MICROSOFT
TRAINING
AND CERTIFICATION

Microsoft Official Curriculum

Module 5: Examining Network Protocols

Contents

Microsoft

Project Lead: Red Johnston
Instructional Designers: Meera Krishna (NIIT (USA) Inc.), Bhaskar Sengupta (NIIT (USA) Inc.)
Instructional Design Contributors: Aneetinder Chowdhry (NIIT (USA) Inc.),
Jay Johnson (The Write Stuff)**,** Sonia Pande (NIIT (USA) Inc.)
Lead Program Manager: Jim Cochran (Volt)
Program Manager: Jamie Mikami (Volt)
Technical Contributors: Rodney Miller, Gregory Weber (Volt)
Testing Leads: Sid Benavente, Keith Cotton
Testing Developer: Greg Stemp (S&T OnSite)
Simulation Developer: Wai Chan (Meridian Partners Ltd.)
Courseware Test Engineers: Jeff Clark, Jim Toland (ComputerPREP, Inc.)
Graphic Artist: Julie Stone (Independent Contractor)
Editing Manager: Lynette Skinner
Editor: Patricia Rytkonen (The Write Stuff)
Copy Editor: Kaarin Dolliver (S&T Consulting)
Online Program Manager: Debbi Conger
Online Publications Manager: Arlo Emerson (Aditi)
Online Support: Eric Brandt (S&T Consulting)
Multimedia Development: Kelly Renner (Entex)
Courseware Testing: Data Dimensions, Inc.
Production Support: Ed Casper (S&T Consulting)
Manufacturing Manager: Rick Terek (S&T OnSite)
Manufacturing Support: Laura King (S&T OnSite)
Lead Product Manager, Development Services: Bo Galford
Lead Product Manager: Gerry Lang
Group Product Manager: Robert Stewart
Simulations and interactive exercises were made with Macromedia Authorware

Instructor Notes

Presentation:
45 Minutes

Lab:
15 Minutes

This module provides students with information about common network protocols supported by Microsoft® Windows® 2000. The module begins with an introduction to protocols, types of protocols, the OSI reference model, and protocol stacks.

The module then describes routable and non-routable protocols and the types of data transmissions in a network. The module next discusses the common protocols supported by Windows 2000, such as TCP/IP, IPX/SPX, NetBEUI, and AppleTalk, and examines their characteristics.

The module continues with a discussion of other communication technologies, such as ATM and IrDA, which are supported by Windows 2000. The module concludes with a description of remote access protocols supported by Windows 2000, such as dial-up protocols and VPN protocols.

A lab in which students identify protocol capabilities follows the last section of the module.

At the end of this module, students will be able to:

- Define a protocol and describe the types of protocols.
- Describe the protocol characteristic that determines if a computer can communicate with other computers in a network.
- Name the common network protocols supported by Windows 2000 and describe their characteristics.
- Name the communication protocols and technologies that are compatible with Windows 2000 and describe their characteristics.
- Describe the protocols used for remote access: dial-up protocols and virtual private network (VPN) protocols.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft PowerPoint® file 2151A_05.ppt
- Module 5, “Examining Network Protocols”

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Review the Delivery Tips and Key Points for each section and topic.
- Study the review questions and prepare alternative answers for discussion.
- Anticipate the questions that students may ask and prepare answers to them.

Module Strategy

Use the following strategy to present this module:

- Introduction to Protocols

  Introduce the concept of a protocol and explain the two types of protocols—open and vendor-specific. Briefly discuss the OSI reference model. Explain protocol stacks but do not attempt to map the types of protocols in a stack to the OSI model.

- Protocols and Data Transmissions

  Explain the difference between routable and non-routable protocols. Describe the three types of data transmissions.

- Common Protocols

  Discuss the common protocols supported by Windows 2000 by examining the characteristics of TCP/IP, IPX/SPX, NetBEUI, and AppleTalk.

- Other Communication Protocols

  Describe the characteristics of other communications technologies supported by Windows 2000, such as ATM and IrDA. Discussion of these protocols should be at a high level.

- Remote Access Protocols

  Discuss the two types of remote access protocols that Windows 2000 supports. Provide high-level descriptions of the characteristics of the different dial-up and VPN protocols.

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 Microsoft Official Curriculum (MOC) courseware.

This module includes only a computer-based interactive lab exercise, and as a result, there are no lab setup requirements or configuration changes that affect replication or customization.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2151A, *Microsoft Windows 2000 Network and Operating System Essentials*.

Lab Results

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

Overview

Slide Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about communication protocols, their characteristics, the common protocols used for network communication, and other protocols compatible with Windows 2000 networks.

- Introduction to Protocols
- Protocols and Data Transmissions
- Common Protocols
- Other Communication Protocols
- Remote Access Protocols

To ensure that computers in a network are able to communicate, they must share a common language known as a *protocol*. A protocol is a set of rules or standards that enables communication between computers in a network. A number of protocols are available today, each having its own set of characteristics and capabilities. However, not every protocol is compatible with all computers and operating systems. To determine if a client computer in a Microsoft® Windows® 2000 network can communicate with other computers in the network, you must be familiar with the protocols supported by the Windows 2000 operating system.

Windows 2000 supports many of the common network protocols available today, as well as other communication protocols, including protocols for remote access. The compatibility of Windows 2000 with different types of protocols enhances the usability of Windows 2000 in different network environments.

At the end of this module, you will be able to:

- Define a protocol and describe the types of protocols.
- Describe the protocol characteristic that determines if a computer can communicate with other computers in a network.
- Name the common network protocols supported by Windows 2000 and describe their characteristics.
- Name the communication protocols and technologies that are compatible with Windows 2000 and describe their characteristics.
- Describe the protocols used for remote access: dial-up protocols and virtual private network (VPN) protocols.

Introduction to Protocols

Slide Objective
To introduce the types of protocols, the OSI model, and the concept of protocol stacks.

Lead-in
Protocols are the rules and procedures that govern the communication between computers in a network.

- **Types of Protocols**
- **Open Systems Interconnection (OSI) Reference Model**
- **Protocol Stacks**

Protocols are software and must be installed on network components that need them. Computers can communicate with each other only if they use the same protocol. If the protocol used by a computer in a network is not compatible with the protocol used by another computer, the two computers cannot exchange information. A variety of protocols are available for use in specific network environments. Although each protocol facilitates basic network communication, each has a different function and accomplishes different tasks.

