MICROSOFT
TRAINING
AND CERTIFICATION

Microsoft Official Curriculum

Module 4: Examining the Network

Contents

Overview	1
Scope of Networks	2
Basic Connectivity Components	3
Network Topologies	9
Network Technologies	15
Expanding the Network	21
Lab A: Examining the Network Architecture	34
Review	36

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:
120 Minutes

Lab:
30 Minutes

This module provides students with information about the hardware aspects of network communication, such as the requirements for incorporating network components, and explores how the structure of a network can affect communication. The module begins with a description of the scope of a network, comparing a Local Area Network (LAN) to a Wide Area Network (WAN).

The module then examines some of the basic connectivity components of a network. Students will learn about network adapters, the different cable types, and wireless communication devices. The module next focuses on the different topologies that can be used in a network. Students will learn to distinguish the features and roles of the various topologies.

The module continues with an overview of the different network technologies, such as Ethernet, token ring, asynchronous transfer mode (ATM), Fiber Distributed Data Interface (FDDI), and frame relay. The module concludes with a description of the hardware used to expand a network. Students will learn about the features of repeaters and hubs, bridges, routers, and gateways. In addition, remote connectivity types, such as Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), X.25, and asymmetric digital subscriber line (ADSL), will be introduced to the students.

A lab in which students examine the components that make up a network infrastructure follows the last section of the module.

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

- Describe the scope of a network.
- Describe some of the components used in a network.
- Describe the topologies used in a network.
- Describe the technologies used in a network.
- Describe the components used in expanding the network.

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_04.ppt
- Module 4, “Examining the Network”

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.
- Read the white paper, *Windows 2000-based Virtual Private Networking: Supporting VPN Interopability*, on the Trainer Materials compact disc.
- 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:

- Scope of Networks

  Introduce the scope of networks and distinguish between a LAN and a WAN.

- Basic Connectivity Components

  Provide an overview of the need for basic connectivity components in a network. Then describe the purpose of the network adapter. Discuss the types of network cables and the characteristics of the wireless communication devices used in a network infrastructure. If time permits, show students samples of different connectivity components.

- Network Topologies

  Explain the various types of network topologies and discuss the features of bus, star, ring, mesh, and hybrid topologies.

- Network Technologies

  Introduce the network technologies used to communicate between computers within LANs and WANs. Differentiate the characteristics of Ethernet, token ring, ATM, FDDI, and frame relay technologies with reference to their access methods and transfer speeds.

- Expanding the Network

  Introduce the tools used to expand a network. Discuss the features of repeaters and hubs, bridges, switches, routers, and gateways. In addition, explain the remote connectivity methods and the features of the physical components of remote access, such as PSTN, ISDN, X.25, and ADSL.

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. 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*.

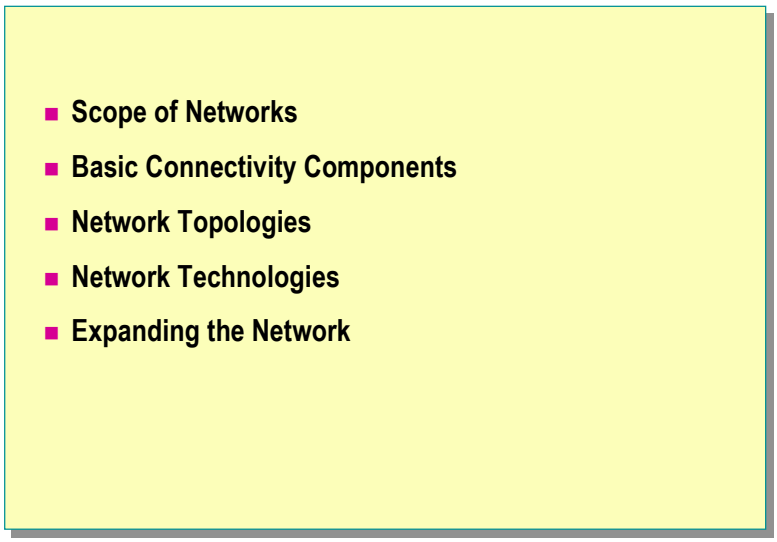
Lab Results

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 the network infrastructure.



To understand a network running Microsoft® Windows® 2000, you need to know what makes up a network. In examining a network, you must first determine the size of the network. You then need to become familiar with the basic connectivity components, such as the cables and communication tools, which are used to build the network. You must be able to differentiate between the multiple network topologies and then determine the suitability of applying a specific network technology to any given network design. You will need to select specific network components that allow for future expansion of the network.

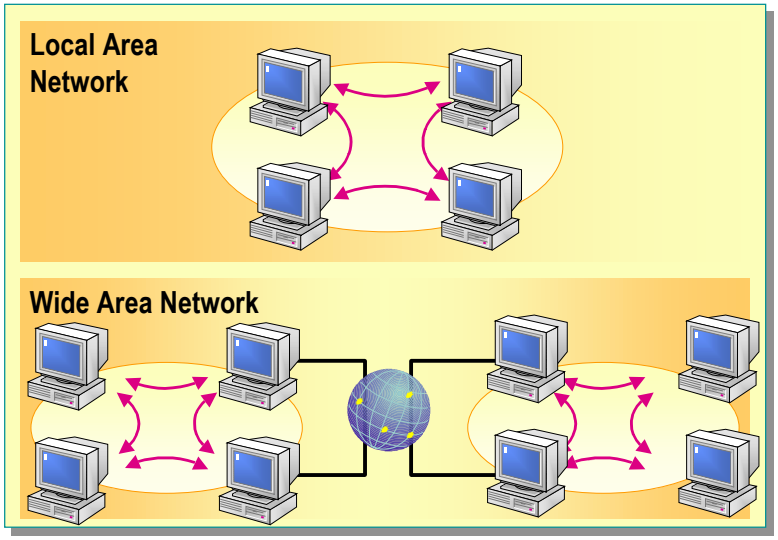
At the end of this module, you will be able to:

- Describe the scope of a network.
- Describe some of the basic connectivity components used in a network.
- Describe the topologies used in a network.
- Describe the technologies used in a network.
- Describe the components used in expanding the network.

Scope of Networks

Slide Objective
To introduce the scope of networks.

Lead-in
The size of your network is defined by its scope.



Key Points
When a WAN has been properly implemented, it appears indistinguishable from a local area network and functions like a LAN.

Delivery Tip
Point out to the students that the scope of a network does not refer merely to the number of computers on the network; it also refers to the distance between computers.

The scope of a network refers to its geographical size. A network can range in size from just a few computers in one office to thousands of computers linked together over great distances.

Network scope is determined by the size of the organization or the distance between users on the network. The scope determines how the network is designed and what physical components are used in its construction.

There are two general types of network scope:

- Local Area Networks
- Wide Area Networks

Local Area Network

A local area network (LAN) connects computers that are located near each other.

For example, two computers connected together in an office or two buildings connected together by a high-speed wire can be considered a LAN. A corporate network that includes several adjacent buildings can also be considered a LAN.

Wide Area Network

A wide area network (WAN) connects a number of computers located at a greater distance from one another.

For example, two or more computers connecting opposite sides of the world is considered a WAN. A WAN can be made up of a number of interconnected LANs. For example, the Internet is really a WAN.

Basic Connectivity Components

Slide Objective
To introduce the basic connectivity components of a network.

Lead-in
The basic connectivity components of a network include the cables, network adapters, and wireless devices that connect the computers to the rest of the network.

- **Network Adapters**
- **Network Cables**
- **Wireless Communication Devices**

The basic connectivity components of a network include the cables, network adapters, and wireless devices that connect the computers in the network.

These components enable data to be sent to each computer on the network, thereby permitting the computers to communicate with each other.

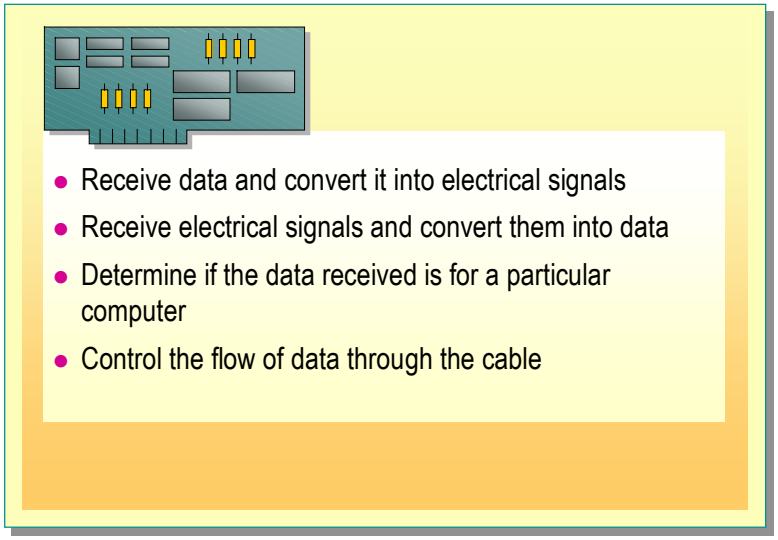
Common connectivity components of a network are:

- Network adapters.
- Network cables.
- Wireless communication devices.

Network Adapters

Slide Objective
To describe the purpose of the network adapter.

Lead-in
Network adapters act as the physical interface, or connection, between the computer and the network cable.



Key Points
Each network adapter has a unique address, called the media access control (MAC), address, that is incorporated into chips on the card.

Network adapters convert data into electrical signals that can be transmitted over a cable.

Network adapters convert electrical signals into data packets that the computer's operating system can understand.

Network adapters constitute the physical interface between the computer and the network cable. Network adapters, also known as network interface cards, are installed into an expansion slot in each computer and server on the network. After the network adapter is installed, the network cable is attached to the adapter's port to physically connect the computer to the network.

As the data passes through the cable to the network adapter, it is formatted into *packets*. A packet is a logical grouping of information that includes a header, which contains location information and user data. The header contains address fields that include information about the data's origin and destination. The network adapter reads the destination address to determine if the packet is to be delivered to this computer. If it is, the network adapter then passes the packet on to the operating system for processing. If not, the network adapter discards the packet.

