School of Computer Science & IT
Department of BCA

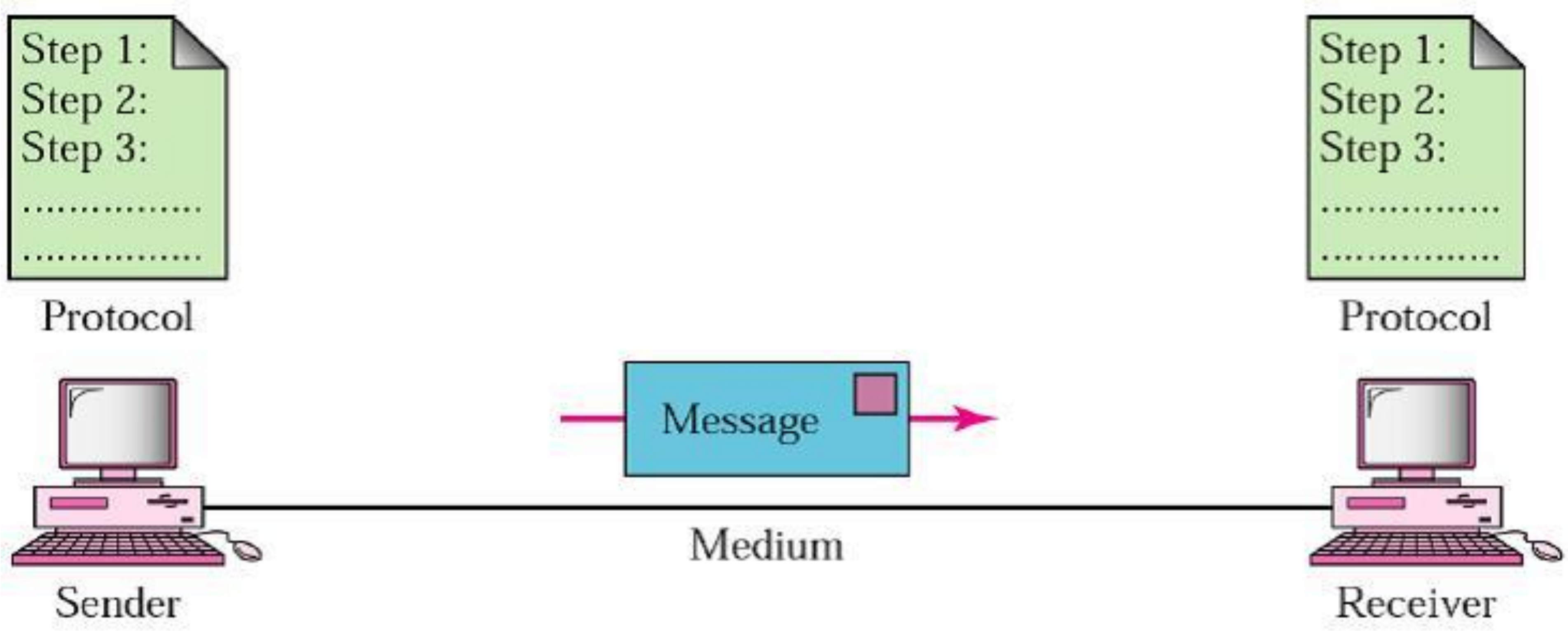
COMPUTER NETWORKS

MODULE 1: NETWORKING FUNDAMENTALS

BASICS OF NETWORK & NETWORKING

- What is data?
  - ➢Facts and statistics collected together for reference or analysis.
  - ➢In computing, data is information that has been translated into a form that is efficient for movement or processing.
- What is communication?
  - ➢Imparting or exchanging of information by speaking, writing, or using some other medium.
  - ➢Communication is simply the act of transferring information from one place, person or group to another.

COMPONENTS IN COMMUNICATION



COMPONENTS IN COMMUNICATION (contd…)

- 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 COMMUNICATION

Data communication is the exchange of data between two devices via some form of transmission medium such as a wire cable.

Data Communication has two types :

1. Local -Local communication takes place when the communicating devices are in the same geographical area, same building, face-to-face between individuals etc.

2. Remote-Remote communication takes place over a distance i.e. the devices are far away from each other.

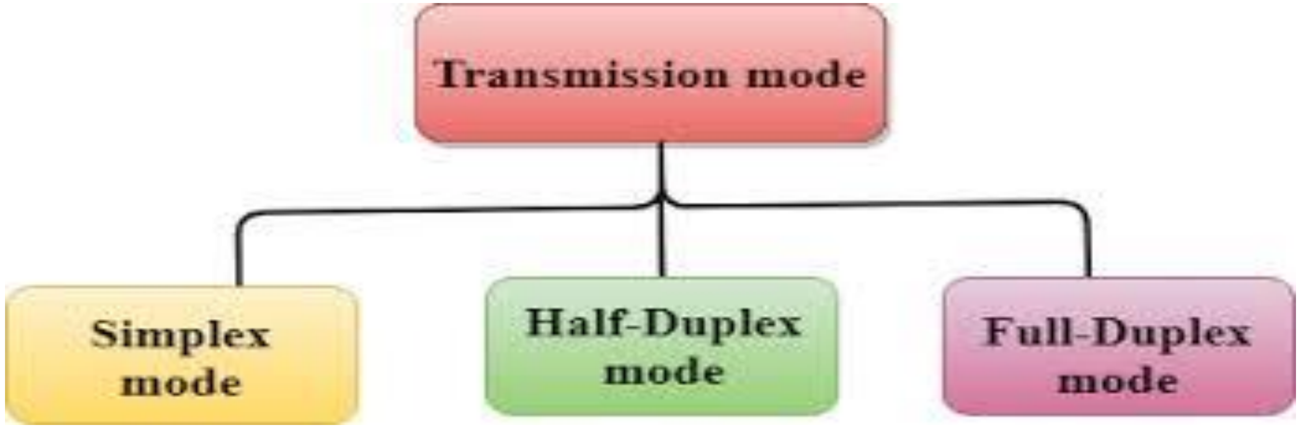
FOUR FUNDAMENTAL CHARACTERISTICS OF DATA COMMUNICATION

- Delivery : Delivery should be done to the correct destination.
- Timeliness : Delivery should be on time.
- Accuracy : Data delivered should be accurate.
- Jitter : Variation in packet arrival.

