# INTRODUCTION
# Module 1- Chapt 1

**Mrs. Madhu Nagaraj**
**Assistant Professor**
**Dept of CSE-Data Science**
**ATMECE**

## Contents

- Data Communications
  - Networks
  - Network Types
- Networks Models
  - Protocol Layering
  - TCP/IP Protocol suite
  - The OSI model
- Introduction to Physical Layer: Transmission media
  - Guided Media
  - Unguided Media: Wireless.
  - Switching: Packet Switching and its types.

# Data Communications

- The word **data** refers to information presented in whatever form is agreed upon by the parties creating and using the data.
- **Data communications** are the exchange of data between two devices via some form of transmission medium such as a wire cable.

## Characteristics of data communication system

- **Delivery** : The system must deliver data to the correct destination .
- **Accuracy** :The system must deliver the data accurately.
- **Timeliness**: The system must deliver data in a timely manner. Data delivered late are useless.
- **Jitter**: Jitter refers to variation in the packet arrival time. For example, Video packets are sent every 30 ms . If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

## Components of a data communication system

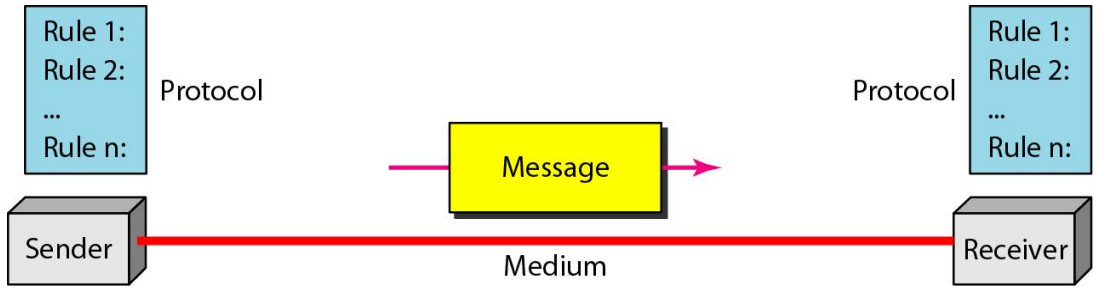



Fig: Five components of data communication

- **Message :** The message is the information (data) to be communicated .
- **Sender:** The sender is the device that sends the data message.
- **Receiver :**The receiver is the device that receives the message.
- **Transmission medium :**The transmission medium is the physical path by which a message travels from sender to receiver.
- **Protocol :** A protocol is a set of rules that govern data communications

## Data Representation

- Text
  - Represented as bit pattern (sequence of bits 0s or 1s)
  - Different set of bit pattern used to represent symbols or characters.
  - Each set is called code
  - Process of representing symbols is called encoding
  - Ex: ASCII,UNICODE
- Numbers
  - Represented as bit pattern
  - Directly converted to binary form
- Audio
  - Recording or broadcasting of sound or music.
  - Continuous not discrete

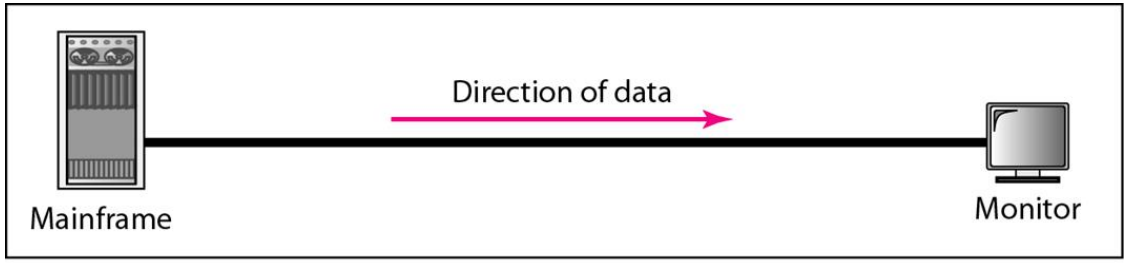
- Video
  - Recording or broadcasting of picture or a movie
  - Produced as :
    - Continuous entity [TV camera]
    - Combination of images-discrete entity
- Images
  - Represented as bit pattern
  - Image is divided into matrix of pixels(smallest element of an image)
  - Each pixel is assigned a bit pattern (size and value of pattern depend on image)
  - Ex: black and white dots (chessboard) -1 bit pattern is enough to represent a pixel, gray scale- 2 bit pattern.
  - Several methods to represent colour images : RGB,YCM

## Data Flow

- Communication between two devices can be
  1. Simplex
  2. Half-duplex
  3. Full-duplex

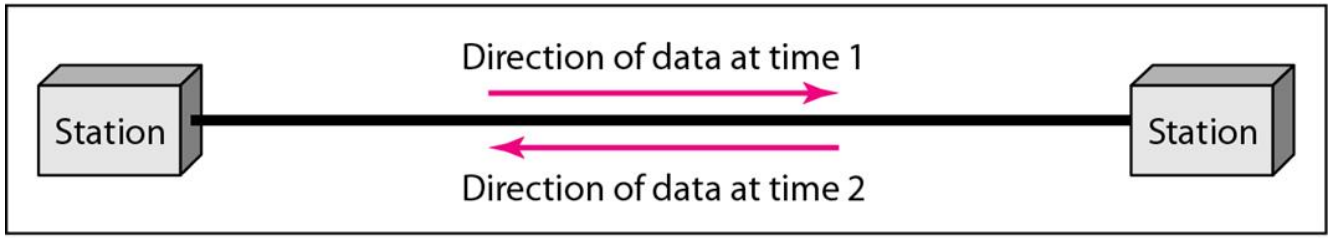
**1. Simplex**

- Communication is unidirectional
- Only one of the two devices on a link can transmit; the other can only receive.
- E.g. : One way street, Keyboard , Monitor.



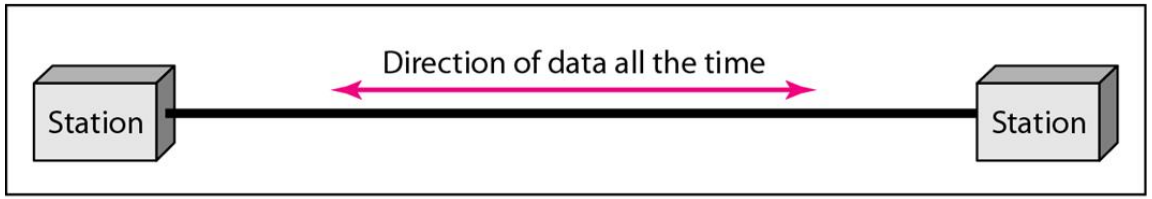
## 2. Half duplex

- Each station can both transmit and receive, but not at the same time.
- When one device is sending, the other can only receive, and vice versa.
- E.g.: Walkie Talkie.




## 3. Full duplex

- Both stations can transmit and receive simultaneously.
- It is like a two way street with the traffic flowing in both the directions at the same time.
- E.g .: Telephone network



## Networks

- A network is a set of devices (often referred to as nodes) connected by communication links.
- A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- A link can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.

## Network Criteria

### 1. Performance

- Measured in terms of:
  - Transit time: time taken to travel a message from one device to another.
  - Response time: time elapsed between enquiry and response.
- Depends on following factors:
  - Number of users
  - Type of transmission medium
  - Efficiency of software
- Evaluated by 2 networking metrics:
  - Throughput (high): how fast we can send the data through network?
  - Delay (small) : how long does it take for an entire message to completely arrive at the destination

**2. Reliability**

- Measured by
  - Frequency of failure.
  - Time taken to recover from a network failure.
  - Network robustness in a disaster.

3. **Security**

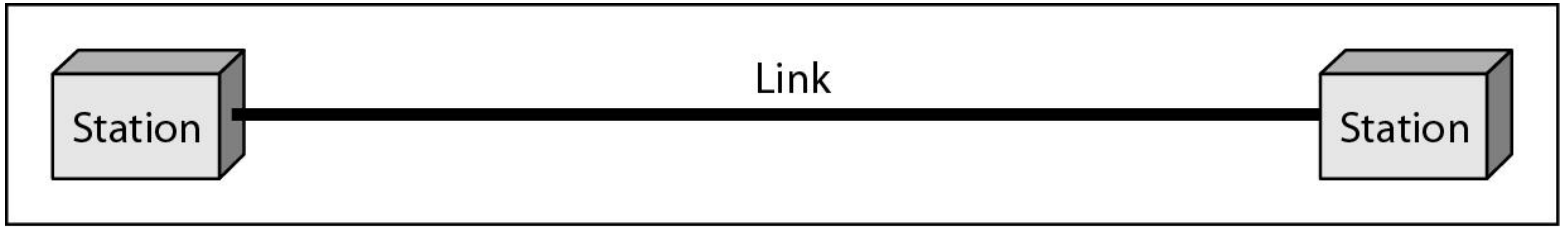
- Protecting data from unauthorized access, damage and development.
- Implementing policies and procedures for recovery from breaches and data losses.

# Physical Structures

## Type of Connection

### 1. Point to Point :

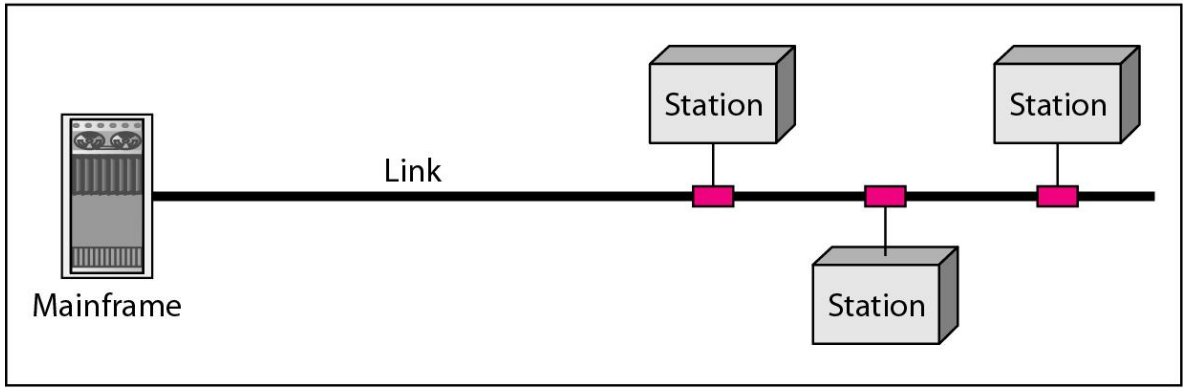
- It provides a dedicated link between two devices .
- The entire capacity of the link is reserved for transmission between those two devices.
- It uses an actual length of wire or cable to connect the two ends.




- When we change TV channels by infrared remote control, we are establishing a point-to-point connection between remote control and TV's control system

## 2. Multipoint

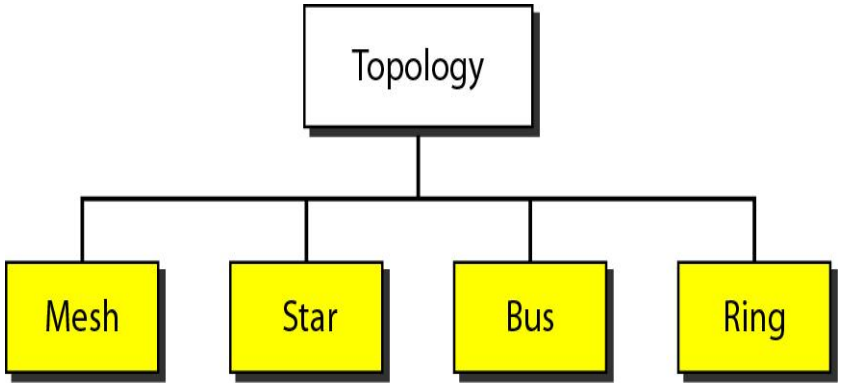
- It is the one in which more than two specific devices share a single link.




- Capacity of the channel is either spatially or temporally shared.
  - Spatially shared : Several devices can use the link simultaneously.
  - Temporally shared : Users take turns.

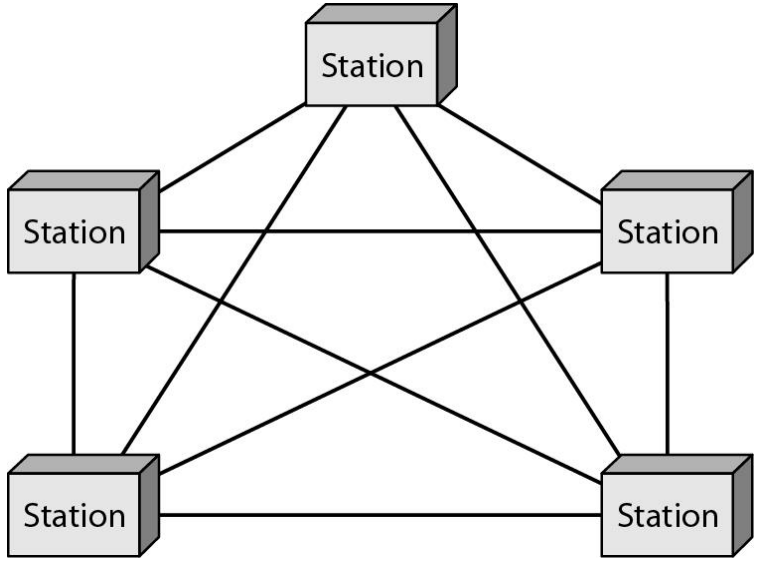
## Physical Topology

- Topology of network is the geometric representation of all links and linking devices to one another
- Basic topologies:
  1. Mesh
  2. Star
  3. Bus and
  4. Ring



## 1. Mesh Topology

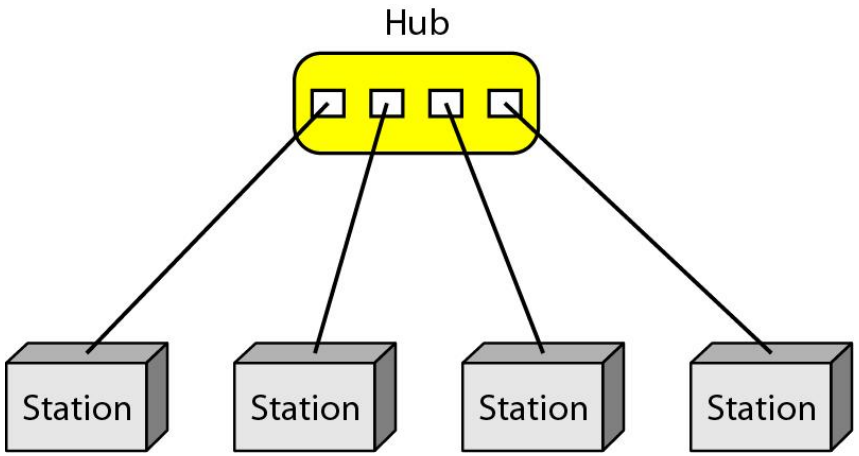
- Point to Point connection
- Every device has a dedicated point-to point link to every device.
- The term dedicated means that the link carries traffic only between the two devices it connects.
- For **n** nodes
  - n(n-1) physical links
  - n(n-1)/2 duplex mode links
- Every device have (n-1) I/O ports to be connected to other (n-1) devices.



- **Advantages:**
  - A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
  - Point-to-point links make fault identificationand fault isolation easy.
  - Privacy or security : When every message travels along a dedicated line, only the intended recipient sees it.
- **Disadvantages:**
  - Difficult installation and reconfiguration.
  - Bulk of wiring occupies more space than available space.
  - Hardware required to connect each link is expensive.
- **Practical example:** connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

## 2. Star Topology

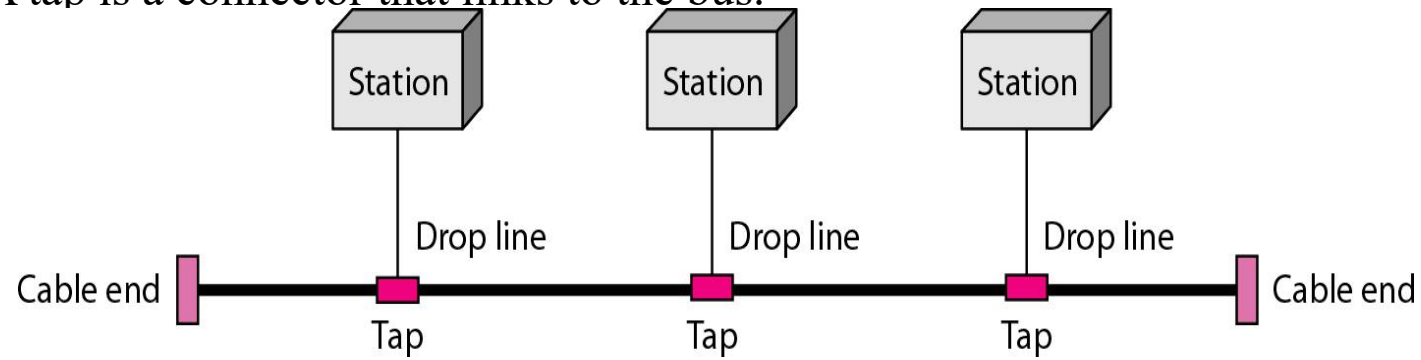
- Point to Point connection
- All the devices are connected to a central controller called a hub
- Dedicated point-to-point link between a device & a hub.
- The devices are not directly linked to one another. Thus, there is no direct traffic between devices.
- The hub acts as a junction:
  - If device-1 wants to send data to device-2,
  - the device-1 sends the data to the hub, then the hub relays the data to the device-2.