Each network adapter has a unique address that is incorporated into chips on the card. This address is called the physical, or media access control (MAC), address.

The network adapter performs the following functions:

- Receives data from the computer's operating system and converts it into electrical signals that are transmitted onto the cable
- Receives electrical signals from the cable and translates them into data that the computer's operating system can understand
- Determines whether data received from the cable is intended for the computer
- Controls the flow of data between the computer and the cabling system

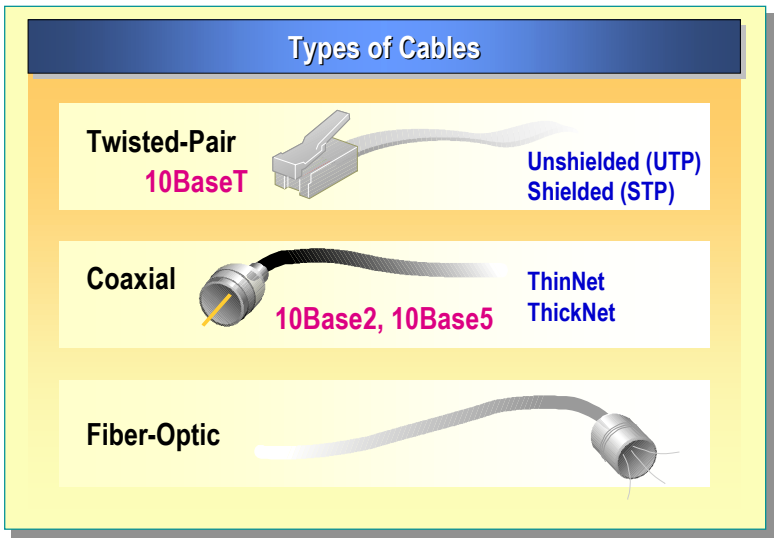
To ensure compatibility between the computer and the network, the network adapter must meet the following criteria:

- Fit in the computer's expansion slot
- Use the correct type of cable connector for the cabling
- Be supported by the computer's operating system

Network Cables

Slide Objective
To describe the network cables that are used in a network infrastructure.

Lead-in
You connect computers to form a network by using cables that act as a network transmission medium to carry signals between computers.



Key Points
Twisted-pair cable is the most common type of cable used in networks.

Coaxial cable is used when the data travels long distances.

Fiber-optic cable is used when you have a need for data to travel at the speed of light.

You connect computers together in a network by using cables to carry signals between computers. A cable that connects two computers or network components is called a *segment*. Cables differ in their capabilities and are categorized according to their ability to transmit data at varying speeds, with different error rates. The three major categories of cables that connect most networks are:

- Twisted-pair
- Coaxial
- Fiber-optic

Twisted-Pair Cable

Twisted-pair cable (10baseT) consists of two insulated strands of copper wire twisted around each other. There are two types of twisted-pair cable: unshielded twisted pair (UTP) and shielded twisted pair (STP). These are the most common cables used in networks and can carry signals for 100 meters (about 328 feet).

- UTP cable is the most popular type of twisted-pair cable and is the most popular LAN cable.
- STP cable uses a woven copper-braid jacket that is more protective and of a higher quality than the jacket used by UTP. STP also uses a foil wrap around each of the wire pairs. This gives STP excellent shielding that protects the transmitted data from outside interference, which in turn allows STP to support higher transmission rates over longer distances than UTP.

Twisted-pair cabling uses Registered Jack 45 (RJ-45) connectors to connect to a computer. These are similar to Registered Jack 11 (RJ-11) connectors.

Coaxial Cable

Coaxial cable consists of a copper wire core surrounded by insulation, a braided metal shielding, and an outer cover. The core of a coaxial cable carries the electronic signals that make up the data. This wire core can be either solid or stranded. There are two types of coaxial cable: ThinNet coaxial cable (10Base2) and ThickNet coaxial cable (10Base5). Coaxial cabling is a good choice when transmitting data over long distances and for reliably supporting higher data rates when using less sophisticated equipment.

Coaxial cable must be terminated at each end.

- ThinNet coaxial cable can carry a signal for approximately 185 meters (about 607 feet).
- ThickNet coaxial cable can carry a signal for 500 meters (about 1,640 feet).

Both ThinNet and ThickNet cable use a connection component, known as a BNC connector, to make the connections between the cable and the computers.

Fiber-Optic Cable

Fiber-optic cable uses optical fibers to carry digital data signals in the form of modulated pulses of light. Because fiber-optic cable carries no electrical impulses, the signal cannot be tapped and its data cannot be stolen. Fiber-optic cable is good for very high-speed, high-capacity data transmission because the signal is transmitted very quickly and with very little interference.

A disadvantage of fiber-optic cable is that it breaks easily if you are not careful during installation. It is more difficult to cut than other cables and requires special equipment to cut it.

Selecting Cables

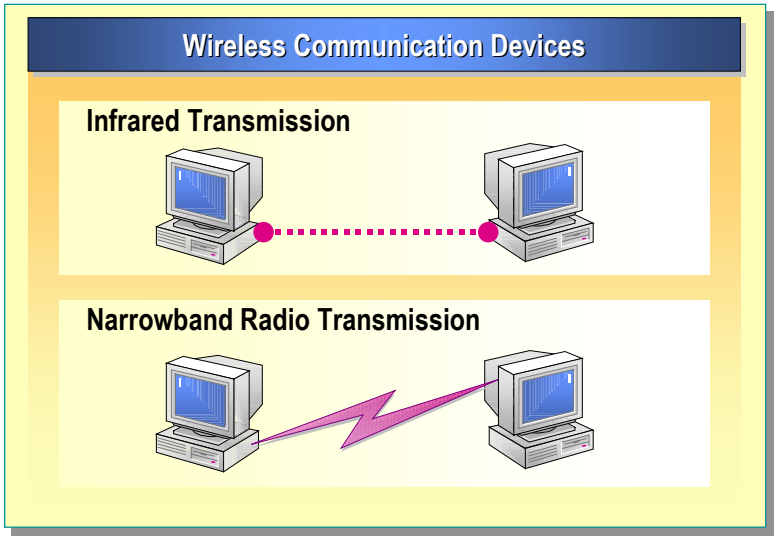
The following table lists considerations for use of the three categories of network cables.

Cable categories	Use if	Do not use if
Twisted-pair	You want a relatively easy installation in which computer connections are simple.	Your LAN requires a high level of signal shielding to protect it from electromagnetic waves that may interfere with the electrical signal carried in the cable. You must transmit data over long distances at high speeds.
Coaxial	You need to transmit data for greater distances than is possible with less expensive cabling.	You need to change the network cables frequently due to relocations.
Fiber-optic	You need to transmit secure data at very high speeds over long distances.	You have a small budget. You do not have the expertise to properly install it and connect devices to it.

Wireless Communication Devices

Slide Objective
To describe the characteristics of the wireless communication devices used in a network infrastructure.

Lead-in
You use wireless components to connect to networks over distances that make using standard network adapters and cabling options technically or economically unfeasible.



Key Point
Except for the technology it uses, a typical wireless network operates almost like a cabled network: a wireless network adapter with a transceiver is installed in each computer, and users communicate with the network just as if they were using cabled computers.

You use wireless components to connect networks over distances for which standard network adapters and cable options are not technically or economically feasible. Wireless networks consist of wireless components communicating with LANs.

Except for the fact that a cable does not connect the computers, a typical wireless network operates almost like a cabled network: a wireless network adapter with a *transceiver* (a device that both transmits and receives analog and digital signals) is installed in each computer. Users communicate with the network as if they were using cabled computers.

There are two common techniques for wireless transmission in a LAN: infrared transmission and narrowband radio transmission.

- Infrared transmission

  Operates by using an infrared light beam to carry the data between devices. There must be a clear line of sight between the transmitting and receiving devices; anything that blocks the infrared signal prevents communication. These systems must generate very strong signals because weak transmission signals are susceptible to interference from light sources, such as windows.

- Narrowband radio transmission

  The user tunes both the transmitter and the receiver to a certain frequency. Narrowband radio does not require line-of-sight focusing because it uses radio waves. However, narrowband radio transmission is subject to interference from steel and load-bearing walls. Narrowband radio is a subscription service. Users pay a fee for radio transmission.

Network Topologies

Slide Objective
To introduce the various types of network topologies.

Lead-in
A network topology describes the arrangement of computers, cables, and other components on a network.

- Bus Topology
- Star Topology
- Ring Topology
- Mesh Topology
- Hybrid Topologies

A network topology is the arrangement of computers, cables, and other components on a network. It is a map of the physical network. The type of topology you use affects the type and capabilities of the network's hardware, its management, and possibilities for future expansion.

Topology is both physical and logical:

- Physical topology describes how the physical components on a network are connected.
- Logical topology describes the way network data flows through the physical components.

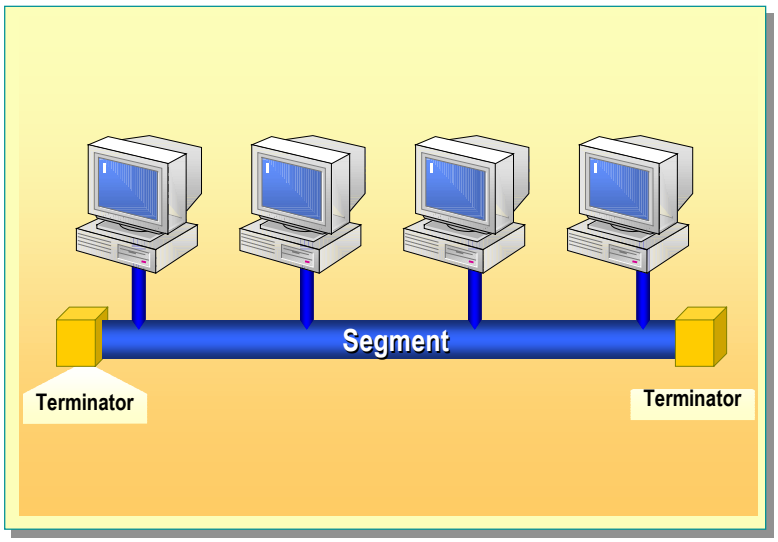
There are five basic topologies:

- *Bus.* Computers are connected to a common, shared cable.
- *Star.* Computers are connected to cable segments that branch out from a central location, or hub.
- *Ring*. Computers are connected to a cable that forms a loop around a central location.
- *Mesh.* Computers on the network are connected to every other computer by cable.
- *Hybrid.* Two or more topologies are used together.