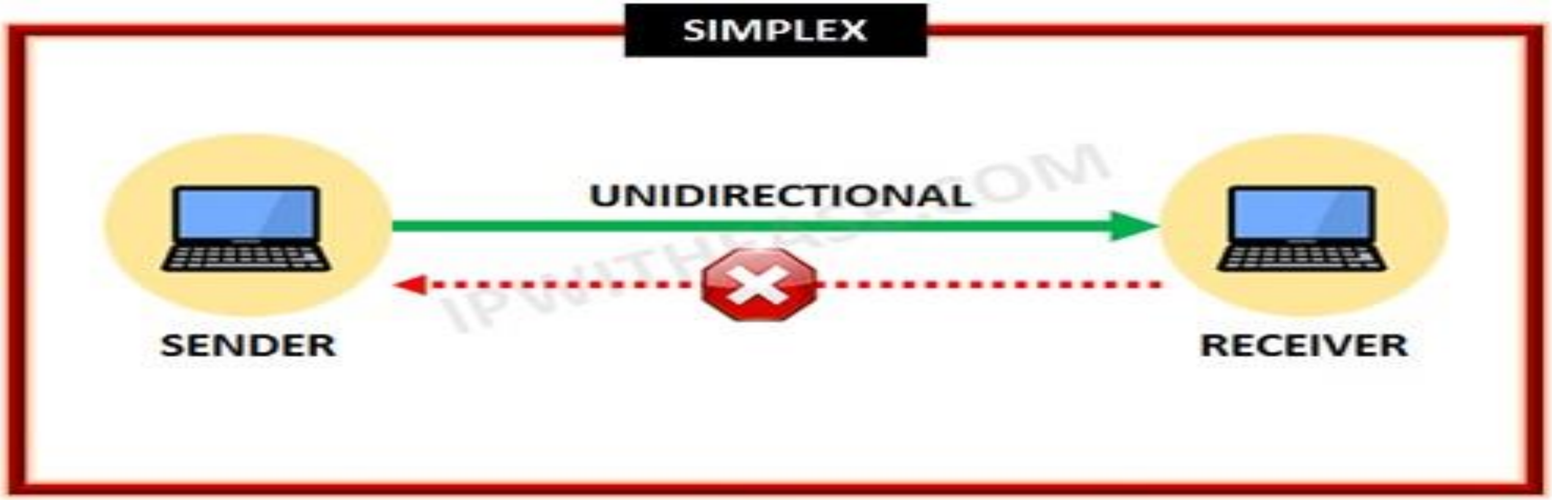
DATA REPRESENTATION

- Numbers
  - 8/16/32 bit integers
  - floating point
- Text
  - ASCII, Unicode
- Images
  - Bit patterns, Graphics formats JPG/GIF/etc.
- Audio → Samples of continuous signal
- Video → Sequence of bitmap images

DIRECTION OF DATA FLOW

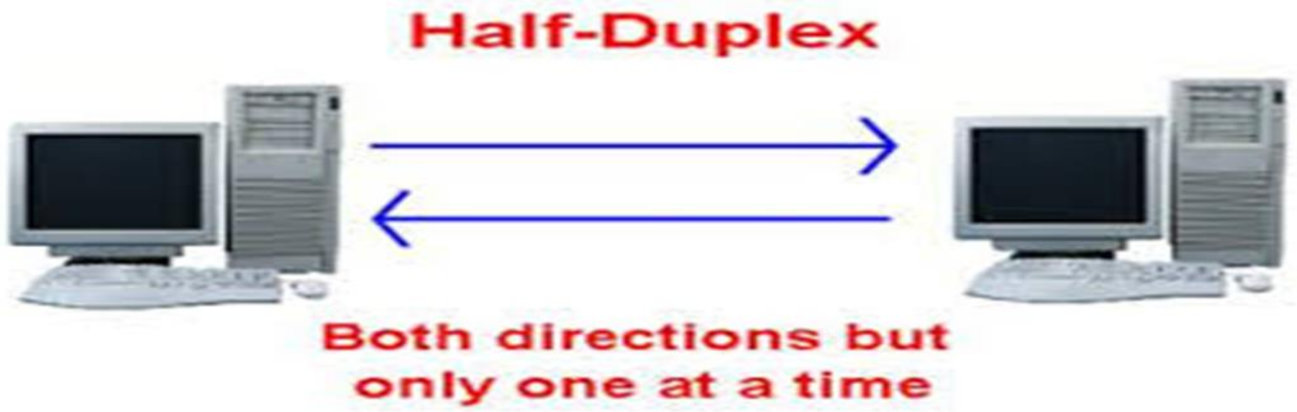


1. Simplex mode: One direction only

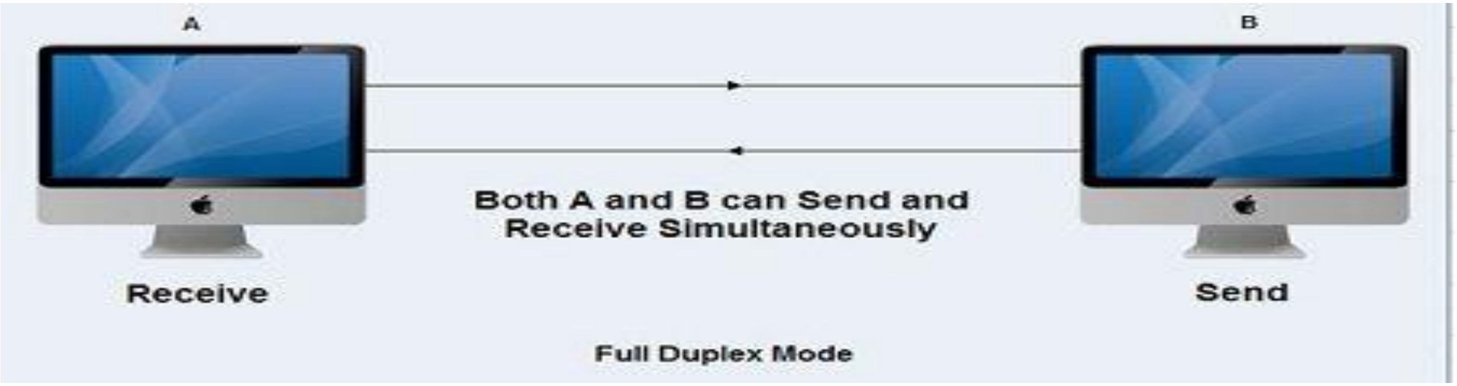


DIRECTION OF DATA FLOW (contd…)

2) Half-duplex: Both directions, one at a time



3) Full-duplex: Both directions simultaneously



NETWORK DEFINITION

- 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.

PURPOSE OF A NETWORK

The purpose of a network is to share resources.

A resource may be -

- A file
- A folder
- A printer
- A disk drive
- Or just about anything else that exists on a computer.

NETWORK CRITERIA

A network must be able to meet certain criteria, these are mentioned below:

- Performance
- Reliability
- Scalability

Performance

It can be measured in following ways :

- Transit time : It is the time taken to travel a message from one device to another.
- Response time : It is defined as the time elapsed between enquiry and response.

NETWORK CRITERIA (contd…)

Other ways to measure performance are :

- Efficiency of software
- Number of users
- Capability of connected hardware

Reliability

- It decides the frequency at which network failure take place. More the failures are, less is the network's reliability.

NETWORK CRITERIA (contd…)

Security

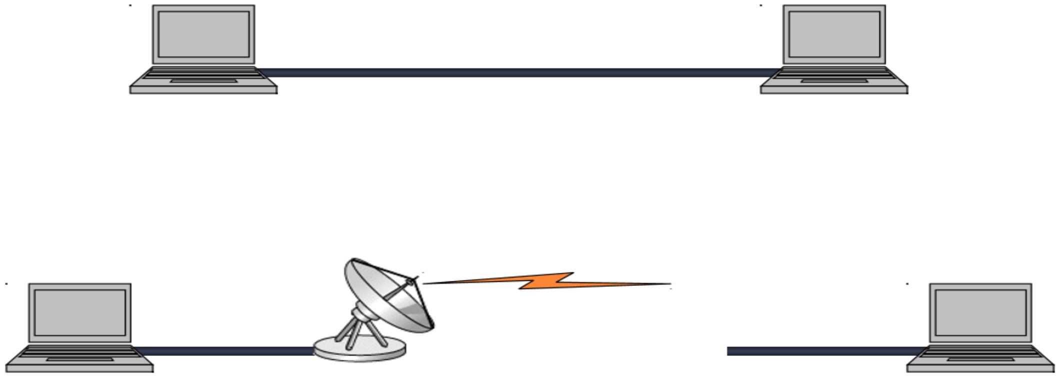
- It refers to the protection of data from the unauthorized user or access. While travelling through network, data passes many layers of network, and data can be traced if attempted. Hence security is also a very important characteristic for networks.

