Creating a VPN Using Windows 2003 Server and XP Professional

Recommended Instructor Preparation for Learning Activity

Instructor Notes: There are two main types of VPNs:

- **User-to-Network**
  This type of VPN allows a client to use a VPN to connect to a secure network, such as a corporate intranet.

- **Network-to-Network**
  This type of VPN connects two networks via a VPN connection. This effectively combines two disparate networks into one, eliminating the need for a Wide Area Network (WAN).

In this article I will explain the basics of VPNs and show you how to set up one yourself using Windows 2003 Server and Windows XP Professional.

Tunneling and VPN Protocols

In a VPN, two computers communicate through a VPN tunnel. Tunneling is the process of encapsulating packets within other packets to protect their integrity and privacy during transit. A tunnel performs such tasks as encryption, authentication, packet forwarding, and masking of IP private addresses. Think of a tunnel as a private link between the two computers; whatever one sends to the other is only visible to the other, even though it is sent through a public network like the Internet.

If you're curious about what goes on under the hood of a VPN, there are three protocols you need to know about -- PPTP, L2TP, and IPSec.

Point-to-Point Tunneling Protocol (PPTP)

This was designed by Microsoft (and other companies) to create a secure tunnel between two computers. PPTP provides authentication and encryption services and encapsulates PPP packets within IP packets. It supports multiple Microsoft networking protocols such as LAN-to-LAN and dialup connections. However, it is proprietary and the encryption is weak.

Layer 2 Tunneling Protocol (L2TP)

This works like PPTP, except that it does not include encryption. L2TP was proposed by Cisco Systems and like PPTP, L2TP supports multiple networking protocols.

IPSec

This protocol addresses the shortcomings of L2TP by providing encryption and authentication of IP packets. As such, L2TP is often used together with IPSec to provide a secure connection.

PPTP and L2TP are among the most likely proposals as the basis for a new Internet Engineering Task Force (IETF) standard.

Setting Up a VPN between Two Computers

In the following sections, you will learn how to set up a VPN host and client -- the host server using Windows 2003 Server and the client using Windows XP Professional.

Preparation:

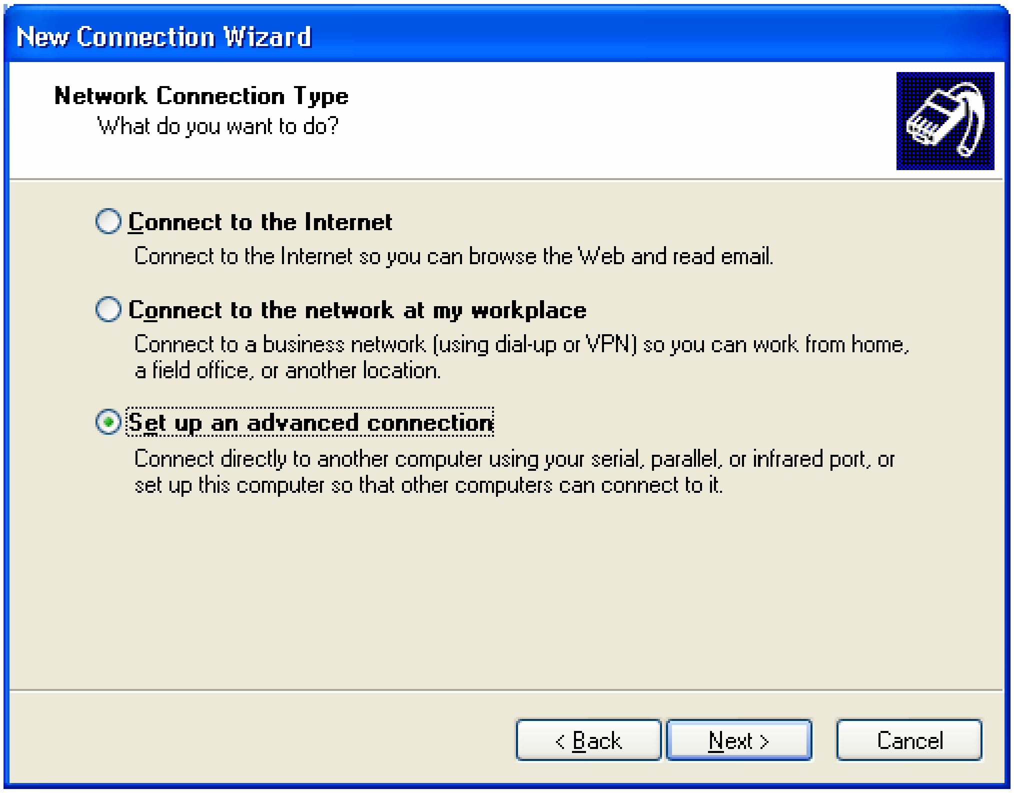
The instructor will setup an 802.11b wireless network that contains:

- A wireless-enabled host running Windows XP Professional Service Pack 2 for each student,
- A Linksys BEFW11S4 router connected to a host running Windows 2003 Server and Local Area Network, and
- Switches (2) are needed to create separate LAN segments or use VLAN's, so the students can demonstrate mastery of the subject.

On the Windows 2003 Host Computer

Let's start with setting up the VPN host.

1. On the desktop, right-click on My Network Places.
2. Select Create a new connection.
3. On the New Connection Wizard window, select Set up an advanced connection (see Figure 1). Click Next.



New Connection Wizard

Network Connection Type
What do you want to do?

○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

○ **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

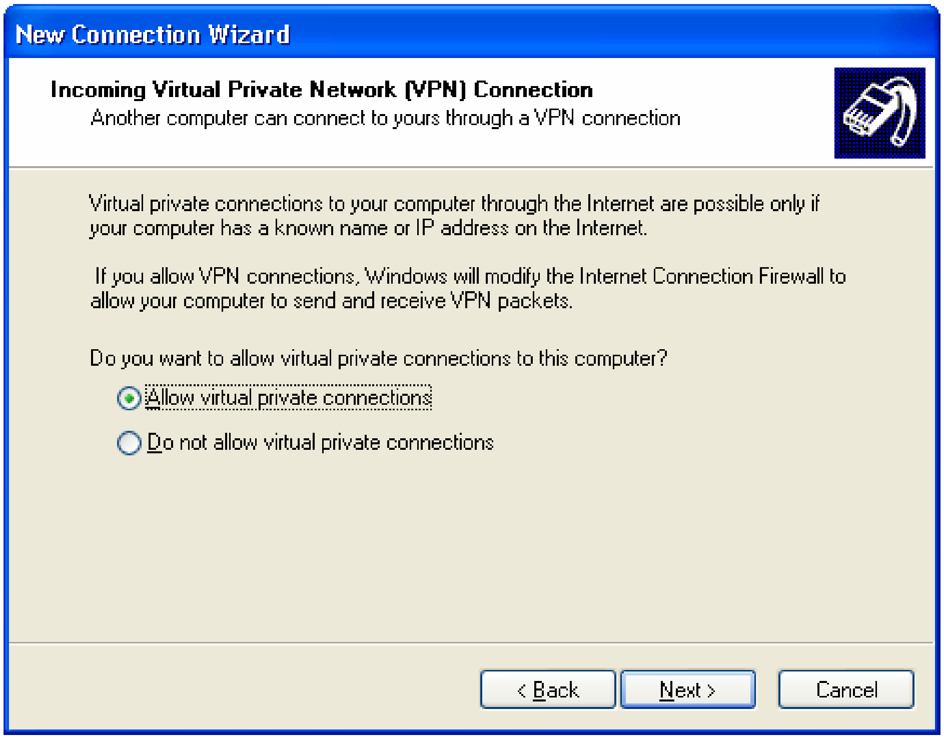
● **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

Figure 1. Choosing the network connection type.

4. Select Accept Incoming connections. Click Next.

5. In the next window, you can select the other devices to accept the incoming connection. Click Next.

6. Select Allow virtual private connections and click Next (see Figure 2).



New Connection Wizard

Incoming Virtual Private Network (VPN) Connection

Another computer can connect to yours through a VPN connection

Virtual private connections to your computer through the Internet are possible only if your computer has a known name or IP address on the Internet.

If you allow VPN connections, Windows will modify the Internet Connection Firewall to allow your computer to send and receive VPN packets.