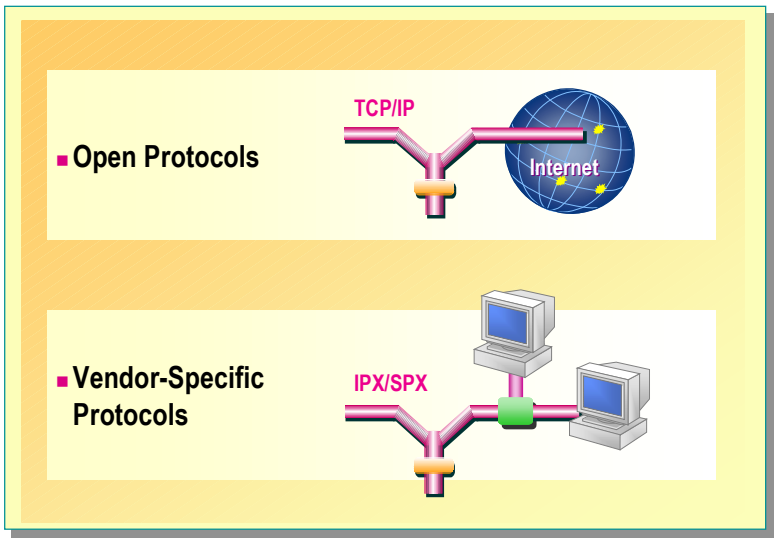
You can understand the function of different protocols by examining the standard model for networks—the Open Systems Interconnection (OSI) reference model. This model is built around a set of seven protocol layers, and each layer is responsible for some function that assists in the transmission of data over the network.

According to the OSI conceptual model, several protocols must work together to ensure the proper transmission of data. In reality, this is achieved with the help of a *protocol stack*. A protocol stack is a collection of protocols that function together to transmit data across a network of computers.

Types of Protocols

Slide Objective
To introduce the two types of network protocols.

Lead-in
Protocols are either open or vendor-specific.



Two types of protocols are available today: open and vendor-specific.

Open Protocols

Open protocols are protocols that are written to publicly known industry standards. A protocol that adheres to these industry standards is compatible with other protocols written to the same standards. Open protocols are nonproprietary (not privately owned). A common example of an open protocol is Transmission Control Protocol/Internet Protocol (TCP/IP), which is used as the standard for communication over the Internet.

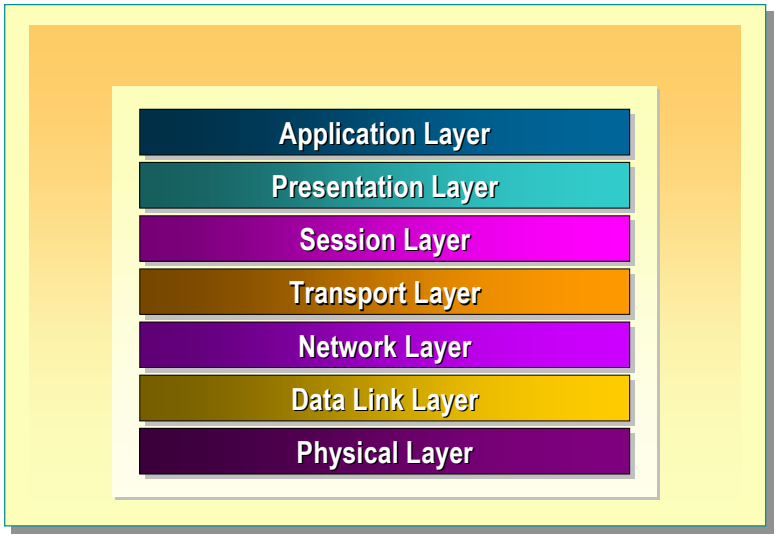
Vendor-Specific Protocols

Vendor-specific protocols are proprietary and have been developed by different vendors for use in specific environments. For example, Novell provides a set of protocols, such as Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX), developed specifically for its NetWare architecture.

Open Systems Interconnection (OSI) Reference Model

Slide Objective
To introduce the seven layers of the OSI model.

Lead-in
The OSI model is built around a set of seven protocol layers.



Key Point
The OSI model divides network communications into seven layers, with each layer having specific functionality for transmitting data on the network.

Delivery Tip
Explain to the class that the function of the protocols working at each layer of the OSI model is defined by the role of that layer in transmitting data.

The need for worldwide standardization of technologies led to the creation of the International Organization for Standardization (ISO). ISO is responsible for standardizing the methods by which computers communicate worldwide. To do so, ISO created a model for network communication, called the Open Systems Interconnection (OSI) reference model, or the OSI model.

OSI Model

The OSI model divides network communications into seven layers. Each layer carries out specific functions in transmitting data on the network.

Before data is moved through the layers of the OSI model, it must be divided into *packets*. A packet is a unit of information that is transmitted as a whole from one computer to another on a network. The network passes a packet from layer to layer, and at each layer some additional formatting is added to the packet.

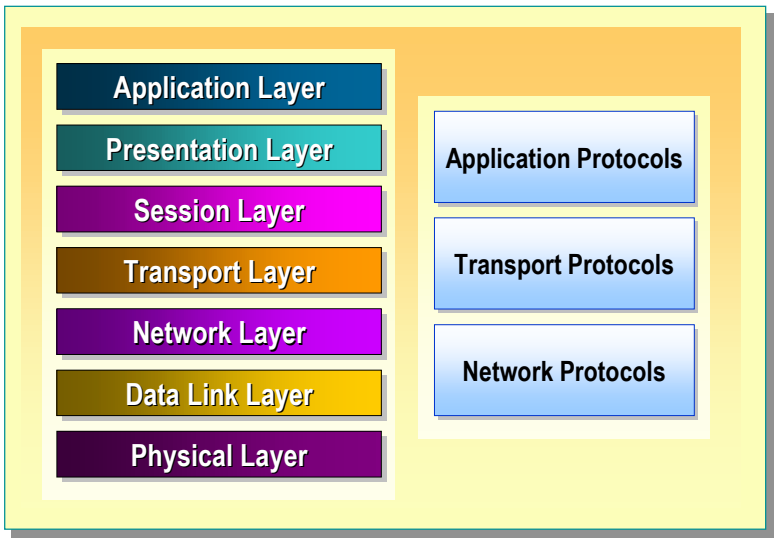
The layer at which a protocol works describes the function of the protocol. Some protocols work only at particular layers of the OSI model.