- **Advantages:**
  - A star topology is less expensive than a mesh topology. Each device needs only one link and one I/O port to connect it to any number of others.
  - Easy to install and reconfigure.
  - Requires less cabling, less expensive than mesh topology.
  - Robustness: If one link fails, only that link is affected. All other links remain active. As a result fault identification and fault isolation becomes easy.
- **Disadvantages :**
  - Dependency of whole topology on one single point, the hub.
- **Example** : Local area network

### 3. Bus Topology

- Multipoint connection
- All the devices are connected to the single cable called bus (backbone)
- Devices are connected to the bus by drop-lines and taps.
- A drop-line is a connection running between the device and the bus (main cable).
- A tap is a connector that links to the bus.

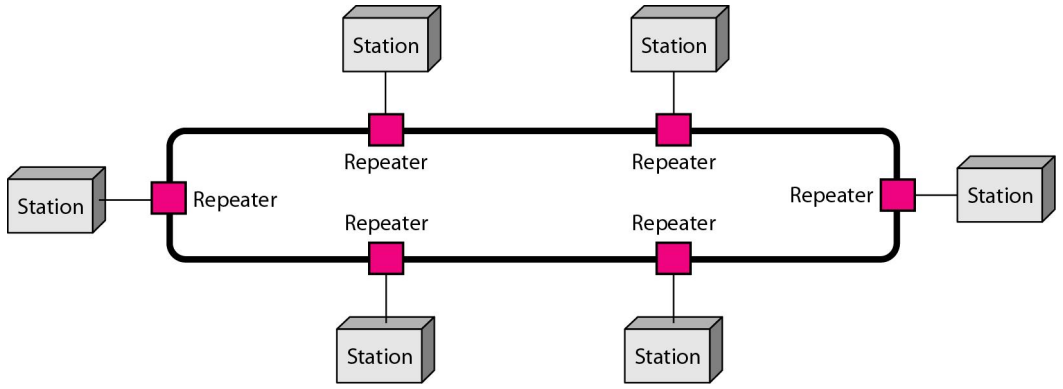


- As a signal travels along the backbone, some of its energy is transformed into heat.
- As a result there is a limit on the number of taps a bus can support and on the distance between those taps.
- **Advantages:**
  - Ease of installation : Backbone cable can be laid along the most path, then connected to the nodes and drop lines.
  - Cable required is the least compared to mesh/star topologies.
  - Redundancy is eliminated : Only the backbone cable stretches through the entire facility.

- **Disadvantages:**
  - Signal reflection at the taps can cause degradation in quality
  - A fault/break in the cable stops all transmission.
  - There is a limit on
    - Cable length
    - Number of nodes that can be connected.
  - Security is very low because all the devices receive the data sent from the source.
- **Example**
  - It is used to implement the basic Ethernet network.

## 4. Ring Topology

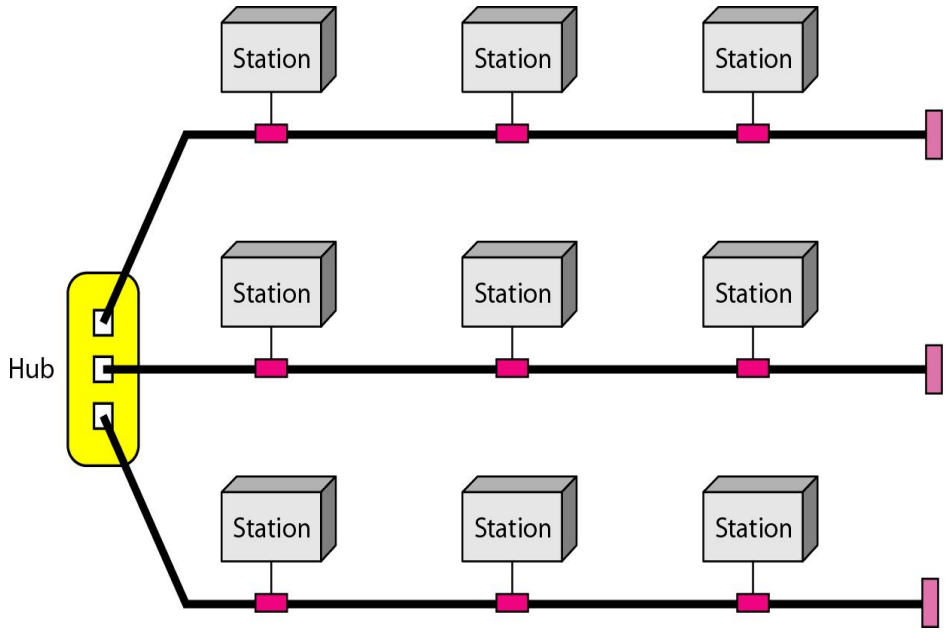
- Each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater.
- When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along



- **Advantages**
  - Easy installation and reconfiguration. To add/delete a device, requires changing only 2 connections
  - Fault isolation is simplified. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network-operator to the problem and its location
  - Congestion reduced: Because all the traffic flows in only one direction.
- **Disadvantages**
  - Unidirectional traffic
  - A fault in the ring/device stops all transmission.
    - The above 2 drawbacks can be overcome by using dual ring.
  - There is a limit on
    - Cable length
    - Number of nodes that can be connected.
  - Slower: Each data must pass through all the devices between source and destination.
- **Example:** Used in industrial control systems, metropolitan area networks, and office networks

## Hybrid Topology

- Example: having a main star topology with each branch connecting several stations in a bus topology



## Categories of Networks

- Network Category depends on its size

1. Local Area Networks (LANs)
2. Wide Area Networks (WANs)
3. Metropolitan Area Networks (MANs)

## 1. Local Area Networks (LANs)

- It is privately owned and links the devices in a single office, building, or campus.
- LAN can be as simple as two PCs and a printer in someone's home office. Its size is limited to a few kilometers.
- LANs are designed to allow resources to be shared between personal computers or workstations.
- The resources to be shared can include hardware (e.g., a printer),software (e.g., an application program).

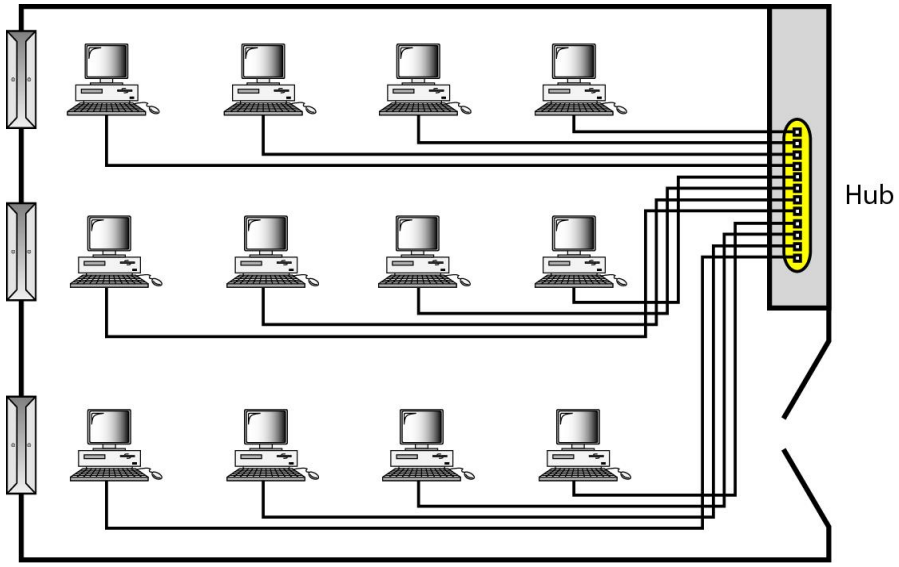


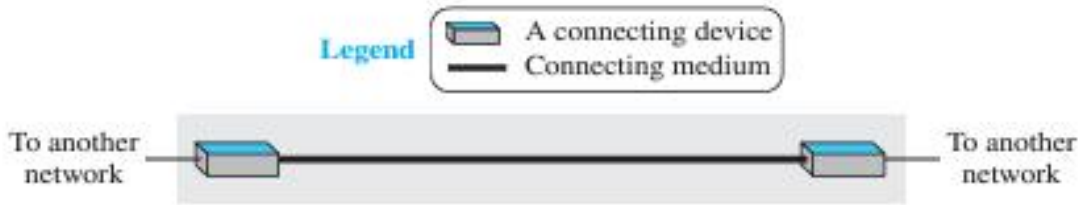

Fig: An isolated LAN connecting 12 computers to a hub in a closet

- **Advantages**:
- Resource Sharing: Computer resources like printers and hard disks can be shared by all devices on the network.
- Expansion: Nowadays, LANs are connected to WANs to create communication at a wider level.

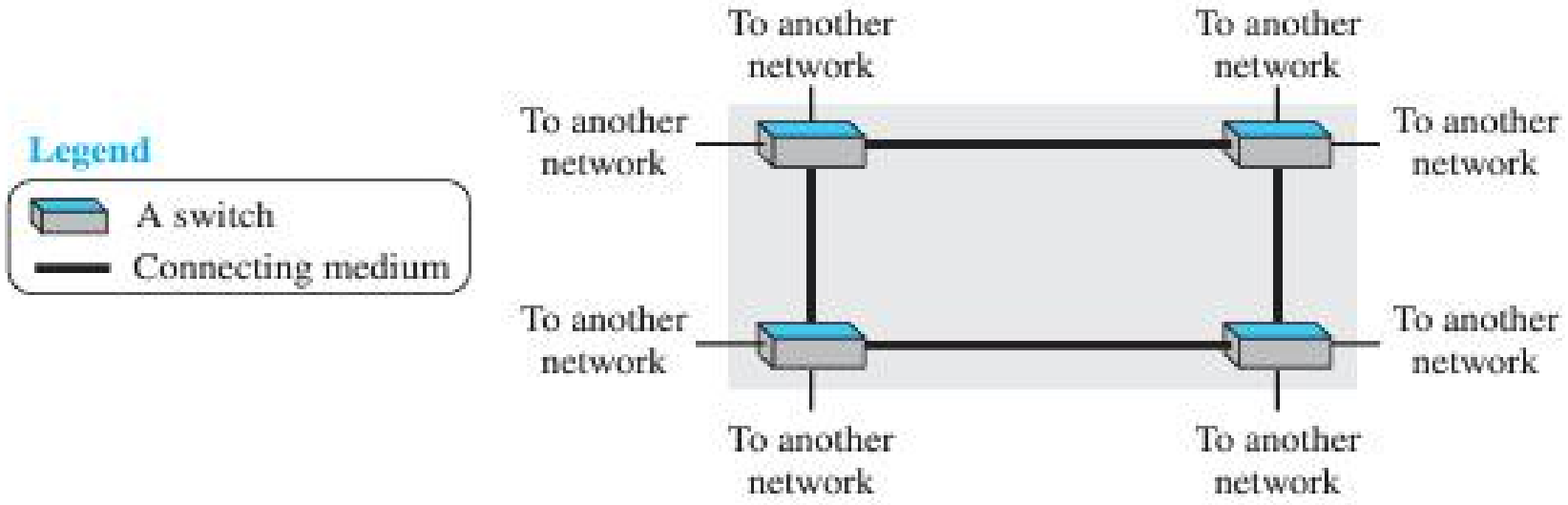
- **Disadvantages**
  - **Limited distance**: Local area networks are used only in buildings or apartment complexes it cannot be occupied in bigger areas.
  - **Installing LAN is expensive**: It is expensive to establish a LAN. Here specialized software is essential to install a server. Communication hardware such as hubs, switches, routers, and cables are expensive to buy.
  - **Limited scalability**: LANs are limited in terms of the number of devices that can be connected to them. As the number of devices increases, the network can become slow and congested.
  - **Single point of failure**: LANs typically have a single point of failure, such as a central server. If this server fails, the entire network can go down.
  - **Maintenance and management**: LANs require regular maintenance and management to ensure optimal performance. This can be time-consuming and costly.

## 2. Wide Area Networks (WAN)

- It provides long-distance transmission of data, image, audio, and video information over large geographic areas that comprise a country, a continent or even the whole world.
- Two types of WAN:
  - Point to Point WAN : A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air).

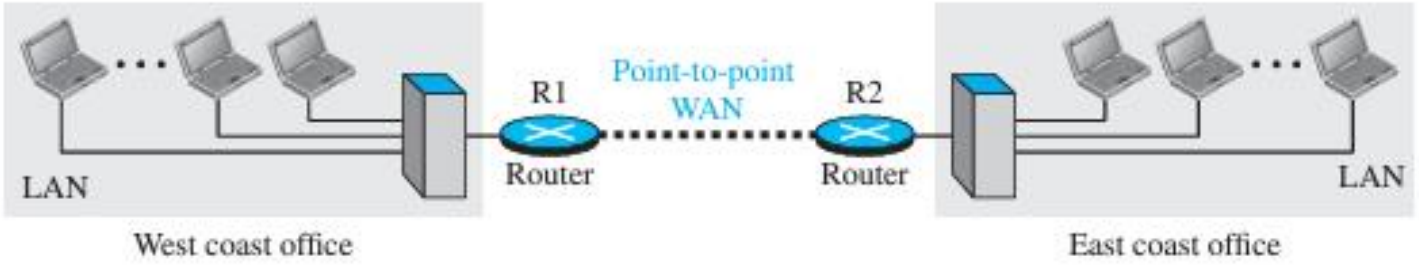


- The switched WAN : A switched WAN is a network with more than two ends. switched WAN is a combination of several point-to-point WANs that are connected by switches.



**Internetwork**

- A network of networks is called an **internet**. ( inter-network)
- As an example, assume that an organization has two offices, one on the east coast and the other on the west coast.
- Each office has a LAN that allows all employees in the office to communicate with each other.
- To make the communication between employees at different offices possible, the management leases a point-to-point dedicated WAN from a service provider, such as a telephone company, and connects the two LANs.
- Now the company has an internetwork, or a private internet. Communication between offices is now possible.




- When a host in the west coast office sends a message to another host in the same office, the router blocks the message, but the switch directs the message to the destination.
- On the other hand, when a host on the west coast sends a message to a host on the east coast, router R1 routes the packet to router R2, and the packet reaches the destination.

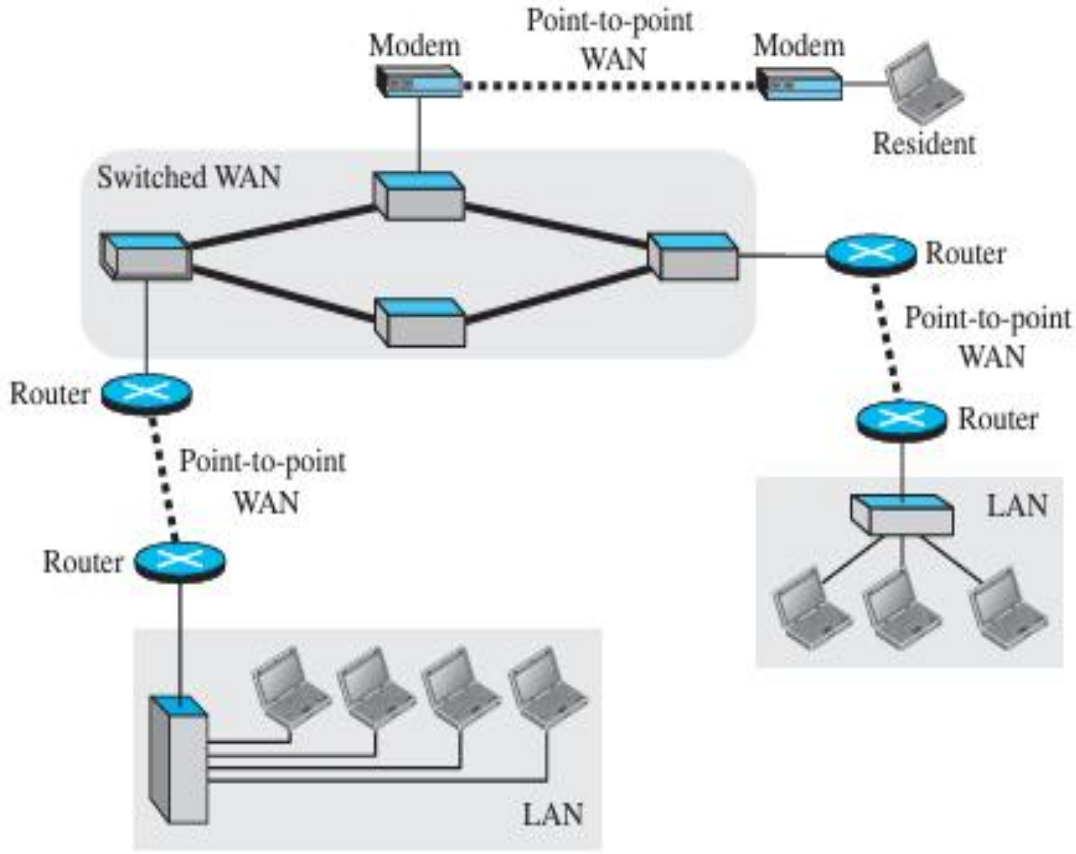
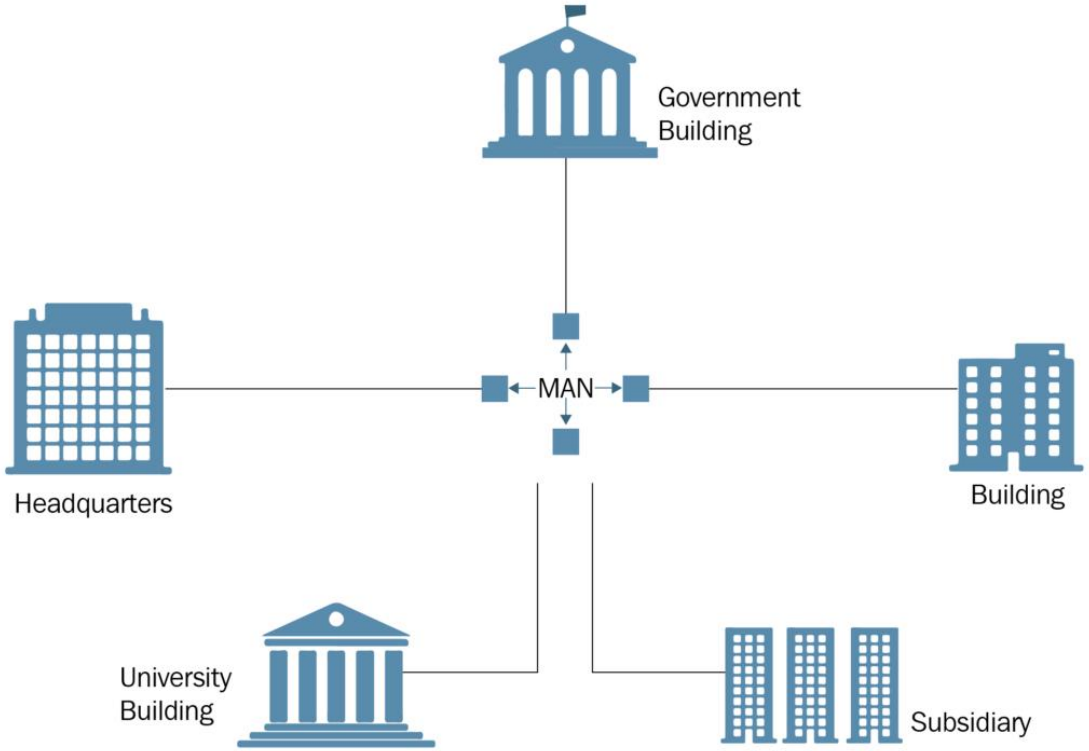



Fig: A heterogeneous network made of four WANs and three LANs

### 3. Metropolitan Area Networks (MAN)

- A metropolitan area network (MAN) is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings.
- A MAN is larger than a local area network (LAN) but smaller than a wide area network (WAN). It is commonly used in large companies or school campuses with multiple buildings.
- It serves as a high-speed network to permit the sharing of regional resources.
- The most common examples of MAN are cable TV networks and telephone company networks.