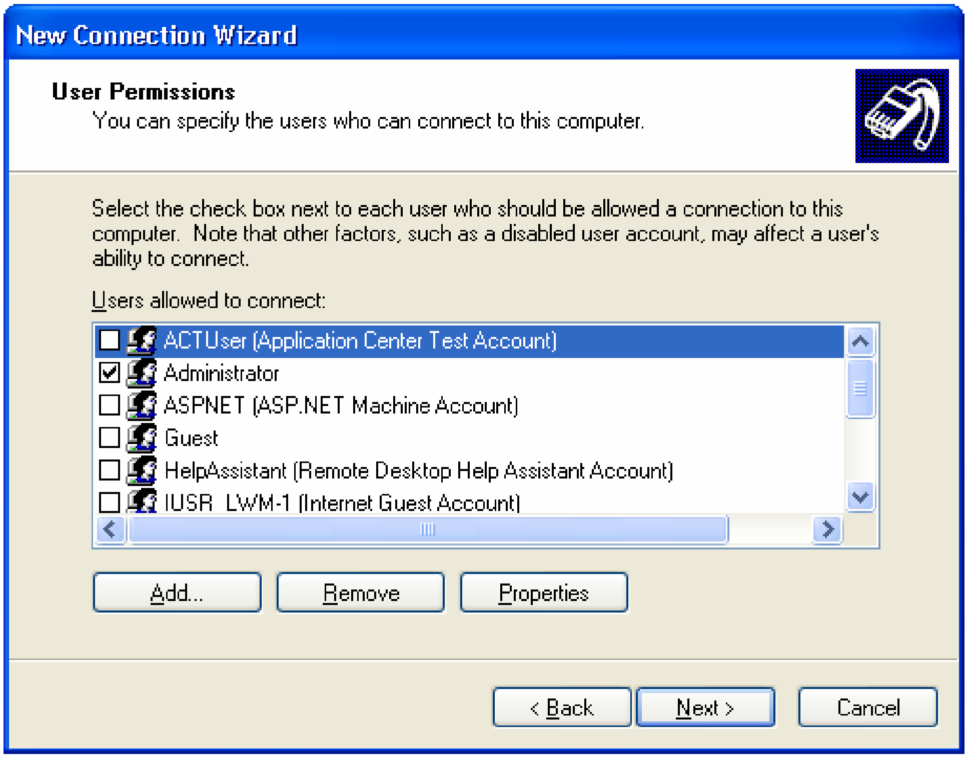
Do you want to allow virtual private connections to this computer?

● Allow virtual private connections

○ Do not allow virtual private connections

Figure 2. Allowing a VPN connection.

7. Select the users you want to allow to connect to your computer using the VPN connection (see Figure 3). Click Next.



New Connection Wizard

User Permissions

You can specify the users who can connect to this computer.

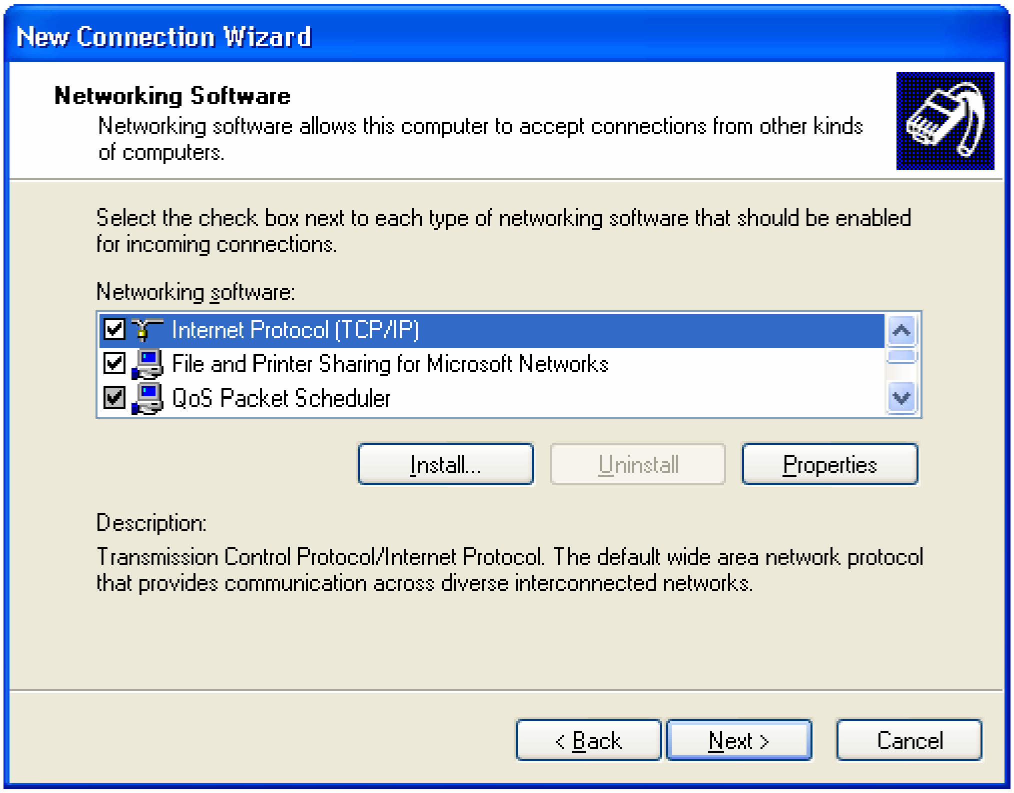
Select the check box next to each user who should be allowed a connection to this computer. Note that other factors, such as a disabled user account, may affect a user's ability to connect.