Bus Topology

Slide Objective
To illustrate a bus topology.

Lead-in
In a bus topology, each computer is attached to a continuous cable called a backbone, which is a segment that connects the entire network in a straight line.



Key Points
Both ends of the cable must be terminated.

All network adapters on the cable receive the data packet.

In a bus topology, all of the computers in a network are attached to a continuous cable, or segment, that connects them in a straight line. In this straight-line topology, a packet is transmitted to all network adapters on that segment.

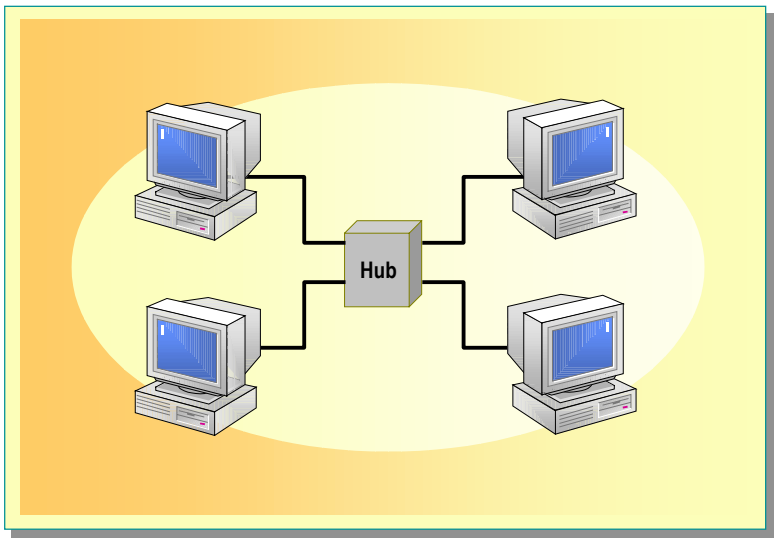
Because of the way electrical signals are transmitted over this cable, the ends of the cable must be terminated by hardware devices called terminators, which act as the boundaries for the signal and define the segment. If there is a break anywhere in the cable or if an end is not terminated, the signal will travel back and forth across the network and all communication will stop.

The number of computers attached to a bus also affects network performance. The more computers there are on the bus, the greater the backup of computers waiting to put data on the bus, and consequently, the slower the network. In addition, because of the way computers communicate in a bus topology, there may be a lot of *noise*. Noise is the traffic generated on the network when computers attempt to communicate with each other simultaneously. An increase in the number of computers results in an increase in noise and a corresponding decrease in network efficiency.

Star Topology

Slide Objective
To illustrate a star topology.

Lead-in
In a star topology, cable segments from each computer on the network are connected to a centralized component.



Key Points
In a star topology, if a single computer fails, only the failed computer is unable to send or receive data.

In a star topology, cable segments from each computer on the network are connected to a central component, or *hub*. A hub is a device that connects several computers together. In a star topology, signals are transmitted from the computer, through the hub, to all computers on the network. On a larger scale, multiple LANs can be connected to each other in a star topology.

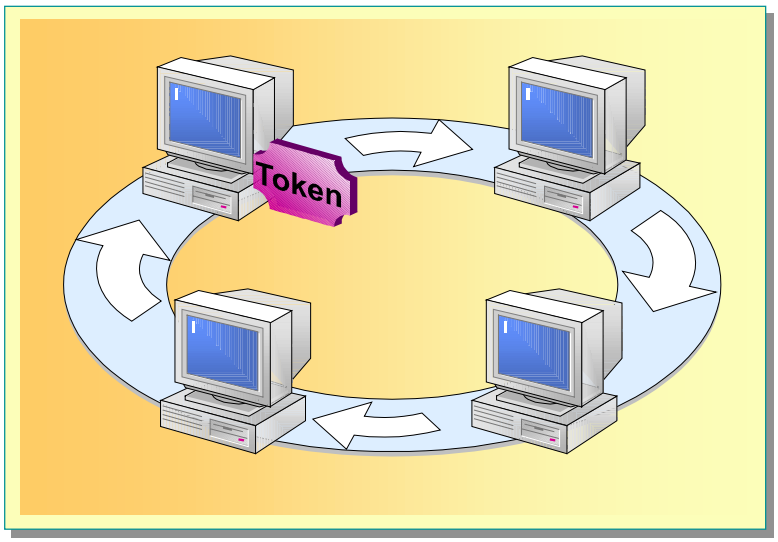
An advantage of the star topology is that if one computer on the star topology fails, only the failed computer is unable to send or receive data. The remainder of the network functions normally.

The disadvantage of using this topology is that because each computer is connected to a hub, if the hub fails, the entire network fails. In addition, noise is created on the network in a star topology.

Ring Topology

Slide Objective
To illustrate a ring topology.

Lead-in
In a ring topology, computers are connected on a single circle of cable.



Key Points
In a ring topology, each computer acts as a repeater, regenerating the signal and sending it on to the next computer. This preserves signal strength.

In a ring topology, computers are connected on a single circle of cable. Unlike the bus topology, there are no terminated ends. The signals travel around the loop in one direction and pass through each computer, which acts as a repeater to boost the signal and send it to the next computer. On a larger scale, multiple LANs can be connected to each other in a ring topology by using ThickNet coaxial or fiber-optic cable.

The advantage of a ring topology is that each computer acts as a repeater, regenerating the signal and sending it on to the next computer, thereby preserving signal strength.

Token Passing

The method of transmitting data around the ring is called token passing. A *token* is a special series of bits that contains control information. Possession of the token allows a network device to transmit data to the network. Each network has only one token.

The sending computer removes the token from the ring and sends the requested data around the ring. Each computer passes along the data until the packet finds the computer that matches the address on the data. The receiving computer then returns a message to the sending computer indicating that the data has been received. After verification, the sending computer creates a new token and releases it to the network.

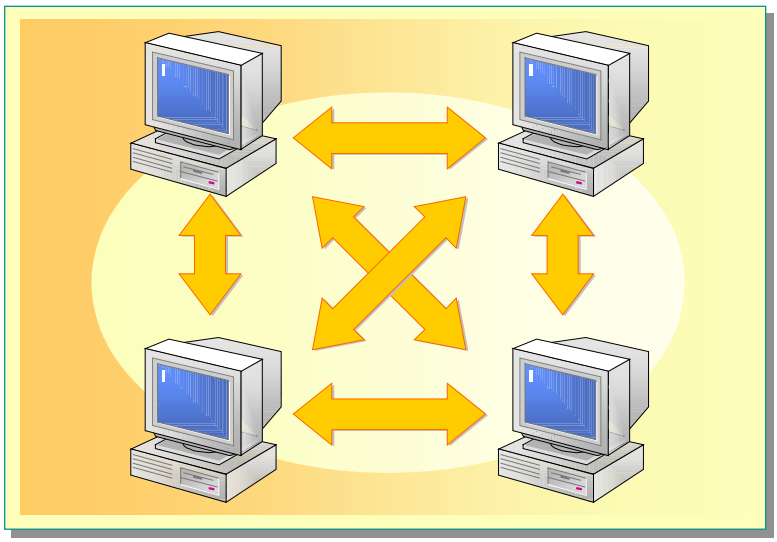
The advantage of a ring topology is that it can handle high-traffic environments better than bus networks. In addition, the impact of noise is reduced in the ring topology.

The disadvantage of a ring topology is that only one computer at a time can send data on a single token ring. Also, ring topologies are usually more expensive than bus technologies.

Mesh Topology

Slide Objective
To illustrate a mesh topology.

Lead-in
In a mesh topology, each computer is connected to every other computer by separate cabling.



Key Points
A mesh topology provides redundant paths through the network so that if one cable fails, another picks up the traffic and the network continues to function.

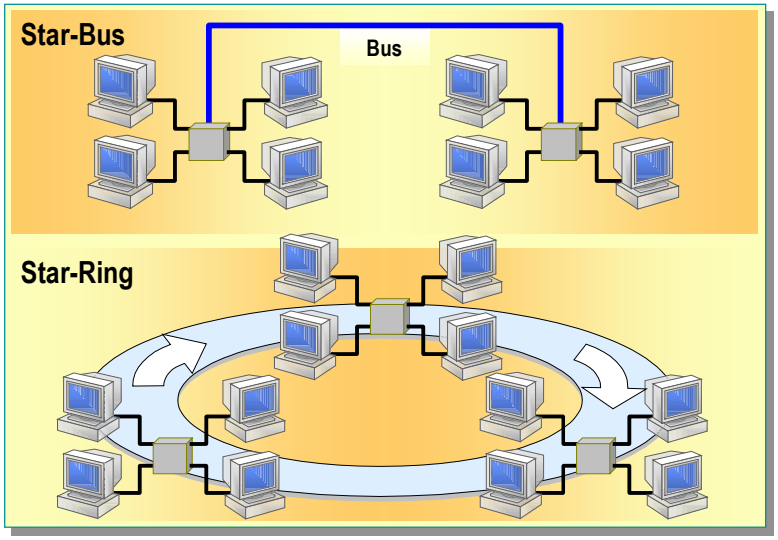
In a mesh topology, each computer is connected to every other computer by a separate cable. This configuration provides redundant paths through the network so that if one cable fails, another carries the traffic and the network continues to function. On a larger scale, multiple LANs can be connected to each other in a mesh topology by using leased telephone lines, ThickNet coaxial cable, or fiber-optic cable.

An advantage of a mesh topology is its back-up capabilities by providing multiple paths through the network. Because redundant paths require more cable than is needed in other topologies, a mesh topology can be expensive.