OSI layer	Function
Application Layer	Defines how applications interact with each other
Presentation Layer	Adds common formatting for data representation
Session Layer	Establishes and maintains communications channels
Transport Layer	Ensures error-free delivery of data
Network Layer	Addresses messages both within and between networks
Data Link Layer	Defines access methods for the physical medium, such as the network cable
Physical Layer	Puts the data on the physical medium

Protocol Stacks

Slide Objective
To introduce the concept of protocol stacks.

Lead-in
A protocol stack is a collection of protocols that work together to transmit data between computers.



Key Point
A protocol stack is a layered set of related protocols that ensure data is properly transmitted in a network.

Delivery Tip
Do not map the types of protocols in a stack to the OSI model layers. Use the graphics to explain to the class that each protocol stack compares to the basic OSI model but may have a different number of layers.

The OSI model defines distinct layers related to packaging, sending, and receiving data transmissions in a network. A layered set of related protocols actually carries out these services. This layered set of protocols running on a network is called a protocol stack. Together, the protocols in the stack handle all tasks required in packaging, sending, and receiving transmissions.

Several protocol stacks are designated as standard protocol models. Some of the common protocol stacks are TCP/IP, IPX/SPX, and AppleTalk. Protocols exist at each layer of these stacks, performing the tasks specified by that layer. Generally, however, the responsibility for performing specific communication tasks in the network is assigned to protocols working as one of three types: application protocols, transport protocols, and network protocols.

Application Protocols

Application protocols provide data exchange between applications in a network. Examples of common application protocols include File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP).

Transport Protocols

Transport protocols provide for communication sessions between computers and ensure that data moves reliably between computers. A common transport protocol is Transmission Control Protocol (TCP).

Network Protocols

Network protocols provide what are called *link services*. These protocols define the rules for communicating in a particular network environment. A common protocol that provides network services is Internet Protocol (IP).

Protocols and Data Transmissions

Slide Objective
To introduce routable and non-routable protocols and the types of data transmissions.

Lead-in
Protocols may or may not support data transmission between network segments through any available path.

- **Routable/Non-Routable Protocols**
- **Types of Data Transmission**

In a large network, it is difficult to manage communication efficiently because of the large volume of network traffic. Network administrators can bypass this problem by dividing large networks into *network segments*. Network segments are smaller networks, which, when combined, form a large network.

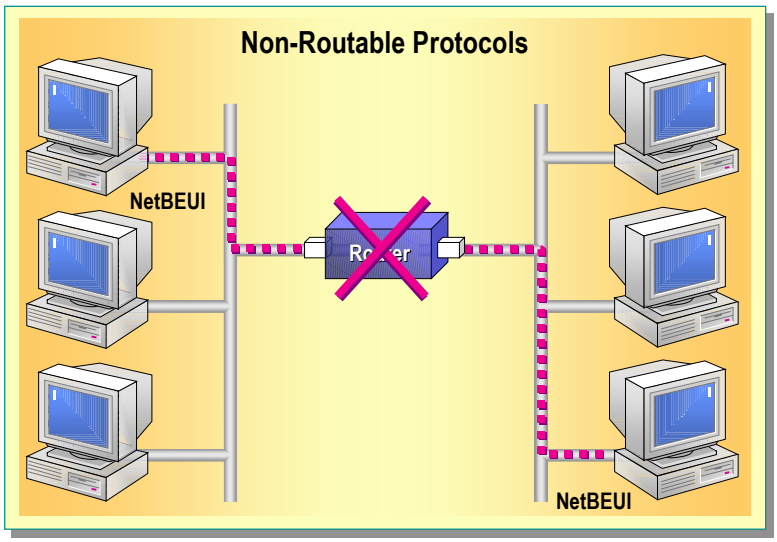
Within a network, data may be transmitted from one network segment to another along any of several available paths. The transmission of data between network segments is called *routing*. However, not every protocol supports routing. Protocols are categorized as routable or non-routable based on their ability or inability to support routing.

The ability of protocols to support routing enables data transmission between computers in different network segments. There are different types of data transmissions. Each transmission type determines which computers in a network receive the transmitted data. Because not all computers on the network may need to receive the transmitted data, you can control to a certain degree which computers receive and process the transmitted data by controlling the type of transmission.

Routable/Non-Routable Protocols

Slide Objective
To illustrate routable and non-routable protocols.

Lead-in
Protocols may or may not support communication between different network segments based on whether the protocols are routable or non-routable.



Key Point
Routable protocols enable computers in one network segment to communicate with those in another segment.

Only computers running routable protocols can transmit data to computers in other network segments.

Delivery Tip
Use the animation to explain the difference between routable and non-routable protocols.

Based on whether or not protocols support routing, they can be categorized as routable or non-routable protocols.

Routable Protocols

Routable protocols support communication between LANs or network segments that may be spread throughout a building, across a small geographic area, such as a college campus, or across the globe, such us the Internet. Routable protocols support the transmission of data from one network segment to another along any of several paths connecting the two network segments. Examples of routable protocols are TCP/IP and IPX/SPX.

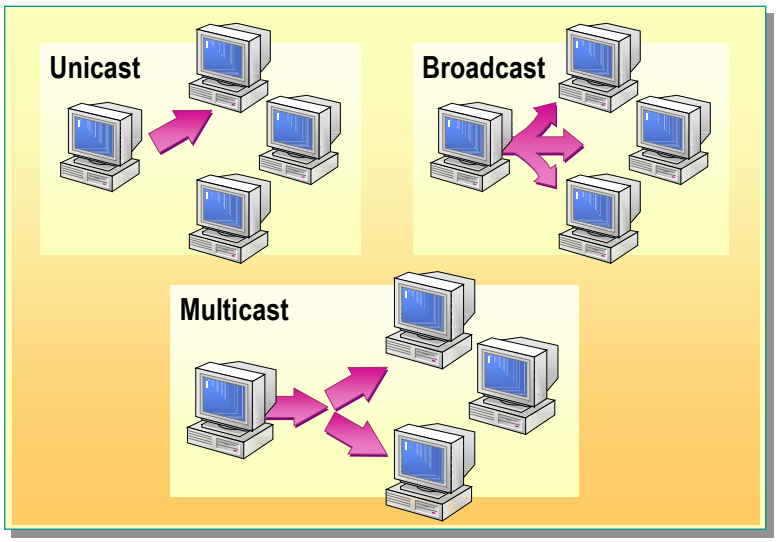
Non-Routable Protocols

Non-routable protocols, unlike routable protocols, do not support the transmission of data from one network segment to another. Computers that use non-routable protocols can communicate only with other computers in the same network segment. NetBEUI and Data Link Control (DLC) are examples of non-routable protocols.