Users allowed to connect:

□ ACTUser (Application Center Test Account)
☑ Administrator
□ ASPNET (ASP.NET Machine Account)
□ Guest
□ HelpAssistant (Remote Desktop Help Assistant Account)
□ IUSR_LWM-1 (Internet Guest Account)

Figure 3. Granting access rights to users.

8. The next window allows you to install additional networking software for this connection (see Figure 4). After you choose your protocols and software, click Next.



New Connection Wizard

Networking Software

Networking software allows this computer to accept connections from other kinds of computers.

Select the check box next to each type of networking software that should be enabled for incoming connections.

Networking software:

☑ Internet Protocol (TCP/IP)
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler

Description:

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

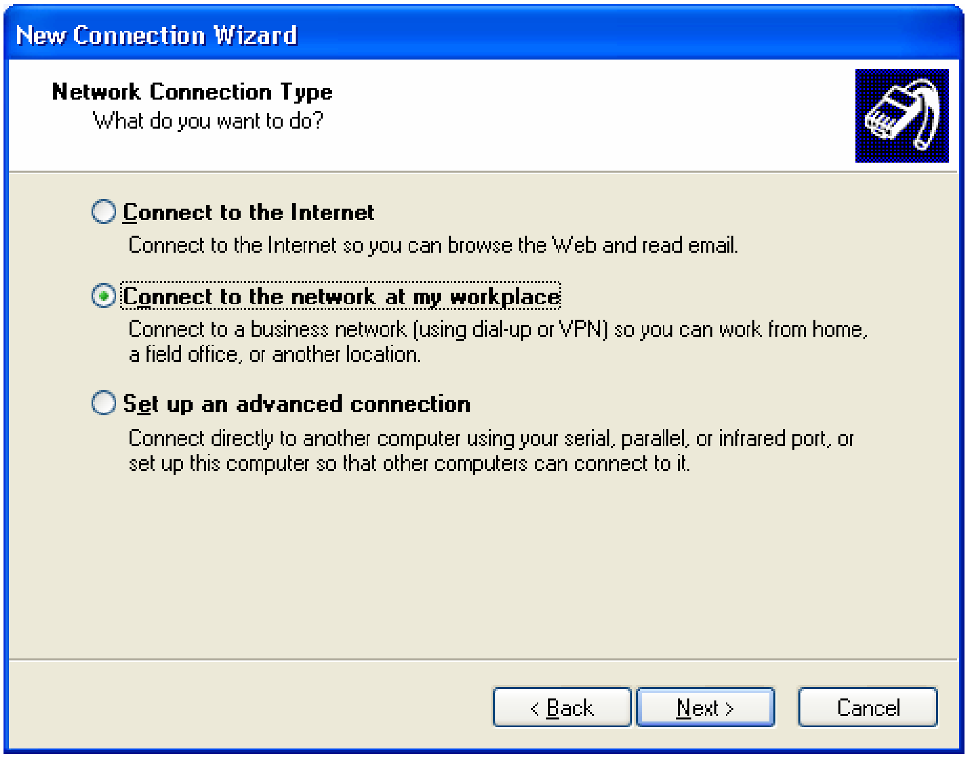
Figure 4. Installing the networking software for the VPN connection.

