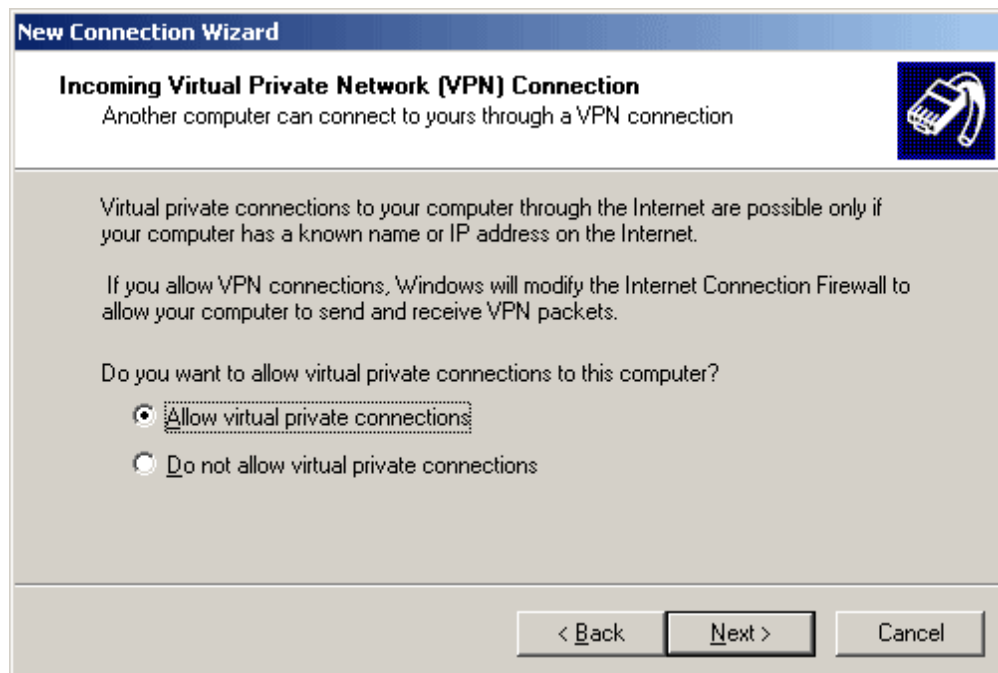
**Tip**

If you're using XP's built-in Internet connection firewall (ICF), Windows will automatically change its configuration to allow VPN packets.

---

If you want the computer to accept VPN connections, select the Allow Virtual Private Connections option, as shown in **Figure E**. You can make the computer both a VPN server and a dial-up server, if desired.

