

MICROSOFT
TRAINING
AND CERTIFICATION

Microsoft Official
Curriculum

Module 10: Supporting Remote Users

Contents

Overview	1
Establishing Remote Access Connections	2
Connecting to Virtual Private Networks	13
Configuring Inbound Connections	17
Configuring Authentication Protocols and Encryption	19
Lab 10A: Configuring a VPN Connection	28
Using Remote Desktop	29
Lab 10B: Configuring and Using Remote Desktop	33
Storing User Names and Passwords to Facilitate Remote Connections	34
Lab 10C: Storing User Names and Passwords	37
Review	38



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, places or events is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2001 Microsoft Corporation. All rights reserved.

Microsoft, BackOffice, MS-DOS, Windows, Windows NT, Active Directory, ActiveX, BackOffice, DirectX are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Instructor Notes

Presentation:
60 Minutes

Labs:
60 Minutes

This module provides students with the skills and knowledge necessary to support remote users. This includes configuring and troubleshooting virtual private network (VPN) connections, other inbound and outbound connections, authentication protocols and encryption, and using Remote Desktop.

After completing this module, students will be able to:

- Create and configure an outbound remote connection on a computer running Microsoft® Windows® XP Professional.
- Connect a computer running Windows XP Professional to a VPN.
- Configure inbound VPN connections on computers running Windows XP Professional.
- Configure authentication protocols and encryption for remote access sessions.
- Configure computers to use Remote Desktop.
- Store user names and passwords to facilitate remote connections.

Materials and Preparation

This section provides the materials and preparation tasks that you need to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2272A_10.ppt

Preparation Tasks

To prepare for this module:

- Read all of the materials for this module.
- Complete the labs.

Instructor Setup for a Lab

This section provides setup instructions that are required to prepare the instructor computer or classroom configuration for a lab.

Lab 10A: Configuring a VPN Connection

► **To prepare for the lab**

1. The IP address or computer name of your partner's computer.
2. A computer running Windows XP Professional configured as a member of a workgroup.

Lab 10B: Configuring and Using Remote Desktop

► **To prepare for the lab**

- There are no setup tasks for this lab.

Lab 10C: Storing User Names and Passwords

► **To prepare for the lab**

- Student computers need access to a computer running Microsoft Windows 2000 Advanced Server configured as a Domain Controller.

Module Strategy

- Overview

In this section, first give an overview of the tasks in the module. Explain that the focus on the modules is on remote access protocols, and the services that use them, including Remote Desktop.

- Establishing Remote Access Connections

In this section, first discuss the hardware devices that are used to make remote connections, and the relative strengths and weaknesses of each. Next, present the information on establishing direct, broadband, dial-up, and cable connections by using the Network Connection Wizard. In the section on establishing a Remote Access session, explain that every time a user makes a remote connection, a remote session is established. Sessions are established on each server on which the user needs to be authenticated. Next, present the information on data transport protocols. Explain that a remote access server running the Routing and Remote Access service uses both Remote Access protocols, and local area network (LAN) protocols. Finally, present the information on configuring multilink connections, and provide scenarios in which the students would consider configuring these connections.

- Connecting to Virtual Private Networks

In this section, first give an overview of VPNs, and explain that they create a virtual space in the Internet through which users can securely transmit data. Next, discuss the VPN protocols, and provide specific examples of when Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP) are used. Explain that if the VPN protocols configured on the remote access client and the remote access server differ, connections may not be possible.

- Configuring Inbound Connections

In this section, discuss configuring inbound connections to a computer running Windows XP Professional, and provide examples of when that may be necessary.

- Configuring Authentication Protocols and Encryption

In this section, first examine the standard and extensible authentication protocols. Next, demonstrate how to configure client authentication protocols and client data encryption. Explain that if a remote access server and a remote access client are using different authentication protocols, communication between them may be impossible.

- Examining the Remote Desktop Feature

In this section, discuss the functionality of the Remote Desktop feature, and explain that it enables users to gain access to their desktop computers from anywhere that they can establish a connection to their network. Emphasize the requirements for using Remote desktop, which include installing Remote Access Connections and Terminal Services client on the remote computer that will be used to connect to the desktop. Emphasize that when one person is accessing a desktop remotely, no one may use the computer locally, or one of the users will be automatically logged off.

- **Configuring Computers to Use Remote Desktop**

In this section, demonstrate how to configure remote and local computers to use Remote Desktop.

- **Storing Usernames and Passwords to Facilitate Remote Connections**In this section, explain how to store user names and passwords to facilitate remote connections. The Stored User Names and Passwords feature is also known as the Windows Keyring, and Credential Manager, although these alternate titles do not appear in the UI. Emphasize the best practices for using stored user names and passwords, and explain how failing to use these best practices may compromise security.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Training and Certification courseware.

Lab Setup

Setup Requirement 1

The labs in this module require students to have completed Lab1C, Upgrading Microsoft Windows 98 to Windows XP Professional.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about supporting remote users, including establishing remote connections, connecting to VPNs, configuring remote authentication protocols and encryption, using the Remote Desktop feature, and storing multiple user names and passwords.

- **Establishing Remote Access Connections**
- **Connecting to Virtual Private Networks**
- **Configuring Inbound Connections**
- **Configuring Authentication Protocols and Encryption**
- **Using Remote Desktop**
- **Storing Usernames and Passwords to Facilitate Remote Connections**

In many organizations, employees often need to share work and resources from different locations. Many workers perform their jobs at remote sites, including their homes and satellite offices away from their normal work place. These employees need the same access to resources and the ability to collaborate with colleagues as if all of the employees are working in a central location. With Microsoft® Windows® XP Professional you can provide remote users full access to organizational resources.

After completing this module, you will be able to:

- Create and configure an outbound remote connection on a computer running Microsoft Windows XP Professional.
- Connect a computer running Windows XP Professional to a virtual private network (VPN).
- Configure inbound VPN connections on computers running Windows XP Professional.
- Configure authentication protocols and encryption for remote access sessions.
- Configure computers to use Remote Desktop.
- Store user names and passwords to facilitate remote connections.

◆ Establishing Remote Access Connections

Topic Objective

To introduce the components of establishing remote connections.

Lead-in

The first step in establishing remote access connections is to configure the outbound connection.

- **Establishing Outbound Connections**
- **Exploring Connection Options**
- **Creating a Direct Cable Connection**
- **Creating Dial-up and Broadband Connections**
- **Establishing a Remote Access Session**
- **Examining Data Transport Protocols**
- **Configuring Multilink Connections**

To establish a remote access connection, you must first establish an outbound connection on the remote computer. Outbound connections are dial-up, broadband, or direct cable connections to another computer.

There are several connection options, each of which uses a different type of hardware. Understanding the relative advantages and disadvantages of each connection option is important to planning and implementing remote access connections.

After the hardware and software are configured for remote access, you can establish a remote access session. A remote access session connects the remote client computer to the remote access server, also known as a gateway. Each remote connection uses data transport protocols. Understanding these protocols is important to understanding how data is protected and delivered during a remote session.

Multilink connections enable users to combine multiple physical links, such as modems and ISDN (Integrated Services Digital Network) lines, to increase the communication bandwidth available to the remote computer. This is important to remote users who may not have access to broadband or other high bandwidth means of communication.

Establishing Outbound Connections

Topic Objective

To describe the types of outbound connections.

Lead-in

The first step in establishing a remote connection is configuring an outbound connection on the remote computer.

■ Internet Connections

- Dialup and broadband connections using a modem, ISDN line, cable modem, or DSL modem

■ Connections to Private Networks

- Dialup or VPN connections

■ Advanced Connections

- Direct cable connections

To establish a remote access connection, you must first configure the outbound connection. *Outbound connections* are connections that are made from a remote access client to a remote access server.

For Your Information

This module does not address server configuration. Instead, it focuses on configuring the client to work with the remote access server.

The remote access server runs the *Routing and Remote Access service*, which supports various data transport protocols and virtual private network (VPN) protocols to enable remote connections. By being familiar with the benefits and limitations of various types of connections and the protocols that each of them employ, you will be able to effectively configure remote connections on computers running Windows XP Professional.

There are three basic types of outbound connections:

- *Internet connections.* Connections to an Internet service provider (ISP) can be configured as dial-up connections or broadband connections that use a cable modem, ISDN line, or DSL (digital subscriber line) modem.
- *Connections to private networks.* Connections to a private network can be configured as dial-up or VPN connections.
- *Advanced connections.* Advanced connections are used to configure a connection directly to another computer by using a cable.

For Your Information

The connection types are explained as three basic types of outbound connections, because that is how the New Connection Wizard displays them.

You configure all outbound connections in Windows XP Professional by using the New Connection Wizard. Much of the work of configuring protocols and services is automated when you use the wizard. By understanding the options in this wizard and the protocols that those options configure, you will be able to configure connections efficiently.