9. Click Next and then click Finish to complete the process.

On the Client

To configure Windows XP to connect to a VPN:

1. On the desktop, right-click on Network Connections.
2. Select Create a new connection.
3. Select **Connect to the network at my workplace** (see Figure 5). Click Next.



Network Connection Type
What do you want to do?

○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

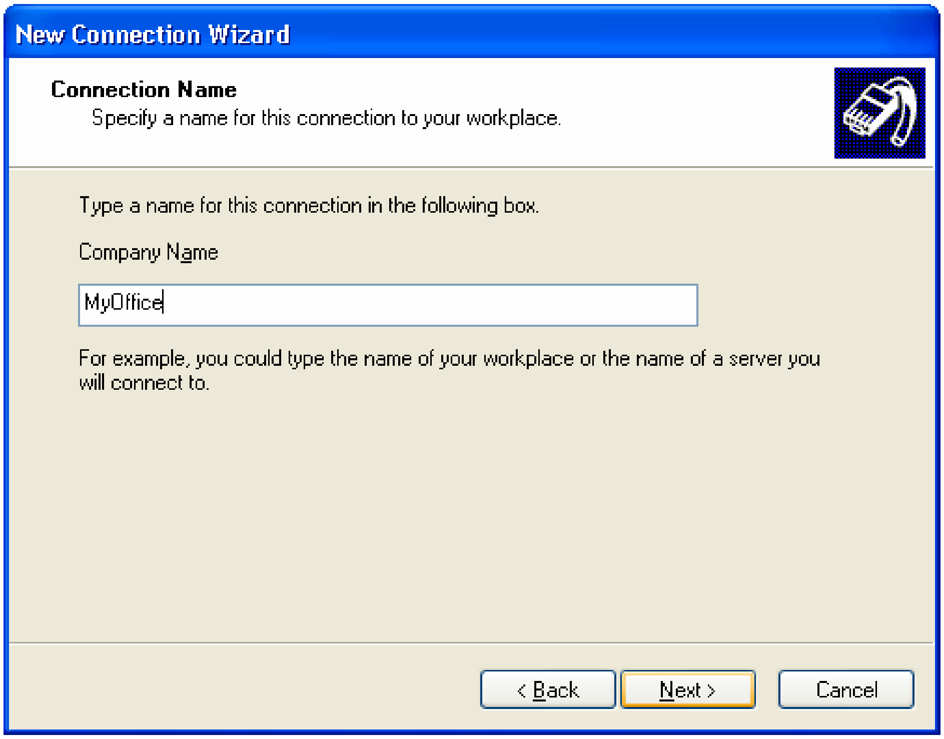
● **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

Figure 5. Selecting the network connection type.