PROPERTIES OF GOOD NETWORK

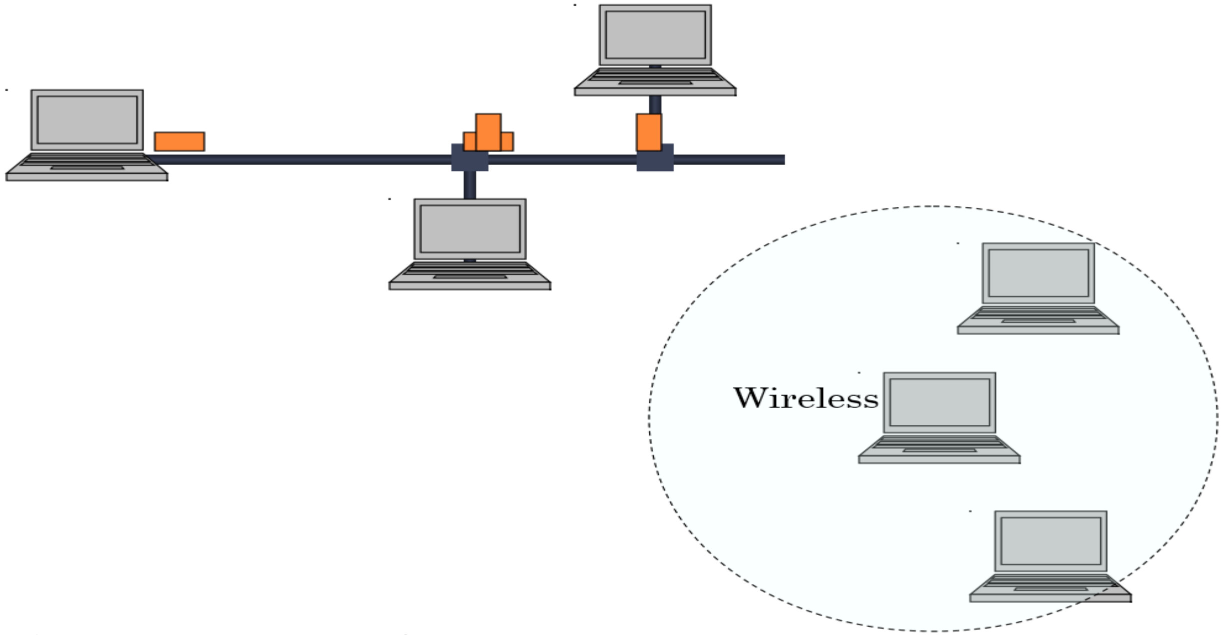
- Interpersonal Communication : We can communicate with each other efficiently and easily example emails, chat rooms, video conferencing etc.
- Resources can be shared : We can use the resources provided by network such as printers etc.
- Sharing files, data : Authorized users are allowed to share the files on the network.

TYPES OF CONNECTIONS

- Point-to-point-Dedicated link



- Multipoint (Timeshared)-Shares a single link



ADVANTAGES OF NETWORKING

- Connectivity and Communication
- Data Sharing
- Hardware Sharing
- Internet Access
- Internet Access Sharing
- Data Security and Management
- Entertainment

THE DISADVANTAGES OF NETWORKING

- Network Hardware, Software and Setup Costs
- Hardware and Software Management and Administration Costs
- Undesirable Sharing
- Illegal or Undesirable Behaviour
- Data Security Concerns

NETWORK TYPES

LOCAL AREA NETWORK (LAN)

- A LAN is a computer network that spans a relatively small area.
- A LAN is usually privately owned and connects some hosts in a single office, building, or campus.
- Each host in a LAN has an identifier, an address that uniquely defines the host in the LAN. A packet sent by a host to another host carries both the source host's and the destination host's addresses.
- Examples of LAN: Home Network, Office Network, Personal Network .

NETWORK TYPES (contd…)

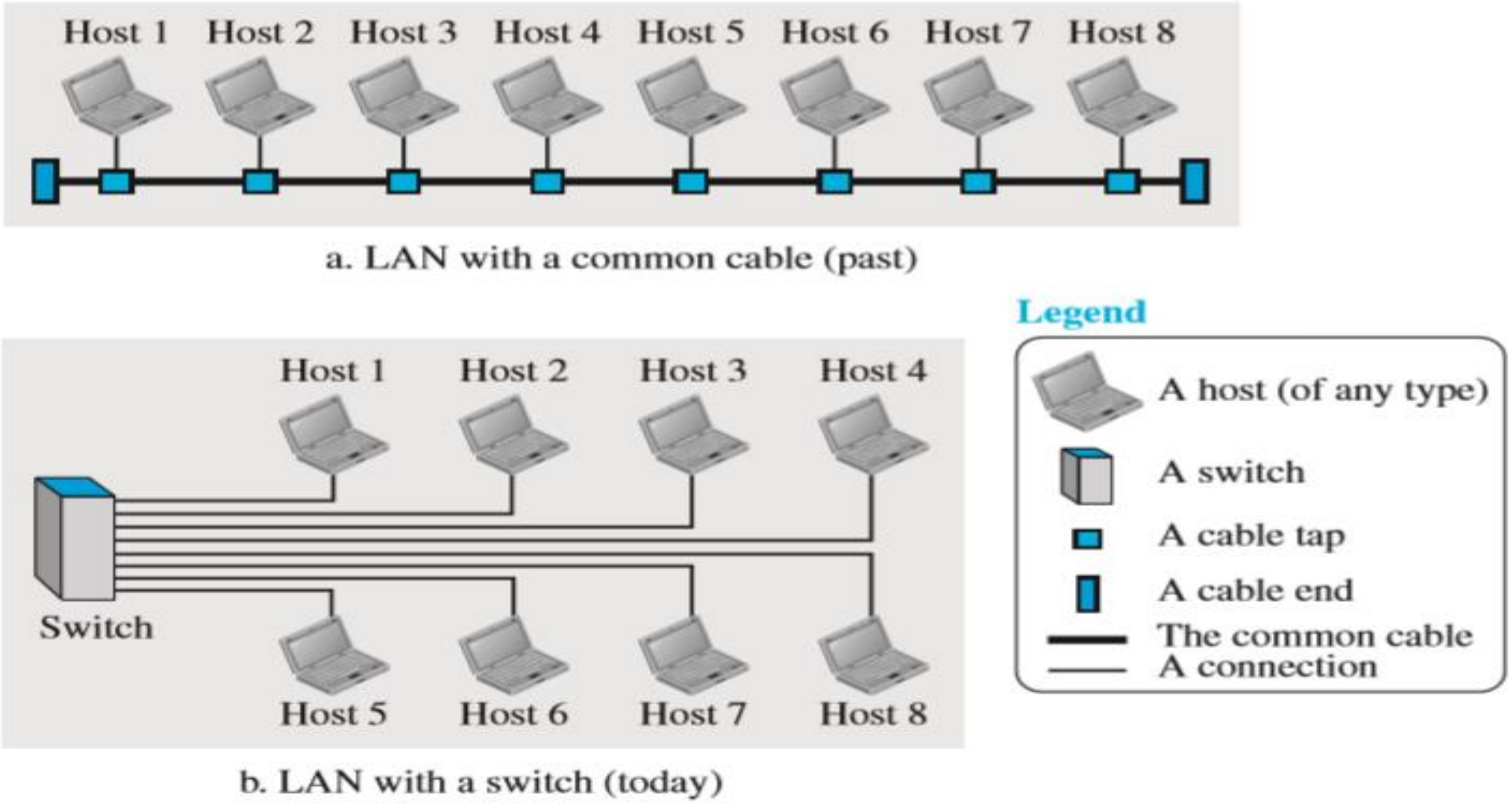


Fig. : An isolated LAN in the past and today.