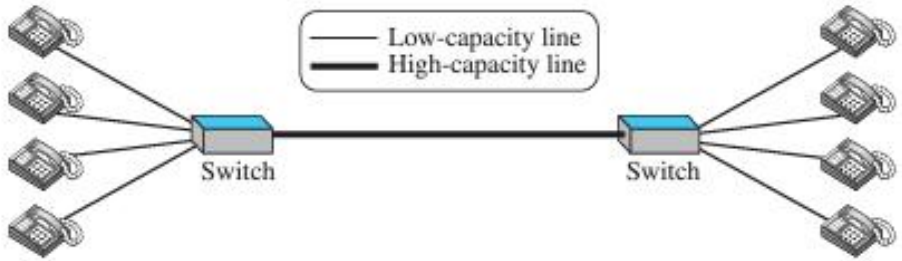

Government
Building
MAN
Headquarters
Building
University
Building
Subsidiary

## Switching

- An internet is a switched network in which a switch connects at least two links together.
- A switch needs to forward data from a network to another network when required.
- The two most common types of switched networks are
    1. circuit-switched
    2. packet-switched networks.

### 1. Circuit-Switched Network

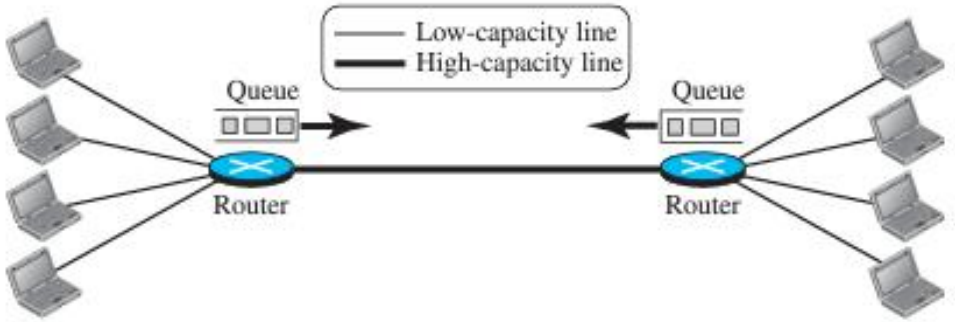
- In a circuit-switched network, a dedicated connection, called a circuit, is always available between the two end systems; the switch can only make it active or inactive.



- In Figure, the four telephones at each side are connected to a switch. The switch connects a telephone set at one side to a telephone set at the other side.
- The thick line connecting two switches is a high-capacity communication line that can handle four voice communications at the same time; the capacity can be shared between all pairs of telephone sets.

**2. Packet-Switched Network**

- In a computer network, the communication between the two ends is done in blocks of data called packets.



- A router in a packet-switched network has a queue that can store and forward the packet.
- Now assume that the capacity of the thick line is only twice the capacity of the data line connecting the computers to the routers.
- If only two computers (one at each site) need to communicate with each other, there is no waiting for the packets.
- However, if packets arrive at one router when the thick line is already working at its full capacity, the packets should be stored and forwarded in the order they arrived.

## The Internet

- Internet is composed of thousands of interconnected networks.

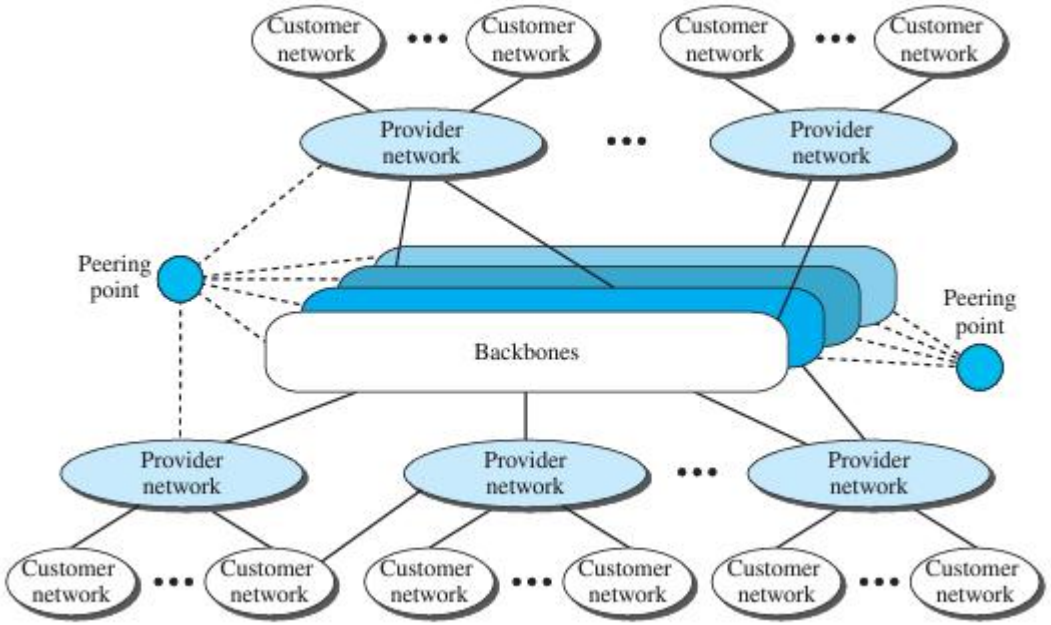



Fig: The Internet today

- At the top level, the backbones are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T, and NTT. The backbone networks are connected through some complex switching systems, called peering points.
- At the second level, there are smaller networks, called provider networks, that use the services of the backbones for a fee.
- The provider networks are connected to backbones and sometimes to other provider networks. The customer networks are networks at the edge of the Internet that actually use the services provided by the Internet.
- They pay fees to provider networks for receiving services. Backbones and provider networks are also called Internet Service Providers (ISPs).
- The backbones are often referred to as international ISPs; the provider networks are often referred to as national or regional ISPs.

## Accessing the Internet

### 1. Using Telephone Networks

- Dial up Service : To the telephone line add a modem that converts data to voice. But it is very slow when line used for internet connection.
- DSL Service : Telephone companies have upgraded their telephone lines to provide higher speed internet services .

### 2. Using Cable Networks

- The cable companies have been upgrading their cable networks to provide internet connection. But speed varies depending on the number of neighbors that use the same cable.

### 3. Using Wireless Networks

- A household or small business can be connected to the internet through a wireless LAN.

### 4. Direct Connection to the internet

- A large organization can become a local ISP and be connected to internet.

# Network Models

## Protocol Layering

- A protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively.
- When communication is
  - Simple -only one simple protocol.
  - complex, we need to divide the task b/w different layers. We need a protocol at each layer, or protocol layering.
- Elements of a Protocol
- Syntax
  - Structure or format of the data
  - Indicates how to read the bits - field delineation
- Semantics
  - Interprets the meaning of the bits
  - Knows which fields define what action
- Timing
  - When data should be sent
  - Speed at which data should be sent or speed at which it is being received.

# Scenarios

## First Scenario

- Communication is so simple that it can occur in only one layer.
- Assume Maria and Ann are neighbors with a lot of common ideas.
- Communication between Maria and Ann takes place in one layer, face to face, in the same language


Fig: single layer protocol

➢ Even in this simple scenario, we can see that a set of rules needs to be followed.

1. Maria and Ann know that they should greet each other when they meet.
2. They know that they should confine their vocabulary to the level of their friendship.
3. Each party knows that she should refrain from speaking when the other party is speaking.

## Second Scenario

- Assume that Ann is offered a higher-level position in her company, but needs to move to another branch located in a city very far from Maria.
- The two friends still want to continue their communication and exchange ideas because they have come up with an innovative project to start a new business when they both retire.
- They decide to continue their conversation using regular mail through the post office.
- They do not want their ideas to be revealed by other people if the letters are intercepted. They agree on an encryption/decryption technique
- Now we can say that the communication between Maria and Ann takes place in three layers

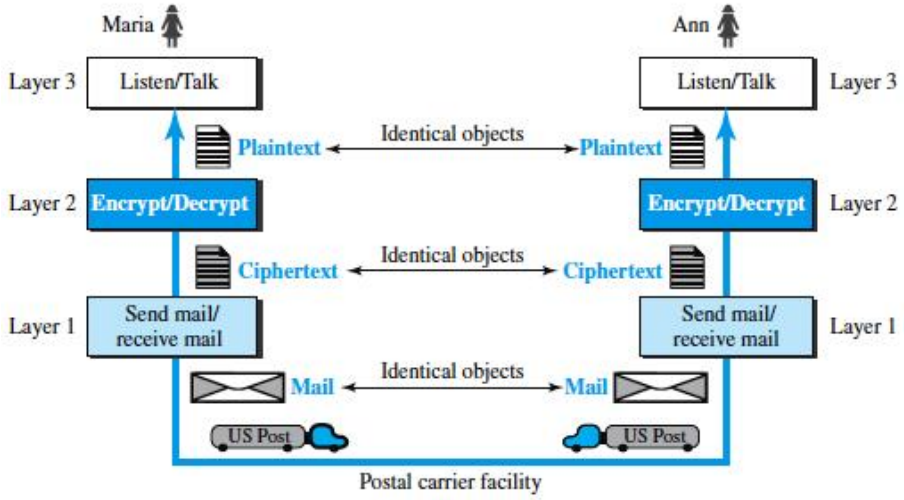



Fig: A three-layer protocol

- Let us assume that Maria sends the first letter to Ann.

**At Maria side:**

- Maria talks to the machine at the third layer as though the machine is Ann and is listening to her.

The third layer machine listens to what Maria says and creates the plaintext which is passed to the second layer machine.

- The second layer machine takes the plaintext, encrypts it, and creates the ciphertext, which is passed to the first layer machine.
- The first layer machine, presumably a robot, takes the ciphertext , puts it in an envelope, adds the sender and receiver addresses, and mails it.

**At Ann's side**

- The first layer machine picks up the letter from Ann's mail box, recognizing the letter from Maria by the sender address.
- The machine takes out the ciphertext from the envelope and delivers it to the second layer machine.
- The second layer machine decrypts the message, creates the plaintext and passes the plaintext to the third-layer machine.
- The third layer machine takes the plaintext and reads it as though Maria is speaking.

- Protocol layering enables us to divide a complex task into several smaller and simpler tasks.
- For example, in Figure 2.2, we could have used only one machine to do the job of all three machines. However, if Maria and Ann decide that the encryption/ decryption done by the machine is not enough to protect their secrecy, they would have to change the whole machine.
- In the present situation, they need to change only the second layer machine; the other two can remain the same. This is referred to as ***modularity***.
- Modularity in this case means independent layers.
- A layer (module) can be defined as a black box with inputs and outputs, without concern about how inputs are changed to outputs

**Advantages of protocol layering**

- Allows to separate the services from the implementation.
  - A layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer; we don't care about how the layer is implemented.
  - For example, Maria may decide not to buy the machine (robot) for the first layer; she can do the job herself. As long as Maria can do the tasks provided by the first layer, in both directions, the communication system works.
- Reduces the complexity at the intermediate system
  - Communication does not always use only two end systems; there are intermediate systems that need only some layers, but not all layers.
  - If we did not use protocol layering, we would have to make each intermediate system as complex as the end systems, which makes the expensive.

## Principles of Protocol Layering

### First Principle

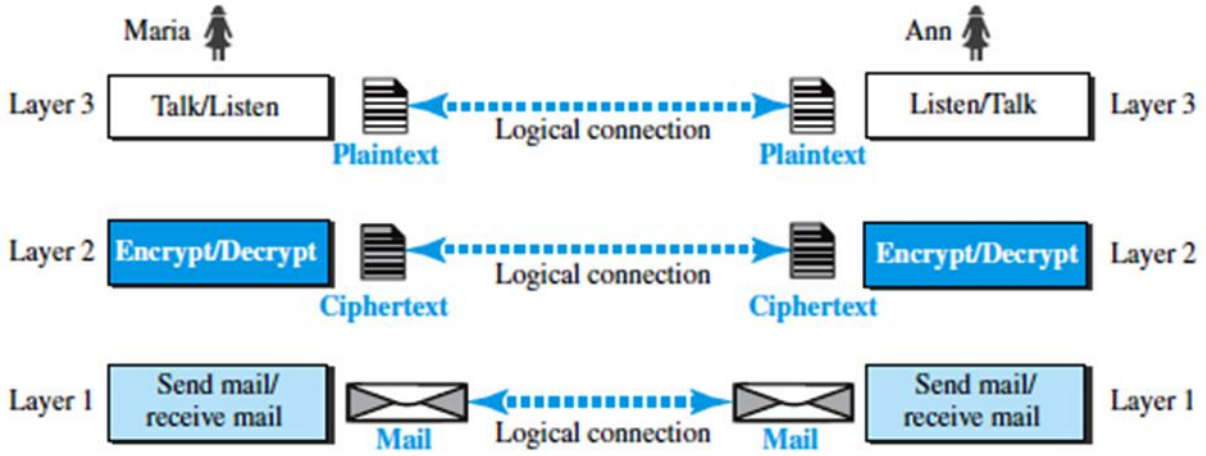
- The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction.
- For example, the third layer task is to listen (in one direction) and talk (in the other direction). The second layer needs to be able to encrypt and decrypt. The first layer needs to send and receive mail.

### Second Principle

- we need to follow in protocol layering is that the two objects under each layer at both sites should be identical.
- For example, the object under layer 3 at both sites should be a plaintext letter. The object under layer 2 at both sites should be a cipher text letter. The object under layer 1 at both sites should be a piece of mail.

## Logical Connections

- Two protocols at the same layer can have a logical Connection
- This means that we hav




- Maria and Ann can think that there is a logical (imaginary) connection at each layer through which they can send the object created from that layer.

- TCP/IP is a protocol-suite used in the Internet today.
- Protocol-suite refers a set of protocols organized in different layers.
- It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality.
- The term hierarchical means that each upper level protocol is supported by the services provided by one or more lower level protocols.
- TCP/IP is thought of as a five-layer model.