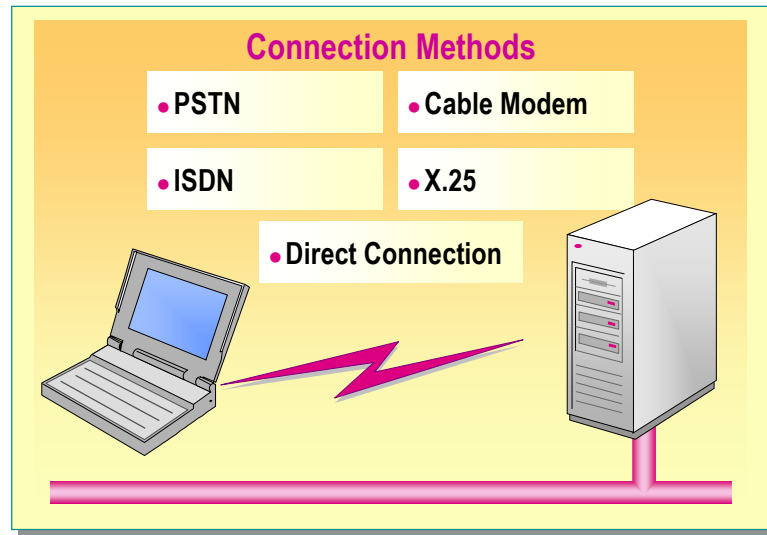
Exploring Connection Options

Topic Objective

To illustrate the connectivity options that Windows XP Professional includes for remote access.

Lead-in

Windows XP Professional can use a wide variety of hardware to create remote access connections.



You can connect remote access clients to a remote access server by using any of several types of connections. Windows XP Professional supports connections over the Public Switched Telephone Network (PSTN), ISDN lines, cable modems, an X.25 network, or direct cable connections. When selecting a connection type to use for remote access, you should consider the advantages and disadvantages of each type of connection, which are explained in the following table.

Hardware type	Advantages	Disadvantages
PSTN	Universal availability; inexpensive modems; higher speeds available with DSL	Toll charges; low speeds unless using DSL; DSL is not available in all locations.
ISDN	Faster than most PSTN connections; dedicated lines; wide availability in urban areas	Low speeds compared with DSL or cable modems.
Cable modem	Very fast connections	Shared bandwidth. Not as available as other connection types.
X.25	Secure, dedicated network	Not globally used.
Direct connection (parallel cables, serial cables, or infrared sensors)	Simple, secure, dedicated connection; inexpensive cables	Distance between computers limited to length of cable or infrared sensor range.

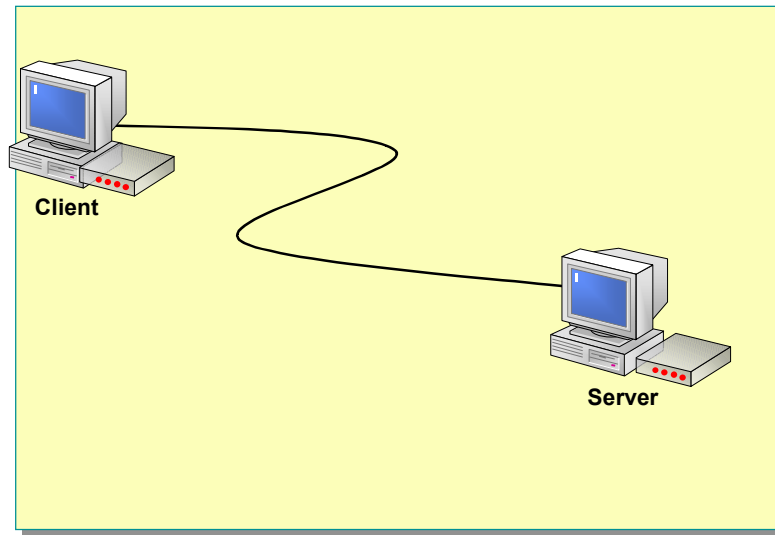
Creating a Direct Cable Connection

Topic Objective

To illustrate key pages in the New Connection Wizard for establishing a direct connection.

Lead-in

You can use the New Connection Wizard to create a direct cable connection to another computer.



You can use the New Connection Wizard to create a direct cable connection to another computer. Although a direct connection is the easiest and most secure way to connect to a computer to which you need to gain access, this option is not feasible if the client and the server are not located at the same physical location. The type of cable determines the maximum length for the cable before communication degradation occurs.

To create a direct connection to a remote server or another computer from a remote client:

Delivery Tip

Demonstrate the New Connection Wizard for the procedure in this topic, and throughout the module.

1. Click **Start**, click **Control Panel**, click **Network and Internet Connections**, click **Network Connections**, and then double-click **New Connection Wizard**.
2. In the New Connection Wizard, read the **Welcome** page, click **Next**, select **Set up an advanced connection**, and then click **Next**.
3. On the **Advanced Connection Options** page, select **Connect directly to another computer**, and then click **Next**.
4. On the **Host or Guest?** page, select **Guest**, and then click **Next**.
5. On the **Connection Name** page, in the **Computer name** box, type a name for the connection.
6. On the **Select a Device** page, select **Communications Port COM1**, and then click **Next**.
7. If you want this connection to be made available to all users of this computer, on the Connection Availability page, click **Anyone's use**, and then click **Next**. If you want to reserve the connection for yourself, select **My use only**, and then click **Next**.
8. On the Completing the New Connection Wizard page, click **Finish**.

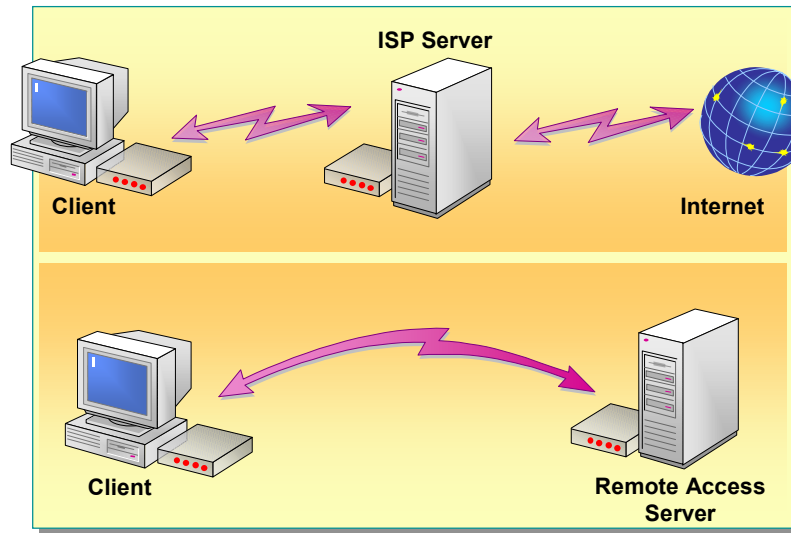
Creating Dial-up and Broadband Connections

Topic Objective

To illustrate how dial-up and broadband connections work.

Lead-in

You can use the New Connection Wizard to create and configure an outbound connection.



You can use the New Connection Wizard to create and configure dial-up and broadband outbound connections to an Internet service provider (ISP), through which you can connect to a private network. You can also create a dial-up connection directly to a private network. A *dial-up connection* is one in which the remote computer uses the Public Switched Telephone Network (PSTN) phone line to dial the number of the ISP server. A *broadband connection*, which can transport many times more data than an ordinary phone line, uses a broadband device such as a cable modem, a DSL modem, or an ISDN phone line.

Creating Dial-up Connections to Private Networks

You can create a dial-up connection directly to a computer or private network by using the New Connection Wizard. To connect to the network by using dial-up remote access, a remote access client uses a communications network, such as the PSTN, to create a physical connection to a port on a remote access server on the private network. This is typically done by using a modem or ISDN adapter to dial in to the remote access server.

Dial-up remote access enables an organization to keep users connected to its network when the users are working remotely. However, if your organization has a large number of users traveling to many locations, the expense of long-distance telephone charges will become significant. An alternative to increasing the size of a dial-up remote access network is to consider using a VPN solution for remote connectivity.

To create a dial-up connection to a private network:

1. Click **Start**, click **Control Panel**, click **Network and Internet Connections**, click **Network Connections**, and then click **New Connection Wizard**.
2. In the New Connection Wizard, read the **Welcome** page, click **Next**, select **Connection to the network at my workplace**, and then click **Next**.
3. Type a name for the connection, and then click **Next**.
4. Select **Dial-up connection**, click **Next**, and type the applicable phone number information. If the phone line used has special requirements, such as dialing 9 first, select **Use dialing rules**, configure the rules, click **Next**, and then complete the wizard.

Note The **Connection to the network at my workplace** option also enables you to create a connection through a VPN. Creating VPN connections is covered in the Configuring a Virtual Private Network Connection topic in this module.