Types of Data Transmissions

Slide Objective
To explain the three types of data transmissions.

Lead-in
Data is transmitted over a network in three ways: unicast, broadcast, and multicast.



Routable protocols enable the transmission of data between computers in different segments of a network. However, high volumes of certain kinds of network traffic, such as the deployment of multimedia applications, can affect network efficiency because it slows down transmission speed. The amount of network traffic generated varies with the three types of data transmissions: unicast, broadcast, or multicast. To understand how each transmission type affects network traffic, you must be familiar with the characteristics of each type of transmission.

Unicast

In a unicast transmission, a separate copy of the data is sent from the source to each client computer requesting it. No other computer on the network needs to process the traffic. However, unicast transmission is not as efficient when multiple computers request the same data because the source transmits multiple copies of the data. Unicast transmission works best when just a small number of client computers request the data. Unicast transmission is also referred to as directed transmission. Most traffic on networks today is unicast.

Broadcast

When data is broadcast, a single copy of the data is sent to all clients on the same network segment as the sending computer. However, if that data must be sent to only a portion of the network segment, broadcast transmission is not an efficient transmission method because data is sent to the whole segment irrespective of whether it is required. This needlessly slows the performance of the network because each client must process the broadcast data.

Multicast

In a multicast transmission, a single copy of the data is sent only to client computers requesting it. Multiple copies of data are not sent across the network. This minimizes the network traffic and enables the deployment of multimedia applications on the network without overburdening the network. Many Internet services use multicasting to communicate with client computers.

Common Protocols

Slide Objective
To introduce common network protocols.

Lead-in
Windows 2000 supports many of the commonly used network protocols.

- **Transmission Control Protocol/Internet Protocol (TCP/IP)**
- **Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)**
- **NetBIOS Enhanced User Interface (NetBEUI)**
- **AppleTalk**

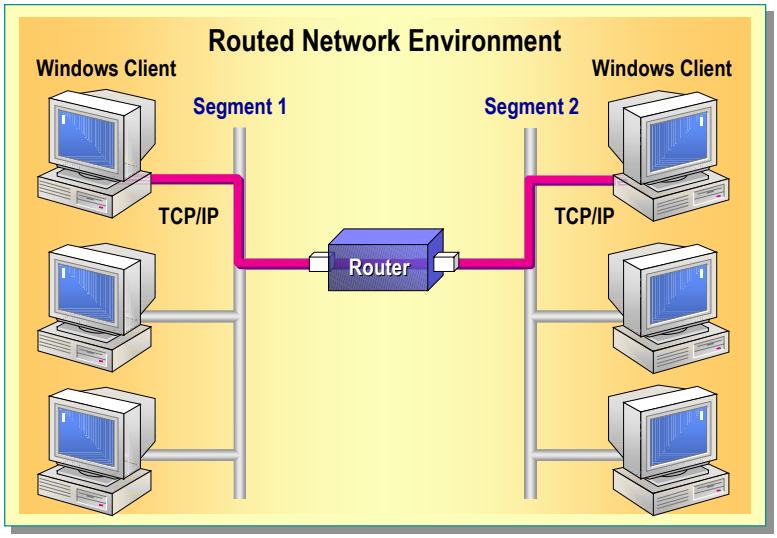
Windows 2000 supports many different networking protocols. Different protocols are needed for communication with systems, devices, and computers in various environments. Some protocols are routable, and others are not. Based on which protocols are used by a client computer, you can determine whether or not that computer can communicate with other computers in a routed Windows 2000 network. The common network protocols that you can use with Windows 2000 are:

- Transmission Control Protocol/Internet Protocol (TCP/IP).
- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).
- NetBIOS Enhanced User Interface (NetBEUI).
- AppleTalk.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Slide Objective
To illustrate how TCP/IP functions in a routed network environment.

Lead-in
TCP/IP is an industry-standard protocol stack that most networks support for its interoperability among different types of computers.



Key Point
TCP/IP is a standard protocol stack that is supported by most networks for its interoperability.

Delivery Tip
Use the graphic on the slide to explain to the class that TCP/IP enables computers to communicate between segments in a routed network environment.

TCP/IP is an industry-standard protocol stack (a layered set of protocols) that enables communication in different networking environments. Because of the interoperability of TCP/IP among different types of computers, most networks support TCP/IP.

TCP/IP supports routing and enables computers to communicate across network segments. Because of this feature, TCP/IP is the standard protocol for communications over the Internet. Its reliable delivery and global use have made TCP/IP a necessity for accessing worldwide information networks, such as the Internet. However, you must configure TCP/IP on all computers with which you want to use the protocol to communicate.

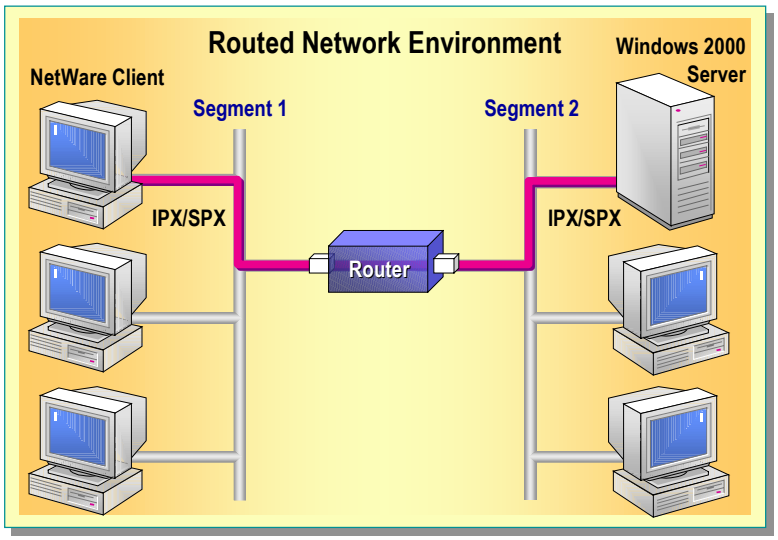
TCP/IP offers the following advantages:

- It is an industry standard. As an industry standard, it is an open protocol that is not controlled by a single organization.
- It contains a set of utilities for connecting dissimilar operating systems.Connectivity between two computers does not depend on the network operating system of either computer.
- It uses scalable, cross-platform, client-server architecture. TCP/IP can expand or shrink to meet the future needs of a network.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

Slide Objective
To illustrate how IPX/SPX functions.