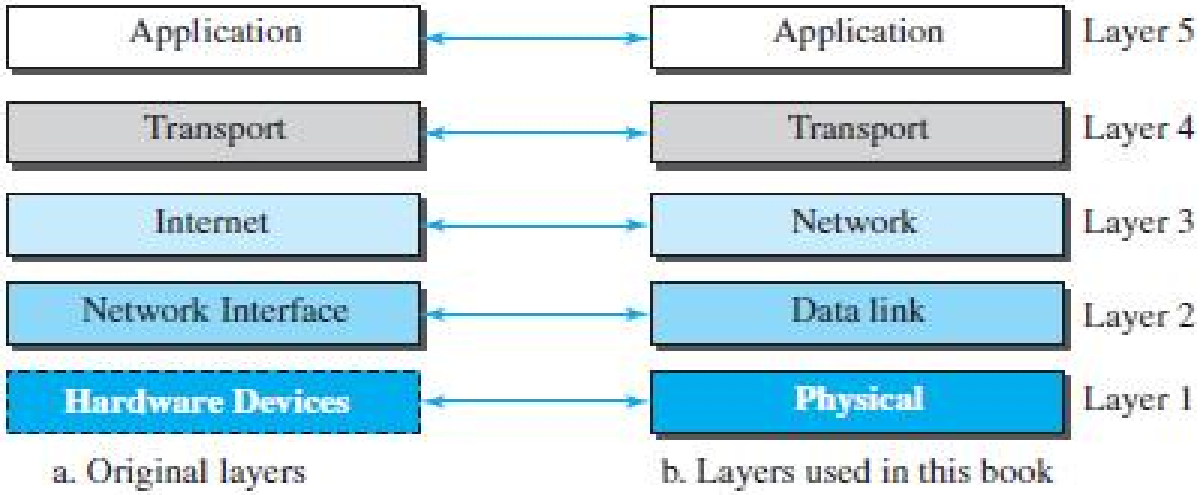



Fig: Layers in TCP/IP protocol suite

## Layered Architecture

- To show how the layers in the TCP/IP protocol suite are involved in communication between two hosts, we assume that we want to use the suite in a small internet made up of three LANs (links), each with a link- layer switch.
- We also assume that the links are connected by one router

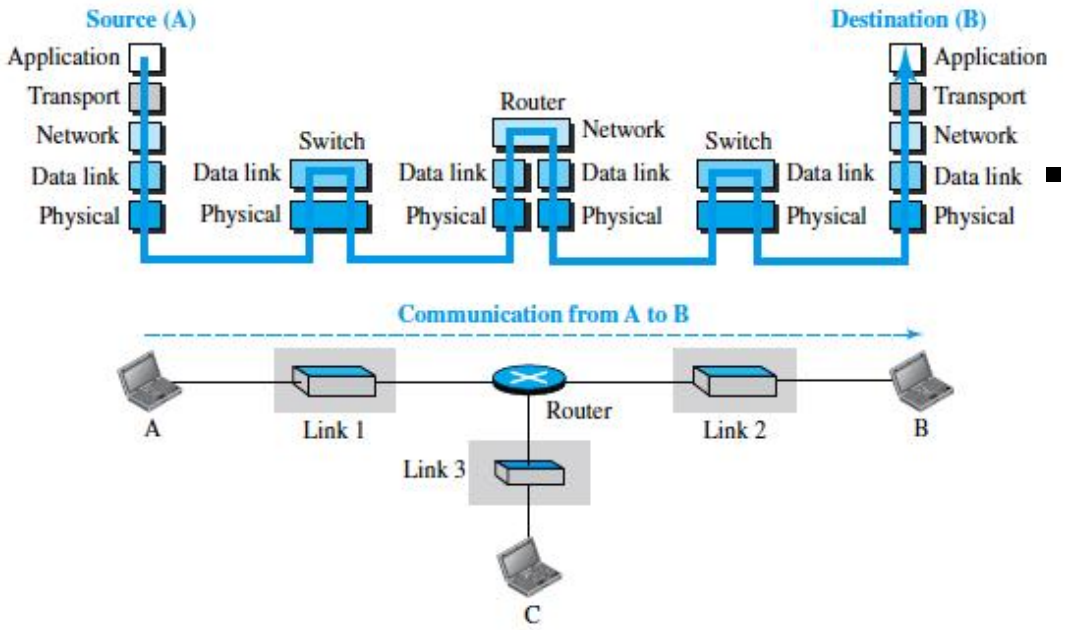



Fig: Communication through an internet

- Let us assume that computer A communicates with computer B.
- As the figure shows, we have five communicating devices in this communication:
  1. source host(computer A)
  2. The link-layer switch in link 1
  3. The router
  4. The link-layer switch in link 2
  5. destination host (computer B).

- Each device is involved with a set of layers depending on the role of thedevice in the internet.
- The two hosts are involved in all five layers
- The source host needs to create a message in the application layer and send it down the layers so that it is physically sent to the destination host.
- The destination host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer.
- The router is involved in only three layers; link-layer switch in a link is involved only in two layers, data-link and physical.

## Layers in the TCP/IP Protocol Suite

- To better understand the duties of each layer, we need to think about the logical connections between layers.

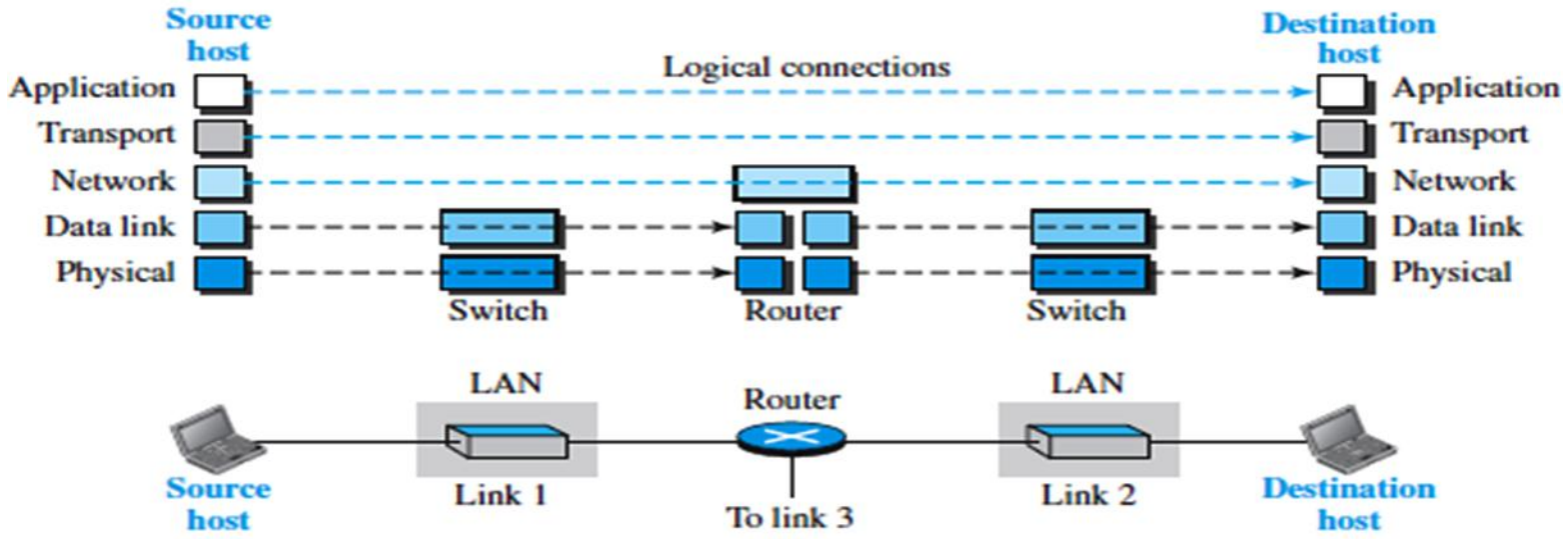



Fig: Logical connections between layers of the TCP/IP protocol suite

- The duty of the application, transport, and network layers is end-to- end.
- The duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router.
- The domain of duty of the top three layers is the internet, and the domain of duty of the two lower layers is the link.
- In the top three layers, the data unit (packets) should not be changed by any router or link-layer switch.
- In the bottom two layers, the packet created by the host is changed only by the routers, not by the link-layer switches.

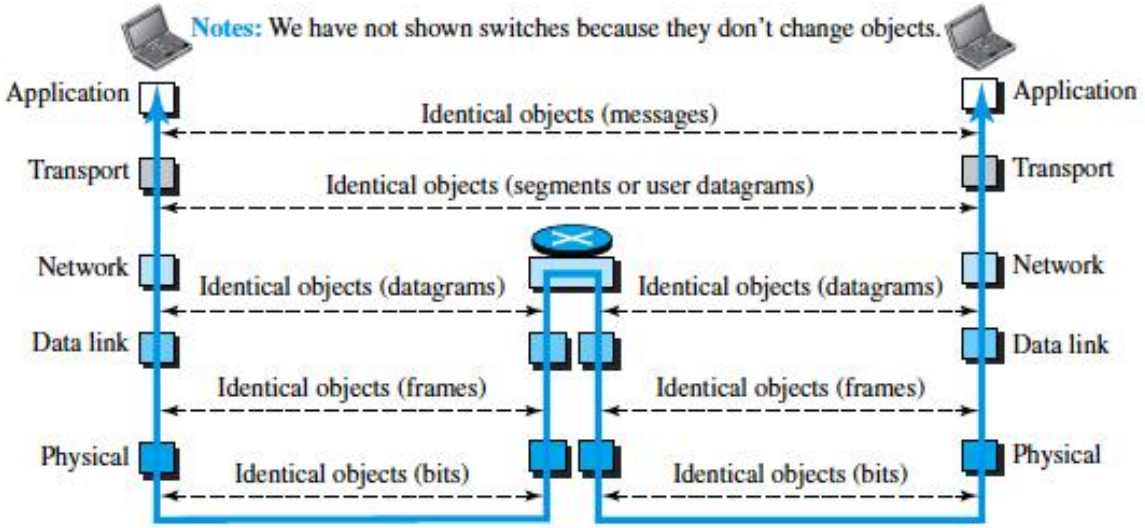



Fig: Identical objects in the TCP/IP protocol suite

- Figure shows the second principle the identical objects at each layer related to each device.
- Although the logical connection at the network layer is between the two hosts, we can only say that identical objects exist between two hops in this case because a router may fragment the packet at the network layer and send more packets than Received.
- The link between two hops does not change the object.

## Description of each Layer

### Physical Layer

- The lowest level in the TCP/IP protocol suite, responsible for carrying individual bits in a frame across the link
- Two devices are connected by a transmission medium (cable or air).
- The transmission medium does not carry bits; it carries electrical or optical signals. So the bits received in a frame from the data-link layer are transformed and sent through the transmission media.

## Data-link Layer

- Responsible for taking the datagram and moving it across the link.
- Internet is made up of several links (LANs and WANs) connected by routers. There may be several overlapping sets of links that a datagram can travel from the host to the destination.
- The routers are responsible for choosing the best links. When the next link to travel is determined by the router, the data-link layer is responsible for taking the datagram and moving it across the link.
- The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN.
- TCP/IP does not define any specific protocol for the data-link layer. It supports all the standard and proprietary protocols.
- The data-link layer takes a datagram and encapsulates it in a packet called a frame.
- Each link-layer protocol may provide a different service. Some link-layer protocols provide complete error detection and correction, some provide only error correction

## Network Layer

- Responsible for creating a connection between the source computer and the destination computer.
- Responsible for host-to-host communication and routing the packet through possible routes.
- The network layer in the Internet includes the main protocol, Internet Protocol (IP),
  - defines the format of the packet, called a datagram at the network layer.
  - defines the format and the structure of addresses used in this layer.
  - responsible for routing a packet from its source to its destination, which is achieved by each router forwarding the datagram to the next router in its path.
- IP is a connectionless protocol that provides no flow control, no error control, and no congestion control services. This means that if any of theses services is required for an application, the application should rely only on the transport-layer protocol.

- The network layer also includes unicast (one-to-one) and multicast (one-to-many) routing protocols.
- A routing protocol does not take part in but it creates forwarding tables for routers to help them in the routing process.
- The network layer also has some auxiliary protocols that help IP in its delivery and routing tasks.
  - The Internet Control Message Protocol (ICMP)- helps IP to report some problems when routing a packet.
  - The Internet Group Management Protocol (IGMP)-helps IP in multitasking.
  - The Dynamic Host Configuration Protocol (DHCP)-helps IP to get thenetwork-layer address for a host.
  - The Address Resolution Protocol (ARP)-IP to find the link-layer address of a host or a router when its network-layer address is given.

## Transport Layer

- Responsible for giving services to the application layer: to get a message from an application program running on the source host encapsulates it in a transport layer packet (called a *segment or a user datagram* and deliver it to the corresponding application program on the destination host through the logical connection
- The logical connection at the transport layer is also end-to-end.
- There are a few transport-layer protocols in the Internet, each designed for some specific task.
- Transmission Control Protocol (TCP)
  - connection-oriented protocol that first establishes a logical connection between transport layers at two hosts before transferring data.
  - creates a logical pipe between two TCPs for transferring a stream of bytes.
  - provides flow control, error control and congestion

- User Datagram Protocol (UDP)
  - Connectionless protocol that transmits user datagrams without first creating a logical connection
  - each user datagram is an independent entity without being related to the previous or the next one
  - does not provide flow, error, or congestion control
  - simplicity, which means small overhead, is attractive to an application program that needs to send short messages and cannot afford the retransmission of the packets involved in TCP, when a packet is corrupted or lost.
- Stream Control Transmission Protocol (SCTP)
  - designed to respond to new applications that are emerging in the multimedia.

## Application Layer

- The logical connection between the two application layers is end to- end.
- The two application layers exchange messages between each other as though there were a bridge between the two layers.
- Communication at the application layer is between two processes(two programs running at this layer).
- The application layer in the Internet includes many predefined protocols
  - The Hypertext Transfer Protocol (HTTP) : accessing the World Wide Web (WWW).
  - The Simple Mail Transfer Protocol (SMTP): e-mail service.
  - The File Transfer Protocol (FTP): File Transfer.
  - The Terminal Network (TELNET) and Secure Shell (SSH): Remote login
  - The Simple Network Management Internet at global and local levels
  - The Domain Name System (DNS): to find the network-layer address of a computer
  - The Internet Group Management Protocol (IGMP): to collect membership in a group.

## Encapsulation and Decapsulation

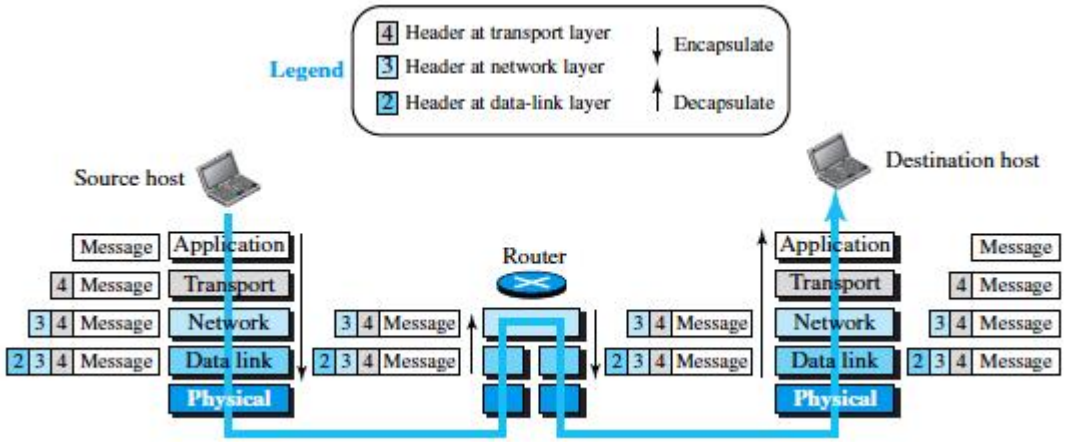



Fig: Encapsulation/Decapsulation

### Encapsulation at the Source Host

1. At the application layer, the data to be exchanged is referred to as a *message*. It does not contain header or trailer and message is passed to transport layer.

2. The transport layer takes the message as the payload, the load that the transport layer should take care of. It adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs plus some more information that is needed for the end-to end delivery of the message, such as information needed for flow, error control, or congestion control. The result is the transport-layer packet, which is called the segment(in TCP) and the user datagram (in UDP). The transport layer then passes the packet to the network layer.
3. The network layer takes the transport-layer packet as data or payload and adds its own header to the payload. The header contains the addresses of the source and destination hosts and some more information used for error checking of the header, fragmentation information, and so on. The result is the network- layer packet, called a datagram. The network layer then passes the packet to the data-link layer.

4. The data-link layer takes the network-layer packet as data or payload and adds its own header, which contains the link-layer addresses of the host or the next hop (the router). The result is the link-layer packet, which is called a frame. The frame is passed to the physical layer for transmission.

**Decapsulation and Encapsulation at the Router**

- At the router, we have both decapsulation and encapsulation because the router is connected to two or more links.

1. After the set of bits are delivered to the data-link layer, this layer decapsulates the datagram from the frame and passes it to the network layer.

2. The network layer only inspects the source and destination addresses in the datagram header and consults its forwarding table to find the next hop to which the datagram is to be delivered. The contents of the datagram should not be changed by the network layer in the router unless there is a need to fragment the datagram if it is too big to be passed through the next link. The datagram is then passed to the data-link layer of the next link.
3. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission.

**Decapsulation at the Destination Host**

- At the destination host, each layer only decapsulates the packet received, removes the payload, and delivers the payload to the next- higher layer protocol until the message reaches the application layer.
- decapsulation in the host involves error checking.

**Addressing**

- we have logical communication between pairs of layers in this model.
- Any communication that involves two parties needs two addresses: source address and destination address.
- Although it looks as if we need five pairs of addresses, one pair per layer, we normally have only four because the physical layer does not need addresses; the unit of data exchange at the physical layer is a bit, which definitely cannot have an address.

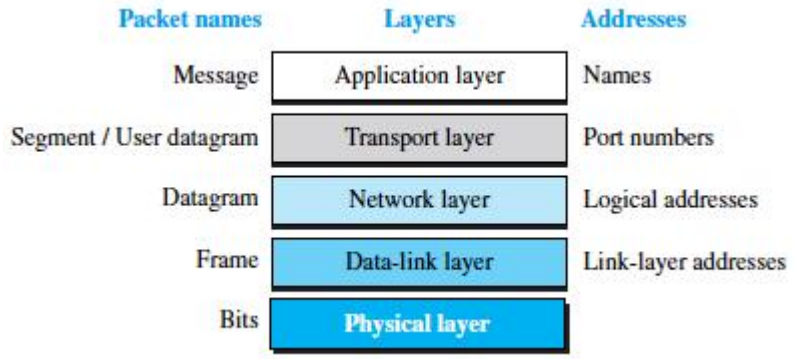



Fig: Addressing in the TCP/IP protocol suite

- There is a relationship between the layer, the address used in that layer, and the packet name at that layer.
- At the application layer, we normally use names to define the site that provides services, such as someorg.com,or the e-mail address, such as somebody@coldmail.com.
- At the transport layer, addresses are called port numbers, and these define the application-layer programs at the source and destination.

- Port numbers are local addresses that distinguish between several programs running at the same time.
- At the network-layer, the addresses are global, with the whole Internet as the scope.
- A network-layer address uniquely defines the connection of a device to the Internet.
- The link-layer addresses, sometimes called MAC addresses, are locally defined addresses, each of which defines a specific host or router in a network (LAN or WAN).