4. Select Virtual Private Network connection. Click Next.

5. Enter a name for the VPN connection (see Figure 6). Click Next.



New Connection Wizard

Connection Name

Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name

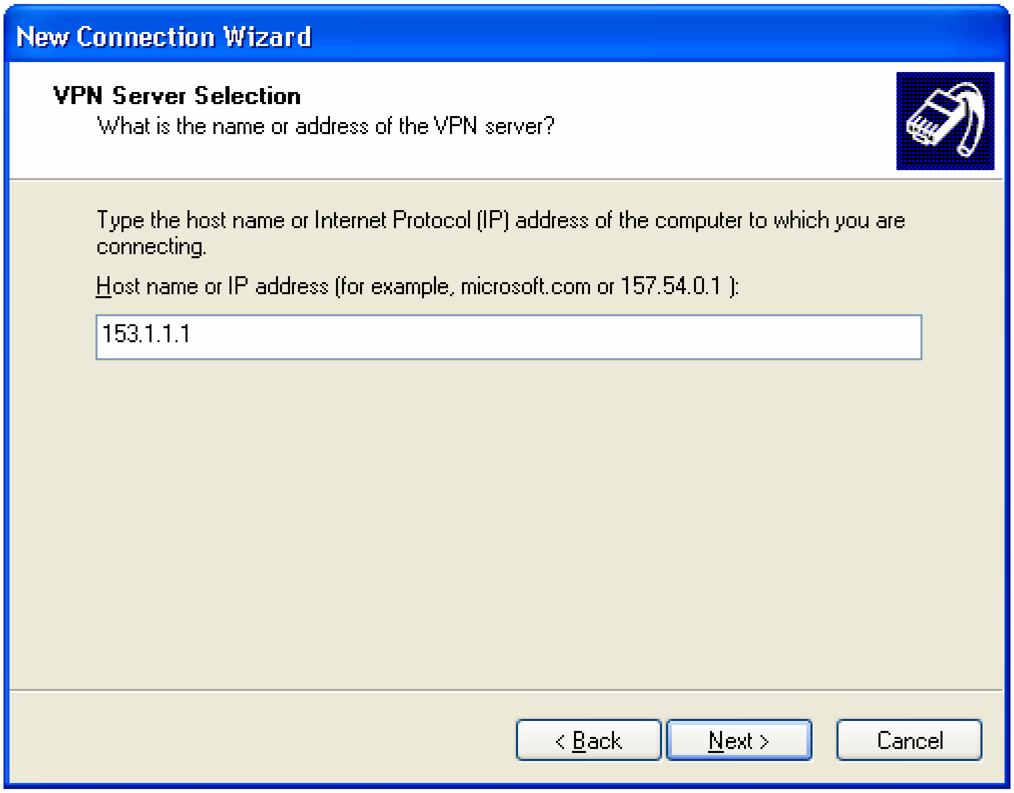
MyOffice

For example, you could type the name of your workplace or the name of a server you will connect to.

Figure 6. Giving your VPN connection a name.

6. Select "Do not dial the initial connection." Click Next.

7. Enter the IP address of the VPN server (see Figure 7). Click Next.



New Connection Wizard

VPN Server Selection

What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1): 153.1.1.1

Figure 7. Specifying the IP address of the VPN host.

8. Select My use only. Click Next.

9. Check the "Add a shortcut to this connection to my desktop" checkbox. Click Finish.

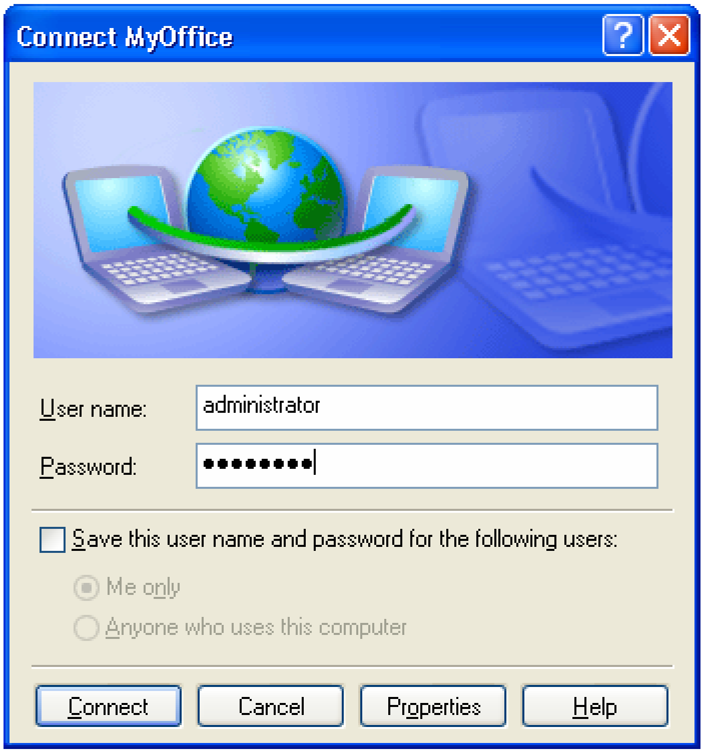
That's it! When the process is completed, an icon will be shown on the desktop (see Figure 8).

Figure 8. The icon for the VPN connection.

Connecting to a VPN

To connect to the VPN server, double-click on the icon MyOffice

and login with your user name information (see Figure 9). You can now work as though you were working on a computer in your office; most (if not all) of your network resources, such as file and print servers will be accessible.