Lead-in
Windows 2000 supports IPX/SPX, a common protocol used with NetWare.



Key Point
IPX/SPX is a routable protocol stack used in NetWare environments.

Delivery Tip
Use the graphic on the slide to explain to the class that IPX/SPX enables a NetWare client computer to communicate with a Windows 2000 server in a routed network environment.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) is a protocol stack developed specifically for NetWare architecture. The IPX/SPX stack includes IPX and SPX. IPX defines the addressing schemes used on a NetWare network, and SPX provides security and reliability to the IPX protocol. IPX is a network-layer protocol that is equivalent to the IP of the TCP/IP protocol stack. SPX provides reliable service at the transport layer.

IPX/SPX has the following characteristics:

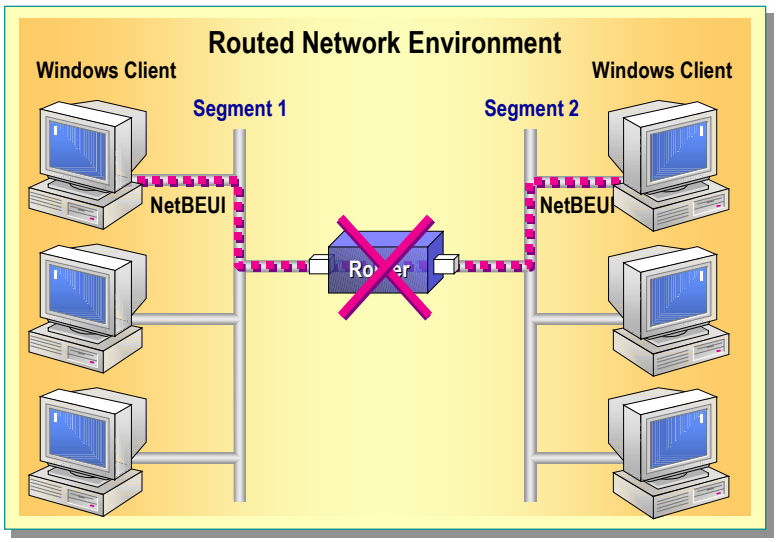
- It is used on networks with NetWare servers.
- It is routable. IPX/SPX enables computers in a routed networking environment to exchange information across segments.

Note NWLink IPX/SPX/NetBIOS Compatible Transport Protocol is a Microsoft version of IPX/SPX and is included with Windows 2000. Client computers running Windows 2000 can use NWLink to access client and server applications running on NetWare servers. NetWare clients can use NWLink to access client and server applications running on Windows 2000-based servers. With NWLink, computers running Windows 2000 can communicate with other network devices, such as printers, that use IPX/SPX. You can also use NWLink in small networks that only use Windows 2000 and other Microsoft client software.

NetBIOS Enhanced User Interface (NetBEUI)

Slide Objective
To illustrate how NetBEUI functions.

Lead-in
NetBEUI is a protocol that is supported by all Microsoft network products, including Windows 2000.



Key Point
NetBEUI is a non-routable protocol supported by all Microsoft network products, including Windows 2000.

Delivery Tip
Use the graphic on the slide to explain to the class that NetBEUI enables communication between Windows-based client computers on the same segments of a routed network environment.

NetBIOS Enhanced User Interface (NetBEUI) was one of the earliest protocols available for use on networks composed of personal computers. It was designed around the Network Basic Input/Output System (NetBIOS) interface to be a small, efficient protocol for use in department-sized LANs of 20 to 200 computers, which would not need to be routed to other subnets.

At present, NetBEUI is used almost exclusively on small, non-routed networks consisting of computers running a variety of operating systems.

Windows 2000-based NetBEUI, known as NetBIOS Frame (NBF), is the underlying implementation of the NetBEUI protocol and is installed on computers running Windows 2000. It provides compatibility with existing LANs that use the NetBEUI protocol.

The advantages of NetBEUI include:

- Small stack size.
- No configuration requirement.
- High speed of data transfer on the network.
- Compatibility with all Microsoft-based operating systems, including Windows 2000.

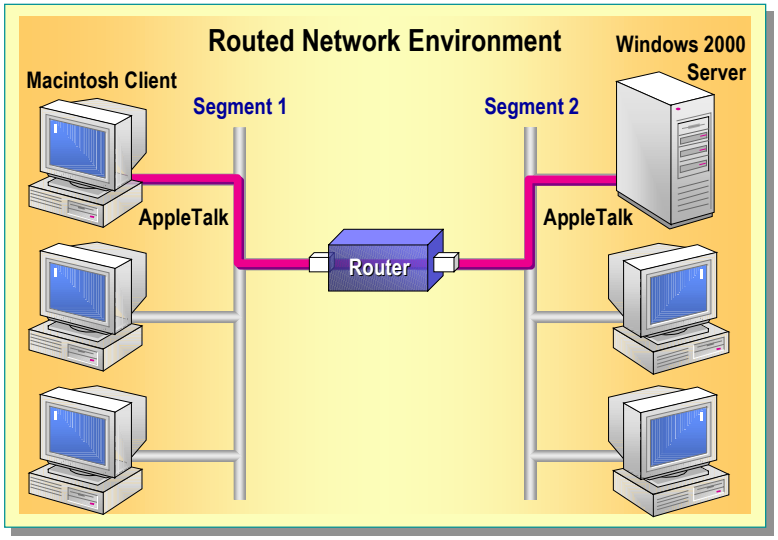
The major disadvantage of NetBEUI is that it does not support routing. Because of this, computers running NetBEUI can communicate only with other computers in the same network segment.