**Multiplexing and Demultiplexing**

- Since the TCP/IP protocol suite uses several protocols at some layers, we can say that we have multiplexing at the source and demultiplexing at the destination.

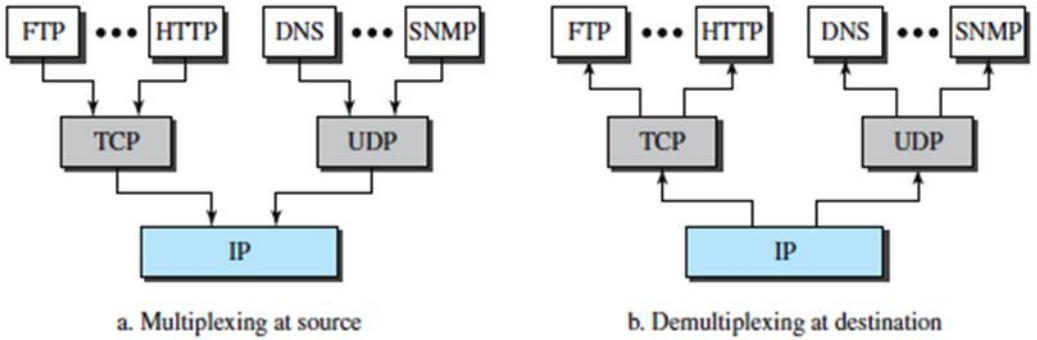



Fig: Multiplexing and demultiplexing

- Multiplexing in this case means that a protocol at a layer can encapsulate a packet from several next-higher layer protocols (one at a time)
- Demultiplexing means that a protocol can decapsulate and deliver a packet to several next-higher layer protocols (one at a time).
- To be able to multiplex and demultiplex, a protocol needs to have a field in its header to identify to which protocol the encapsulated packets belong.

- At the transport layer, either UDP or TCP can accept a message from several application-layer protocols.
- At the network layer, IP can accept a segment from TCP or a user datagram from UDP.
- IP can also accept a packet from other protocols such as ICMP, IGMP, and so on.
- At the data-link layer, a frame may carry the payload coming from IP or other protocols such as ARP

# The OSI Model

- The International Organization for Standardization (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.
- ISO is the organization; OSI is the model.
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.

- The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

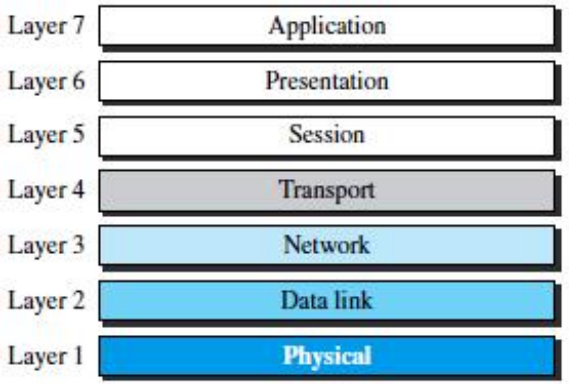



Fig: The OSI Model

- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.
- It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network

## OSI versus TCP/IP

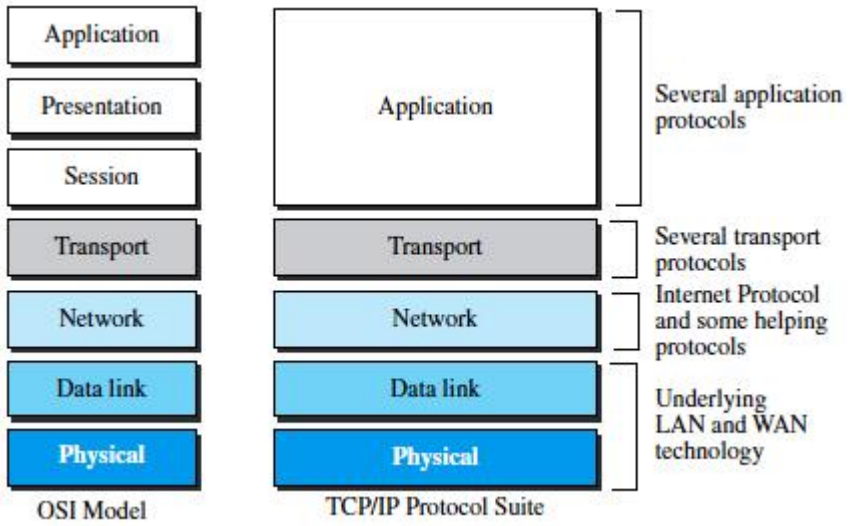



Fig: TCP/IP and OSI model

- Two layers, session and presentation are missing from the TCP/IP protocol suite.
- The application layer in the suite is usually considered to be the combination of three layers in the OSI model
- TCP/IP has more than one transport-layer protocol. Some of the functionalities of the session layer are available in some of the transport-layer protocols.

- The application layer is not only one piece of software. Many applications can be developed at this layer.
- If some of the functionalities mentioned in the session and presentation layers are needed for a particular application, they can be included in the development of that piece of software.

**Lack of OSI Model's Success**

- OSI was completed when TCP/IP was fully in place and a lot of time and money had been spent on the suite; changing it would cost a lot.
- Some layers in the OSI model were never fully defined.
- For example, although the services provided by the presentation and the session layers were listed in the document, actual protocols for these two layers were not fully defined, nor were they fully described, and the corresponding software was not fully developed.
- when OSI was implemented by an organization in a different application, it did not show a high enough level of performance to entice the Internet authority to switch from the TCP/IP protocol suite to the OSI model.

# Introduction to Physical Layer

- One of the major functions of the physical layer is to move data in the form of electromagnetic signals across a transmission medium
- **Transmission media** is a pathway that carries the information from sender to receiver.
- We use different types of cables or waves to transmit data. Data is transmitted normally through electrical or electromagnetic signals.
- Transmission media are located below the physical layer
- Computers use signals to represent data. Signals are transmitted in form of electromagnetic energy.

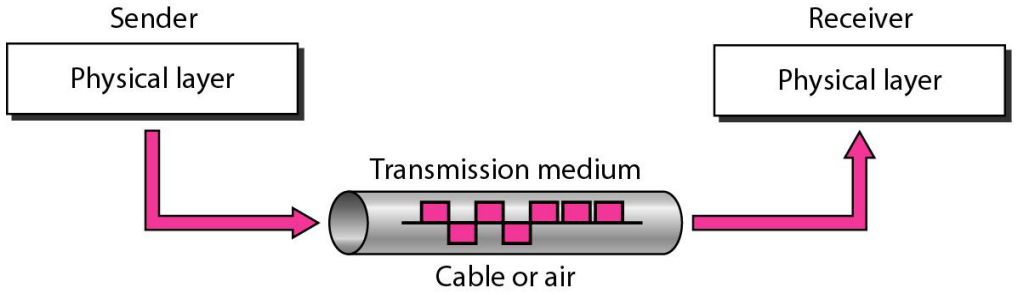
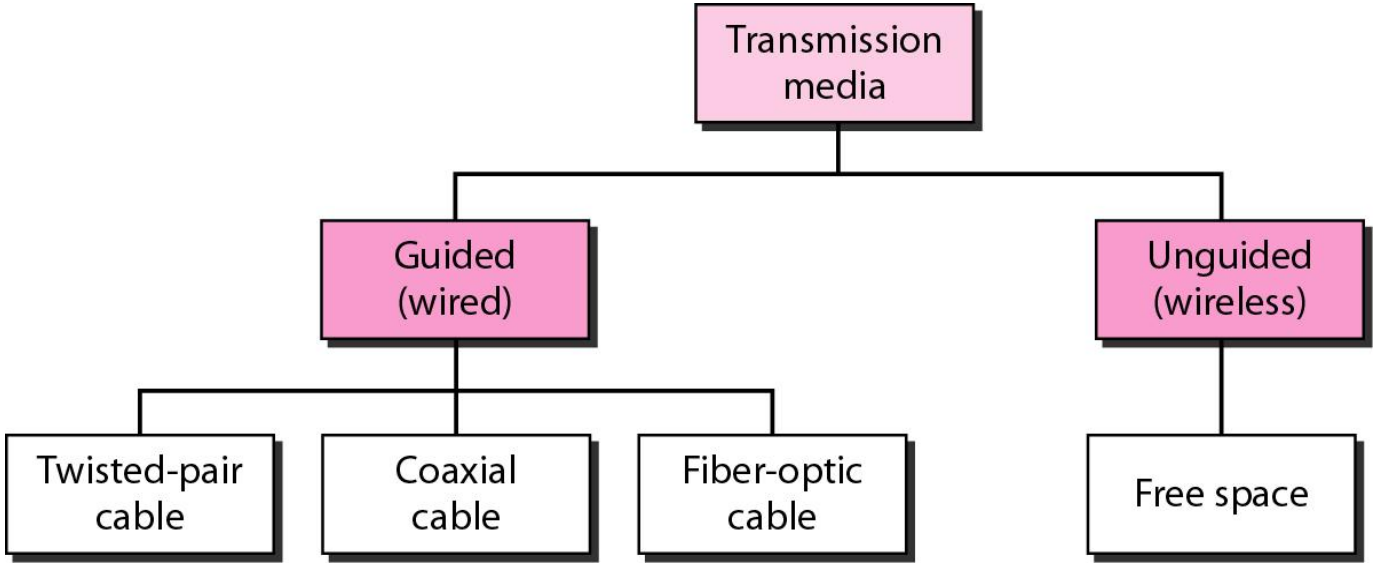



Fig: Transmission medium and physical layer

## Classification of Transmission media



## Guided Media

- Guided media, which are those that provide a conduit from one device to another include twisted pair cable, coaxial cable, and fiber optic cable.

## Twisted-pair cable

- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together

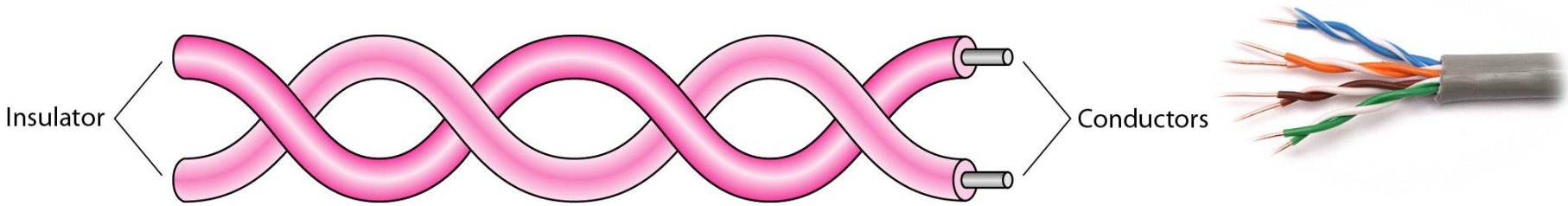
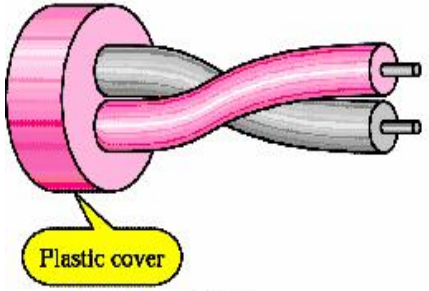



Fig: Twisted-pair cable

## Unshielded versus Shielded Twisted–pair cable

### UTP

- Pair of unshielded wires wound around each other
- Easiest to install
- Applications
  - Telephone subscribers connect to the central telephone office
  - DSL lines
  - LAN – 10Mbps or 100Mbps

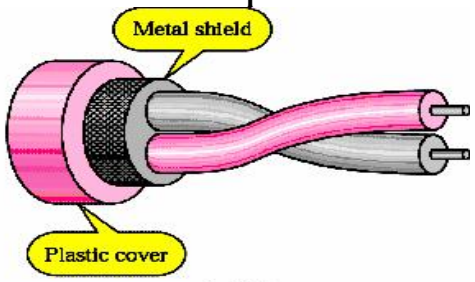


a. UTP

### STP

- Pair of wires wound around each other placed inside a protective foil wrap
- Metal braid or sheath foil that reduces interference

  Harder to handle (thick, heavy)



b. STP

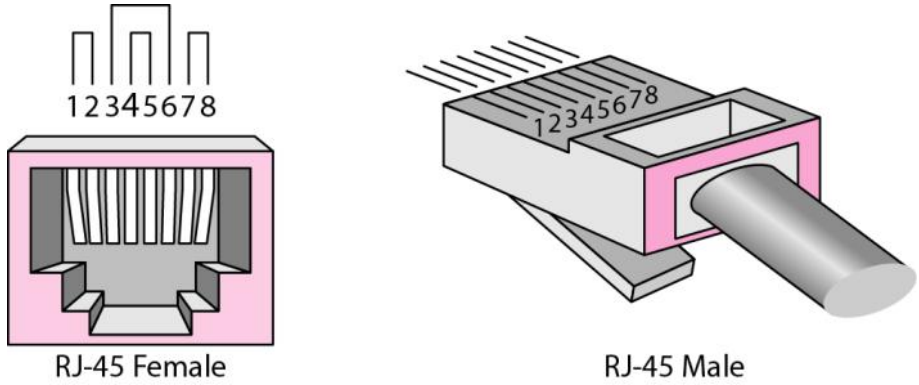
- Applications
  - STP is used in IBM token ring networks.
  - Higher transmission rates over longer distances.

**Categories**

- The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories.
- Categories are determined by cable quality, with 1 as the lowest and 7 as the highest. Each EIA category is suitable for specific uses.

| Category | Specification | Data Rate (Mbps) | Use |
|---|---|---|---|
| 1 | Unshielded twisted-pair used in telephone | < 0.1 | Telephone |
| 2 | Unshielded twisted-pair originally used in T lines | 2 | T-1 lines |
| 3 | Improved CAT 2 used in LANs | 10 | LANs |
| 4 | Improved CAT 3 used in Token Ring networks | 20 | LANs |
| 5 | Cable wire is normally 24 AWG with a jacket and outside sheath | 100 | LANs |
| 5E | An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference | 125 | LANs |
| 6 | A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate. | 200 | LANs |
| 7 | Sometimes called *SSTP (shielded screen twisted-pair)*. Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate. | 600 | LANs |

## UTP connector( Registered Jack:RJ45)




- RJ45 is a keyed connector , meaning the connector can be inserted in only one way

**Applications of Twisted pair**

Used in

1. Telephone lines to provide voice and data channels (local loop)
2. The DSL lines that are used by the telephone companies to provide high-data-rate connections
3. Local area networks, such as 10-base-Tand 100base-T

**Advantages of Twisted pair:**

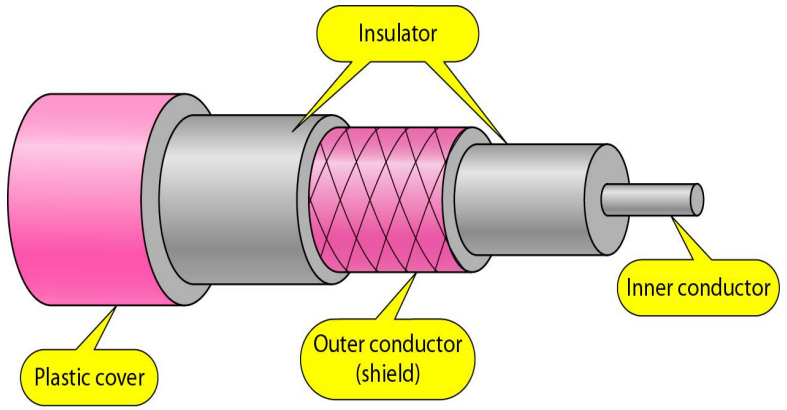
- Cheap
- Easy to work with

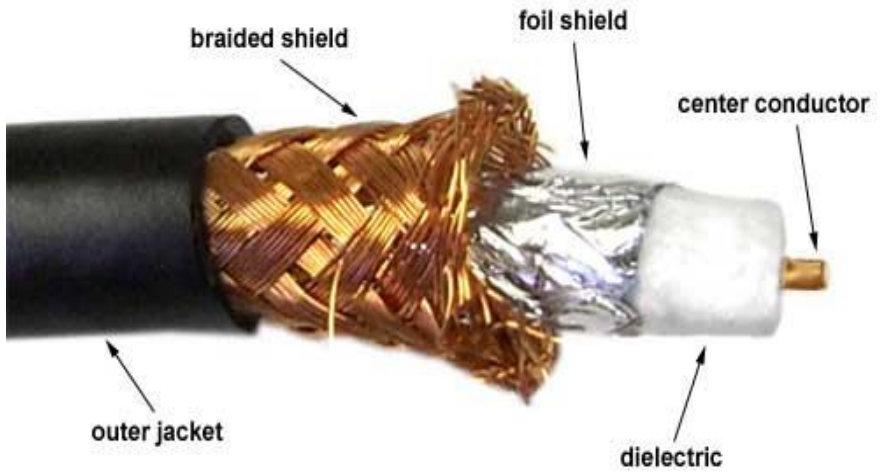
**Disadvantages of Twisted pair:**

- Low data rate
- Short range

## Co-axial Cable

- Co-axial cable carries signal of higher frequency ranges than twisted pair cable




- Inner conductor is a solid wire
- Outer conductor serves as a shield against noise and a second conductor

## Categories of coaxial cables

- Coaxial cables are categorized by Radio Government (RG) ratings, RG is De Jure standards