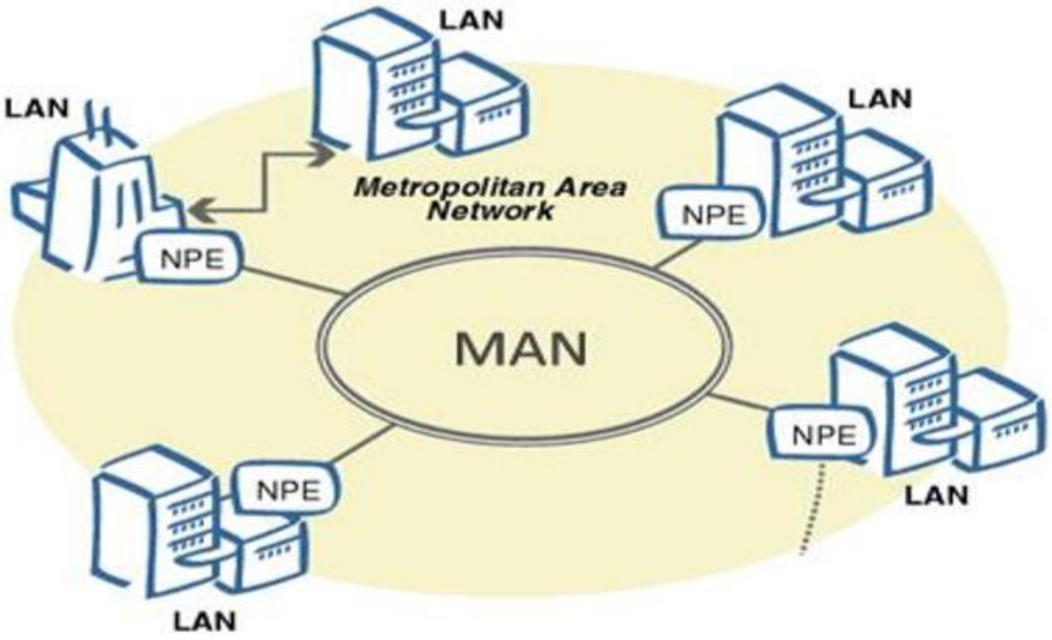
NETWORK TYPES (contd…)

METROPOLITAN AREA NETWORK (MAN)

- A MAN is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).
- It is also used to mean the interconnection of several local area networks by bridging them with backbone lines.
- The working mechanism of a MAN is similar to an Internet Service Provider (ISP), but a MAN is not owned by a single organization. Like a WAN, a MAN provides shared network connections to its users.

NETWORK TYPES (contd…)

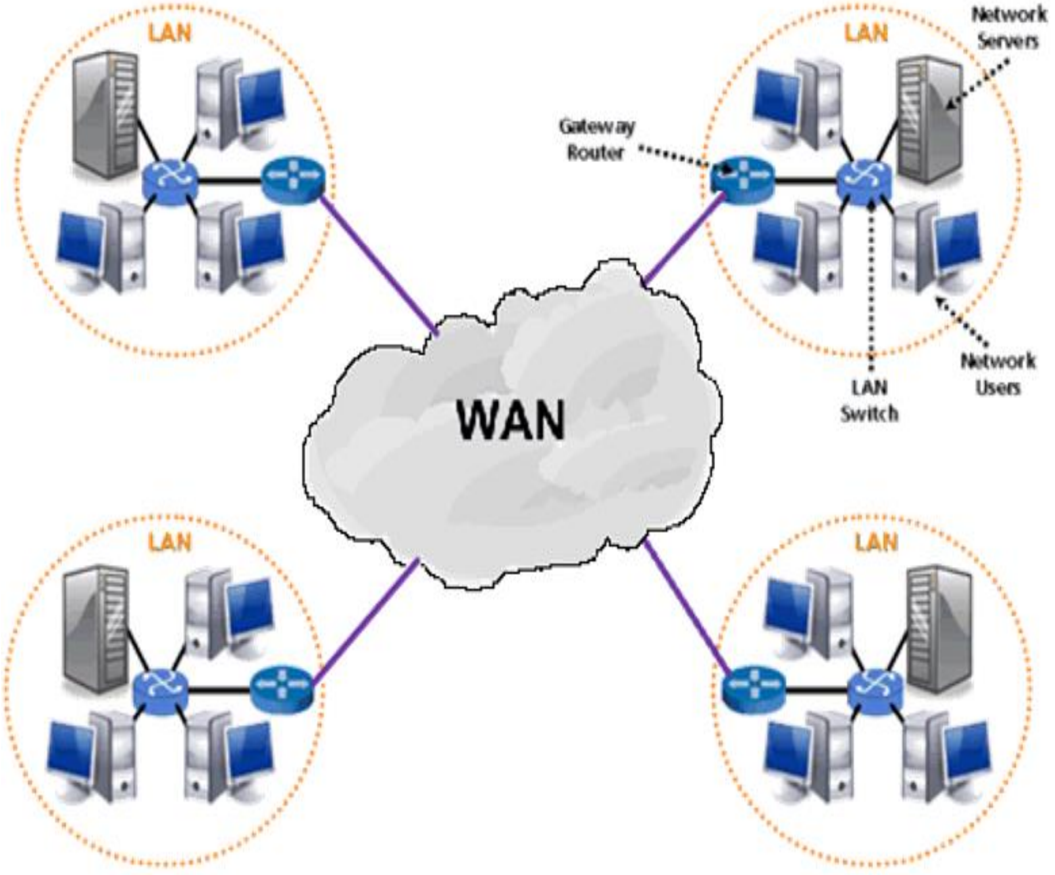
- A MAN mostly works on the data link layer, which is Layer 2 of the Open Systems Interconnection (OSI) model.



NETWORK TYPES (contd…)

WIDE AREA NETWORK (WAN)

- A WAN is a network that exists over a large-scale geographical area. A WAN connects different smaller networks, local area networks (LANs) and metro area networks (MANs).
- A WAN interconnects connecting devices such as switches, routers, or modems.

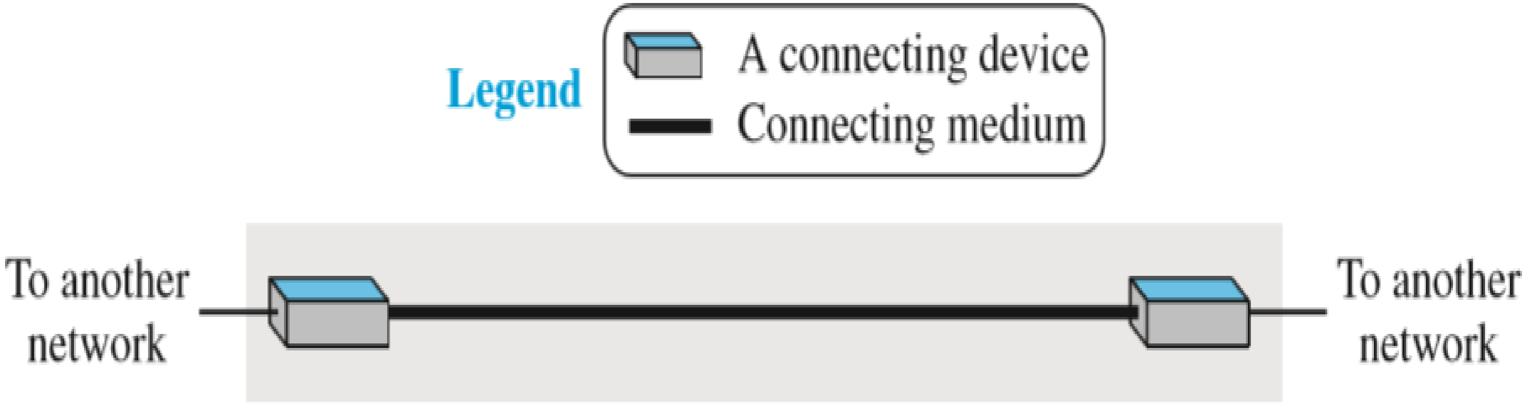


WIDE AREA NETWORK (contd…)