Note Network Basic Input/Output System (NetBIOS) allows applications to access the network functionality of the operating system and manage the network names used to communicate on a network.

AppleTalk

Slide Objective
To illustrate how AppleTalk functions.

Lead-in
Windows 2000 supports AppleTalk, a routable protocol used with Apple Macintosh networks.



Key Point
AppleTalk is a routable protocol stack used in Apple Macintosh environments.

Delivery Tip
Use the graphic on the slide to explain to the class that AppleTalk enables a Macintosh client computer to communicate with a Windows 2000-based server in a routed network environment.

AppleTalk is Apple Computer's proprietary protocol stack designed to enable Apple Macintosh computers to share files and printers in a network environment.

Some of the characteristics of the AppleTalk protocol are:

- It enables Macintosh clients to access a server running Windows 2000.
- It is routable. Computers running AppleTalk can communicate across segments in a routed network environment.
- It enables Macintosh clients to access print services provided by a server running Windows 2000 if Print Server for Macintosh is installed on the server.

Other Communication Protocols

Slide Objective
To introduce other communication technologies supported by Windows 2000.

Lead-in
In addition to supporting most commonly used networking protocols, the Windows 2000 operating system supports other communication protocols and technologies, such as ATM and IrDA.

- **Asynchronous Transfer Mode (ATM)**
- **Infrared Data Association (IrDA)**

In addition to supporting most commonly used networking protocols, the Windows 2000 operating system supports other communication protocols and technologies, such as:

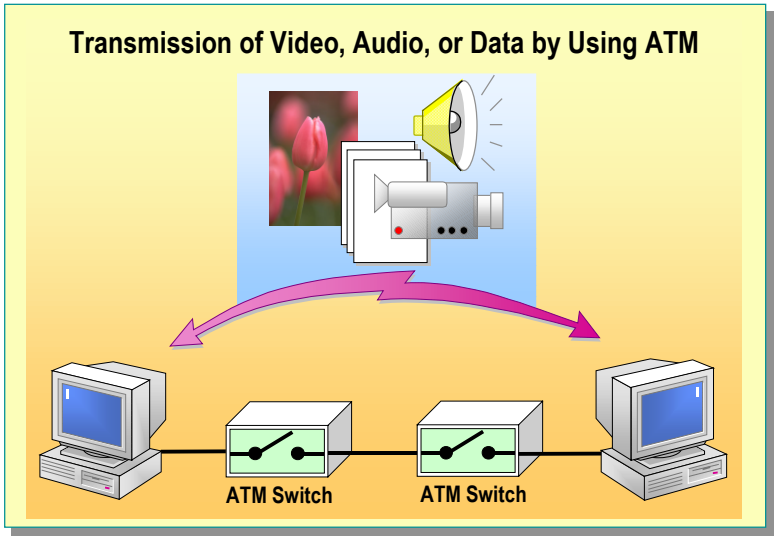
- Asynchronous transfer mode (ATM).
- Infrared Data Association (IrDA).

ATM and IrDA are both international standards for communication technologies. ATM was developed for the high-speed transmission of multimedia content, and IrDA was developed for wireless connectivity.

Asynchronous Transfer Mode (ATM)

Slide Objective
To illustrate how ATM functions.

Lead-in
ATM is a high speed, connection-oriented protocol that transports multiple types of traffic across a network.



Key Point
ATM is a high-speed, connection-oriented protocol that transports multiple types of traffic across a network.

Delivery Tip
Use the graphic on the slide to explain to the class that ATM enables a high-speed transmission of multimedia applications between computers in a network.

Asynchronous transfer mode (ATM) is a high-speed protocol that transports multiple types of traffic across a network. The ATM technology was developed from international standards for the simultaneous transmission of data, voice, and video over a network at high speed. A device called an ATM switch is used to enable network communication by using the ATM protocol. Client computers communicate with each other by means of a network of ATM switches.

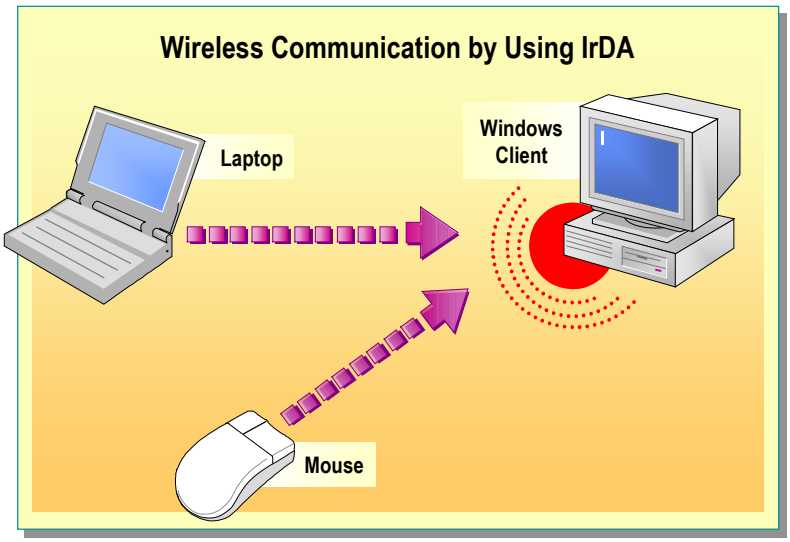
Some of the characteristics of ATM are:

- It provides a single network connection that can reliably mix voice, video, and data. ATM can simultaneously transport such electronic communication as telephone calls, movies, and the e-mail and files contained on a Web server.
- It provides high-speed communication.
- It assures that no single type of data overuses the line. It efficiently allocates network bandwidth, thereby guaranteeing the reliability of the connection.

Infrared Data Association (IrDA)

Slide Objective
To illustrate how IrDA functions.

Lead-in
IrDA enables wireless communication between a variety of devices, such as cameras, laptops, and printers.



The Infrared Data Association (IrDA) is an association that defined the group of short-range, high speed, bidirectional wireless infrared protocols, generically referred to as IrDA. The IrDA protocol stack enables computers running Windows 2000 to connect easily to peripheral devices or other computers without the use of connecting cables. For example, Windows 2000 automatically detects infrared devices, such as other computers or cameras, which are within range of each other. IrDA enables users to transfer information and share resources, such as printers, cameras, portable computers, desktop computers, and personal digital assistants (PDAs).