Figure E

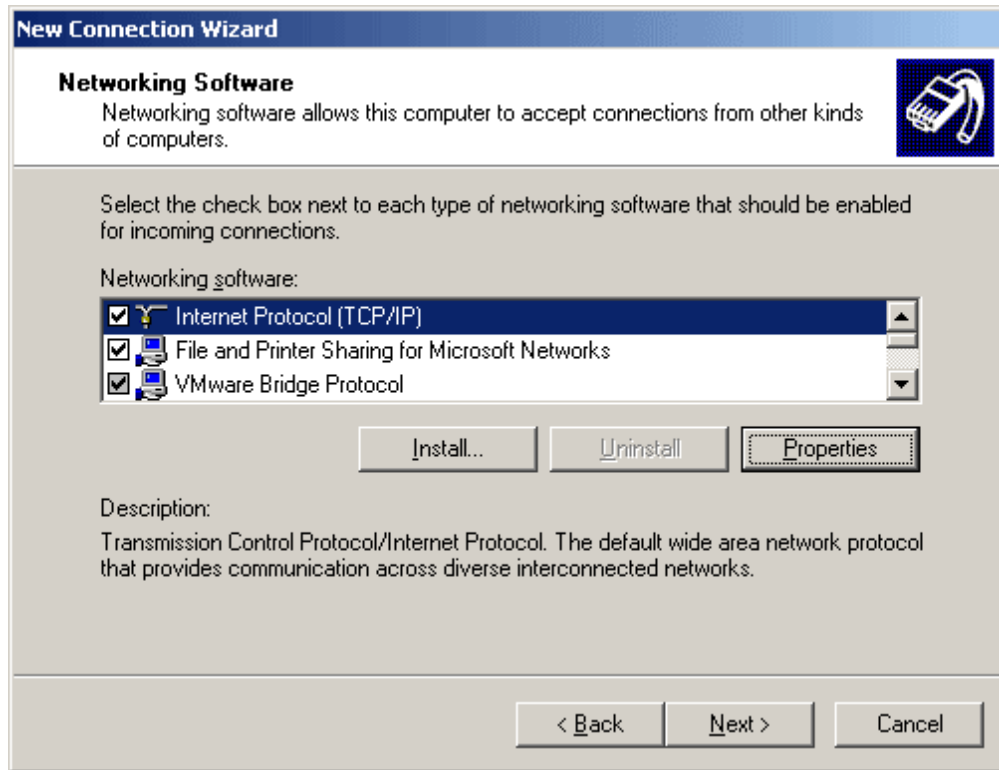


You can allow VPN connections from the intranet or, if your computer has a public IP address/name, from the Internet.

Click Next to take you to the User Permissions page. Select the checkboxes of the local user accounts to which you want to grant remote access. If the desired users are not shown, you can add new users by clicking the Add button and typing in a user name and password. Click Next.

On the Networking Software page, select the networking components that you want to have available for incoming connections, as shown in **Figure F**.

Figure F



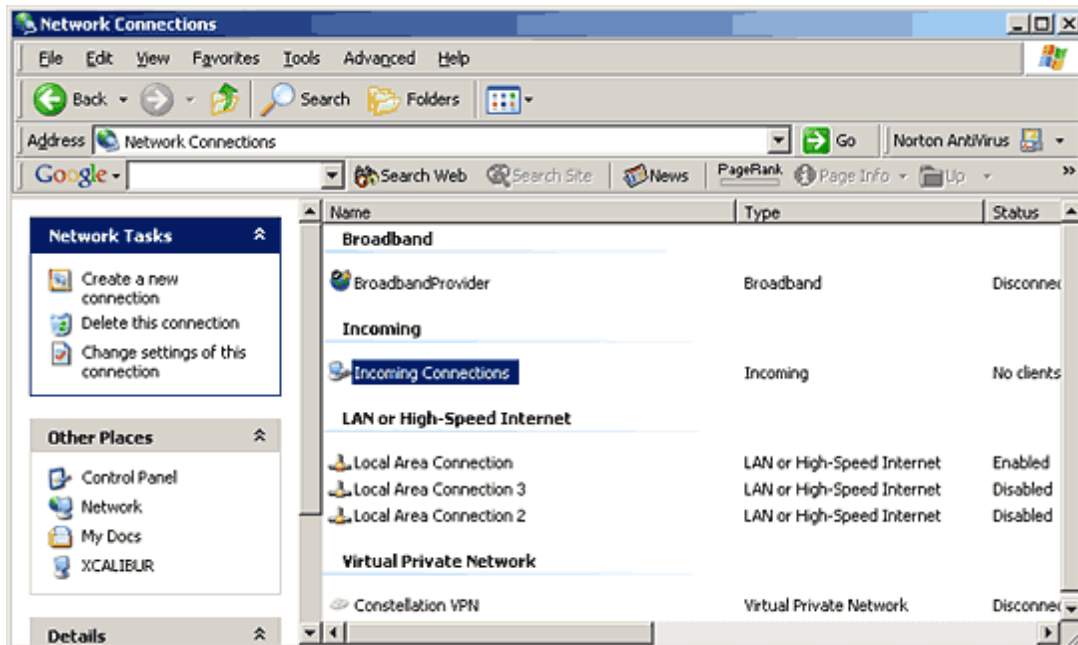
Select the networking software components to be enabled for incoming connections.

You can install additional components by clicking the Install button. For example, if you want the remote user to be able to connect to other computers on the LAN that are running only the NWLink (IPX/SPX) networking protocols, you can install it by selecting Protocols.

When you click Next, this will complete the Wizard and configure your incoming connection(s). Now it will appear in your Network Connections folder, as shown in **Figure G**.