Two distinct examples of WANs today are -

1) <u>Point-to-Point WAN</u>

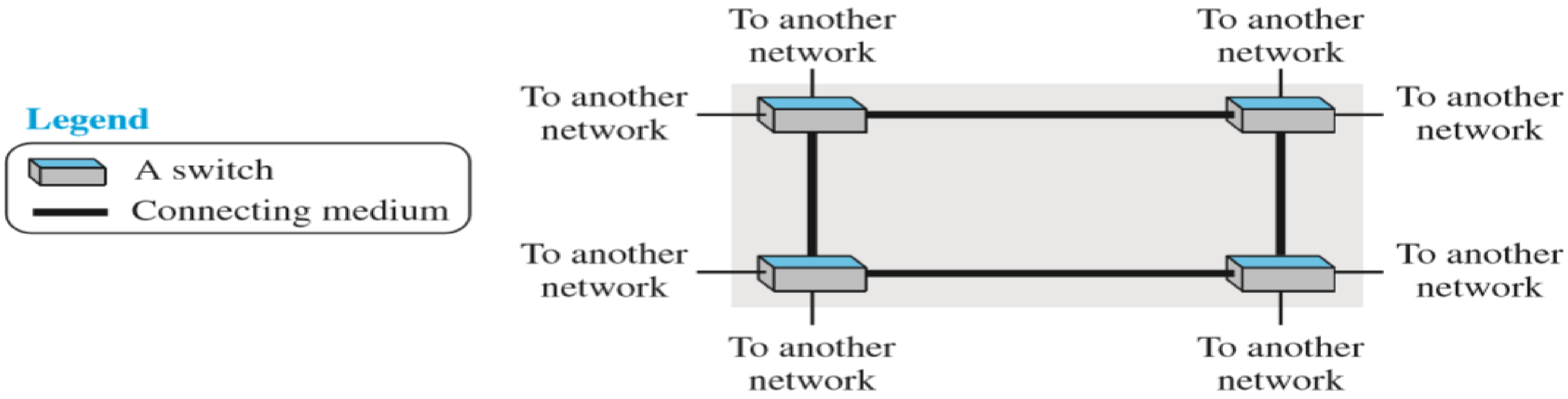
- A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air).



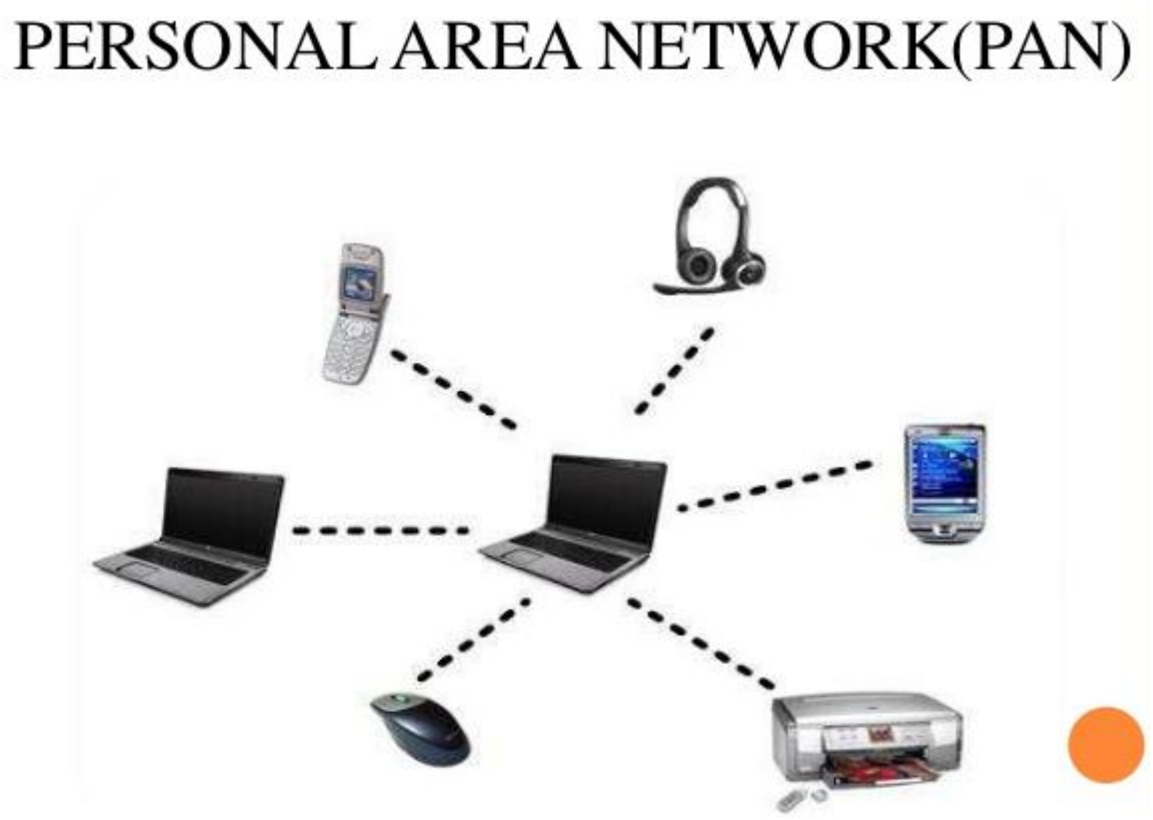
WIDE AREA NETWORK (contd…)

2) Switched WAN

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



NETWORK TYPES (contd…)



PERSONAL AREA NETWORK(PAN)

NETWORK TYPES(contd…)

Personal area network (PAN)

- PAN is a computer network for interconnecting devices centered on an individual person's workspace. A PAN provides data transmission among devices such as computers, smartphones, tablets and personal digital assistants.
- PANs can be used for communication among the personal devices themselves, or for connecting to a higher-level network and the Internet where one master device takes up the role as gateway. A PAN may be wireless or carried over wired interfaces such as USB.
- PAN is the interconnection of information technology devices within the range of an individual person, typically within a range of 10 meters.

NETWORK TYPES(contd…)

Wireless personal area network (WPAN)

- It is virtually a synonym since almost any personal area network would need to function wirelessly.

- Conceptually, the difference between a PAN and a wireless LAN is that the former tends to be centered around one person while the latter is a local area network (LAN) that is connected without wires and serving multiple users.

NETWORK TYPES (contd…)

Internetwork

- When two or more networks are connected, they make an internetwork, or internet.

- 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.