Hybrid Topologies

Slide Objective
To illustrate hybrid topologies.

Lead-in
In a hybrid topology, two or more topologies are combined to form a complete network design.



Key Points
In a hybrid topology, if a single computer fails, it does not affect the remainder of the network.

In a hybrid topology, two or more topologies are combined to form a complete network design. Networks are rarely designed using only one type of topology. For example, you may want to combine a star with a bus topology to benefit from the advantages of each.

Two types of hybrid topologies are commonly in use: star-bus topology and star-ring topology.

Star-Bus

In a star-bus topology, several star topology networks are linked to a bus connection. After a star configuration is full, you can add a second star and use a bus connection to connect the two star topologies.

In a star-bus topology, if a single computer fails, it will not affect the rest of the network. However, if the central component, or hub, that attaches all computers in a star fails, all computers attached to that component fail and are unable to communicate.

Star-Ring

In the star-ring topology, the computers are connected to a central component as in a star network. These components, however, are wired to form a ring network.

Like the star-bus topology, if a single computer fails, it will not affect the rest of the network. By using token passing, each computer in a star-ring topology has an equal chance of communicating. This allows for greater network traffic between segments than in a star-bus topology.

Network Technologies

Slide Objective
To introduce the technologies used in a network.

Lead-in
You use different network technologies to communicate between computers within LANs and WANs.

- **Ethernet**
- **Token Ring**
- **Asynchronous Transfer Mode (ATM)**
- **Fiber Distributed Data Interface (FDDI)**
- **Frame Relay**

You use different network technologies to communicate between computers within LANs and WANs. You may use a combination of technologies to get the best cost-benefit and maximum efficiency from your network design.

Many network technologies are available, including:

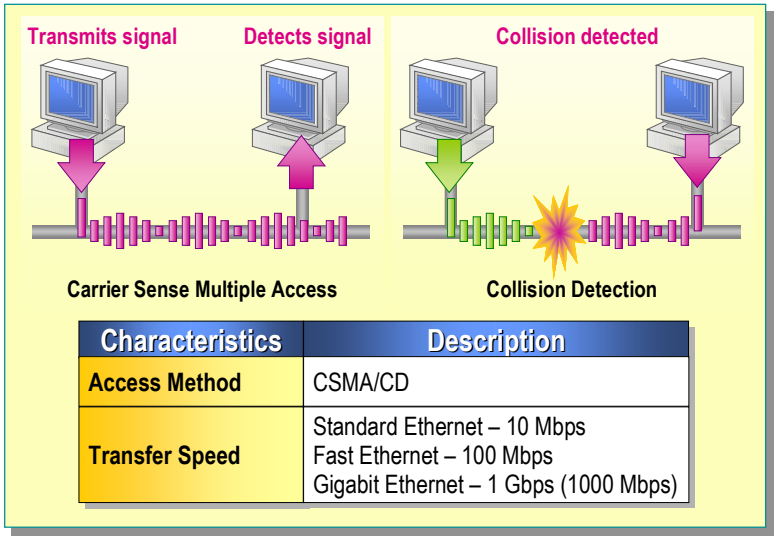
- Ethernet.
- Token ring.
- Asynchronous transfer mode (ATM).
- Fiber Distributed Data Interface (FDDI).
- Frame relay.

One of the ways in which these technologies differ is the set of rules that each uses to place data onto the network cable and to remove data from the cable. This is called *access method*. When data moves on the network, these various access methods regulate the flow of network traffic.

Ethernet

Slide Objective
To describe how Ethernet works.

Lead-in
Ethernet is a popular LAN technology that uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) between clients and runs over a variety of cable types by using a bus topology.



Characteristics	Description
Access Method	CSMA/CD
Transfer Speed	Standard Ethernet – 10 Mbps Fast Ethernet – 100 Mbps Gigabit Ethernet – 1 Gbps (1000 Mbps)

Delivery Tip
Describe the Ethernet technology. Use the student notes and the slide for supportive details

Define the CSMA/CD data access method and describe how it works in an Ethernet network.

Key Points
Ethernet is passive, which means it requires no power source of its own, and thus does not fail unless the cable is physically cut or improperly terminated.

Ethernet can use multiple communication protocols and can connect mixed computing environments, including Netware, UNIX, Windows, and Macintosh.

Ethernet is a popular LAN technology that uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) between clients over a variety of cable types. Ethernet is passive, which means it requires no power source of its own, and thus does not fail unless the cable is physically cut or improperly terminated. Ethernet is connected by using a bus topology in which the cable is terminated at both ends.

Ethernet uses multiple communication protocols and can connect mixed computing environments, including Netware, UNIX, Windows, and Macintosh.

Access Method

The network access method used for Ethernet is Carrier Sense Multiple Access with Collision Detection (CSMA/CD). CSMA/CD is a set of rules that determines how network devices respond when two devices attempt to send data on the network simultaneously. Transmission of data by multiple computers simultaneously over the network causes a collision. Each computer on the network, including clients and servers, checks the cable for network traffic. Only when a computer detects that the cable is free and that there is no traffic on the cable does it send data. After the computer has transmitted data on the cable, no other computer can transmit data until the original data has reached its destination and the cable is again free.

After detecting a collision, a device waits a random delay time and then attempts to retransmit the message. If the device detects a collision again, it waits twice as long before trying to retransmit the message.

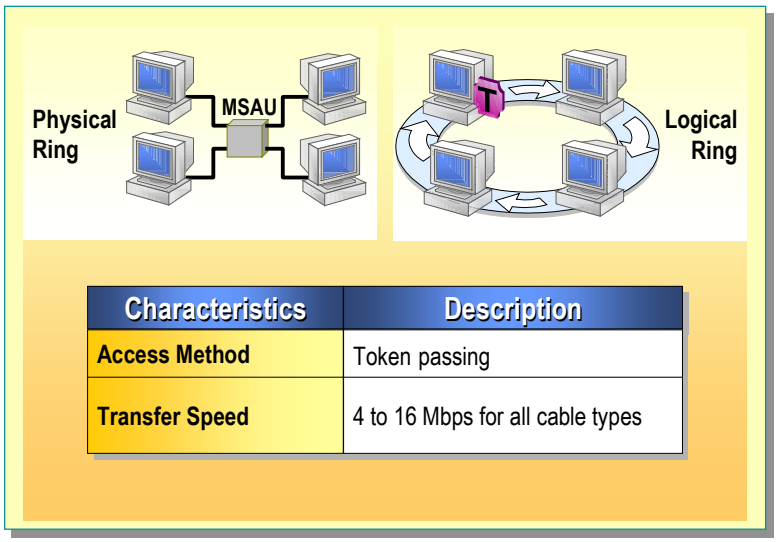
Transfer Speed

Standard Ethernet, called 10BaseT, supports data transfer rates of 10 Mbps over a wide range of cabling. Faster versions of Ethernet are also available. Fast Ethernet (100BaseT) supports data transfer rates of 100 Mbps, and Gigabit Ethernet supports data rates of 1 Gbps (gigabits per second) or 1,000 Mbps.

Token Ring

Slide Objective
To describe how a token ring network functions.

Lead-in
Token ring networks are implemented in a star-wired ring; computers on the network are connected to a central component.



Characteristics	Description
Access Method	Token passing
Transfer Speed	4 to 16 Mbps for all cable types

Delivery Tip
Describe the token ring technology. Use the student notes and slide for supportive details.

Explain the token passing access method and how it works in a token ring network.

Key Points
The logical ring represents the token's path between computers. The physical ring is wired through a central component called a multistation access unit (MSAU).

Token ring networks are implemented in a ring topology. The physical topology of a token ring network is the star topology, in which all computers on the network are physically connected to a hub. The physical ring is wired through a hub called a multistation access unit (MSAU). The logical topology represents the token's path between computers, which is similar to a ring.

Access Method

The access method used in a token ring network is token passing. A token is a special series of bits that travels around a token ring network. A computer cannot transmit unless it has possession of the token; while the token is in use by a computer, no other computer can transmit data.

When the first computer on the token ring comes online, the network generates a token. The token travels around the ring to each computer until one of the computers takes control of the token.

When a computer takes control of the token, it sends a data frame out on the network. The frame proceeds around the ring until it reaches the computer with the address that matches the destination address in the frame. The destination computer copies the frame into its memory and marks the frame in the frame status field to indicate that the information was received.

The frame continues around the ring until it arrives at the sending computer, where the transmission is acknowledged as successful. The sending computer then removes the frame from the ring and transmits a new token back on the ring.

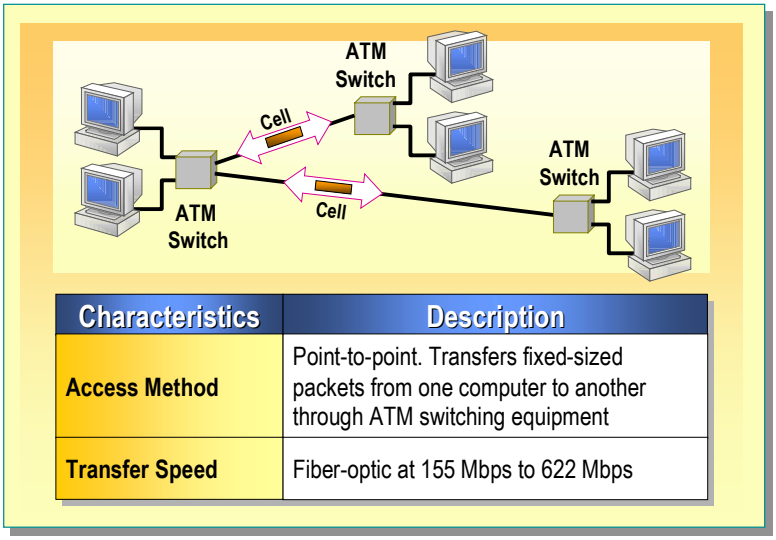
Transfer Speed

The transfer speed in a token ring network is between 4 and 16 Mbps.

Asynchronous Transfer Mode

Slide Objective
To describe how asynchronous transfer mode works.

Lead-in
Asynchronous transfer mode is an advanced implementation of packet switching that sends fixed-size packets over LANs or WANs.