Connecting Through the Internet

To create an Internet connection to an ISP, select **Connect to the Internet** on the **Network Connection Type** page in the New Connection Wizard. There are two reasons that organizations sometimes prefer to have employees gain access to secure and non-secure resources by using the Internet. First, using the Internet does not require an organization to use a large pool of modems; second, long-distance charges are not incurred if the ISP has a local number that the user can dial to make a connection. Using an ISP to gain access to the organization's network is a good solution for organizations that want to use the Internet as a part of their network infrastructure.

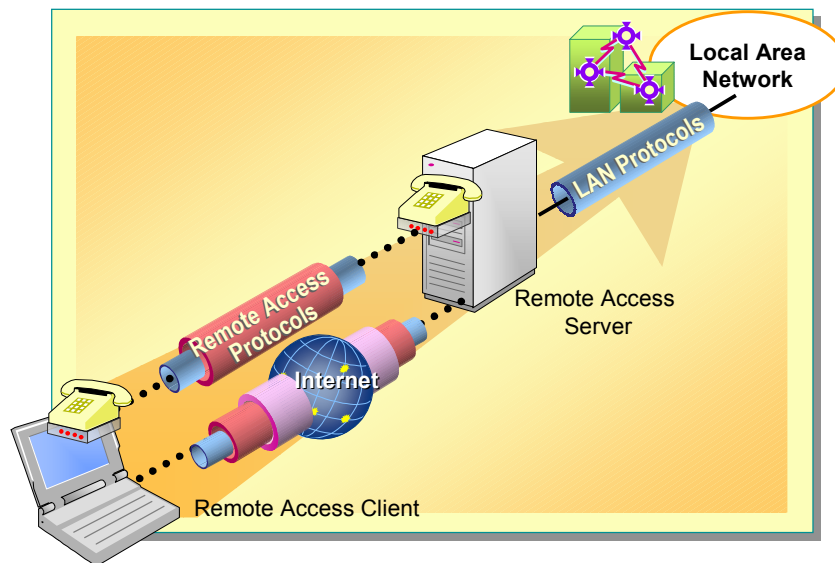
Establishing a Remote Access Session

Topic Objective

To illustrate the process that occurs when establishing a remote access connection.

Lead-in

Remote or mobile employees can connect to the corporate network by using remote access.



After configuring the outbound remote access connections, you can establish a remote access connection.

Users run remote access software and initiate a connection to the remote access server. This connection uses a remote access protocol, such as the Point-to-Point (PPP) Multilink Protocol.

The remote access server to which a remote client connects runs the Routing and Remote Access service. Routing and Remote Access uses both remote access protocols and LAN protocols to enable clients to connect to remote access servers. *Remote access protocols* control transmission of data over wide area network (WAN) links, whereas *LAN protocols* control transmission of data within the local area network.

By using this connection, the client sends data to and receives data from the remote access server. The data is encoded by a protocol such as Transmission Control Protocol/Internet Protocol (TCP/IP) and is then encapsulated in a remote access protocol.

All services typically available to a LAN-connected user are enabled for a remote user through the remote access connection. These services include file and print sharing, Web server access, and messaging.

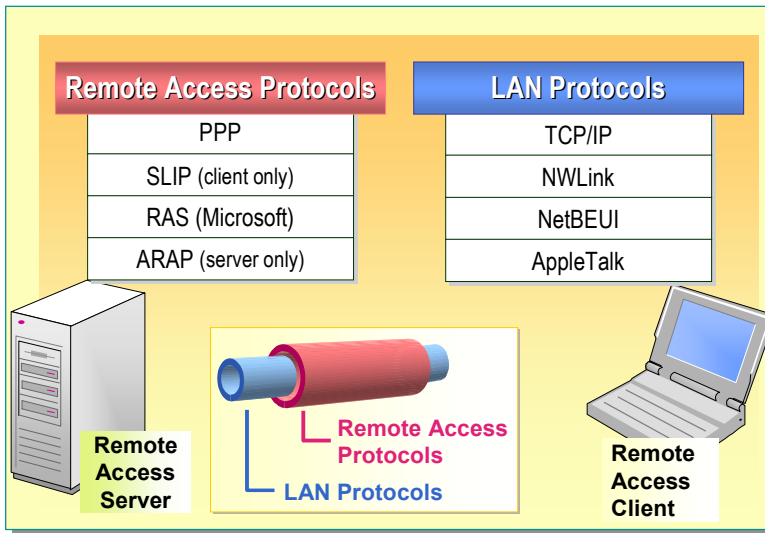
Examining Data Transport Protocols

Topic Objective

To introduce the protocols that are used for remote access.

Lead-in

Windows XP uses both remote access protocols and LAN protocols to support remote access.



Windows XP uses a remote access protocol to establish a connection between the remote access devices, which are usually modems. Windows XP Professional then uses LAN protocols to establish communication between the two computers. When a remote access client communicates with a server, Routing and Remote Access encapsulates the data in a LAN protocol packet for transport in the LAN. This packet is then encapsulated in a remote access protocol packet for transport to the server.

Remote Access Protocols

Windows XP Professional supports several remote access protocols to provide clients using a dial-up connection with access to a variety of remote access servers.

PPP

PPP enables remote access clients and servers to operate together in a network. For example, clients running Windows XP Professional can connect to remote networks through any server that uses PPP. Similarly, computers running other remote access software can also use PPP to dial in to a computer running Windows XP Professional configured with an incoming connection. This is the most commonly used remote access protocol.

Serial Line Internet Protocol (SLIP)

SLIP enables Windows XP Professional-based computers to connect to a SLIP server. SLIP is most commonly used with Telnet, and is not suitable for most modern remote access applications. Windows XP Professional does not include a SLIP server component.

RAS

RAS is an older protocol used by Microsoft. Client computers running Windows XP Professional use the RAS protocol to connect to remote access servers running Microsoft Windows NT® 3.1, Microsoft Windows for Workgroups, Microsoft MS-DOS®, or LAN Manager.

LAN Protocols

Windows XP Professional configured for incoming connections supports the following LAN protocols:

- TCP/IP
- NWLink

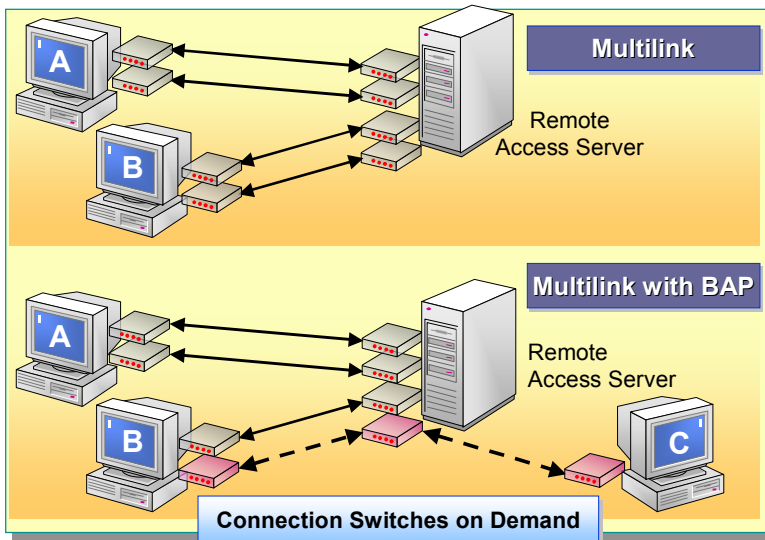
Configuring Multilink Connections

Topic Objective

To describe the purpose of, and illustrate the process of, configuring multilink connections on a remote access client.

Lead-in

Multilink enables physical connection devices to be grouped into a larger, more efficient, logical connection device with more bandwidth.



Multilink enables users to combine analog modem paths, ISDN paths, and even mixed analog and digital communications links on client and server computers. Multilinking combines multiple physical links into a logical bundle to increase the bandwidth available to the client computer.

Key Points

Multilink is primarily associated with dial-up connections. It is usually unnecessary to use with broadband connections.

Multilink enables your computer to use two or more communications ports as if they were a single port of greater bandwidth. Therefore, if you use two modems to connect to the Internet, you can connect at double the speed of a single modem. For example, a computer with four modems operating at 56 kilobits per second (Kbps), and a telephone line for each modem, can connect to a remote access server that has multiple modems and maintains a sustained transfer rate of 224 Kbps. Four 128-Kbps ISDN lines would return a throughput rate of 512 Kbps. To dial multiple devices, your connection and your remote access server must both have Multilink enabled.

The Multilink feature in Routing and Remote Access uses the PPP Multilink protocol. Windows XP also supports the Bandwidth Allocation Protocol (BAP) for dynamic multilinking.

PPP Multilink

The PPP Multilink protocol combines the bandwidth of two or more communication lines to create a single virtual data connection, providing scalable bandwidth based on the volume of data. Routing and Remote Access can use Multilink over multiple modems, ISDN, or X.25 cards. Both the client and remote access server must have Multilink enabled.

BAP

BAP enhances Multilink by dynamically adding or dropping links on demand. BAP is especially valuable to operations that have carrier charges based on bandwidth utilization. BAP is a PPP control protocol that works with PPP to provide bandwidth on demand.