IrDA enables wireless communication between any two infrared devices within range of each other. For example, two users traveling with laptop computers can transfer files by setting up an IrDA connection, instead of by using cables or floppy disks. IrDA automatically configures the connection when the portable computers are placed within close proximity. In addition, IrDA enables a computer to access resources that are attached to another computer. For example, if a user with a laptop computer needs to print a document, the user can create an IrDA connection with a computer that is connected to a printer, either locally or on a network. When that connection is established, the user, with appropriate permissions, can print over the IrDA connection.

The characteristics of IrDA wireless communication include:

- A worldwide standard for wireless infrared connectivity.
- Ease of implementation and use.
- No risk of radiation from infrared rays.
- No electromagnetic noise.
- No government regulatory issues.
- Minimum crosstalk (signal overflow from adjacent cable).

Remote Access Protocols

Slide Objective
To introduce the topics related to remote access protocols.

Lead-in
Remote access requires protocols that enable the connection between the client and the server. Depending on your requirements, you can choose the appropriate protocol.

- **Dial-up Protocols**
- **VPN Protocols**

In Windows 2000, you can establish a remote connection by using either dial-up remote access or a virtual private network (VPN). To establish a remote access connection to a Windows 2000 network, you can select from the following remote access protocols:

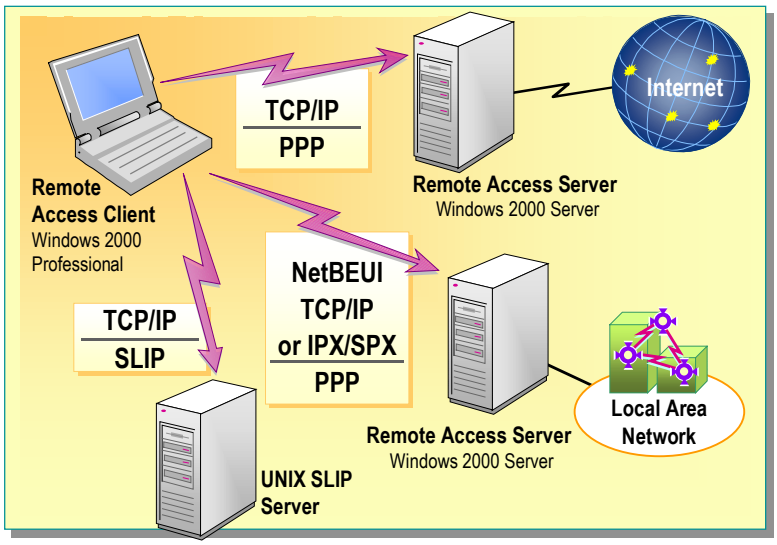
- Dial-up protocols
- VPN protocols

These remote access protocols are supported by Windows 2000 and provide interoperability with third party remote access components. Understanding the features of each protocol will help you decide which protocol is appropriate for your network.

Dial-up Protocols

Slide Objective
To illustrate the dial-up remote access protocols used by remote access clients and servers.

Lead-in
In dial-up connectivity, you can use either the SLIP protocol or the PPP protocol to provide clients with access to a variety of remote access servers.



Key Point
Windows 2000 does not provide a SLIP server because SLIP servers are less secure and less efficient than PPP servers.

Windows 2000 supports dial-up remote access protocols, such as Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP), to provide clients with access to a variety of remote access servers.

SLIP

SLIP allows remote access clients to connect to a remote access server through a modem. This allows client computers running Windows 2000 to connect to SLIP servers. A SLIP server is a remote access protocol component on the remote access server that services connection requests from SLIP clients. Although client computers running Windows 2000 can connect to SLIP servers, Routing and Remote Access does not itself include a SLIP server component. Therefore, you cannot use a computer running Windows 2000 as a SLIP server. Instead, you can use a server running UNIX as a SLIP server.

SLIP is an industry standard protocol that addresses TCP/IP connections made over serial lines. SLIP is supported by Routing and Remote Access and gives clients running Windows 2000 access to Internet services. SLIP has several limitations:

- Support is limited to TCP/IP. You cannot use SLIP to directly transfer other network protocols, such as IPX/SPX or NetBEUI.
- A static IP address is required. SLIP requires the client to configure all of the TCP/IP configuration parameters, such as the IP address, prior to establishing a connection to the server.
- It typically relies on text-based logon authentication sessions and usually requires a scripting system to automate the logon process.
- It transmits authentication passwords as clear text. This might result in a security compromise because passwords are not encrypted during user authentication.

PPP

PPP is a set of industry-standard protocols that enable remote access clients and servers to operate in a network consisting of components manufactured by multiple vendors. PPP supports encrypted password authentication. PPP is an enhancement to the original SLIP specification and provides a standard method for sending network data over a point-to-point link.

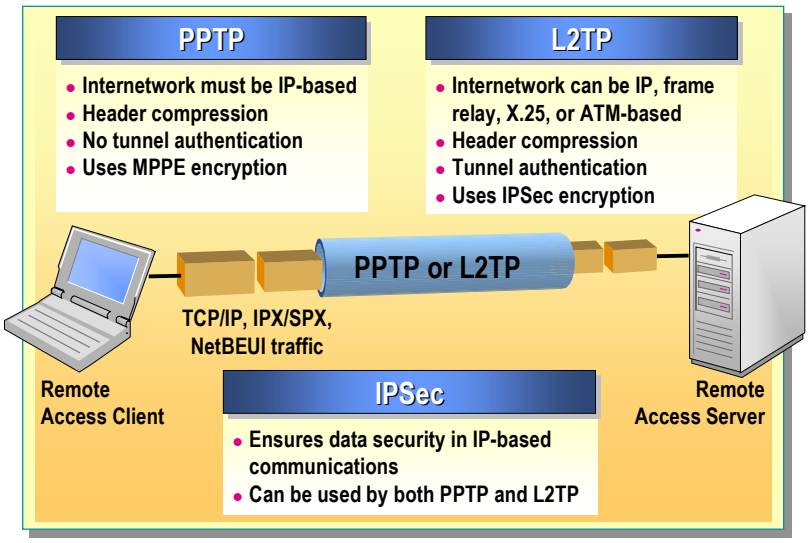
PPP support enables computers running Windows 2000 to connect to remote networks through any server that complies with PPP standards. PPP compliance also enables a server to receive calls from, and provide access to, other vendors' remote access software.