Characteristics	Description
Access Method	Point-to-point. Transfers fixed-sized packets from one computer to another through ATM switching equipment
Transfer Speed	Fiber-optic at 155 Mbps to 622 Mbps

Delivery Tip
Describe the asynchronous transfer mode technology. Use the student notes and slide for supportive details.

Describe the cell relay access method and how it is applied in ATM.

Key Points
ATM's transmission speed enables it to transmit voice, real-time video, CD-quality audio, imaging, and megabit data transmission.

Asynchronous transfer mode (ATM) is a packet-switching network that sends *fixed-length packets* over LANs or WANs, instead of the variable-length packets used in other technologies. Fixed-length packets, or cells, are data packets that contain only basic path information, allowing switching devices to route the packet quickly. Communication occurs over a point-to-point system that provides a permanent and virtual data path between each station.

Using ATM, you can send data from a main office to a remote location. The data travels from a LAN over a digital leased line to an ATM switch and into the ATM network. It passes through the ATM network and arrives at another ATM switch in the destination LAN.

Because of its expanded bandwidth, ATM can accommodate:

- Voice.
- Real-time video.
- CD-quality audio.
- Imaging data, such as real-time radiology.
- Megabit data transmission.

Access Method

An ATM network uses the point-to-point access method. This access method transfers fixed-length packets from one computer to another through ATM switching equipment. The result is a technology that transmits a small, compact data packet at a high speed.

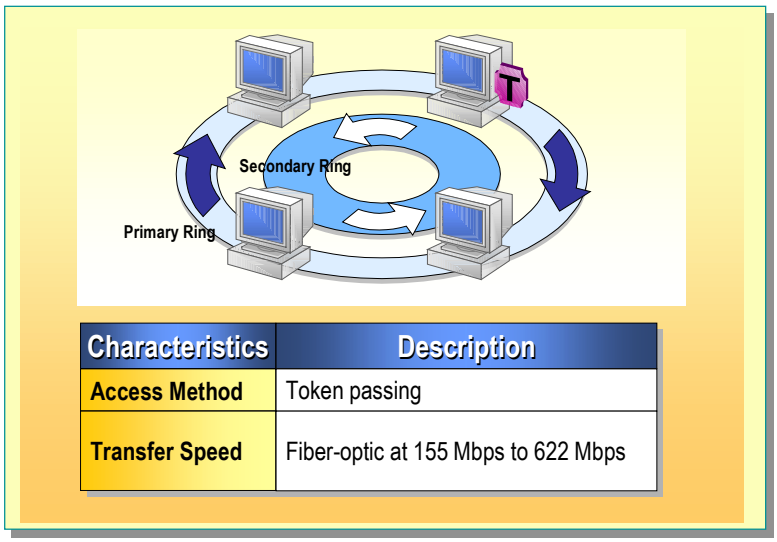
Transfer Speed

The transfer speed in an ATM network is between 155 and 622 Mbps.

Fiber Distributed Data Interface

Slide Objective
To described how Fiber Distributed Data Interface works.

Lead-in
A Fiber Distributed Data Interface network is used to provide high-speed connections for various types of networks.



Characteristics	Description
Access Method	Token passing
Transfer Speed	Fiber-optic at 155 Mbps to 622 Mbps

Delivery Tip
Describe the Fiber Distributed Data Interface technology. Use the student notes and the slide for supportive details.

Describe the token passing access method and how it is used in FDDI.

Key Points
FDDI provides a fast backbone to an existing LAN or WAN.

A Fiber Distributed Data Interface (FDDI) network provides high-speed connections for various types of networks. FDDI was designed for use with computers that required speeds greater than the 10 Mbps available from Ethernet or the 4 Mbps available from existing token ring architectures. An FDDI network can support several low-capacity LANs that require a high-speed backbone.

An FDDI network consists of two similar streams of data flowing in opposite directions around two rings. One ring is called the primary ring and the other is called the secondary ring. If there is a problem with the primary ring, such as a ring failure or a cable break, the ring reconfigures itself by transferring data to the secondary ring, which continues transmitting.

Access Method

The access method used in an FDDI network is token passing. A computer on an FDDI network can transmit as many packets as it can produce within a predetermined time before releasing the token. As soon as a computer has finished transmitting or after a predetermined transmittal time is up, the computer releases the token.

Because a computer releases the token when it finishes transmitting, several packets can circulate on the ring at the same time. This method of token passing is more efficient than that on a standard token ring network, which allows only one frame at a time to circulate. This method of token passing also provides greater data throughput at the same transmission rate.

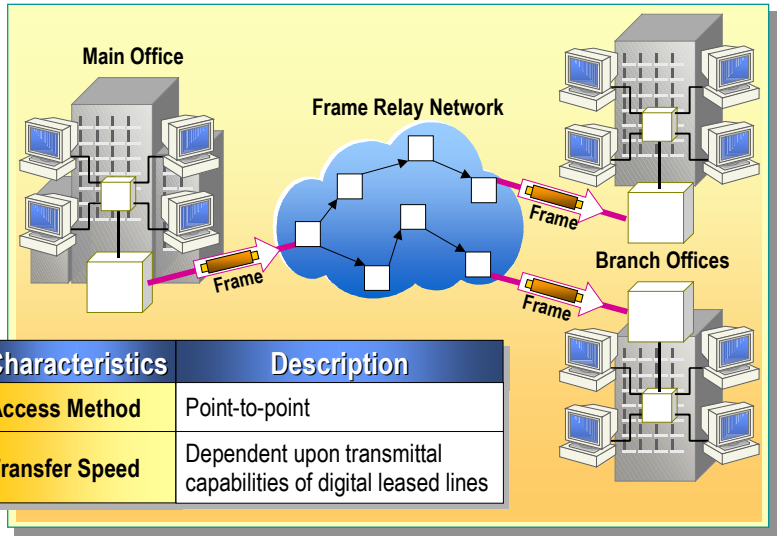
Transfer Speed

The transfer speed in an FDDI network is between 155 and 622 Mbps.

Frame Relay

Slide Objective
To describe how frame relay works.

Lead-in
Frame relay is a packet-switching network that sends variable-length data packets over LANs or WANs.



Characteristics	Description
Access Method	Point-to-point
Transfer Speed	Dependent upon transmittal capabilities of digital leased lines

Delivery Tip
Describe the frame relay technology. Use the student notes and slide for supportive details.

Define the point-to-point access method and how it works in a frame relay network.

Key Points
This type of network gives you quick access to data transfer that you pay for only as you need it.

Frame relay is a packet-switching network that sends *variable-length packets* over LANs or WANs. Variable length packets, or frames, are data packets that contain additional addressing and error handling information necessary for delivery.

Communication occurs over a network that provides a permanent and virtual data path between each station. This type of network uses wide area digital or fiber-optic links and gives you quick access to data transfer that you pay for only as you need it.

Packet switching is a method used to send data over a WAN by dividing a large package of data into smaller pieces (packets). These pieces are sent through a packet switch, which sends the individual packets across the WAN using the best route currently available. Although these packets may travel along different paths, the receiving computer can reassemble the pieces into the original data frame.

However, you could have a permanent virtual circuit (PVC) established, which would use the same path for all of the packets. This allows for a faster transmission than by normal frame relay networks and eliminates the need for packet disassembly and reassembly.

Access Method

Frame relay uses the point-to-point access method. This access method transfers variable-sized packets from one computer directly to another, instead of between several computers and peripherals.

Transfer Speed

Frame relay allows for data transfer that is as fast as the provider can supply over digital leased lines.

Expanding the Network

Slide Objective
To introduce the tools you use to expand the network.

Lead-in
There are several tools that you can use to expand an existing network.

- Repeaters and Hubs
- Bridges
- Switches
- Routers
- Gateways
- Remote Access Connectivity Types
- Public Switched Telephone Network (PSTN)
- Integrated Services Digital Network (ISDN)
- X.25
- Asymmetric Digital Subscriber Line (ADSL)

Delivery Tip
This is only an introduction to the topics that follow. Do not spend too much time on this page.

To cater to the growing networking needs of an organization, you need to expand the size or improve the performance of a network. You cannot make networks larger just by adding new computers and more cable. Each network topology or architecture has limits. You can, however, install components to increase the size of the network within its existing environment.

Components that enable you to expand the network include:

- Repeaters and Hubs

  Repeaters and hubs retransmit an electrical signal received on one connection point (port) to all ports in order to maintain the integrity of the signal.
- Bridges

  Bridges enable data to be passed between LANs.
- Switches

  Switches enable high-speed passing of data to LANs.
- Routers

  Routers enable passing of data through LANs or WANs, depending on the destination network of the data.
- Gateways

  Gateways enable passing of data through LANs or WANs and function so that computers using different protocols can communicate with each other.

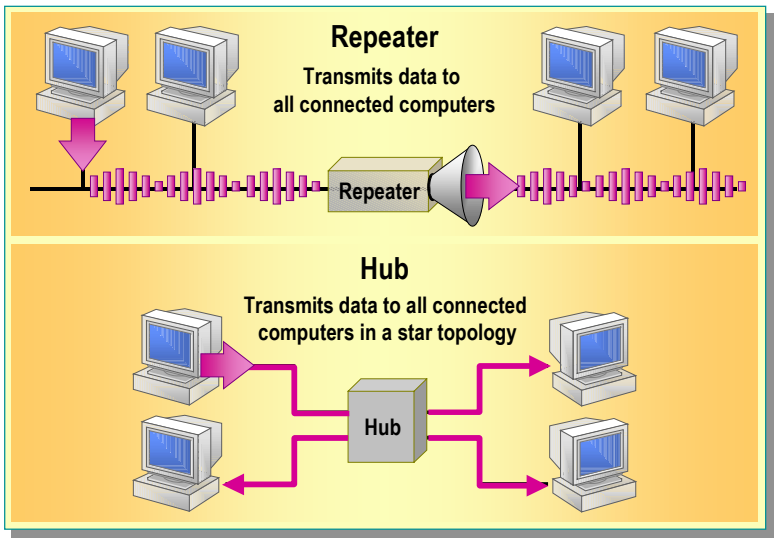
You can also expand a network by allowing users to connect to the network from a remote location. To establish a remote connection, the three components required are a remote access client, a remote access server, and physical connectivity. Microsoft Windows 2000 enables remote client computers to connect to remote access servers by using:

- Public Switched Telephone Network (PSTN).
- Integrated Services Digital Network (ISDN).
- X.25.
- Asymmetric Digital Subscriber Line (ADSL).