Key Points

Multilink can only be configured on connections in which multiple devices were selected during setup. If you did not select multiple devices, you will need to recreate the connection.

Configuring Multilink on the Remote Access Client

To configure an outbound connection using multiple devices, you must have selected multiple devices when you created the connection. If you did not select multiple devices, you will need to recreate the connection using multiple devices. If you did select multiple communication devices, you can then add or change devices using the following procedure:

1. Right-click the connection on which you want to enable the dialing of multiple devices, and then click **Properties**.
2. On the **General** tab, select the check boxes for all of the devices that you want the connection to use, and then select **All devices call same numbers**.
3. On the **Options** tab, in **Multiple devices**, do one of the following:
 - a. If you want Windows XP Professional to dial only the first available device, click **Dial only first available device**, and then click **Configure**.
 - b. If you want Windows XP Professional to use all of your devices, click **Dial all devices**, and then click **Configure**.
 - c. If you want Windows XP Professional to dynamically dial and hang up devices as needed, click **Dial devices only as needed**, click **Configure**, and then perform the following actions.
 - i. In the **Automatic Dialing and Hanging Up** dialog box, under **Automatic Dialing**, select the **Activity at least** percentage and **Duration at least** time that you want to set. Another line is dialed when connection activity reaches this level for the amount of time that you specify.
 - ii. Under **Automatic hangup**, select the **Activity no more than** percentage and **Duration at least** time that you want to set. A device is disconnected when connection activity decreases to this level for at least the amount of time that you specify, and then click **OK**.
4. Click **OK**.

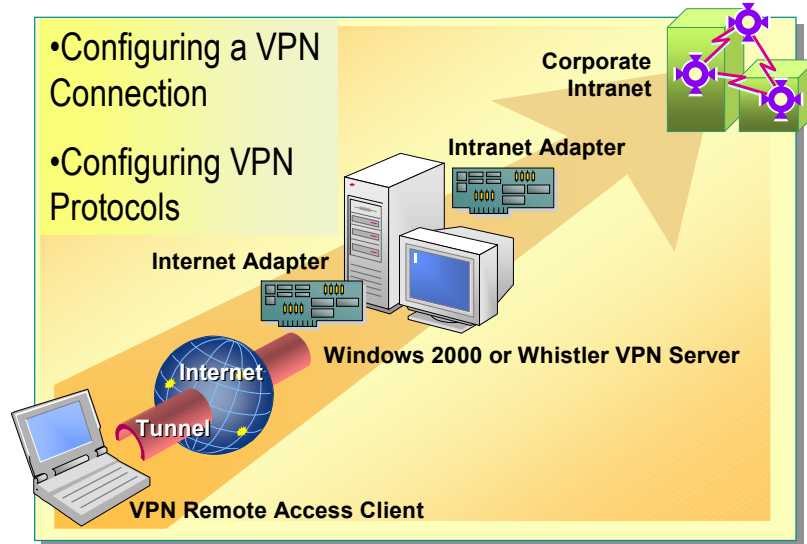
◆ Connecting to Virtual Private Networks

Topic Objective

To describe how VPN connections work and how to establish them.

Lead-in

A Virtual Private Network (VPN) provides a virtual network across an existing physical network, such as the Internet.



VPN protocols encapsulate data packets inside PPP data packets. The VPN creates a tunnel across the existing network infrastructure to send and receive the data. In this context, a *tunnel* is a secure communication route within the existing network.

Key Points

VPNs work by putting normal data packets inside PPP packets. Most VPN connections start with a connection to an ISP.

There are multiple ways that a client can connect to a network by using a VPN.

Typically, users will connect to the VPN by first connecting to an ISP and then connecting to the VPN gateway, which is the remote access server, through that Internet connection. In this case, the virtual tunnel extends from the client computer to the remote access server. The connection to the ISP and then the VPN can be configured to be a single-step process for the client.

Delivery Tip

Draw a diagram where the VPN tunnels start and stop in these two different cases.

The ISP can also create the tunnel on behalf of the client. When this occurs, the client connects to the ISP and provides a network logon. Then the ISP creates the tunnel and forwards the logon request to the client's network. In this case the tunnel extends from the ISP to the remote access server. The connection from the client to the ISP is not part of the VPN tunnel; but rather, it is a standard dial-up connection.

Note A VPN does not require a dial-up connection. It only requires connectivity between the client and the server. If the client is directly attached to a LAN that uses IP, and it can reach a server through the LAN, you can establish a tunnel across the LAN.

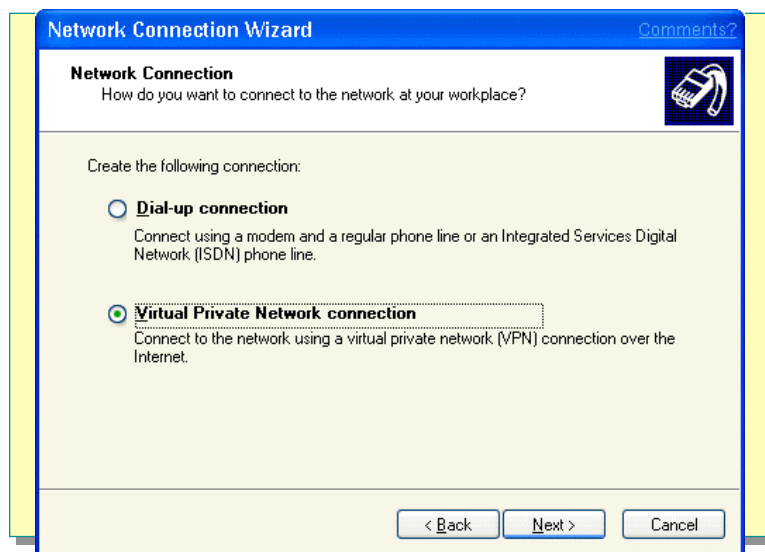
Configuring a Virtual Private Network Connection

Topic Objective

To describe the process for creating an outbound VPN connection.

Lead-in

You use the New Connection Wizard to create an outbound VPN connection.



A Virtual Private Network (VPN) provides a virtual network across an existing physical network, such as the Internet. By using the Internet in this way, organizations can reduce their long-distance telephone expenses and rely on existing infrastructure instead of managing their own infrastructures. Traveling employees can dial the local ISP and then make a VPN connection back to the corporate network. Dialing the local ISP eliminates the long-distance charges or toll calls associated with a dial-up connection.

To create a connection to a VPN:

1. Click **Start**, click **Control Panel**, click **Network and Internet Connections**, click **Network Connections**, and then double-click **Make a New Connection**.
2. In the New Connection Wizard, read the **Welcome** page, click **Next**, select **Connection to the network at my workplace**, and then click **Next**.
3. Click **Virtual Private Network connection**, and then click **Next**.
4. Type a name for the connection, and then click **Next**.
5. On the **Public Network** page, choose whether to have a connection automatically started, and then click **Next**.
6. Type the name or address of the VPN server, and then click **Next**.
7. If you want this connection to be made available to all users of this computer, click **Anyone's use**, and then click **Next**.

If you want to reserve the connection for your use only, click **My use only**, and then click **Next**.

8. On the **Account Information** page, type your name, password, and password confirmation, select any options you want to enable, click **Next**, and then click **Finish**.

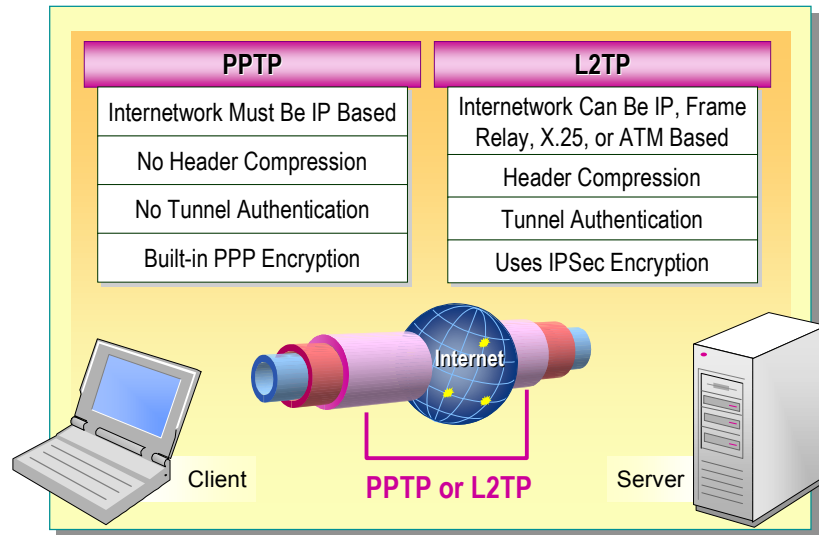
Configuring Virtual Private Network Protocols

Topic Objective

To list the differences between PPTP and L2TP.

Lead-in

The two supported VPN protocols, PPTP and L2TP, have different features and capabilities.