The PPP architecture enables clients to use any combination of NetBEUI, TCP/IP, and IPX/SPX network transport protocols. You can run applications written to the IPX/SPX, NetBIOS, or Windows Sockets (WinSock) interface on a remote computer running Windows 2000. The PPP architecture enables a server to download and configure TCP/IP parameters.

VPN Protocols

Slide Objective
To list the features of the VPN protocols used by remote access clients and servers.

Lead-in
Virtual private networks (VPNs) provide remote access without relying on hardware by using an additional protocol that allows users to connect to LANs over their existing Internet or dial-up connections.



Delivery Tip
The slide for this topic is animated. First display the graphic, and then display the features of PPTP, L2TP, and IPSec as you talk about them.

Key Point
VPNs work by putting normal data packets inside encrypted PPP packets.

You can use virtual private networks (VPNs) to provide remote access without having to rely on dial-up networking hardware, such as modems, on the remote access servers. VPNs use an additional protocol that allows users to connect to LANs over their existing Internet or dial-up connections. These connections can be secure even though the connection may use public Internet hardware.

VPN protocols encapsulate TCP/IP, IPX/SPX, or NetBEUI data packets inside PPP data packets. The remote access server, with the help of the client, performs all security checks and validations and enables data encryption, making it safe to send data over non-secure networks, such as the Internet. Typically, users connect to the VPN by first connecting to an Internet service provider (ISP) and then connecting to the VPN ports through that Internet connection.

VPNs use either Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol (L2TP) to establish connections.

Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) enables the secure transfer of encapsulated data from a PPTP client to a PPTP server across a TCP/IP internetwork, such as the Internet. PPTP encapsulates PPP frames in TCP/IP packets for transmission over an internetwork. Because of this encapsulation, you can use all features of PPP, including TCP/IP, IPX/SPX, NetBEUI, and Microsoft Point-to-Point Encryption (MPPE), in a PPTP virtual private network.

Windows 2000 supports PPTP, which you can use in private LAN-to-LAN networking.

Layer Two Tunneling Protocol (L2TP)

Layer Two Tunneling Protocol (L2TP) is an industry standard tunneling protocol. Like PPTP, L2TP uses the authentication and compression mechanisms of PPP. Unlike PPTP, L2TP does not utilize MPPE to encrypt PPP frames. Instead, L2TP relies on Internet Protocol Security (IPSec) for encryption services. The result is that L2TP-based virtual private network connections are typically a combination of L2TP and IPSec. For an encrypted L2TP virtual private network, both the client and the server must support L2TP and IPSec.

L2TP allows any combination of TCP/IP, IPX/SPX, or NetBEUI traffic to be encrypted and then sent over any medium that supports point-to-point packet delivery, such as Ethernet, X.25, frame relay, or asynchronous transfer mode (ATM).

IPSec

Internet Protocol Security (IPSec) ensures data security in TCP/IP-based communications by providing an additional layer of network security. IPSec integrates with the security inherent in Windows 2000 to safeguard intranet and Internet communications. The VPN protocols, PPTP and L2TP, can be combined with the security provided by IPSec to provide data security.

IPSec provides data integrity and encryption. It is superior to PPTP, which uses MPPE encryption. Using IPSec results in both increased demands on the CPU resources of the client and the server and an increased network payload.

Lab A: Identifying Protocol Capabilities

Slide Objective
To introduce the lab.

Lead-in
In this lab, you will identifywhich protocols are used to communicate with other computers on another segment and the different types of transmissions made by computers on the network.

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Identify which protocols are used to enable communication with other computers on another segment of a network.
- Identify the different types of transmissions made by computers on the network.

Lab Setup

This lab is a simulation. To complete this lab, you need the following:

- A computer running Microsoft Windows 2000, Microsoft Windows NT® version 4.0, Microsoft Windows 98, or Microsoft Windows 95.
- A minimum display resolution of 800 x 600 with 256 colors. (16-bit recommended).
- Microsoft Internet Explorer 5 or later.

► To start the lab

1. Log on to Windows 2000 as Administrator with a password of **password**.
2. On the desktop, double-click the **Internet Explorer** icon.
3. On the Student Materials Web page, click **Lab Simulations**.
4. Click **Identifying Protocol Capabilities**.
5. Read the introduction information, and then click the link to begin the simulation.

Estimated time to complete this lab: 15 minutes

Review

Slide Objective
To reinforce module objectives by reviewing key points.

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

- Introduction to Protocols
- Protocols and Data Transmissions
- Common Protocols
- Other Communication Protocols
- Remote Access Protocols

1. You want to modify an existing protocol to better suit your networking needs. You realize that you can use an open protocol for this purpose. Which of the following protocols can you use?

   A. IPX/SPX.

   B. AppleTalk.

   C. NetBEUI.

   D. TCP/IP.

   D. TCP/IP.

2. The users in your network need to conduct business over the Internet. Which protocol will you install in the network to allow the users to communicate over the Internet?

   A. IPX/SPX.

   B. TCP/IP.

   C. AppleTalk.

   D. NetBEUI.

   B. TCP/IP.

3. You have a small workgroup that uses Windows 2000 and other Microsoft-based operating systems. You need to install a protocol that requires minimal configuration to enable communication within the workgroup. Which protocol will you install?

   A. IPX/SPX.

   B. TCP/IP.

   C. AppleTalk.

   D. NetBEUI.

   D. NetBEUI.

4. You need to transfer large amounts of audio, video, and data files simultaneously over a network. Which of the following protocols enables the high-speed transmission of this data over the network?

   A. ATM.

   B. TCP/IP.

   C. IrDA.

   D. NetBEUI.

   A. ATM.

5. You want to set up a Windows 2000-based server to enable remote clients to connect to the server by using SLIP or PPP. Can you do this? If so, does it require configuration?

   A. Yes. The setup configurations are automatic.

   B. Yes, you can do it without any additional configurations.

   C. No, because Windows 2000 cannot be used as a SLIP server.

   D. No, because Windows 2000 cannot be used as a PPP server.

   C. No, because Windows 2000 cannot be used as a SLIP server.