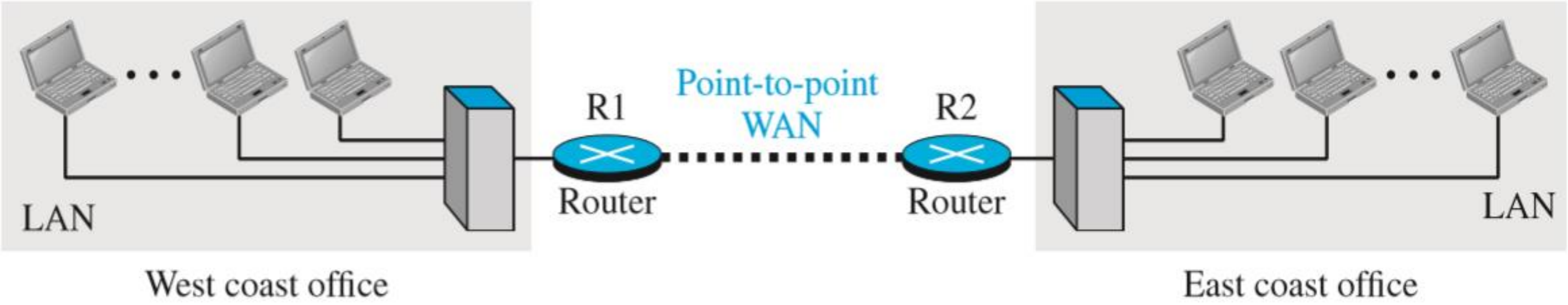


Fig. : An internetwork made of two LANs and one point-to-point WAN

NETWORK TERMS- HOST, WORKSTATIONS, SERVER, CLIENT, NODE

Host

A network host is a computer or other device connected to a computer network. A network host may offer information resources, services, and applications to users or other nodes on the network. A network host is a network node that is assigned a network layer host address

Workstations

A workstation is a special computer designed for technical or scientific applications. Intended primarily to be used by one person at a time, they are commonly connected to a local area network and run multi-user operating systems.

NETWORK TERMS - HOST, WORKSTATIONS, SERVER, CLIENT, NODE (contd…)

Server

computer is a core component of the network, providing a link to the resources necessary to perform any task.

Client

computers normally request and receive information over the network client. Client computers also depends primarily on the central server for processing activities

TYPES OF NETWORK ARCHITECTURE

TYPES OF NETWORK ARCHITECTURE

1) PEER-TO-PEER NETWORK -

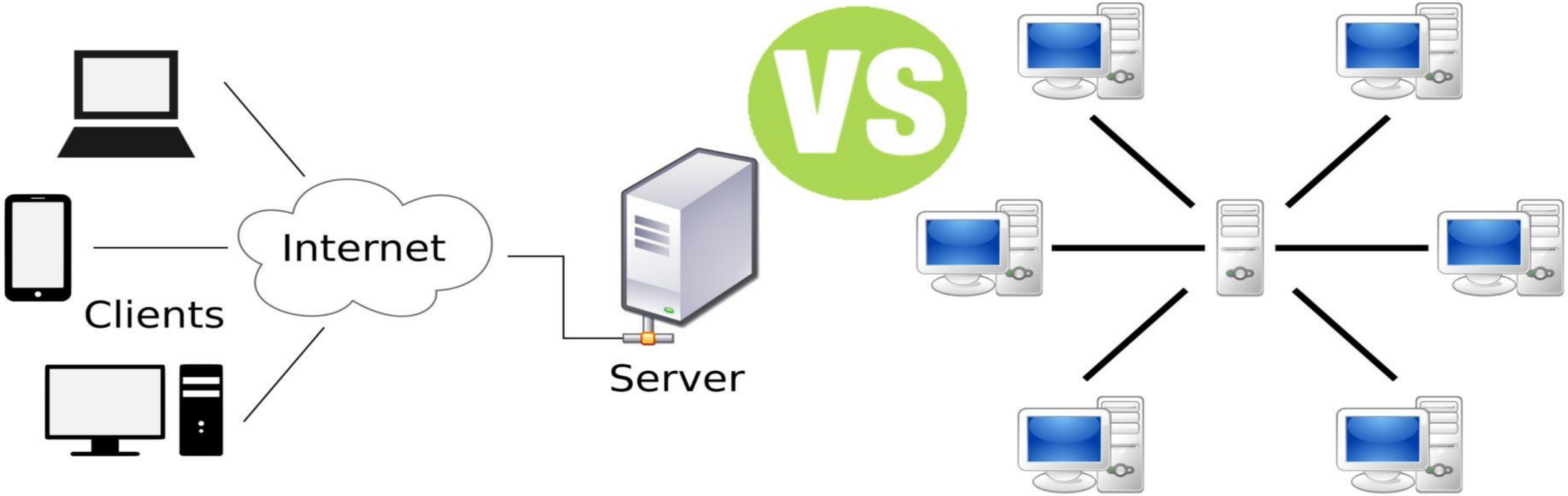
- Good for small environments, usually up to 10 computers
- No dedicated network administrator
- Each computer must have specific permissions assigned
- Sharing resources can become a problem if the computer with the resource is down
- Security is a serious issue

TYPES OF NETWORK ARCHITECTUR (contd…)

2) CLIENT/SERVER NETWORK –

- A server has a special Network Operating system (NOS) to help provide resources to multiple users
- Client/Server environments usually have one or more network administrators
- Problems can include access, security, and integrity of data
- Backups are needed in this environment