The protocols that can be used for a VPN have different capabilities and features. VPNs use either the Point-to-Point Tunneling Protocol (PPTP) or the Layer Two Tunneling Protocol (L2TP) to establish connections. Windows XP Professional allows you to specify which protocol to use when creating an outgoing VPN connection.

PPTP and L2TP

Both PPTP and L2TP use PPP to provide an initial envelope for the data and to append additional headers for transport through an existing network. Some of the key differences between PPTP and L2TP are listed in the following table.

Key Points

Differences between PPTP and L2TP include Connectivity, Header Compression, Authentication, and Encryption.

Feature	PPTP	L2TP
<i>Connectivity</i>	PPTP requires an IP-based internetwork.	Performs over a wide range of WAN connection media such as IP, frame relay, or ATM. Requires that tunnel media provide packet-oriented, point-to-point connectivity.
<i>Header Compression</i>	Does not support header compression. Operates with six byte headers.	Supports header compression. When enabled, operates with headers of four bytes.
<i>Authentication</i>	Does not support tunnel authentication or IPSec.	Supports tunnel authentication. VPN connections using L2TP can use IPSec.
<i>Encryption</i>	Automatically uses PPP encryption.	If configured, provides a secure tunnel by using IPSec. No automatic encryption.

Configuring the VPN Protocol on the Remote Client

You can configure the remote client to automatically choose which VPN protocol to use, or to use only PPTP or L2TP. To configure the client VPN protocol:

Demonstrate configuring the VPN protocol. Explain how to choose a VPN server type, and when to choose the three options in the **PPP Settings** dialog box.

1. Right-click the VPN connection that you want to configure, and then click **Properties**.
2. On the **Networking** tab, under **Type of VPN server I am calling**, select **Automatic**, **PPTP VPN** or **L2TP IPSec VPN** and then click **Settings**.
3. In the **PPP Settings** dialog box, select or clear the following options:
 - **Enable LCP extensions**. Specifies whether Link Control Protocol (LCP) extensions are enabled. LCP extensions may cause an inability to connect when you call servers by using older versions of PPP software. If consistent problems occur, clear this check box. If you clear the check box, LCP cannot send Time-Remaining and identification packets or request callback during LCP negotiation of PPP.
 - **Enable software compression**. Offers software data compression in addition to support for modem compressions. Therefore, when this option is enabled, you do not need to turn on modem compression to benefit from faster throughput.
 - **Negotiate multi-link for single link connections**. Specifies whether multilink negotiation is enabled for a single-link connection. If your remote access server supports this feature, you may notice improved audio quality. If you enable this option, you may not be able to connect to remote access servers that do not support this feature.
4. Click **OK** to close the **PPP Settings** dialog box, and then click **OK** to close the **Virtual Private Connection Properties** page.

Configuring Inbound Connections

Topic Objective

To describe the reasons for and steps in configuring inbound connections.

Lead-in

You can configure a computer running Windows XP Professional to accept inbound remote connections.

- **Configuring Devices**
- **Enabling VPN Connections**
- **Configuring User Permissions**
- **Choosing and Configuring Network Software**

You can also use the New Connection Wizard to configure a computer running Windows XP Professional to accept incoming dial-up or VPN connections. You configure a computer to accept incoming connections so that users can gain remote access to resources on that computer, and the network to which it is connected. When configuring the computer, you determine which hardware and protocols to use, and which users can use the inbound connections.

To configure an inbound connection on a computer running Windows XP Professional:

1. Click **Start**, click **Control Panel**, click **Network and Internet Connections**, click **Network Connections**, and then double-click **Make a New Connection**.
2. In the New Connection Wizard, read the **Welcome** page, click **Next**, select **Setup an advanced connection**, and then click **Next**.
3. Select **Accept incoming connections**, and then click **Next**.

The wizard will lead you through a series of pages, described in the following sections, which enable you to configure the computer and user permissions.

Configuring Devices

You can configure the computer to accept incoming connections through the Internet, a phone line, or a direct cable connection. On the **Devices for Incoming Connections** page, you select the devices that you want to accept incoming connections. Only those devices currently installed will display; you cannot add devices in this wizard. You can configure hardware settings and terminal window settings for any device by selecting the device and then clicking **Properties**. If you are configuring a modem, you can select the modem, and then click **Properties** to configure call preferences, such as timeout settings, and data connection preferences, such as port speed and data protocol.

Enabling VPN Connections

On the **Incoming Virtual Private Network (VPN) Connections** page, you can choose whether or not to allow inbound VPN connections to the computer. If you want to accept inbound VPN connections over the Internet, the computer must have a known IP address or computer name on the Internet. If you choose to accept inbound VPN connections, Windows XP Professional will modify the Internet Connection Firewall to enable your computer to send and receive VPN packets.

Configuring User Permissions

On the **User Permissions** page, you can specify which users or groups can connect to the computer, and configure properties for each user or group. The configurable properties are passwords and callback methods.

Choosing and Configuring Networking Software

The **Network Software** page displays the default protocols, services, and clients configured for inbound connections, which are:

Delivery Tip

Demonstrate this portion of the wizard, and discuss when to add additional services, clients, and protocols.

- TCP/IP
- File and Printer Sharing for Microsoft Networks
- QoS (Quality of Service) Packet Scheduler
- Client for Microsoft Networks

You may want to configure the TCP/IP properties. The options include allowing callers to gain access to the LAN in addition to resources on the computer, and specifying TCP/IP address assignment. You can choose to have IP addresses automatically assigned by the DHCP, specify a range of addresses to use, or enable the calling computer to specify its own address.

You can also add clients, services, and protocols to enable the computer to accept inbound connections from computers that use networking software other than the defaults listed in this section.

◆ Configuring Authentication Protocols and Encryption

Topic Objective

To list topics relevant to authentication protocols.

Lead-in

There are several different protocols that can be used to authenticate users on a network. You must be able to configure the remote client to communicate with the network.

- **Standard Authentication Protocols**
- **Extensible Authentication Protocols**
- **Configuring Client Authentication Protocols**
- **Configuring Client Data Encryption**

Remote access servers use authentication to determine the identity of users attempting to connect to the network remotely. After a user is authenticated, the user receives the appropriate access permissions and is allowed to connect to the network.

The correct and secure authentication of user accounts is critical for the security of a network. Without authentication, unauthorized users can gain access to your network.

Running on the remote access server, Routing and Remote Access uses several protocols to perform authentication, and also allows for the use of Extensible Authentication Protocols (EAPs), through which you can load third-party protocols.

Data encryption can also be very important when using a network. Some data, for instance medical records, product plans, or trade secrets, are as sensitive in nature as passwords. Windows XP Professional enables you to encrypt the data that the authenticated user sends.

As an Information Technology (IT) professional supporting remote users, you may need to configure the remote client computer to use the same authentication and encryption protocols that the remote server is using.

Standard Authentication Protocols

Topic Objective

To list the level of security and appropriate use of standard authentication protocols.

Lead-in

Windows XP Professional supports many different standard authentication protocols, some of which are more secure than others.

Protocol	Security	Use when
PAP	<i>Low</i>	The client and server cannot negotiate using more secure validation
SPAP	<i>Medium</i>	A Shiva client calls in to a Windows Server, or a Windows XP client calls in to a Shiva Server
CHAP	<i>High</i>	You have clients that are not running Microsoft operating systems
MS-CHAP	<i>High</i>	You have clients running Windows NT version 4.0 and later, or Microsoft Windows 95 and later
MS-CHAP v2	<i>High</i>	You have dial-up clients running Windows 2000 or later, or VPN clients running Windows NT 4.0 or Windows 98 or later

Windows XP Professional supports many different authentication protocols that have varying levels of security. Only those protocols that you enable can be used to authenticate users to the remote access server.

PAP

The Password Authentication Protocol (PAP) uses clear-text passwords, which are unencrypted. If the passwords match, the server grants access to the remote access client. This protocol provides little protection against unauthorized access.

SPAP

The Shiva Password Authentication Protocol (SPAP) is a two-way reversible encryption mechanism employed by Shiva, a hardware manufacturer. SPAP encrypts the password data that is sent between the client and server and is, therefore, more secure than PAP.

CHAP

The Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that negotiates a secure form of encrypted authentication by using Message Digest 5 (MD5). CHAP uses the industry-standard MD5 one-way encryption scheme to encrypt the response, providing a high level of protection against unauthorized access. By encrypting the response, you can prove to the server that you know your password without actually sending the password over the network. The authentication process works as follows:

1. The remote access server sends a challenge, consisting of a session identifier and an arbitrary challenge string, to the remote access client.
2. The remote access client sends a response that contains the user name and a one-way encryption of the challenge string, the session identifier, and the password.
3. The remote access server checks the response, and if the response is valid, allows the connection.

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is a one-way, encrypted password authentication protocol. If the server uses MS-CHAP as the authentication protocol, it can use Microsoft Point-to-Point Encryption (MPPE) to encrypt data to the client or server.