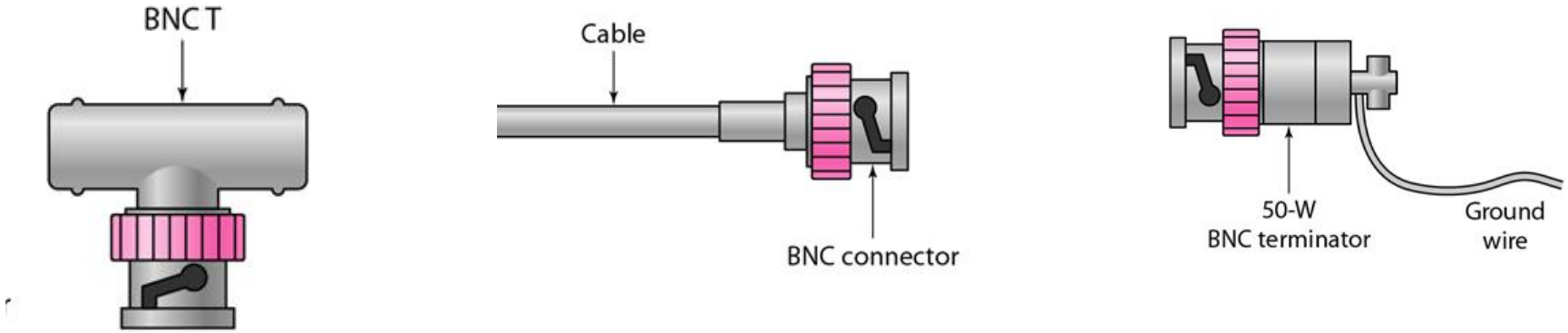
| *Category* | *Impedance* | *Use* |
|---|---|---|
| RG-59 | 75 Ω | Cable TV |
| RG-58 | 50 Ω | Thin Ethernet |
| RG-11 | 50 Ω | Thick Ethernet |

## Coaxial Cable Connectors

### BNC Connectors – Bayone Neil Concelman

- To connect coaxial cable to devices we need coaxial connectors
- BNC Connector is used at the end of the cable to a device
  - Example: TV set conenction

- BNC T connector used to Ethernet networks to branch out connection to computer or other devices
- BNC terminator is used at the end of the cable to prevent the reflection of the signal




1. **BNC connector:** Used in TV
2. **BNCT:** Ethernet network
3. **BNC terminator:** End of the cable to prevent the reflection of the signal

**Applications of coaxial cable**

1. Analog telephone network where a single cable could carry 10,000 voice signals. Later it was used in Digital telephone networks where cable can carry 600Mbps
2. Cable TV network: hybrid network use coaxial cable only at the network boundaries , near the consumer. Cable TV use RG-59
3. Traditional Ethernet LANs.10-base-2 or “Thin Ethernet”, uses RG-58 coax cable to transmit data at 10 Mbps with a range of 185m.10-base-5,or “Thick Ethernet”, uses RG-11 to transmit 10 Mbps with rang of 500 m

**Advantages**

- Easy to wire
- Easy to expand
- Moderate  level of Electro Magnetic Interference

**Disadvantage**

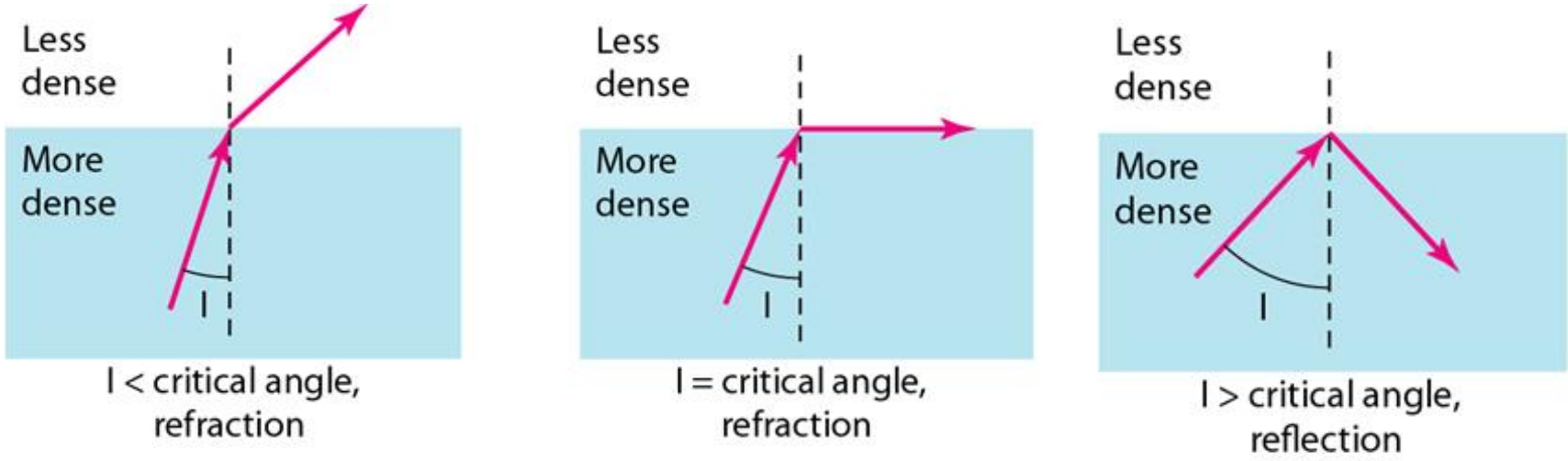
- Single cable failure can take down an entire network
- Cost of installation of a coaxial cable is high due to its thickness and stiffness
- Cost of maintenance is also high

## Fiber-Optic Cable

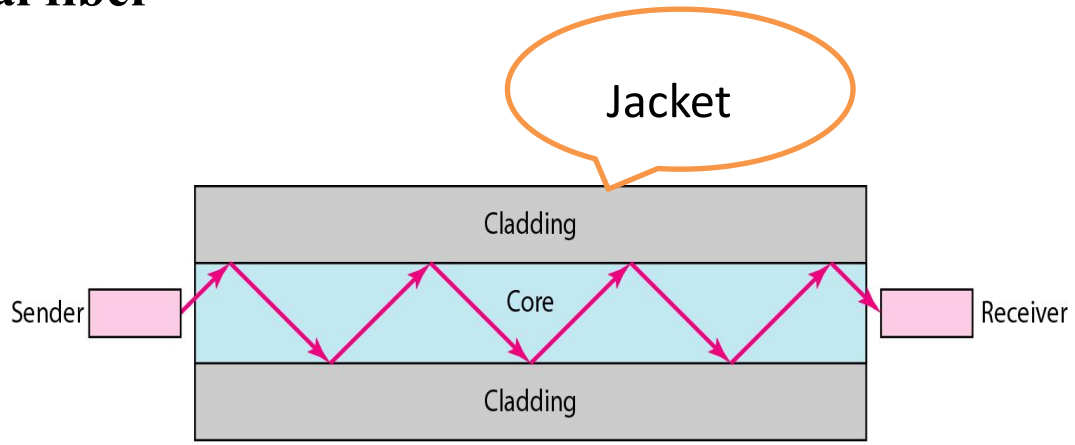
- A fiber optic cable is made of glass or plastic and transmit signals in the form of light.
- Light travels in a straight line
- If light goes from one substance to another then the ray of light changes direction

**Bending of light ray**

- Angle of Incidence (I): the angle the ray makes with the line perpendicular to the interface between the two substances
- Critical Angle: the angle of incidence which provides an angle of refraction of 90-degrees.

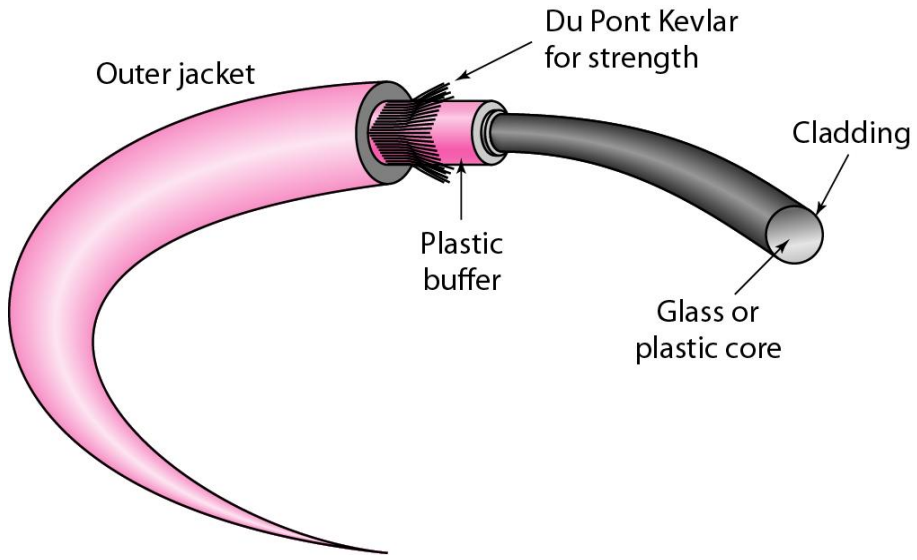



## Optical fiber

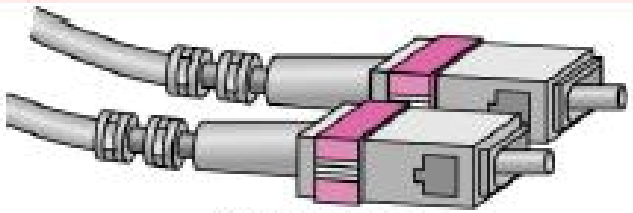


- An optical fiber cable has a cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket(outer part of the cable).
- Uses reflection to guide light through a channel
- Core is of glass or plastic surrounded by Cladding
- Cladding is of less dense glass or plastic

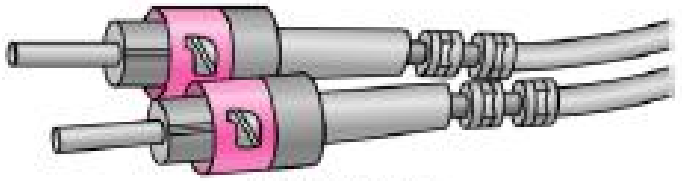
## Fiber Construction



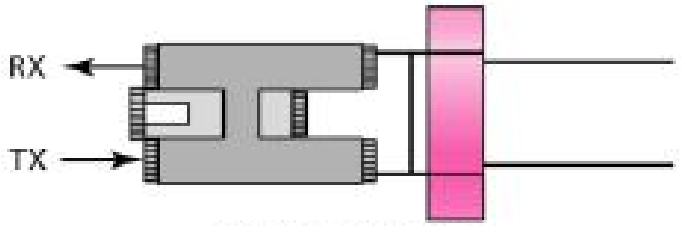
# Fiber-optic cable connectors



SC connector



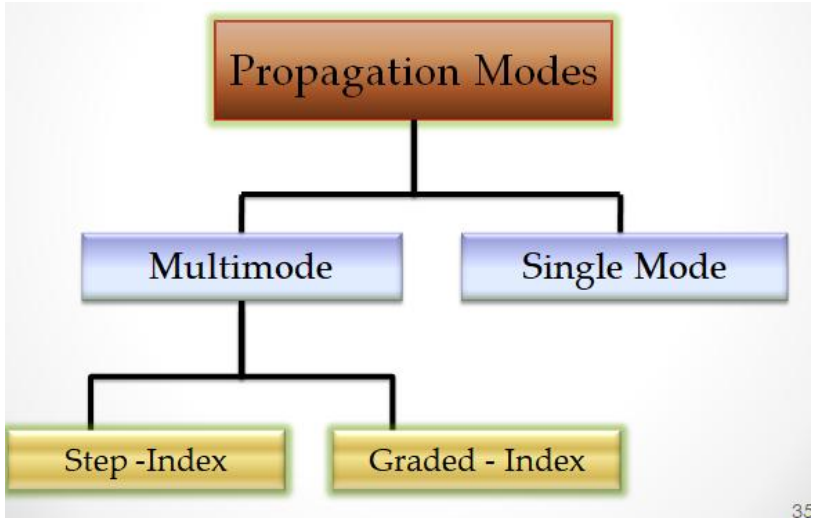
ST connector




MT-RJ connector

1. SC (subscriber channel): used for TV cable
2. ST (Straight Tip): used for connect cable with networking devices
3. MT-RJ: Network

## Propagation Modes



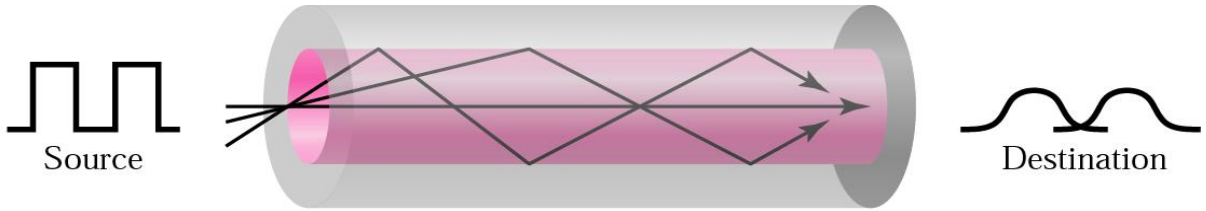

**1. Single-mode fiber**

- Has a small core size of 8–10 micrometers, allowing only one mode of light to pass through.
- Single-mode fiber is used for long-distance transmissions and high-bandwidth applications.

**2. Multimode fiber**

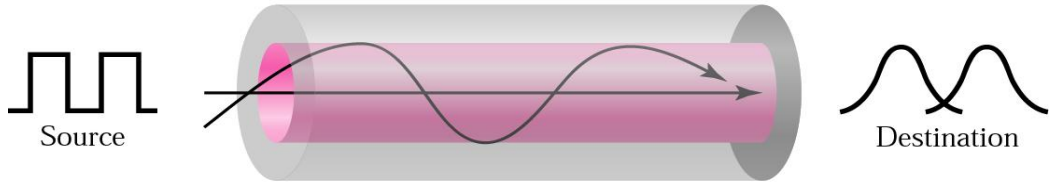
- Has a larger core size of 50–62.5 micrometers, allowing multiple modes of light to pass through.
- Multimode fiber is used for shorter distances and lower bandwidth applications.

- In **multimode step-index fiber,** the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding.
- The term *step-index* refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.




a. Multimode, step-index

- A second type of fiber, called **multimode graded-index fiber,** decreases this distortion of the signal through the cable. The word *index* here refers to the index of refraction. A graded index fiber, therefore, is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge.




b. Multimode, graded-index

- **Single-mode** uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.


c. Single-mode

**Applications of Fiber-optic cable**

Used in

1. Cable TV network: hybrid network use a combination of optical fiber and coax cable.

   Optical provides the backbone while coaxial cable provide the connation to the user.

2. Local area networks such as 100base-FX(fast Ethernet) and 1000base-XLANs.

3. Backbone networks because its wide bandwidth

**Advantages**

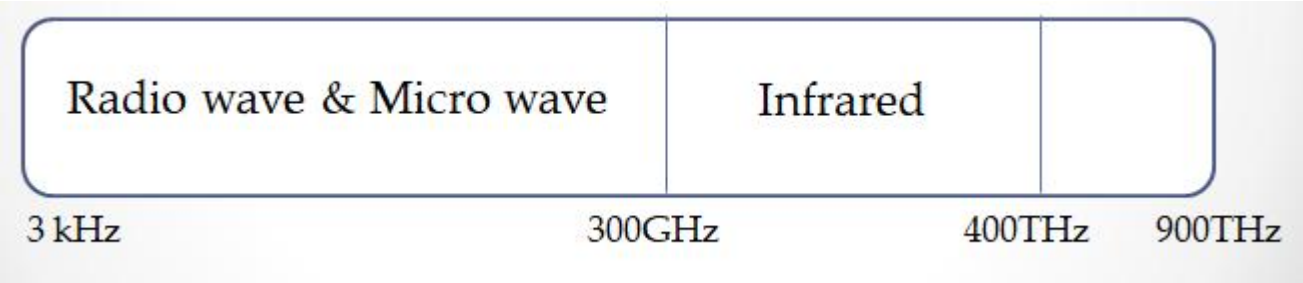
- Higher Bandwidth
- Less signal attenuation
- Immunity to electromagnetic interference (noise)
- Resistance to corrosive materials. Glass is more resistance to corrosive material
- Light weight. Fiber cables are much lighter than copper cables
- Greater immunity to tapping: copper cables create antenna effects that can easily tapped

**Disadvantages**

- Installation and maintenance. It's a new technology. Its installation and maintenance require expertise that is not yet available every where
- Unidirectional light propagation. If we need bidirectional , two fibers are needed.
- Cost. The cable and the interfaces are more expensive than those of other guided media. If the demand of BW is not high , often use of optical fiber can not be justified

## Unguided Media: Wireless

- Unguided media transport electromagnetic waves without using a physical conductor it is known as wireless communication.
- Signals broadcast through free space and available to capable receiver
- Electro magnetic spectrum for wireless communication:

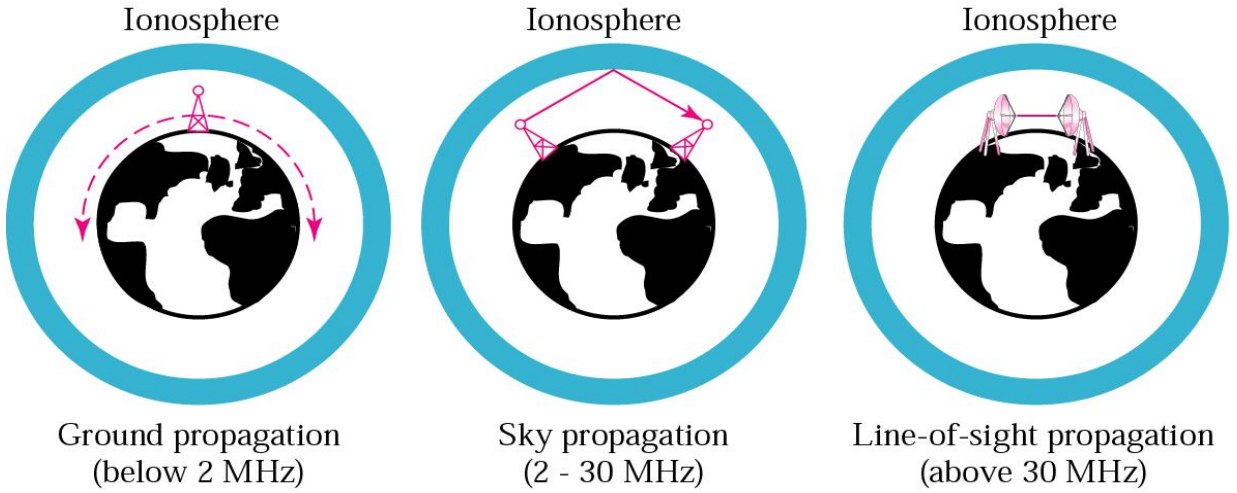



**Propagation methods**

- Unguided signals travels from the source to destination in several ways it is known as propagation.