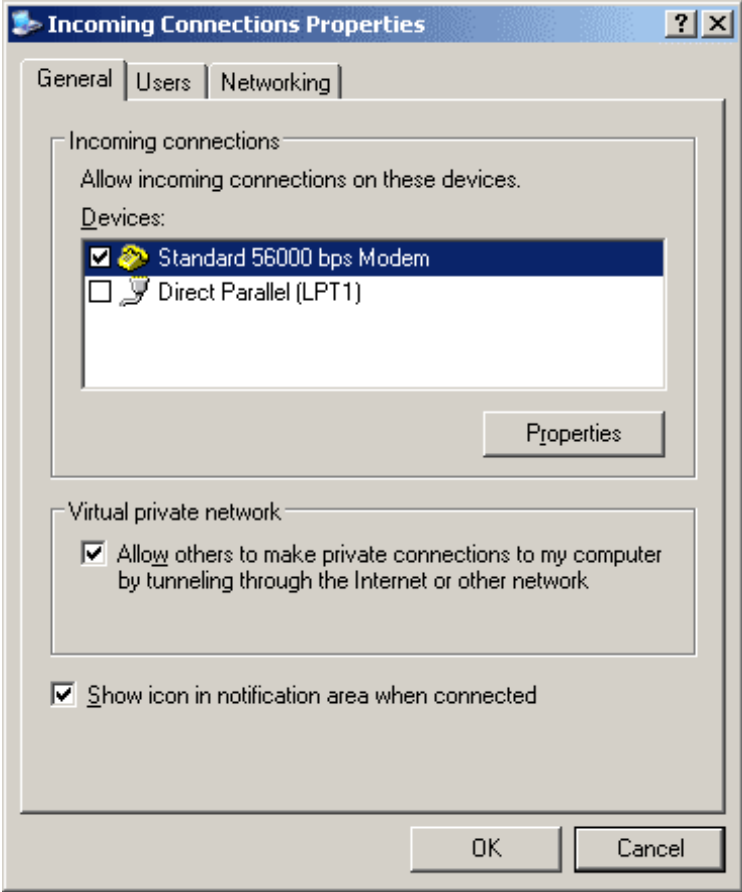
Figure G



Once you've set up the computer to accept incoming connections, a new icon appears in the Network Connections folder.

You can modify the configuration later by double-clicking the Incoming Connections icon or right-clicking and selecting Properties. This will open the Properties sheet shown in **Figure H**, which has three tabs: General, Users, and Networking.

Figure H



Use the Incoming Connections properties sheet to modify the configuration.

Remote access security issues

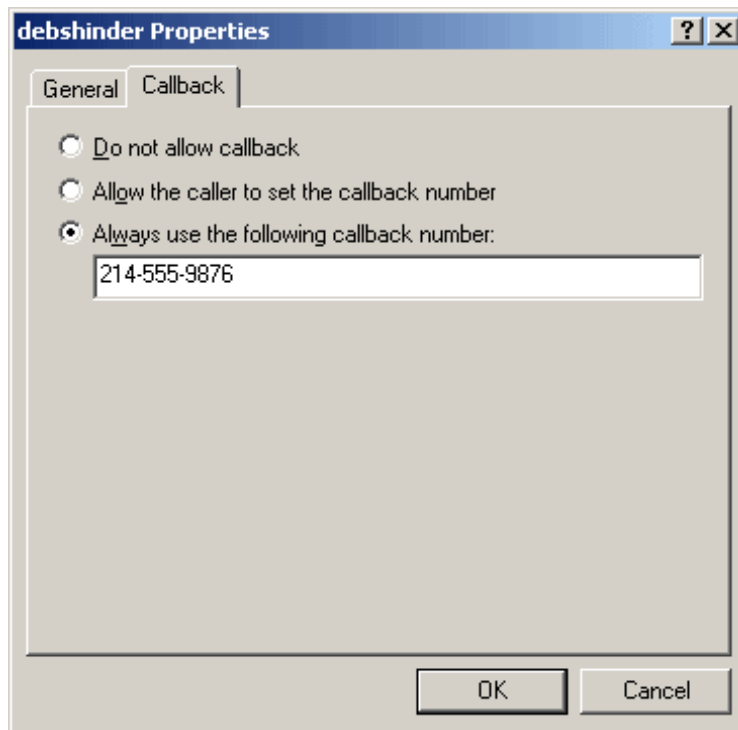
There are several modifications to the default settings that you can make to increase the security of your remote access connections.