MS-CHAP v2

A newer version of MS-CHAP, Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2), is available. This new protocol provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving data.

For VPN connections, Microsoft Windows 2000 Server offers MS-CHAP v2 before offering MS-CHAP. Windows XP Professional dial-up and VPN connections can use MS-CHAP v2. Computers running Microsoft Windows NT 4.0 and Microsoft Windows 98 can use MS-CHAP v2 authentication for VPN connections only.

Selecting Authentication Protocols

The following table describes the situations in which you use the protocols discussed in this section.

Protocols	Security	Use when
PAP	Low	The client and server cannot negotiate by using a more secure form of validation.
SPAP	Medium	Connecting to a Shiva LanRover, or when a Shiva client connects to a Windows-based remote access server.
CHAP	High	You have clients that are not running Microsoft operating systems.
MS-CHAP	High	You have clients running Windows 2000 or later, Windows NT 4.0, or Microsoft Windows 95 or later.
MS-CHAP v2	High	You have dial-up clients running Windows 2000 or later, or VPN clients running Windows NT 4.0 or Windows 98 or later. MS-CHAP v2 is the most secure form of authentication.

Extensible Authentication Protocols

Topic Objective

To list the key points related to the EAP protocol.

Lead-in

EAP is designed to provide proprietary and future authentication methods.

- **Allows the Client and Server to Negotiate the Authentication Method That They Will Use**
- **Supports Authentication by Using**
 - MD5-CHAP
 - Transport Layer Security
 - Additional third-party authentication methods
- **Ensures Support of Future Authentication Methods Through an API**

The Extensible Authentication Protocol (EAP), an extension of PPP, allows for customized authentication to remote access servers. The client and the remote access server negotiate the exact authentication method to be used.

EAP Authentication

EAP supports authentication by using:

- *MD5-CHAP*. The Message Digest 5 Challenge Handshake Authentication Protocol (MD5-CHAP) encrypts user names and passwords with an MD5 algorithm.
- *Transport Layer Security*. Transport Layer Security (TLS) is used for smart card, as well as other, intermediary security devices. Smart cards require a card and reader. The smart card electronically stores the user certificate and private key.
- *Additional, third-party authentication methods*. Vendors can use EAP to add their own authentication methods, such as smart cards. *Smart cards* are physical cards that provide passwords and may use several authentication methods, including the use of codes that change with each use.

To enable EAP authentication, open Routing and Remote Access, right-click your server, and then click **Properties**. The configuration settings are on the **Security** tab. You enable and configure specific EAP types on the **Authentication** tab of the **Edit Dial-in Profile** dialog box for the remote access policy.

Through the use of the EAP application programming interfaces (APIs), independent software vendors can supply new client and server authentication methods for technologies such as smart cards, biometric hardware (such as retina or fingerprint scanners), and authentication technologies that are not yet developed. Smart cards are the most widely adopted technology that uses the EAP protocol.

Smart Card Description and Features

A smart card is a credit card sized device you can use for storing sign-in passwords, and other personal information. Smart cards provide tamper-resistant and portable security solutions for tasks such as securing e-mail and logging on to a domain.

Support for smart cards is a feature of the public key infrastructure (PKI) that Microsoft has integrated into Windows XP. Smart cards provide:

- Tamper-resistant storage for protecting passwords and other forms of personal information.
- Isolation of security-critical computations involving authentication, digital signatures, and key exchange.
- A way to take logon information and other private information with you for use on computers at work, home, or on the road.

Smart Card Authentication Methods

A smart card can be used to authenticate users in a Windows 2000 network in two ways.

Interactive Log On

Interactive log on with a smart card begins when the user inserts the smart card reader, which signals the Windows XP Professional operating system to prompt for a PIN instead of a username, domain, and password.

Remote Access

A remote log on involves two separate authentications. The first authentication is to the remote access server, and results in remote access policies being applied to the client. The second authentication is to the network, and uses EAP Transport Level (EAP_TLS) protocols for authentication.

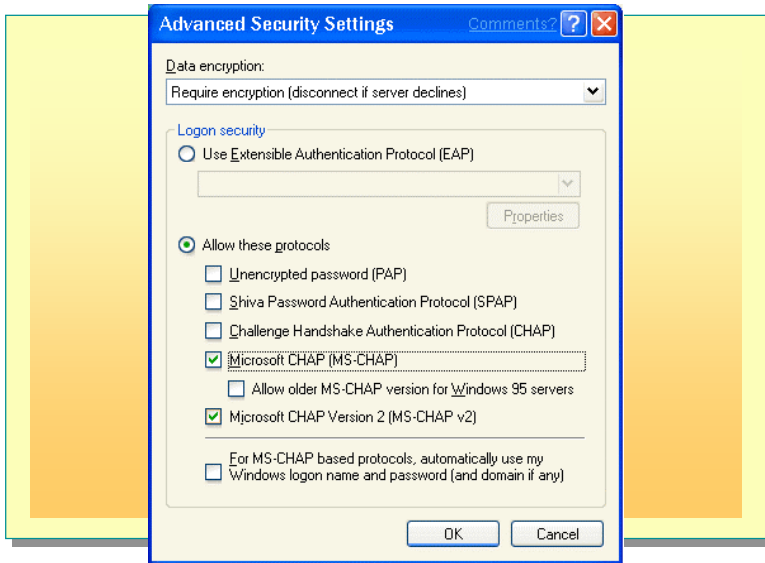
Configuring Client Authentication Protocols

Topic Objective

To describe the process for configuring client authentication protocols.

Lead-in

To configure authentication protocols, you first create the connection, and then right-click it to configure its properties.



Client authentication protocols determine which servers a remote access client can communicate with. If a client and server use different authentication protocols, they may not be able to establish a remote access session.

To configure authentication protocols on a client computer running Windows XP Professional:

1. Right-click the outbound VPN connection for which you want to configure protocols, and then click **Properties**.
2. In the **Virtual Private Connection Properties** dialog box, click the **Security** tab, select **Advanced (custom settings)**, and then click **Settings**.
3. Under **Logon security**, do one of the following:

To use EAP, select **Use Extensible Authentication Protocols (EAP)**, select a type of EAP in the drop-down list, click **OK**, and then click **OK** to close the dialog box.

To use other protocols, select **Allow these protocols**, select the protocols to use, click **OK**, and then click **OK** to close the dialog box.

When you choose EAP protocols, you have the option of choosing to use a smart card or an encrypted certificate. If you choose to use one of these options, there are additional configurable settings that can be configured by clicking the **Properties** button.

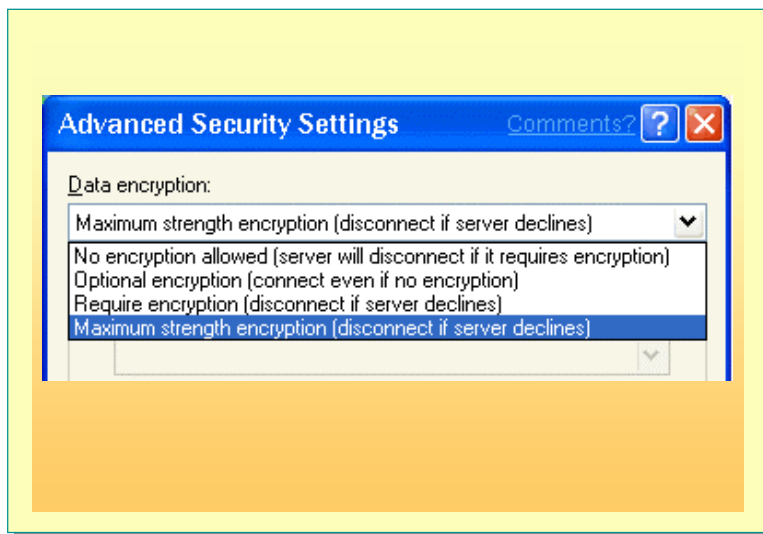
Configuring Client Data Encryption

Topic Objective

To illustrate how to configure data encryption

Lead-in

IPSec ensures secure communication over an IP network by using encryption.



Data encryption provides security by encrypting, or encoding, data that is sent between a remote access client and a remote access server. For situations that require the highest degree of security, the administrator can set the server to force encrypted communications. Clients attempting to connect to that server must encrypt their data or the server will refuse their connection.

Important Data encryption is only available if you use MS-CHAP, MS-CHAP v2, or TLS (an EAP protocol) as the authentication protocol.

Configuring Data Encryption Rules

To configure data encryption rules, right-click the VPN connection that you want to configure, click **Properties**, click the **Security** tab, select **Advanced**, click **Settings**, and then select a rule from the **Data encryption** drop-down list.

The following four data encryption rules are available:

- *No encryption allowed* (server will disconnect if it requires encryption). Use this option only when you are transmitting data that does not need to be protected.
- *Optional encryption* (connect even if no encryption). Use this option when some data need encryption, but encryption is not required for all data.
- *Require encryption* (disconnect if server declines). Use this option when all communications must be encrypted
- *Maximum strength encryption* (disconnect if server declines). Use this option when you require the highest level of encryption for all communications. Lower level of encryption will not be accepted by the server.