**They are three types:**

1. Ground propagation
2. Sky propagation
3. Line-of-Sight Propagation



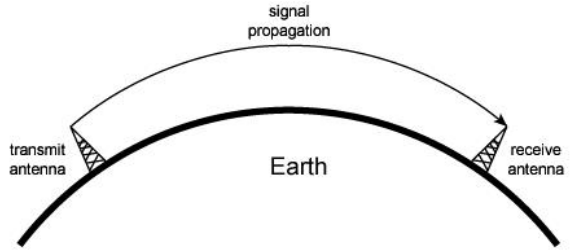
**Ground propagation**:

- Radio waves travel through the lowest portion of the atmosphere
- Touching the earth.

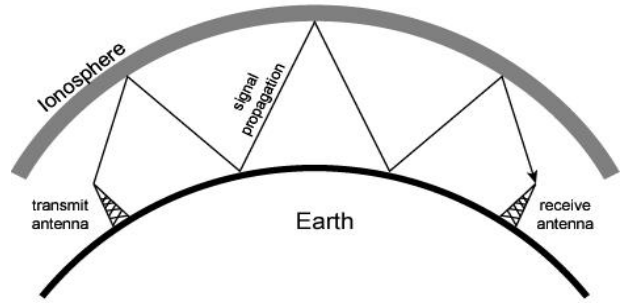
**Sky propagation**:

- Radio waves  radiate to the ionosphere then they are reflected back to earth.
- **Line-of-Sight Propagation**:

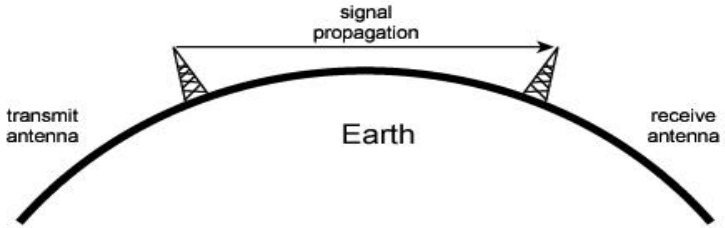
  In straight lines directly from antenna to antenna



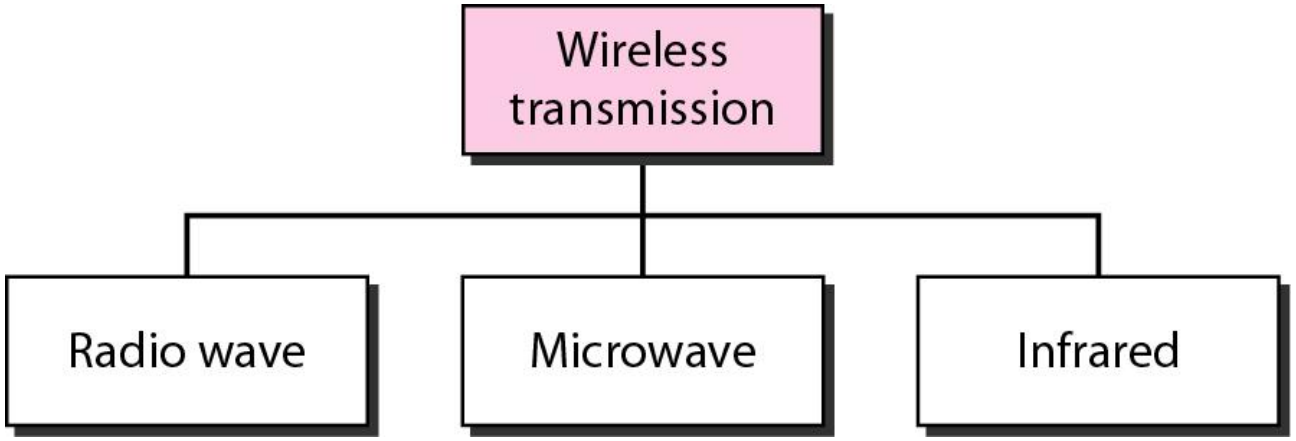

(a) Ground-wave propagation (below 2 MHz)




(b) Sky-wave propagation (2 to 30 MHz)




(c) Line-of-sight (LOS) propagation (above 30 MHz)


Wireless transmission
Radio wave
Microwave
Infrared

## Radio Waves

- Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. Frequencies between 3 KHz and 1 GHz.
- Used for multicasts(multiple way) communications, such as radio and television, and paging system.
- Radio waves can penetrate buildings easily, so that widely use for indoors & outdoors communication.
- Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio.

**Omnidirectional Antenna**

- Radio waves use **omnidirectional antennas** that send out signals in all directions.
- Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas.

**Applications**

- The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers.
- AM and FM radio, television,cordless phones, and paging are examples of multicasting.

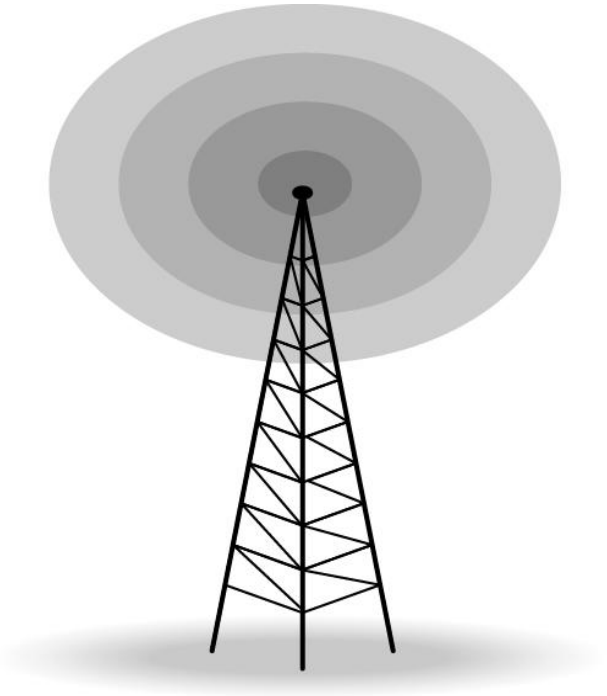


Fig: Omnidirectional antenna

## Microwaves

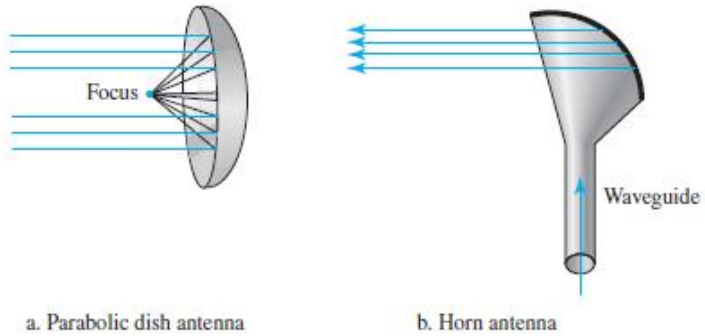
- Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.
- Microwaves are unidirectional.
- There are two types of micro waves data communication system : terrestrial and satellite
- Micro waves are widely used for one to one communication between sender and receiver, example: cellular phone, satellite networks and in wireless LANs(wifi), WiMAX, GPS

- The following describes some characteristics of microwave propagation:

1. Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall. The curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate by using microwaves. Repeaters are often needed for long distance communication.
2. Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.
3. The microwave band is relatively wide, almost 299 GHz. Therefore wider subbands can be assigned, and a high data rate is possible.
4. Use of certain portions of the band requires permission from authorities.

## Unidirectional Antenna

- Microwaves need **unidirectional antennas** that send out signals in one direction.
- Two types of antennas are used for microwave communications: the parabolic dish and the Horn




- A **parabolic dish antenna** is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus.
- A **horn antenna** looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem (resembling a handle) and deflected outward in a series of narrow parallel beams by the curved head.

## Applications

- Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

## Infrared

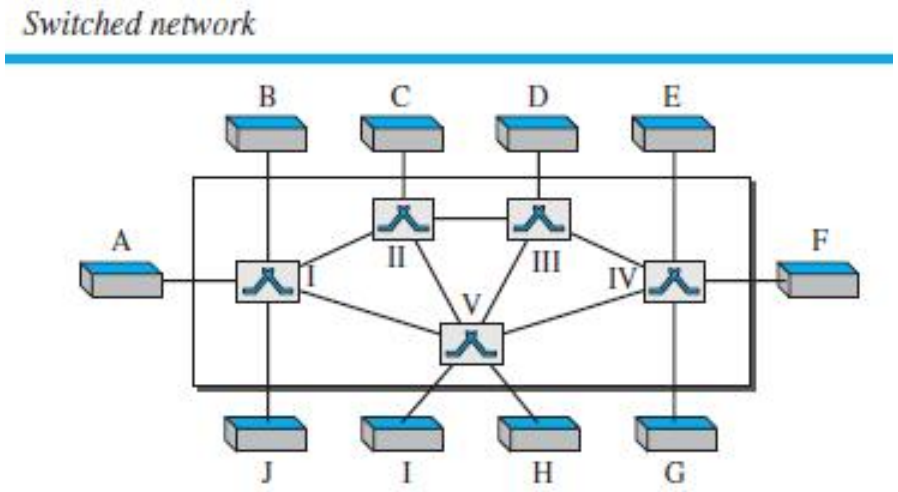
- **Infrared waves,** with frequencies from 300 GHz to 400 THz (wavelengths from 1 mmto 770 nm), can be used for short-range communication.
- Infrared waves, having high frequencies, cannot penetrate walls.
- Example: Remote control, File sharing between two phones, Communication between a PC and peripheral device,

## Applications

- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation
- The *Infrared Data Association* (IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between
- devices such as keyboards, mice, PCs, and printers.
- For example, some manufacturers provide a special port called the IrDA port that allows a wireless keyboard to communicate with a PC.

## Switching

- how to connect  Whenever we have multiple devices?
  - make a point-to-point connection between each pair of devices (a mesh topology) ?
  - make a connection between a central device and every other device (a star topology)?
- impractical and wasteful when applied to very large networks.
  - The number and length of the links require too much infrastructure to be cost-efficient
  - the majority of those links would be idle most of the time.
- A better solution is switching.
- A switched network consists of a series of interlinked nodes, called switches creating temporary connections between two or more devices linked to the switch.




- The **end systems** (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

## Packet switching

- In a packet-switched network, there is no resource reservation; resources are allocated on demand.
- The size of the packet is determined by the network and the governing protocol.
- When a switch receives a packet, no matter what the source or destination is, the packet must wait if there are other packets being processed.
- As with other systems in our daily life, this lack of reservation may create delay. For example, if we do not have a reservation at a restaurant, we might have to wait.
- Two types of packet-switched networks: datagram networks and virtual circuit networks.

## Datagram Networks

- Each packet is treated independently of all others.
- Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone.
- Packets in this approach are referred to as ***datagrams***.
- Datagram switching is normally done at the network layer.

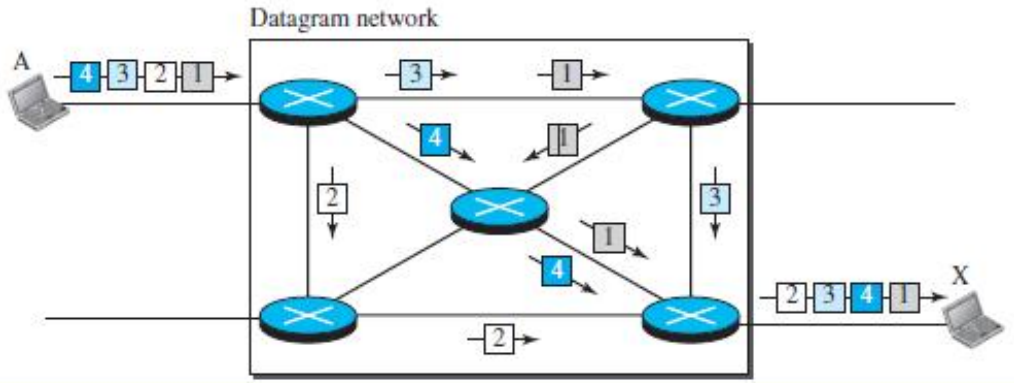



**Figure :** *A datagram network with four switches (routers)*

- The datagram networks are sometimes referred to as connectionless networks.
- The term connectionless here means that the switch (packet switch) does not keep information about the connection state.
- There are no setup or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.
- In this type of network, each switch (or packet switch) has a routing table which is based on the destination address.
- The routing tables are dynamic and are updated periodically.
- The destination addresses and the corresponding forwarding output ports are recorded in the tables.

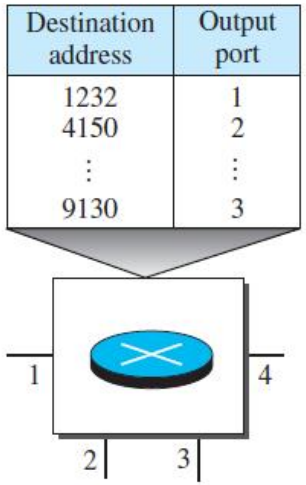



Fig: Routing table in a datagram network

- Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet.
- When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.
- The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet.

## Efficiency

- The efficiency of a datagram network is better than that of a circuit-switched network ; resources are allocated only when there are packets to be transferred.
- If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.

## Delay

- There may be greater delay in a datagram network than in a virtual-circuit network.
- Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded.
- In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message.

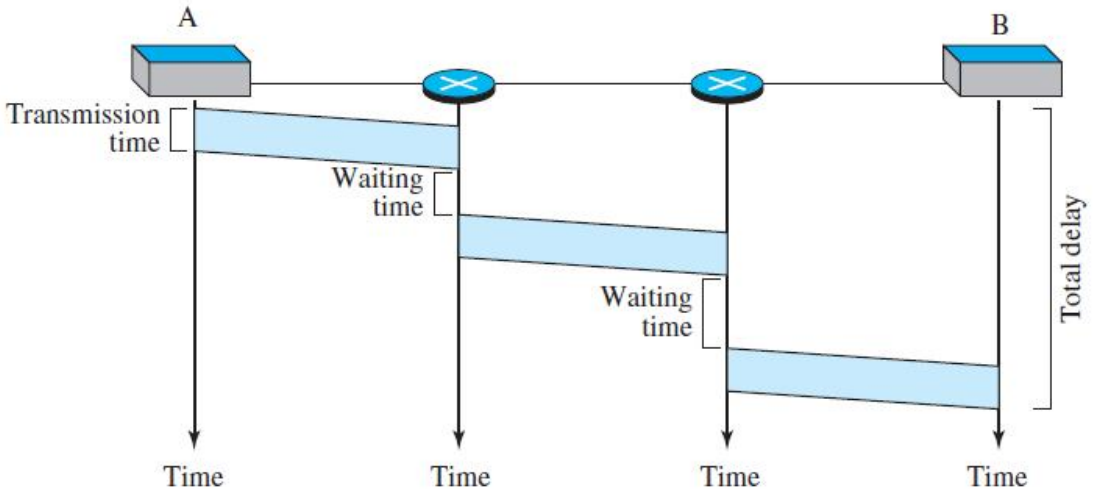



**Figure :***Delay in a datagram network*

- The packet travels through two switches. There are three transmission times ($3T$), three propagation delays (slopes $3\tau$ of the lines), and two waiting times ($w1 + w2$).
- We ignore the processing time in each switch. The total delay is

$$\text{Total delay} = 3T + 3\tau + w_1 + w_2$$

## Virtual-Circuit Networks

- A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.
    1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
    2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
    3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what the next switch should be and the channel on which the packet is being carried), not end-to-end jurisdiction.

- As in a circuit-switched network, all packets follow the same path established during the connection.
- A virtual-circuit network is normally implemented in the data-link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer.