Repeaters and Hubs

Slide Objective
To illustrate how repeaters and hubs work.

Lead-in
Repeaters and hubs are used to expand a network by adding two or more segments of cabling.



Delivery Tip
Describe how to use repeaters and hubs to expand a network.

Use the student notes and the animated slides for supportive details.

Key Points
Repeaters are inexpensive ways to expand cable length without sacrificing data loss.

Hubs enable you to connect several computers to a central point without data loss.
A hub broadcasts the data packet to all of the computers and segments that are attached to it.

You can use repeaters and hubs to expand a network by adding two or more segments of cabling. These commonly used devices are inexpensive and easy to set up.

Repeaters

Repeaters receive signals and retransmit them at their original strength and definition. This increases the practical length of a cable. (If a cable is very long, the signal weakens and becomes unrecognizable.) Installing a repeater between cable segments enables signals to travel farther.

Repeaters do not translate or filter signals. For a repeater to work, both segments connected to the repeater must use the same access method. For example, a repeater cannot translate an Ethernet packet into a token ring packet.

Repeaters do not act as filters to restrict the flow of problem traffic. Repeaters send every bit of data from one cable segment to another, even if the data consists of malformed packets or packets not destined for a computer on another segment.

Use a repeater to:

- Connect two segments of similar or dissimilar cabling.
- Regenerate the signal to increase the distance transmitted.
- Transmit all traffic in both directions.
- Connect two segments in the most cost-effective manner.

Hubs

Hubs are connectivity devices that connect computers in a star topology. Hubs contain multiple ports for connecting to network components. If you use a hub, a break in the network does not affect the entire network; only the segment and the computer attached to that segment fail. A single data packet sent through a hub goes to all connected computers.

There are two types of hubs:

- *Passive Hubs*. Send the incoming signal directly through their ports without any signal processing. These hubs are usually wiring panels.
- *Active Hubs.* Sometimes called *multiport repeaters*, receive incoming signals, process the signals, and retransmit them at their original strengths and definitions to the connected computers or components.

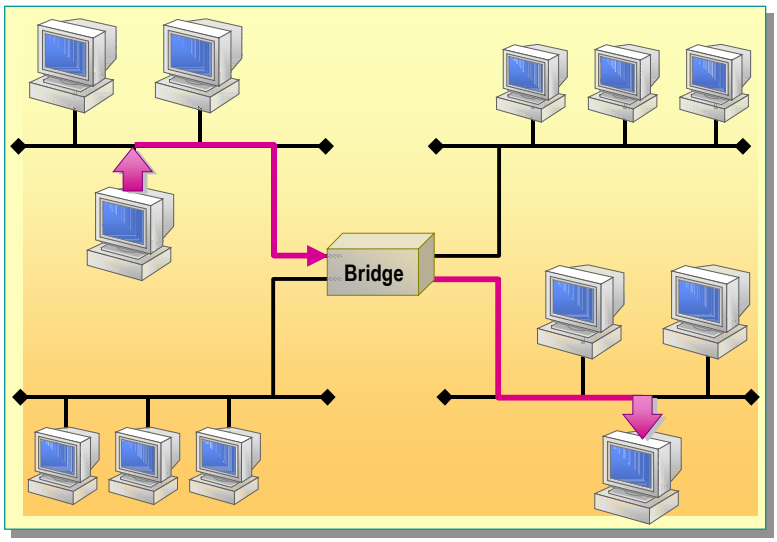
Use a hub to:

- Easily change and expand wiring systems.
- Use different ports to accommodate a variety of cable types.
- Enable central monitoring of network activity and traffic.

Bridges

Slide Objective
To illustrate how bridges work.

Lead-in
A bridge is a device that passes data packets between multiple network segments that use the same communications protocol.



Delivery Tip
Describe how a bridge is used to expand a network. Use the student notes and animated slide for supportive details.

Key Points
A bridge broadcasts packets to a computer if it recognizes the location of the destination address. If it does not recognize the destination address, it forwards the packets to all segments attached to the bridge.

A bridge is a device that passes data packets between multiple network segments that use the same communications protocol. A bridge passes one signal at a time. If a packet is destined for a computer within the sender's own network segment, the bridge retains the packet within that segment. If the packet is destined for another segment, it passes the packet to that segment.

MAC Addresses

As traffic passes through the bridge, information about the sending computers' MAC addresses is stored in the bridge's memory. The bridge uses this information to build a table based on these addresses. As more data is sent, the bridge develops a bridging table that identifies each computer and its location on network segments. When the bridge receives a packet, the source address is compared to the source address listed in the table. If the source address is not present in the table, it is added to the table. The bridge then compares the destination address with the destination address listed in the table. If a bridge recognizes the location of the destination address, it forwards the packet to this address. If it does not recognize the destination address, it forwards the packet to all segments.

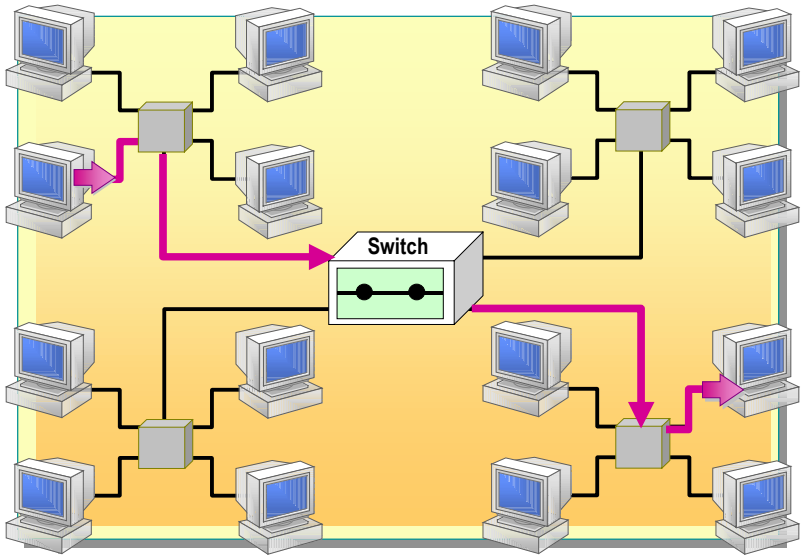
Use a bridge to:

- Expand the length of a segment.
- Provide for an increased number of computers on the network.
- Reduce traffic bottlenecks resulting from an excessive number of attached computers.
- Split an overloaded network into two separate networks, thereby reducing the amount of traffic on each segment and making each network more efficient.
- Link dissimilar physical cables, such as twisted-pair and coaxial Ethernet cables.

Switches

Slide Objective
To illustrate how switches function.

Lead-in
Switches are similar to bridges but offer a more direct network connection between the source and destination computers.



Delivery Tip
Describe how switches are used to expand a network. Use the student notes and the animated slide for supportive details.

Key Points
When a switch receives a data packet, it forwards the data packet to the destination computer only.

Switches are similar to bridges but offer a more direct network connection between the source and destination computers. When a switch receives a data packet, it creates a separate internal connection, or segment, between any two of its ports and forwards the data packet to the appropriate port of the destination computer only, based on information in each packet's header. This insulates the connection from the other ports and gives the source and destination computers access to the full bandwidth of a network.

Unlike a hub, switches are comparable to a telephone system with private lines. In such a system, if one person calls someone, the operator or telephone switch connects them on a dedicated line. This allows more conversations to take place at any one time.

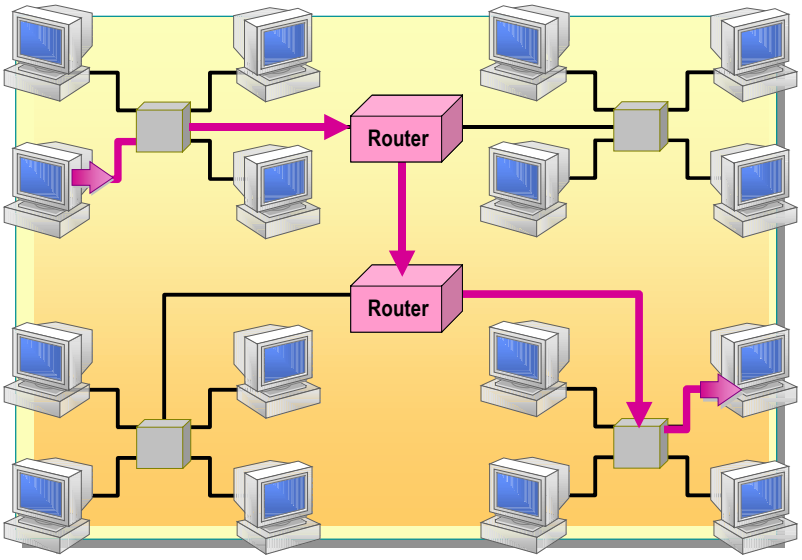
Use a switch to:

- Send a packet directly from the source computer to the destination computer.
- Provide for a greater rate of data transmission.

Routers

Slide Objective
To illustrate how routers function.

Lead-in
A router is a device that acts like a bridge or switch but provides increased functionality.



Delivery Tip
Describe how a router is used to expand a network. Use the student notes and the animated slide for supportive details.

Key Points
Using the network addresses of computers and sophisticated routing information, a router can send data over the most direct path between the source and destination computers.

A router is a device that acts like a bridge or switch but provides more functionality. In moving data between different network segments, routers examine a packet header to determine the best path for the packet to travel. A router knows the path to all of the segments on the network by accessing information stored in the routing table. Routers enable all users in a network to share a single connection to the Internet or a WAN.

Use a router to:

- Send packets directly to a destination computer on another networks or segment.