Encrypting Data by Using MPPE

MPPE encrypts data that moves between a PPTP connection and the VPN server. It has three levels of encryption: strongest (128-bit), strong (56-bit), and basic (40-bit) schemes. When a remote access server uses a level of encryption higher than the level of encryption used by the client, the two computers cannot communicate.

For Your Information

In some countries/regions, for example France, it is illegal to use encryption higher than 128-bit.

Note For 128-bit encryption, you must download the Windows 2000 high encryption pack from the Windows Update Web site. Many computers outside of the United States cannot communicate with computers using 128-bit or higher encryption.

Encrypting Data by Using IPSec

IP security (IPSec) provides computer-level authentication, as well as data encryption, for L2TP-based VPN connections. IPSec negotiates a secure connection between the remote client and the remote tunnel server before the L2TP connection is established, which secures user names, passwords, and data.

IPSec is a framework of open standards for ensuring secure private communications over IP networks. It does so by using authentication and encryption. IPSec provides aggressive protection against private network and Internet attacks. IPSec is transparent to the user. Clients negotiate a security association that functions as a private key to encrypt the data flow.

The typical IPSec policy is configured as a computer-based Group Policy. Therefore, when the computer connects to the network, the Group Policy setting is applied to the computer before the user logs on.

Lab 10A: Configuring a VPN Connection

Topic Objective

To introduce the lab.

Lead-in

In this lab, you configure a VPN connection.



Objectives

After completing this lab, you will be able to:

- Configure Windows XP Professional to allow incoming VPN connections.
- Configure and test an outgoing VPN connection by using the New Connection Wizard.

Prerequisites

Before working on this lab, you must have:

- Completed Lab 1C, Upgrading Windows 98 to Windows XP Professional.
- A computer running Microsoft Windows XP Professional.

Lab Setup

To complete this lab, you need the following:

- The IP address or computer name of your partner's computer.
- A computer running Windows XP Professional configured as a member of a workgroup.

Scenario

Your organization has employees that travel to remote locations. You do not have the resources to set up a worldwide network that would allow dial-up connections to these locations. Instead, you will need to configure a VPN server on the Internet and allow your staff to connect to your network through the VPN connection.

Estimated time to complete this lab: 30 minutes

◆ Using Remote Desktop

Topic Objective

To introduce the Remote Desktop feature, and how to configure it.

Lead-in

Remote desktop enables users to gain access to their desktop from a remote computer.

- **Examining the Remote Desktop Feature**
- **Configuring Computers to Use Remote Desktop**

The Remote Desktop feature of Windows XP Professional enables you to remotely gain access to your Windows XP Professional desktop from another computer on your network. This means that you can connect to your computer from another location and have access to all of your applications, files, and network resources as though you were located in front of your work computer. While you are operating the computer remotely, no one may use your work computer locally. However, an administrator may log on to the computer while you have a are connected remotely, in which case your remote session will be terminated.

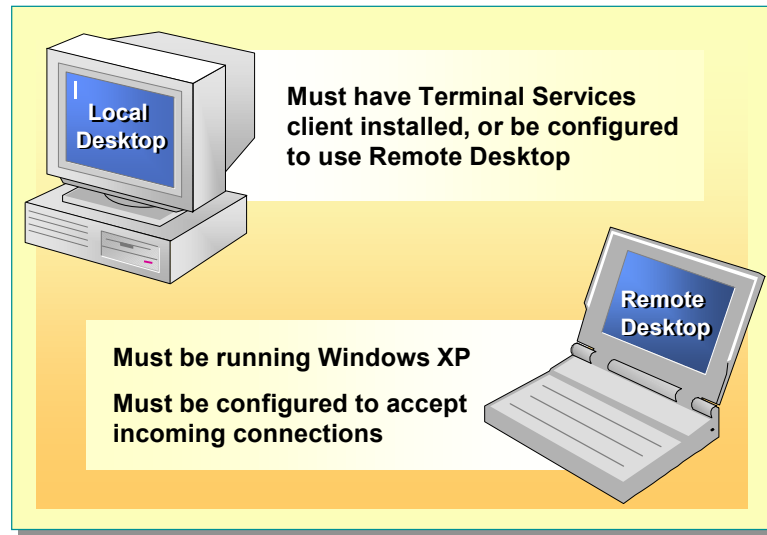
Examining the Remote Desktop Feature

Topic Objective

To describe the uses of the Remote desktop Desktop feature.

Lead-in

The Remote Desktop feature of Windows XP Professional enables you to gain access to a Windows session that is running on your computer when you are located at another computer.



Remote Desktop enables remote users to participate in a variety of scenarios, including:

- *Working at home or another site.* Gain access to work in progress on your office computer from your home computer, including full access to all local and remote devices.
- *Collaborating with a colleague.* Gain access to your desktop from a colleague's office to perform a variety of tasks, such as debugging code, updating a Microsoft PowerPoint® presentation, or proofreading a document, just as if you were working on your desktop in your own office.

Key Points

While you have remote access to the computer desktop, no one else can interact with the computer. If you are connected remotely, and someone logs on to the computer locally, your remote connection will be severed.

To use the Remote Desktop feature, you need the following:

- A computer to which you want to gain access that is running Windows XP Professional and is connected to a LAN or the Internet.
- A second computer with access to the LAN through a network connection, modem, or VPN connection. This computer must have the Remote Desktop Connections program or the Terminal Services client installed.
- Proper user accounts and permissions. To gain access to a computer's desktop remotely, you must be either an administrator, or a member of the Remote Users group on that computer.

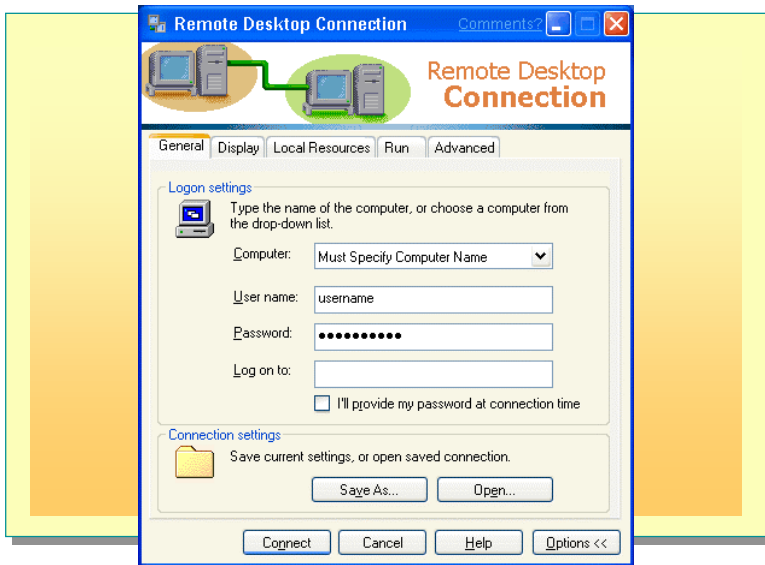
Configuring Computers to Use Remote Desktop

Topic Objective

To explain how to configure computers to enable Remote Desktop on the **Remote Desktop Connection** page.

Lead-in

To enable Remote Desktop, you must configure both the remote and local computers.



To enable Remote Desktop, you need to configure the computer to which you want to gain remote access, which will be the remote computer. Next, configure the computer from which you will connect, which will be the local computer.

Configuring a Computer to Use Remote Desktop

To configure the local computer to enable Remote Desktop, you need the following:

- Access to the remote computer, which is the computer running Windows XP Professional, by way of a LAN, modem, or VPN connection.
- Remote Desktop Connections or a Terminal Services client installed on the computer.

To configure the remote computer to enable Remote Desktop:

1. Click **Start**, right-click **My Computer**, and then click **Properties**.
2. On the **Remote** tab, select the **Allow users to connect remotely to this computer** check box.
3. Ensure that you have the proper permissions to connect to your computer remotely. You must be an administrator, or a member of the Remote Desktop Users group on the computer.
4. Click **OK**.

If the computer you will use to connect to your remote desktop is running Windows XP Professional, you can configure the Remote Desktop Connection on the **Remote Desktop Connection** page. To open the **Remote Desktop Connection** page, click **Start**, click **All Programs**, click **Accessories**, click **Communications**, and then click **Remote Desktop Connection**.

Delivery Tip

Demonstrate the additional tabs available and their configurable settings.

The only information that you must enter on the **Remote Desktop Connection** page is the name of the computer to which you will connect. However, if you click **Options**, the page will display five tabs, each of which contains configurable settings

Security Best Practices for Remote Desktop

Because Remote Desktop enables remote connection to your computer, you should configure the computer to be as secure as possible, thus preventing your data from being seen by others who may connect to your computer remotely.