Connect MyOffice

User name: administrator

Password: ●●●●●●●●●

□ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

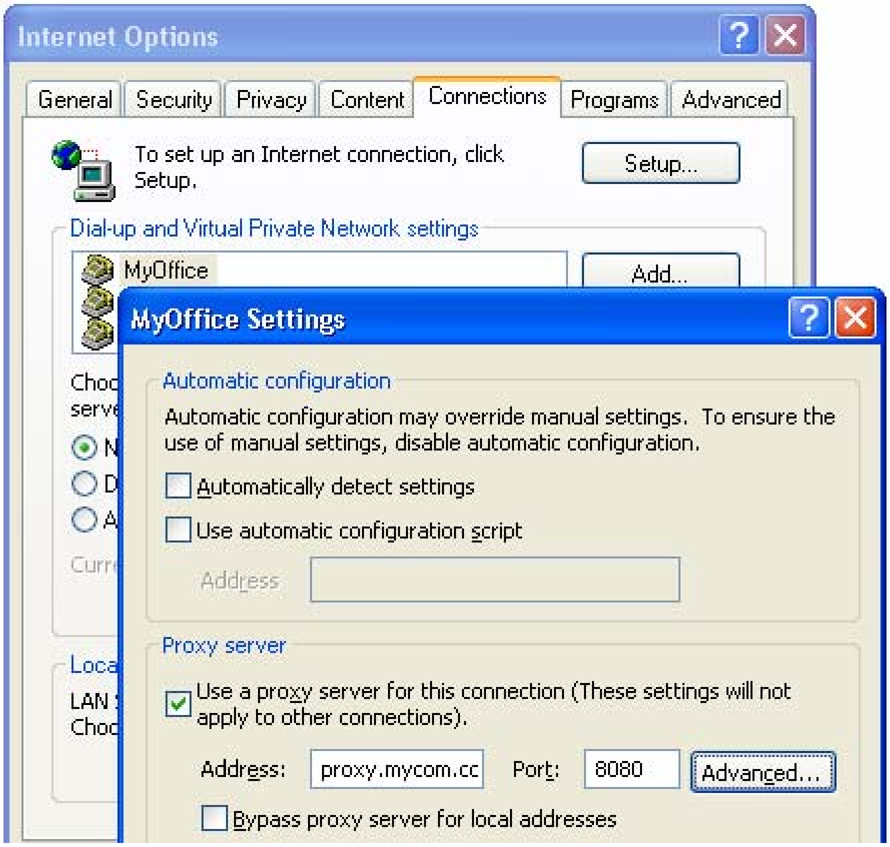
Figure 9. Logging in to a VPN connection.

Tip

Resist the temptation to check the box titled "**Save this User Name and Password for the following users**". If you enable this, your password will be saved on your computer, and if your computer is stolen or compromised, an attacker will be able to connect to the VPN and access everything it protects.

Problem with Proxy Servers

One common error you might encounter has to do with setting a proxy server in Internet Explorer. My ISP does not require me to use a proxy server when surfing the Web. But when I connect to the VPN server in my workplace, I am suddenly unable to connect to the Web. As it turned out, my company requires me to use a proxy server to connect to the Web. With the proxy server configured in IE, I am now able to connect to the Web (see Figure 10). Check with your network administrator for proxy information, and how to set it up.



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

MyOffice

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for this connection (These settings will not apply to other connections).

Address: proxy.mycom.cc Port: 8080

□ Bypass proxy server for local addresses

Figure 10. Setting a proxy server for a VPN connection.

IPSec and PPTP Pass Through

Most routers support a feature known as "IPSec and PPTP pass through." You may need to enable that feature on your router; check its documentation for details.

IPSec and PPTP are security protocols that provide authentication and encryption over the Internet. The "pass through" feature of the router allows secure packets to flow through the router but the router itself does not perform any authentication or encryption operation.

IPSec works in two modes -- transport mode and tunnel mode. Transport mode secures IP packets from source-to-destination, whereas tunnel mode puts an IP packet into another packet that is sent to the tunnel's endpoint. Only tunnel mode (ESP) IPSec can be passed through.