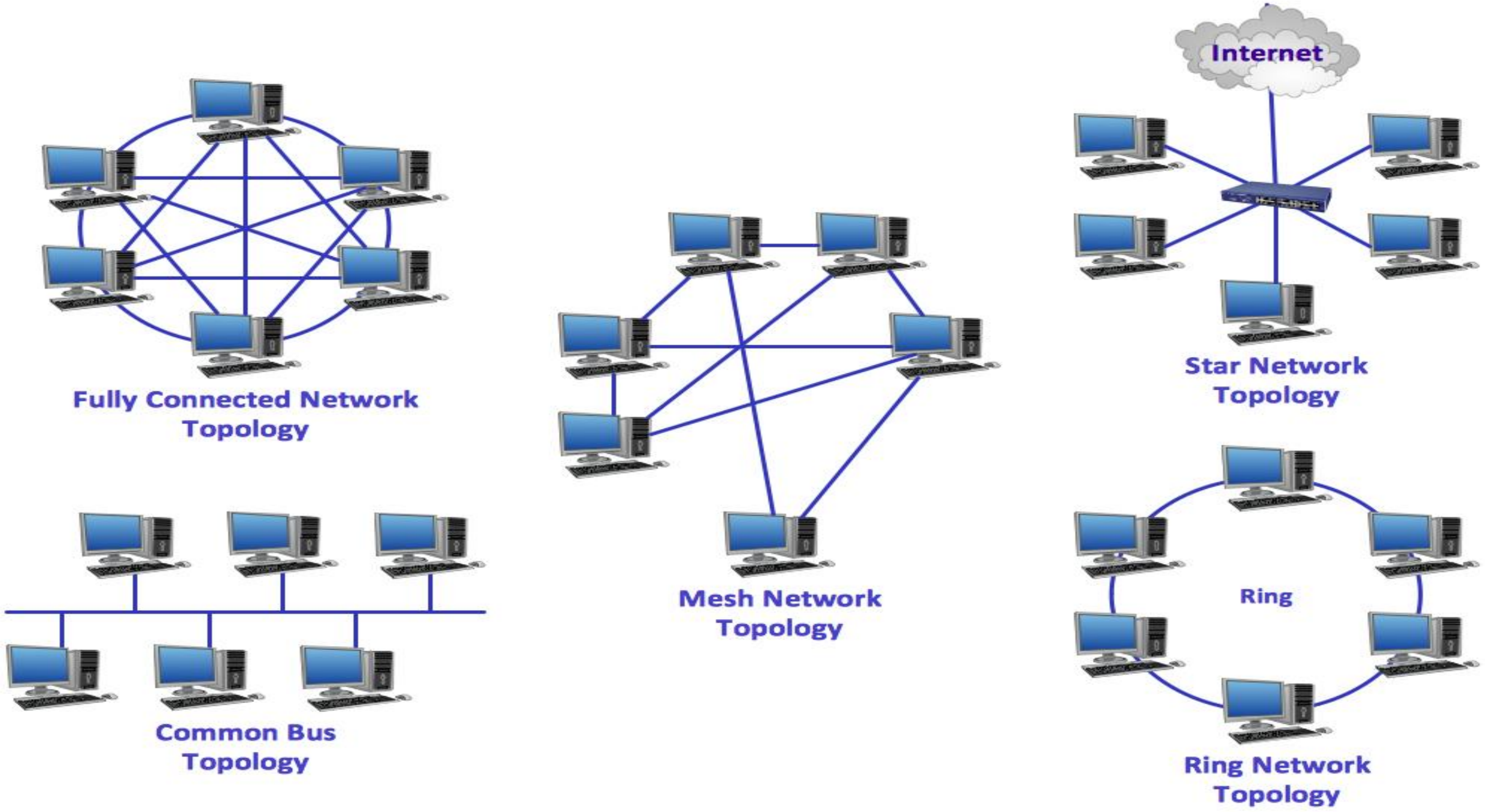
DIFFERENCE BETWEEN CLIENT SERVER NETWORK AND PEER TO PEER NETWORK



NETWORK TOPOLOGY

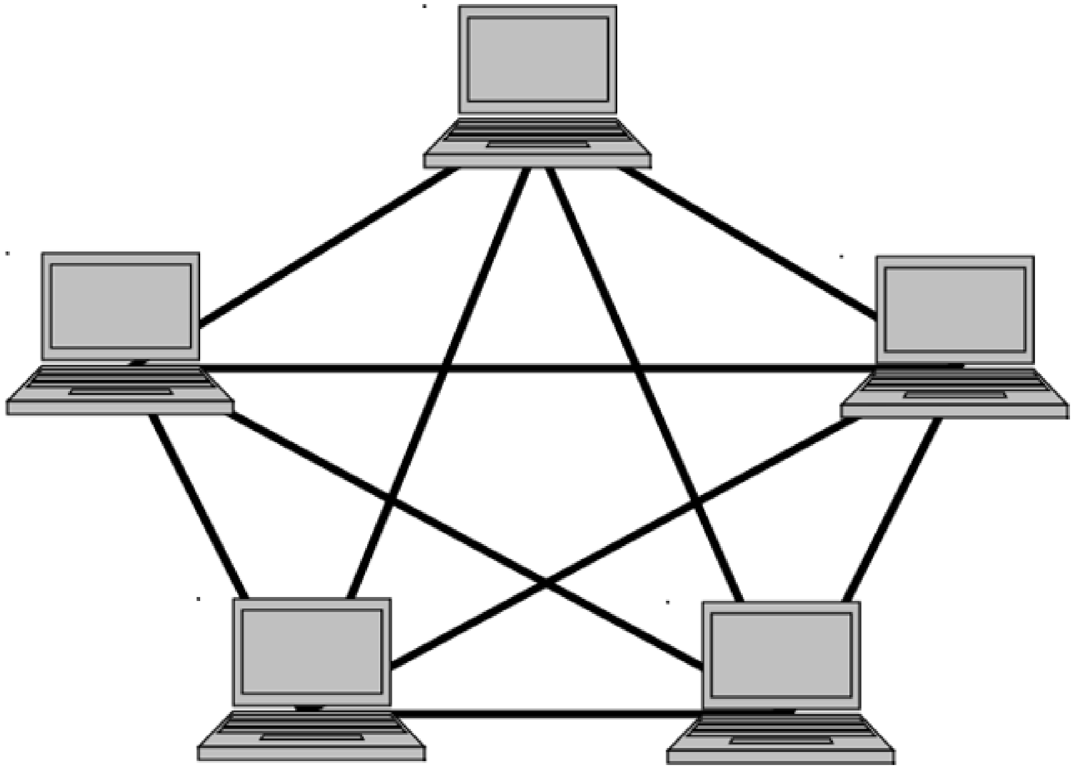
- A topology is a way of “laying out” the network. Topologies can be either physical or logical.
- Physical topologies describe how the cables are run.
- Logical topologies describe how the network messages travel.

TYPES OF TOPOLOGY



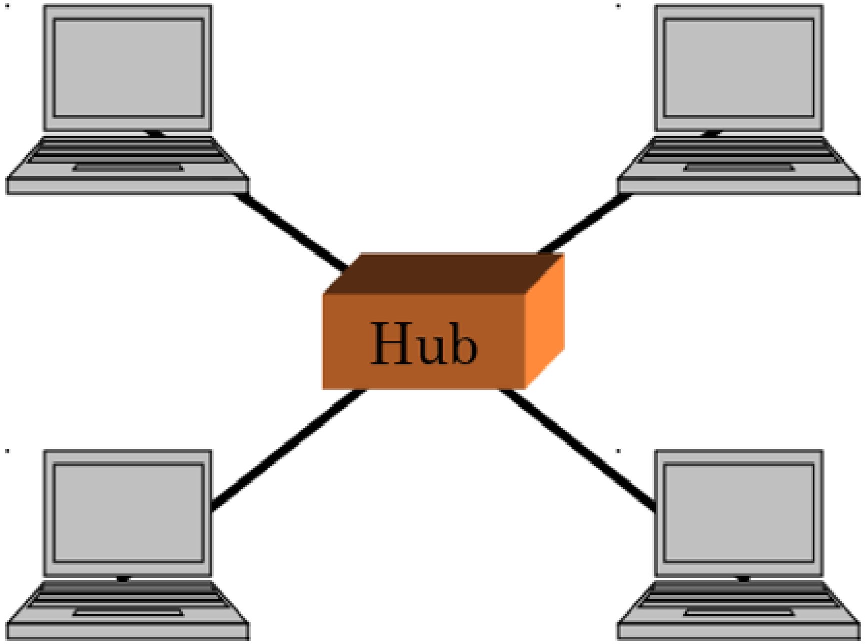
FULLY CONNECTED MESH TOPOLOGY

- Pros:
  - Dedicated links
  - Robustness
  - Privacy
  - Easy to identify fault
- Cons:
  - A lot of cabling
  - I/O ports
  - Difficult to remove



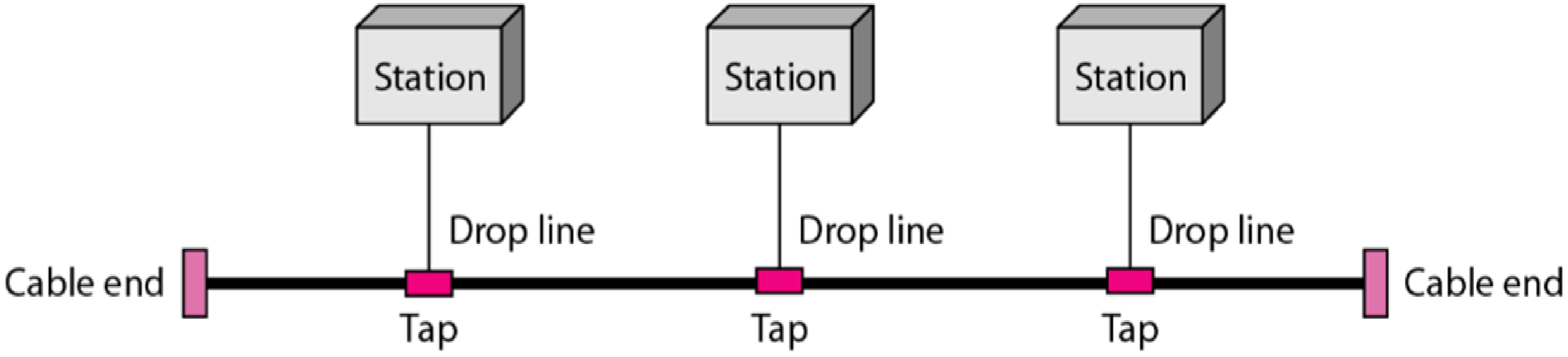
STAR TOPOLOGY

- Pros:
  - One I/O port per device
  - Little cabling
  - Easy to install
  - Robustness
  - Easy to identify fault
- Cons:
  - Single point of failure
  - More cabling still required