The following list contains best practices to increase security

- To increase security, add yourself to the Remote Desktop Users group for your computer, rather than to the Administrators group. As a member of the Remote Desktop Users group, you do not have to log on as an administrator to gain access to your computer remotely. Therefore, if the security of your remote connection is compromised, the intruder will not have administrative privileges. Moreover, you should avoid running your computer while you are logged on as an administrator unless you are doing tasks that require administrator-only privileges.
- Require all Remote Desktop users to log on by using a strong password. This password level is especially important if your computer is connected directly to the Internet by way of a cable modem or DSL connection. *Strong passwords* are at least eight characters, and must contain a capital or a special character in position two through seven.

Lab 10B: Configuring and Using Remote Desktop

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will configure and use remote desktop.



Objectives

After completing this lab, you will be able to:

- Configure Remote Desktop on a computer running Windows XP Professional.
- Connect to a computer running Remote Desktop.

Prerequisites

Before working on this lab, you must have:

- Experience logging on and off Windows XP Professional.

Lab Setup

To complete this lab, you need the following:

- Completed Lab 1C, Upgrading Windows 98 to Windows XP Professional.
- A computer running Microsoft Windows XP Professional.

Scenario

The organization that you support has a custom-developed application that the users would like to be able to run from home. However, many of their home computers do not have the resources, such as memory, processor or disk space, to be able to run the application. You need to configure the new feature called Remote Desktop that is now available on their computers running Windows XP Professional.

Estimated time to complete this lab: 15 minutes

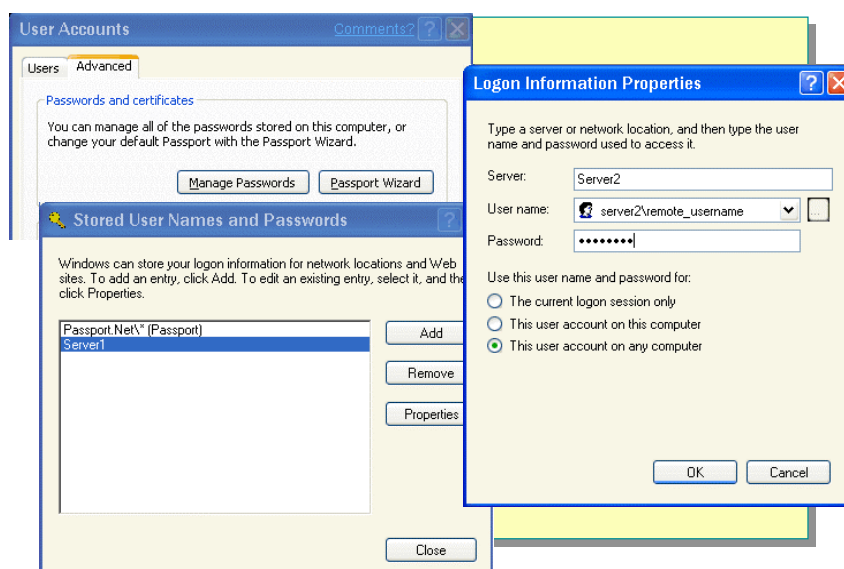
Storing User Names and Passwords to Facilitate Remote Connections

Topic Objective

To introduce the Stored User Names and Password feature.

Lead-in

Stored User Names and Passwords is a feature that allows you to easily connect to different servers that require different credentials.



When you log on to a computer running Windows XP Professional, you provide a user name, password, and security database to be authenticated against. On a stand-alone computer the database is the Security Accounts Manager (SAM). In a domain, the database is the Active Directory™ directory service. These supplied credentials become your security context for connecting to other computers on networks or over the Internet.

There may be cases when you want to use different user names and passwords to connect to different resources. A remote user may need to log on by using one set of credentials, and then connect to several secure remote access servers, each of which requires a different user name and password. Windows XP Professional enables users to store multiple sets of credentials for future use. Stored credentials can be specific to a unique server, or generic so that they will be supplied to all secure servers that the user attempts to gain access to.

The Stored User Names and Passwords feature also enables stored credentials to be stored as a part of a user's profile. Therefore, these credentials will travel with the user from computer to computer anywhere on the network.

To add credentials to Stored User Names and Passwords:

1. Click **Start**, click **Control Panel**, and then click **User Accounts**.
2. On the **Advanced** tab of the **User Accounts** page, click **Manage Passwords**, and then on the **Stored User Names and Passwords** page, click **Add**.
3. Enter a server name or network location, user name, and password for the resources that you want to gain access to, select when to use these credentials, and then click **OK**.

How Stored User Names and Passwords Works

When Windows XP Professional attempts to connect to a new resource on a network, it supplies to the target resource the set of credentials used to log on. If these credentials are not sufficient to provide the level of access requested, the user is prompted to enter new credentials on the **Logon Information Properties** dialog box that displays. The user can choose to have the credentials that they enter apply to the current logon session only, to the user account on the current computer only, or to the user account on any computer. If the user applies the credentials to the user account on any computer, the credentials are stored in that user's profile.

Benefits of Stored User Names and Passwords

Users who need to be authenticated using various sets of credentials benefit from Stored User Names and Passwords in the following ways:

- Requires users to log on only once, without needing to log off and on to supply multiple credentials.
- Stores any number of credentials for later use.
- Stores credentials in the user's profile to provide portability of the credentials to any computer on the network.

Best Practices for Stored User Names and Passwords

The following are best practices to observe when using the Stored User Names and Passwords feature:

- Use different passwords for individual credentials.
Having different passwords for each resource helps to ensure that one compromised password does not compromise all security.
- Use strong passwords for all credentials.
This feature does not remove the vulnerability of using weak passwords. Use strong passwords for all credentials.

Important Often, a user's e-mail address is in the form of *user_name@organization_name*, for example *jonmorris@contoso.com*. For this reason, users should never use a network password as a password for an Internet site that also requires, or reads through a cookie, their e-mail addresses. As a result, the site will be supplied with their user names, passwords, and company name, which constitutes a high security risk.

- Change passwords regularly.

Although strong passwords help to protect resources, it is possible for an intruder to eventually determine a password given sufficient time, technical expertise, and determination. Because of the potential intrusion, it is important to periodically change passwords to help minimize damage if a password is compromised without the user's knowledge.

- Use the **This logon session only** option, when appropriate.

Some credentials may be used infrequently. Other credentials may be used only for extremely sensitive resources that the user wants to protect very carefully. In these cases, the credentials should be stored for **This logon session only** by selecting that option in the **Logon Information Properties** dialog box.

Lab 10C: Storing User Names and Passwords

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will configure stored user names and passwords.



Objectives

After completing this lab, you will be able to:

- Store user names and passwords.
- Use the Stored User Names and Passwords feature.

Prerequisites

Before working on this lab, you must have:

- Completed Lab 1C, Upgrading Windows 98 to Windows XP Professional.
- A computer running Microsoft Windows XP Professional operating in a workgroup.
- Access to a computer running Microsoft Windows 2000 Advanced Server configured as a domain controller.

Scenario

You work onsite providing customer support. The organization has created a vendor account on its network for you to log on and be authenticated. You have additional accounts, including one for your own organization's domain. You want to use the Stored User Names and Passwords feature to simplify logging on to these different networks and resources.

Estimated time to complete this lab: 15 minutes

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- **Establishing Remote Access Connections**
- **Connecting to Virtual Private Networks**
- **Configuring Inbound Connections**
- **Configuring Authentication Protocols and Encryption**
- **Examining the Remote Desktop Feature**
- **Configuring Computers to Use Remote Desktop**
- **Storing Usernames and Passwords to Facilitate Remote Connections.**

-
1. A user reports that when she attempts to connect to a remote access server, she receives the following error: "The remote computer refused to be authenticated using the configured authentication protocol. The line has been disconnected." What could be the cause?

The authentication protocols on the client do not match the authentication protocol on the remote access server. The protocols on the client need to be reconfigured to match the server.

2. Where does a VPN tunnel start and stop when: (a) the user connects to the VPN by first connecting to an ISP and then to the VPN gateway? Where does a VPN tunnel start and stop when (b) the ISP creates the tunnel on behalf of the client?

(a) The tunnel extends from the client computer to the remote access server.

(b) The tunnel extends from the ISP to the remote access server. The connection from the client to the ISP is not part of the VPN tunnel.

3. What are the major differences between PPTP and L2TP?

Connectivity: PPTP requires an IP-based network.

Header Compression: L2TP supports header compression to four bytes; PPTP has six byte headers.

Authentication: L2TP supports tunnel authentication and IPsec; PPTP does not.

Encryption: PPTP automatically encrypts by using PPP; L2TP has no automatic encryption, but supports IPsec.

4. A user in the department that you support will be absent from the office for an extended period, but still wants to be able to work. However, his personal computer does not support the applications running on his desktop computer. What is a possible solution?

Configure Remote Desktop on his computer at work, and give him the links to install the appropriate Terminal Service client on his home computer. Make sure that the user has dial-in permissions, so that he can dial in and run the application on his computer at work while sitting in front of his computer at home.