  Routers use a more complete packet address than do bridges, for example, to determine which router or client should next receive each packet. Routers ensure that packets travel the most efficient paths to their destinations. If a link between two routers fails, the sending router can determine an alternate route to keep traffic moving.

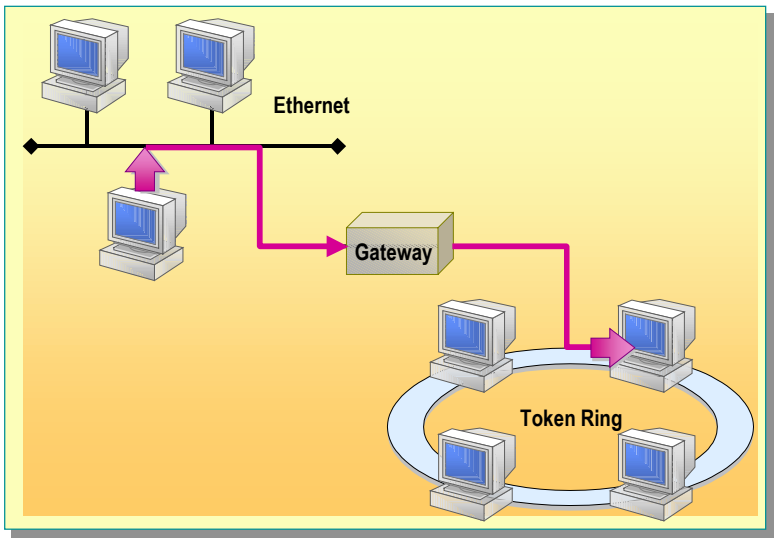
- Reduce stress on the network.

  Routers read addressed network packets only and pass information only if the network address is known. Therefore, they do not pass corrupted data. This ability to control the data passing through the router reduces the amount of traffic between networks and enables routers to use these links more efficiently than bridges can.

Gateways

Slide Objective
To illustrate how a gateway functions.

Lead-in
Gateways enable communication between different architectures and environments.



Key Points
Use a gateway to communicate between two networks that have different communication protocols, data-formatting structures, languages, and architecture.

Gateways enable communication between different network architectures. A gateway takes the data from one network and repackages it, so that each network can understand the other network's data.

A gateway is like an interpreter. For example, if two groups of people can physically talk to each other but speak different languages, they need an interpreter to communicate. Similarly, two networks can have a physical connection but need a gateway to translate network communication.

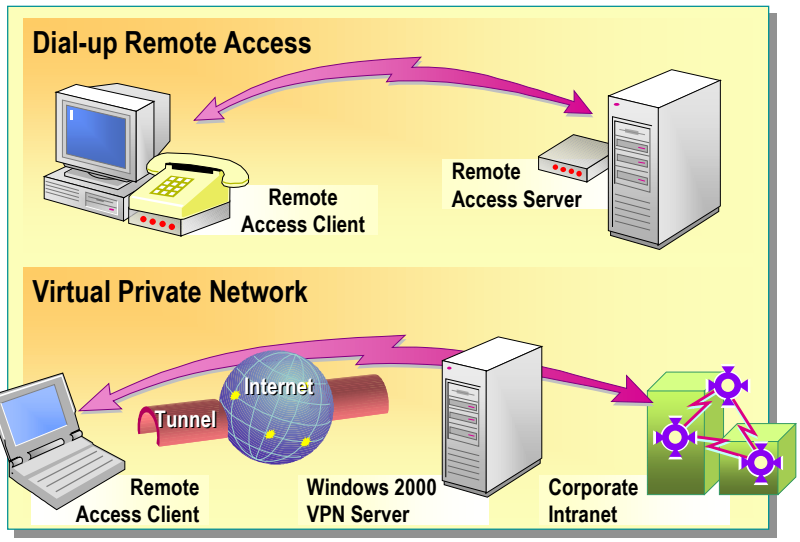
Use a gateway to link two systems that do not use the same:

- Architecture.
- Set of communication rules and regulations.
- Data-formatting structures.

Remote Access Connectivity Types

Slide Objective
To illustrate the different types of remote access connectivity.

Lead-in
When connecting to a network from a remote location, you can either connect using a dial-up connection that requires telephone lines or create a virtual private line that uses the existing connections.



Key Points
Dial-up remote access enables a client to use the telecommunications infrastructure to connect to a remote access server.

A virtual private network (VPN) connects the components and resources of one network to another network by allowing the user to tunnel through the Internet or another public network without any additional hardware.

Windows 2000 enables users to connect to a network from a remote location through a variety of hardware, such as modems. A modem enables a computer to communicate over telephone lines. The remote access client connects to the remote access server, which acts as a router, or a gateway, for the client to the remote network. A telephone line commonly provides the physical connectivity between the client and server. The remote access server runs the Routing and Remote Access feature in Windows 2000 to support remote connections and to provide interoperability with other remote access solutions.

The two types of remote access connectivity provided in Windows 2000 are dial-up remote access and virtual private network (VPN).

Dial-up Remote Access

Windows 2000 Server provides dial-up remote access to users who dial corporate intranets. Dial-up equipment installed on a remote access server running Windows 2000 answers incoming connection requests from dial-up networking clients. The dial-up equipment answers the call, verifies the caller's identity, and transfers data between the dial-up networking client and the corporate intranet.

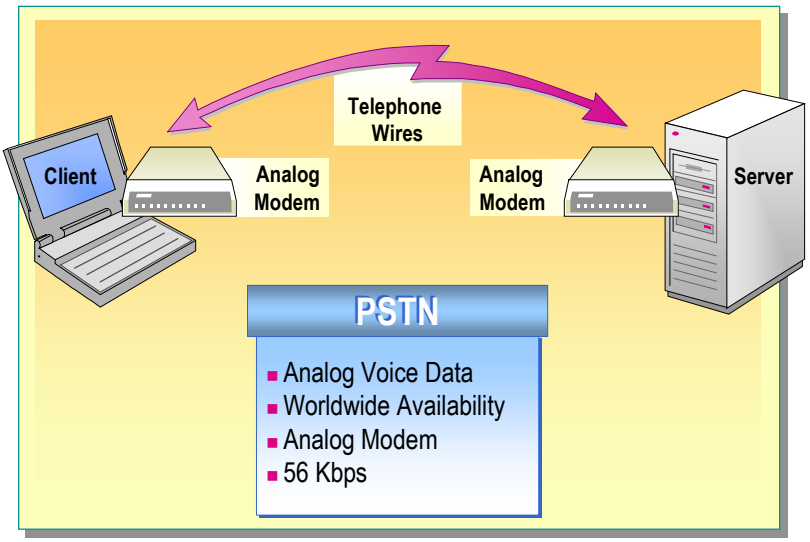
Virtual Private Network

A virtual private network (VPN) uses encryption technology to provide security and other features formerly available only in private networks. VPNs provide this security through a process called *tunneling*. Tunneling is a method of using an internetwork infrastructure to securely transfer data from one network to another network. A VPN enables telecommuters and employees at remote locations to establish a secure connection to a corporate server that is connected to both the corporate LAN and a public internetwork, such as the Internet. From the user's perspective, the VPN provides a point-to-point connection between the user's computer and a corporate server. The intermediate internetwork is transparent to the user because it appears as if the remote access client is connected directly to the corporate LAN/remote access server.

Public Switched Telephone Network (PSTN)

Slide Objective
To illustrate how a PSTN connection functions in remote access.

Lead-in
PSTN is the most common communication method because it uses inexpensive modems. It supports analog communication at speeds of up to 56 Kbps.



Key Point
PSTN is universally available and inexpensive.

Public Switched Telephone Network (PSTN) refers to the international telephone standard based on using copper wires for transmitting analog voice data. This standard was designed to carry only the minimal frequencies necessary to distinguish human voices. Because PSTN was not designed for data transmissions, there are limits to the maximum data transmission rate of a PSTN connection. In addition, analog communication is susceptible to line noise that causes a reduction in the data transmission rate.

A key advantage of PSTN is its worldwide availability and low-cost hardware due to mass-production.

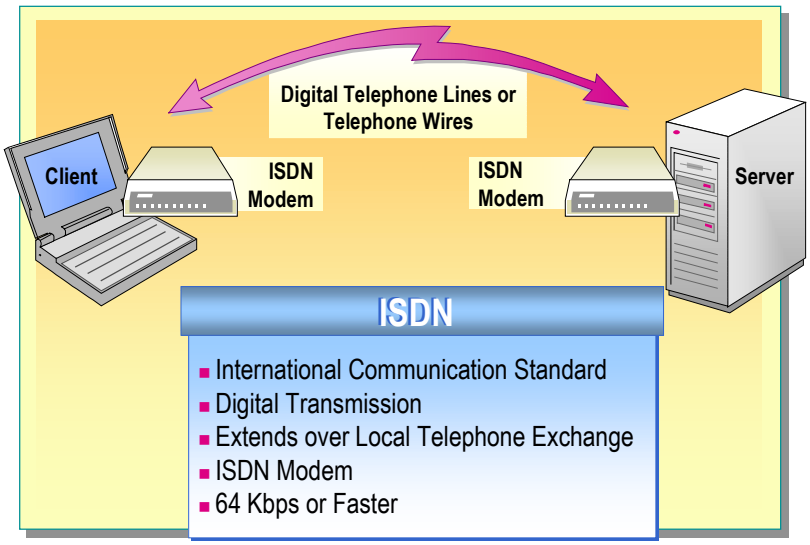
Analog Modem

Dial-up remote access equipment consists of an analog modem for the remote access client and another for the remote access server. An analog modem is a device that enables a computer to transmit information over a standard telephone line. Because a computer is digital and a telephone line is analog, analog modems are needed to convert digital to analog and vice versa. For large organizations, the remote access server is attached to a modem bank containing hundreds of modems. With analog modems at both the remote access server and the remote access client, the maximum bit rate supported by PSTN connections is 56,000 bits per second, or 56 kilobits per second.

Integrated Services Digital Network (ISDN)

Slide Objective
To illustrate how the ISDN connection is used in remote access.