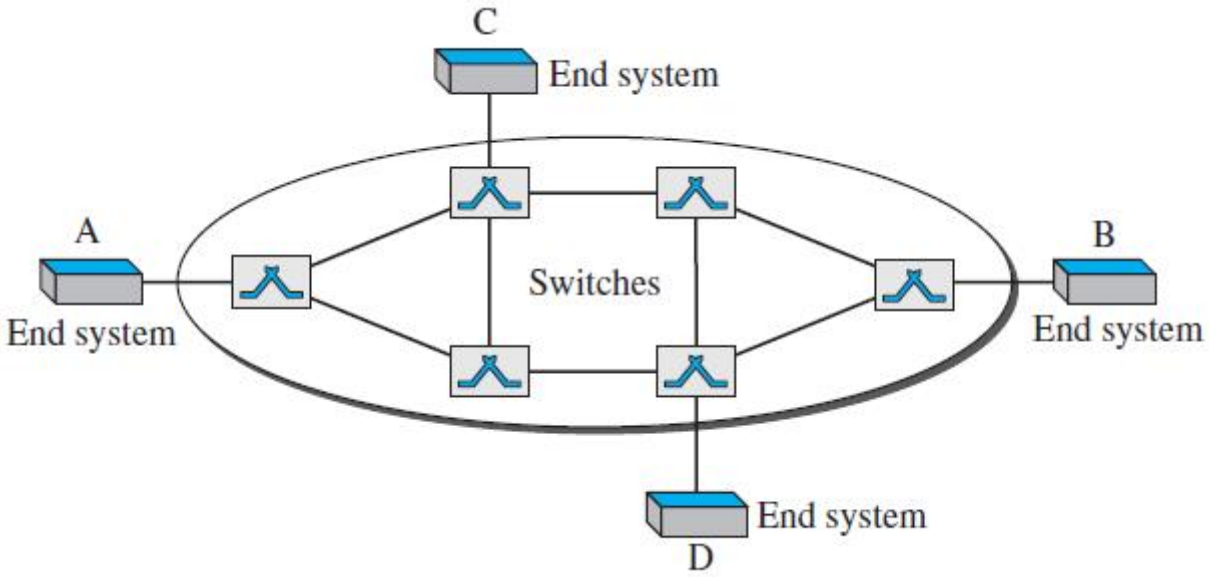
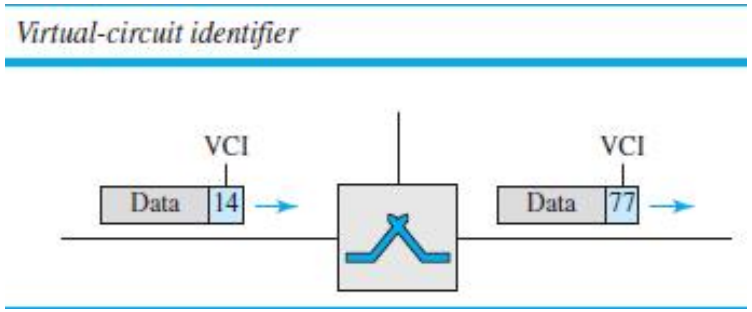



**Figure :** *Virtual-circuit network*

**Addressing**

- In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).
- Global Addressing
  - A source or a destination needs to have a global address—an address that can be unique in the scope of the network or internationally if the network is part of an international network. A global address in virtual-circuit networks is used only to create a virtual-circuit identifier.
- Virtual-Circuit Identifier
  - The identifier that is actually used for data transfer is called the virtual-circuit identifier (VCI) or the label. A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI.




**Three Phases**

- A source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown.
- In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection.
- In the teardown phase, the source and destination inform the switches to delete the corresponding entry.
- Data transfer occurs between these two phases.

**Data-Transfer Phase**

- To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit.
- The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up.
- The data-transfer phase is active until the source sends all its frames to the destination.
- The procedure at the switch is the same for each frame of a message. The process creates a virtual circuit, not a real circuit, between the source and destination.

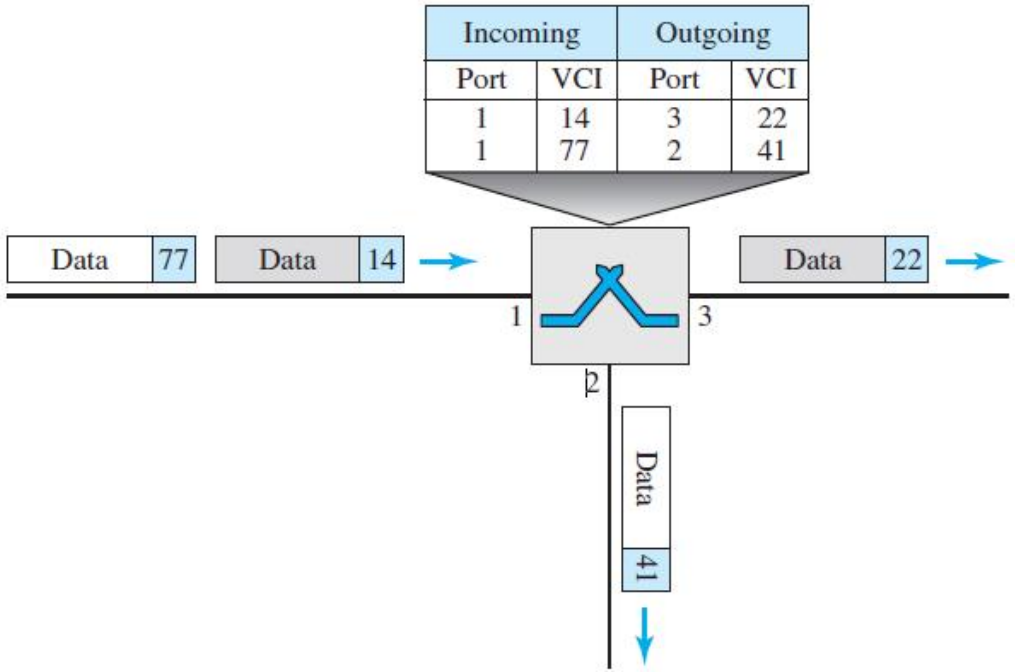



*Fig: Switch and tables in a virtual-circuit network*

- a frame arriving at port 1 with a VCI of 14.
- When the frame arrives, the switch looks in its table to find port 1 and a VCI of 14.
- When it is found, the switch knows to change the VCI to 22 and send out the frame from port 3.

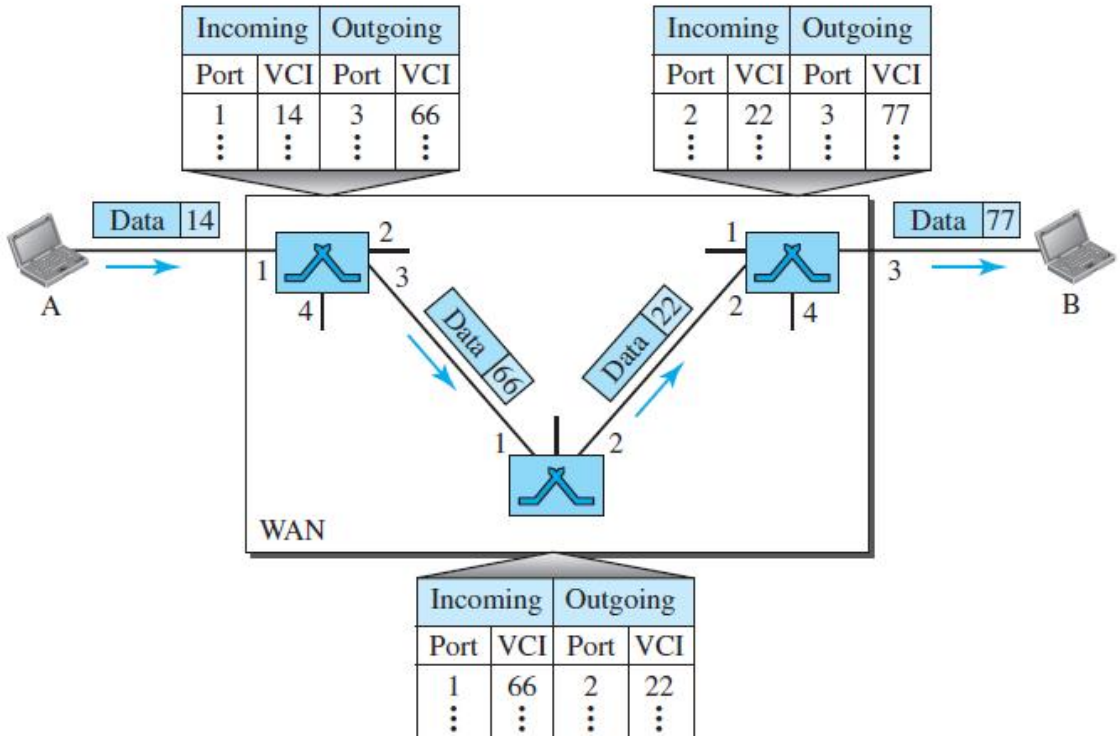



**Figure :** *Source-to-destination data transfer in a virtual-circuit network*

- Figure shows how a frame from source A reaches destination B and how its VCI changes during the trip.
- Each switch changes the VCI and routes the frame.

- **Setup Phase**
  In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B.
- Two steps are required: the setup request and the acknowledgment.

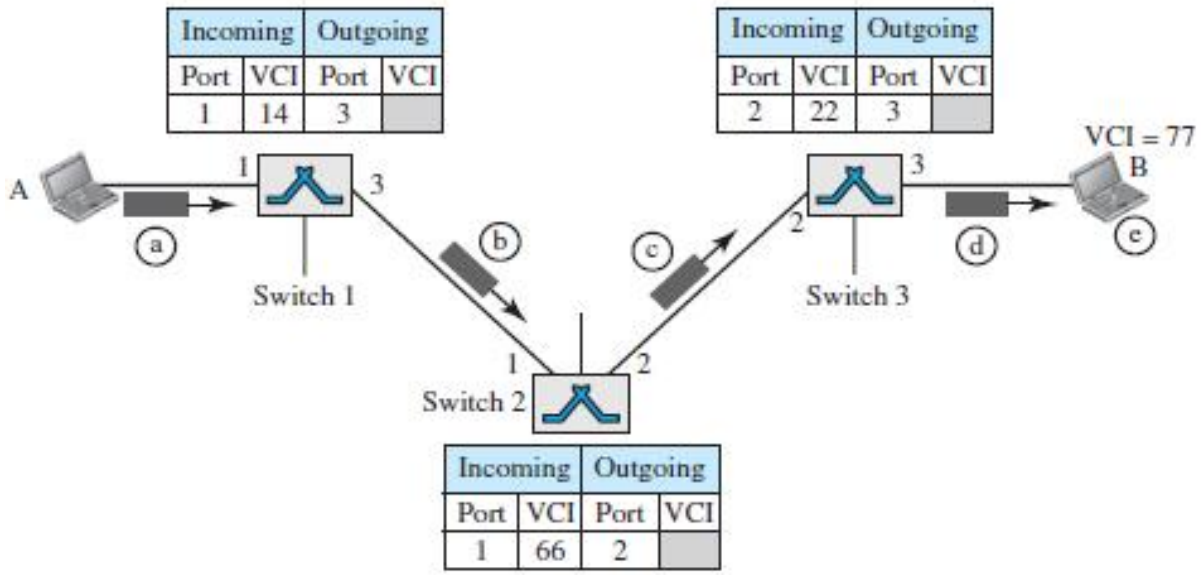
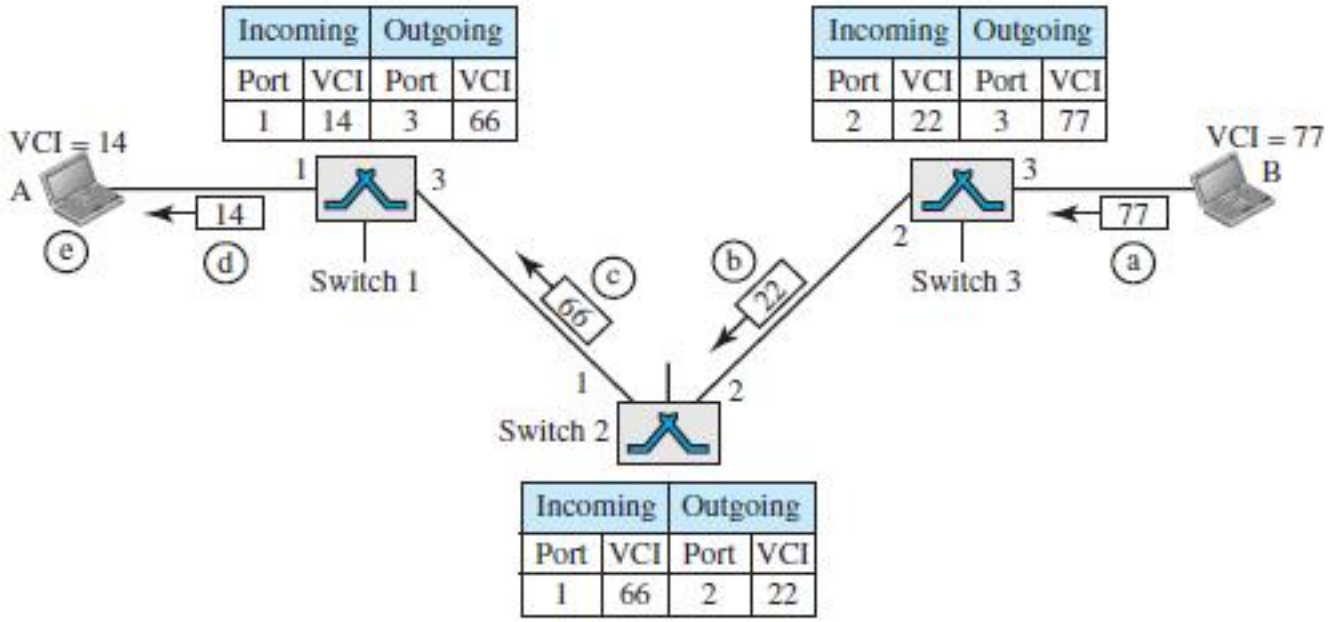



**Figure :** *Setup request in a virtual-circuit network*

- **a.** Source A sends a setup frame to switch 1.
- **b.** Switch 1 receives the setup request frame. It knows that a frame going from A to B goes out through port 3. For the moment, assume that it knows the output port. The switch creates an entry in its table for this virtual circuit, but it is only able to fill three of the four columns. The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). It does not yet know the outgoing VCI, which will be found during the acknowledgment step. The switch then forwards the frame through port 3 to switch 2.
- **c.** Switch 2 receives the setup request frame. The same events happen here as at switch 1; three columns of the table are completed: in this case, incoming port (1), incoming VCI (66), and outgoing port (2).
- **d.** Switch 3 receives the setup request frame. Again, three columns are completed: incoming port (2), incoming VCI (22), and outgoing port (3).
- **e.** Destination B receives the setup frame, and if it is ready to receive frames from A, it assigns a VCI to the incoming frames that come from A, in this case 77. This VCI lets the destination know that the frames come from A, and not other sources.

- **Acknowledgment**
  A special frame, called the acknowledgment frame, completes the entries in the switching tables.



- **a.** The destination sends an acknowledgment to switch 3. The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed. The frame also carries VCI 77, chosen by the destination as the incoming VCI for frames from A. Switch 3 uses this VCI to complete the outgoing VCI column for this entry. Note that 77 is the incoming VCI for destination B, but the outgoing VCI for switch 3.
- **b.** Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCI in the table, chosen in the previous step. Switch 2 uses this as the outgoing VCI in the table.
- **c.** Switch 2 sends an acknowledgment to switch 1 that contains its incoming VCI in the table, chosen in the previous step. Switch 1 uses this as the outgoing VCI in the table.
- **d.** Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosen in the previous step.
- **e.** The source uses this as the outgoing VCI for the data frames to be sent to destination B.

**Teardown Phase**

- In this phase, source A, after sending all frames to B, sends a special frame called a teardown request.
- Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables.

**Efficiency**

- In virtual-circuit switching, all packets belonging to the same source and destination travel the same path, but the packets may arrive at the destination with different delays if resource allocation is on demand.
- Resource reservation in a virtual-circuit network can be made during the setup or can be on demand during the data-transfer phase.
- In the first case, the delay for each packet is the same; in the second case, each packet may encounter different delays.

## Delay

- In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown.
- If resources are allocated during the setup phase, there is no wait time for individual packets.

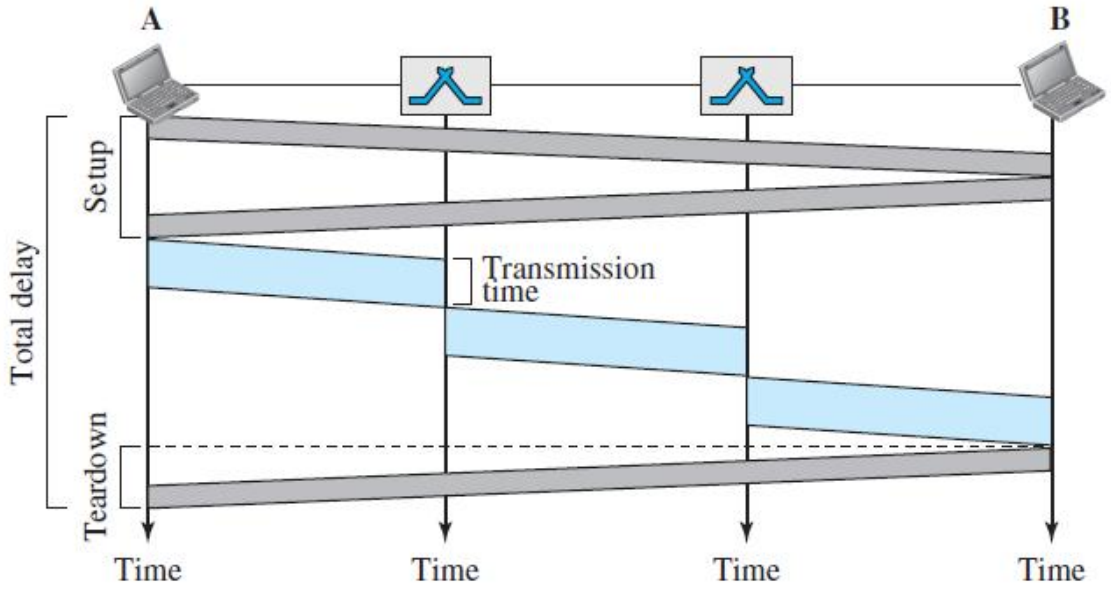



**Figure :** *Delay in a virtual-circuit network*

- The packet is traveling through two switches (routers).
- There are three transmission times ($3T$), three propagation times ($3\tau$), data transfer depicted by the sloping lines, a setup delay (which includes transmission and propagation in two directions), and a teardown delay (which includes transmission and propagation in one direction).
- We ignore the processing time in each switch. The total delay time is

$$\text{Total delay} + 3T + 3\tau + \text{setup delay} + \text{teardown delay}$$