Requiring callback for dial-up connections

If the dial-up remote user will always be calling from the same location, you can set up the user's properties to require callback. This will ensure that someone who has obtained the user's password credentials won't be able to connect from someplace other than the user's calling location. To do this, click the Users tab of the Incoming Connections properties sheet, highlight the user for whom you want to require callback, and click the Properties button.

On the user's properties sheet, click the Callback tab and select the option to Always Use The Following Callback Number. Then type the user's phone number into the box, as shown in **Figure I**.

Figure 1



You can require callback on dial-up connections for increased security.

When callback is required, the server will hang up as soon as the user enters his or her credentials, and call the user's computer back at the specified location.

---

#### Tip

In addition to requiring callback from a specific number, you have a couple of other callback options. If the remote access calls are long distance and you want the bill for the session to be paid at the server end, you can select Allow The Caller To Set The Callback Number. Then the user will be prompted to enter a phone number when dialing in, and the server will disconnect and call that number back. You can also choose Do Not Allow Callback, which is the default setting.

---

#### Preventing remote users from accessing the LAN

By default, when you set up an XP computer to accept incoming connections, remote users will be able to access the LAN to which that computer is connected. If you want to limit access to the XP remote access server computer only, select the Networking tab in the Incoming Connections Properties box. Click Internet Protocol (TCP/IP) and click the

Properties button. On the Incoming TCP/IP Properties page, uncheck the box under Network Access that says Allow Callers To Access My Local Area Network.

This properties box also allows you to specify whether TCP/IP addresses will be assigned to remote users automatically using DHCP, to specify a range of addresses that can be assigned to remote users, and to specify whether a calling computer will be allowed to specify its own IP address (disabled by default).

#### Disabling file and print sharing for remote connections

If remote users will not need access to the files and printers on the server (for example, if they will be connecting only to share the Internet connection on the XP computer), you can increase security by disabling file and print sharing for the remote connections.

Click the Networking tab in the Incoming Connections Properties box, and uncheck the checkbox labeled File and Printer Sharing for Microsoft Networks under Network Components.

---

#### Tip

XP Pro is capable of accepting VPN connections using either PPTP with MPPE, or L2TP with IPSec encryption (for better security). By default, VPN connections use PPTP. However, L2TP can be forced from the client end.

---

#### Do not allow calling computers to specify their own IP addresses

The Incoming TCP/IP Properties box has a checkbox that you can check to allow calling computers to specify their own IP address instead of assigning them one via DHCP or from a defined range.

Checking this box can present a security risk, because a knowledgeable intruder could impersonate a legitimate client that has been previously connected to the network by specifying the same IP address, and would then be able to access resources that were accessed by the legitimate remote access client.

#### Troubleshooting remote access issues

Some of the following are a few common problems that are encountered when you set up an XP remote access server:

- **The Make New Connection Wizard only contains the Dial-up option and the Accept Incoming Connection choice is not available.** This can happen when the telephony service or the Remote Access Connection Manager service is stopped. Check in Computer Management | Services and Applications | Services to ensure that the services are started.

- **A remote user is immediately disconnected after dialing up the computer that has been configured to be a remote access server.** The first thing to check is the Users tab, to ensure that the account has been given the right to connect remotely. Another problem may be that you have configured the remote access server to require all users to secure their passwords and data. You can uncheck this box on the Users tab or instruct the users to use securely encrypted passwords and data.
- **Clients connecting to your computer can't access resources on other computers on the LAN, even though you have checked the checkbox to allow them to do so.** Allocating a set of IP addresses for remote clients that are not a subset of the LAN addresses can cause this problem. In this case, you should either change the allocated address range so that it will be a subset of the LAN addresses, or configure the computers on the LAN with a default gateway setting that matches the IP address of the incoming connections computer.

Many remote access problems are caused by configuration or hardware difficulties at the client end.