Lead-in
ISDN communication is much faster than PSTN. ISDN supports communication speeds of up to 128 Kbps by using two B channels.



Key Point
ISDN is faster than most PSTN connections and is widely available in urban areas.

Integrated Services Digital Network (ISDN) is an international communications standard for sending voice, video, and data over digital telephone lines and standard telephone wires. ISDN has the ability to simultaneously deliver two connections over a single pair of telephone lines. The two connections may be in any combination of data, voice, video, or fax. The single line uses an ISDN subscriber service, which is called Basic Rate Interface (BRI). BRI has two channels, called B channels, at 64 Kbps each, which carry the data, and one data channel at 16 Kbps for control information. The two B channels can be combined to form a single 128 Kbps connection.

The other ISDN transmission rate service, Primary Rate Interface (PRI), has 23 B channels and one 64 Kbps D channel and uses more wire pairs. PRI is much more expensive to run than BRI and is not commonly selected by individual remote access users. In most cases, BRI is preferred when using ISDN for remote access.

Digital Transmission

ISDN is a digital transmission, as opposed to the analog transmission of PSTN. ISDN lines must be used at both the server and remote site. In addition, you must install an ISDN modem in both the server and the remote client.

Extends over Local Telephone Exchange

ISDN is not simply a point-to-point connection as a leased line. ISDN networks extend from the local telephone exchange to the remote user and include all of the telecommunications and switching equipment lying between them.

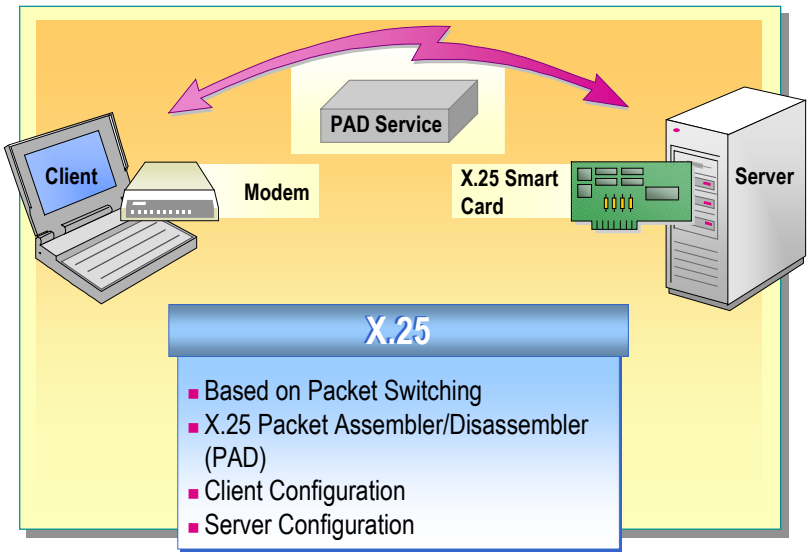
ISDN Modem

Dial-up remote access equipment consists of an ISDN modem each for the remote access client and the remote access server. ISDN offers much faster communication than PSTN, communicating at speeds of 64 Kbps or faster.

X.25

Slide Objective
To illustrate the X.25 connection that is used in remote access.

Lead-in
X.25 provides a secure and dedicated network service that allows client and server to communicate at different speeds.



Key Point
X.25 is a secure and dedicated network.

In an X.25 network, data is transmitted using packet switching. X.25 utilizes data communications equipment to create an elaborate, worldwide network of packet-forwarding nodes that deliver an X.25 packet to its designated address.

X.25 Packet Assembler/Disassembler (PAD)

Dial-up remote access clients can directly access an X.25 network by using an X.25 packet assembler/disassembler (PAD). A PAD allows the use of terminals and modem connections without necessitating expensive client hardware and connectivity to talk directly to X.25. Dial-up PADs are a practical choice for remote access clients because they do not require that you plug an X.25 line into the back of the computer. The only requirement for a dial-up PAD is the telephone number of the PAD service for the carrier.

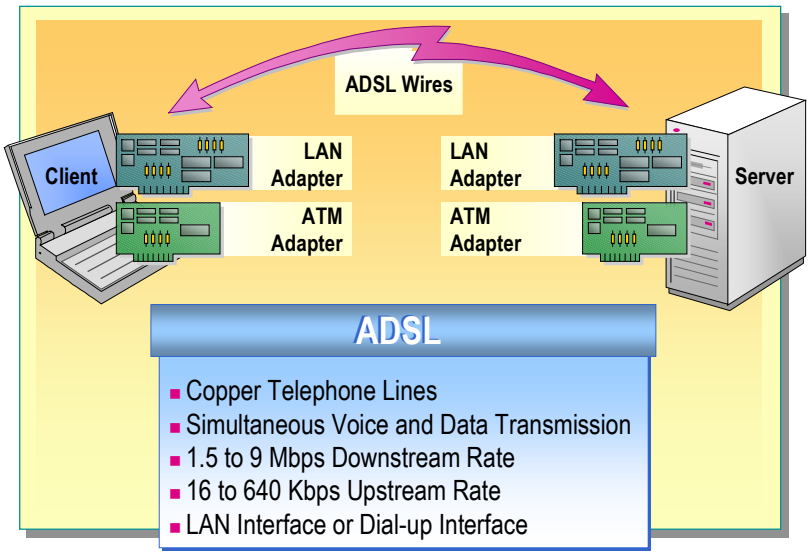
In Windows 2000, Routing and Remote Access provides access to the X.25 network in one of two configurations shown in the following table.

Dial-up configuration	Direct configuration
You can make a dial-up connection to the X.25 network by using asynchronous PADs. The PAD converts serially transmitted data into X.25 packets. When the PAD receives a packet from an X.25 network, it puts the packet out on a serial line, making communication possible between the client and the X.25 network.	You can make a direct connection to the X.25 network through an X.25 smart card. An X.25 smart card is a hardware card with a PAD embedded in it. The smart card acts like a modem. To the personal computer, a smart card looks like several communication ports attached to PADs.

Asymmetric Digital Subscriber Line (ADSL)

Slide Objective
To illustrate the ADSL connection that is used in remote access.

Lead-in
ADSL is a new, high-speed technology that usually has a much higher rate of data transmission downstream than upstream.



Key Points
Asymmetric digital subscriber line (ADSL) is a technology that allows more data to be sent over existing copper telephone lines.

When receiving data, ADSL supports data rates from 1.5 to 9 Mbps. When sending data, ADSL supports data rates from 16 to 640 Kbps.

When an ADSL adapter appears as a LAN interface, the ADSL connection operates in the same way as a LAN connection to the Internet.

Asymmetric digital subscriber line (ADSL) is a technology that allows more data to be sent over existing copper telephone lines. ADSL accomplishes this by using the portion of a telephone line's bandwidth not utilized by voice, thereby allowing for simultaneous voice and data transmission.

Typical remote access users receive much more information than they send. The asymmetric nature of the ADSL connection fits well with most Internet and remote business use. When receiving data, ADSL supports data rates from 1.5 to 9 Mbps. When sending data, ADSL supports data rates from 16 to 640 Kbps. Although ADSL provides higher data transmission rates than do PSTN and ISDN connections, the client computer can receive data at a faster rate than it can send data.

LAN Interface or Dial-up Interface

ADSL equipment can appear to Windows 2000 as either a LAN interface or a dial-up interface. When an ADSL adapter appears as a LAN interface, the ADSL connection operates in the same way as a LAN connection to the Internet. When an ADSL adapter appears as dial-up interface, ADSL provides a physical connection and the individual packets are sent using asynchronous transfer mode (ATM). An ATM adapter with an ADSL port is installed in both the remote access client and remote access server.

Lab A: Examining the Network Architecture

Slide Objective
To introduce the lab.

Lead-in
In this lab, you will examine the components that make up a network infrastructure.

Objectives

After completing this lab, you will be able to:

- Describe the principles and components of network architecture.
- Describe the scope of Local Area Networks (LANs) and Wide Area Network (WANs).
- Describe the basic connectivity components, such as the different types of cabling and the network adapters.
- Describe network topologies: bus, star, ring, mesh, and hybrid (a combination of two or more topologies in a single network design).
- Describe the different network technologies: Ethernet, token ring, FDDI, ATM, and frame relay.

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 **Examining the Network Architecture**.
5. Read the introduction information, and then click the link to begin the simulation.

Estimated time to complete this lab: 30 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.

- Scope of Networks
- Basic Connectivity Components
- Network Topologies
- Network Technologies
- Expanding the Network

1. The organization you work for has just merged with another company, which has offices in five countries in Europe and Asia. Your job is to expand the network so that all offices of the newly merged organization are connected. What will the resulting network be called, and which network components could you use to connect the offices?

   Wide Area Network (WAN). You can use packet-switching networks, ISDN, microwave transmitters or satellite links to connect the remote offices.

2. You are sending a file from your computer to another computer on your network. Which functions does the network adapter perform to send this file across the network?

   The network adapter receives the data from the operating system, converts the data into electrical signals, and transmits it onto the network.

3. You are troubleshooting a network that is experiencing intermittent connectivity problems. You trace the cables back to a location in the center of your office, where all of the cables are connected to a central wiring closet. What is the term used to describe the physical topology of this network?

   Star topology.

4. Your organization uses an Ethernet network at its headquarters. What happens to this network as more and more computers are added to it if bridges, switches, or routers are not added as well?

   As more computers are added, more collisions occur, and less data can be transmitted on the network.

5. Your network has expanded from several computers to several hundred computers, and users are now complaining that the network is slow. You do not have the budget to upgrade the cabling or to change the type of network, so you choose to divide the network into segments to increase the data throughput on each segment. You want to do this without making any changes to the computers on the network. Which network component(s) can you use?

   A bridge or a switch. A router could be used, but it would require that you change the network configuration of the computers on your network.

6. Your users need access to the company's intranet from their homes. Which methods are available to provide this access?

   Dial-up remote access.

   Virtual private network.

7. You want to provide fast Internet access to the users in your intranet so that the rate of receiving data is much higher than the rate of sending data. Which method will enable you to provide this access?

   ADSL.