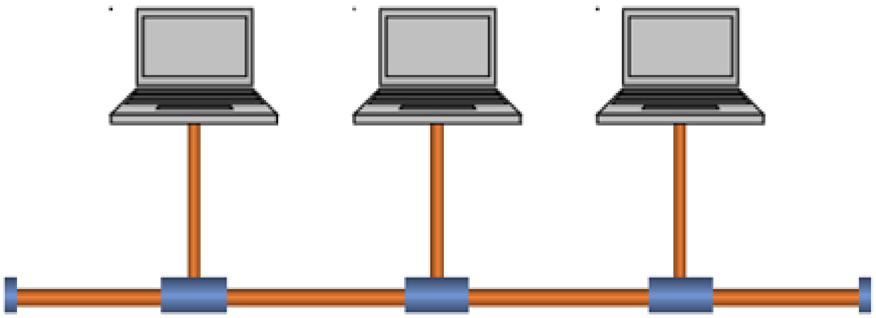


BUS TOPOLOGY

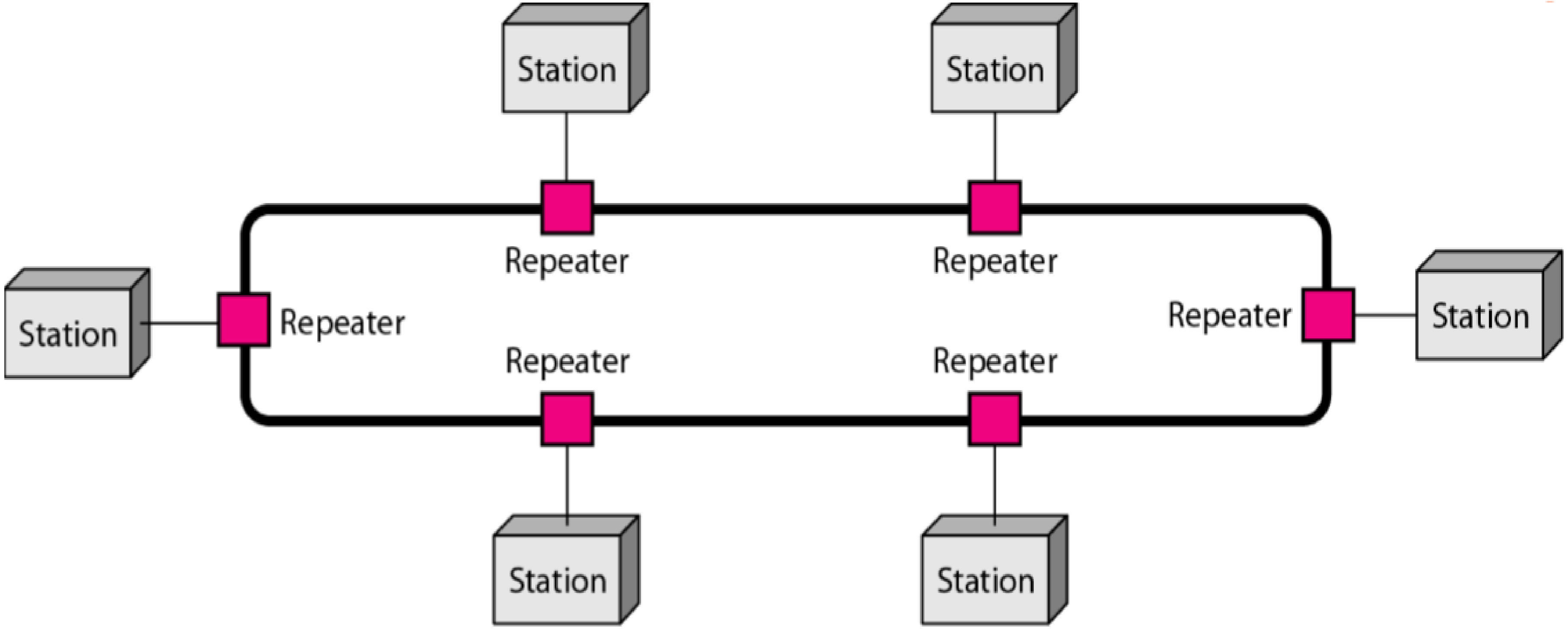
- Pros:
  - Little cabling
  - Easy to install



- Cons:
  - Difficult to modify
  - Difficult to isolate fault
  - Break in the bus cable stops all transmission

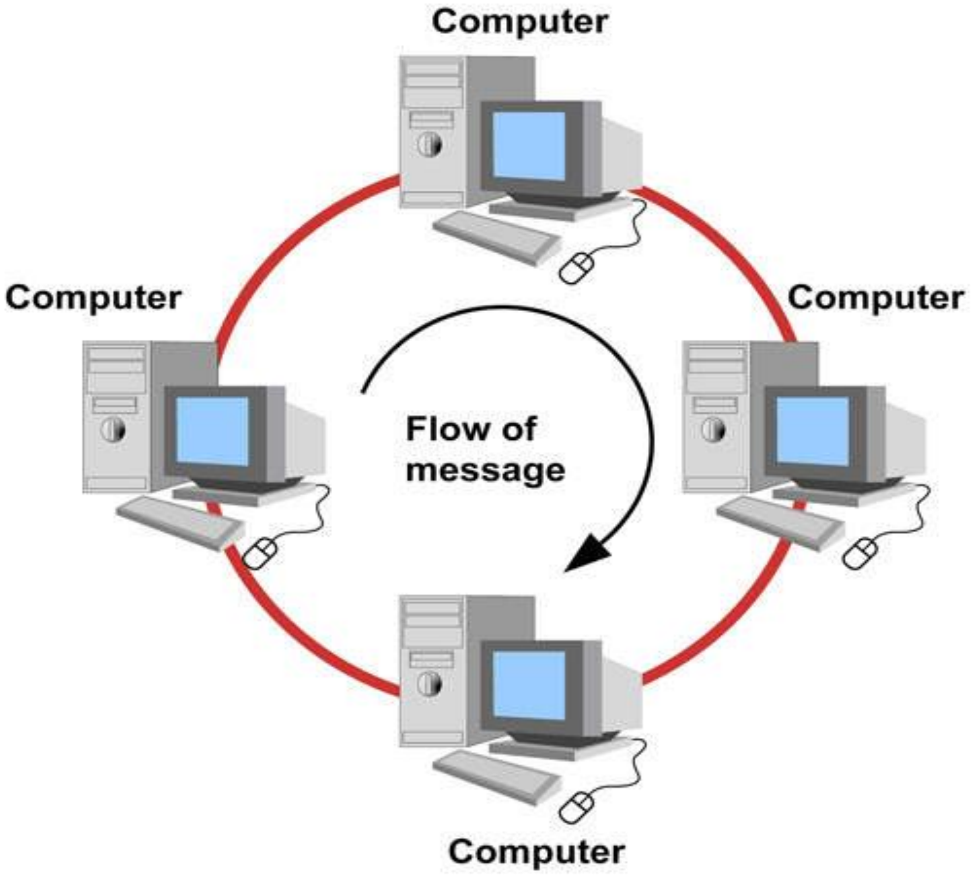


RING TOPOLOGY

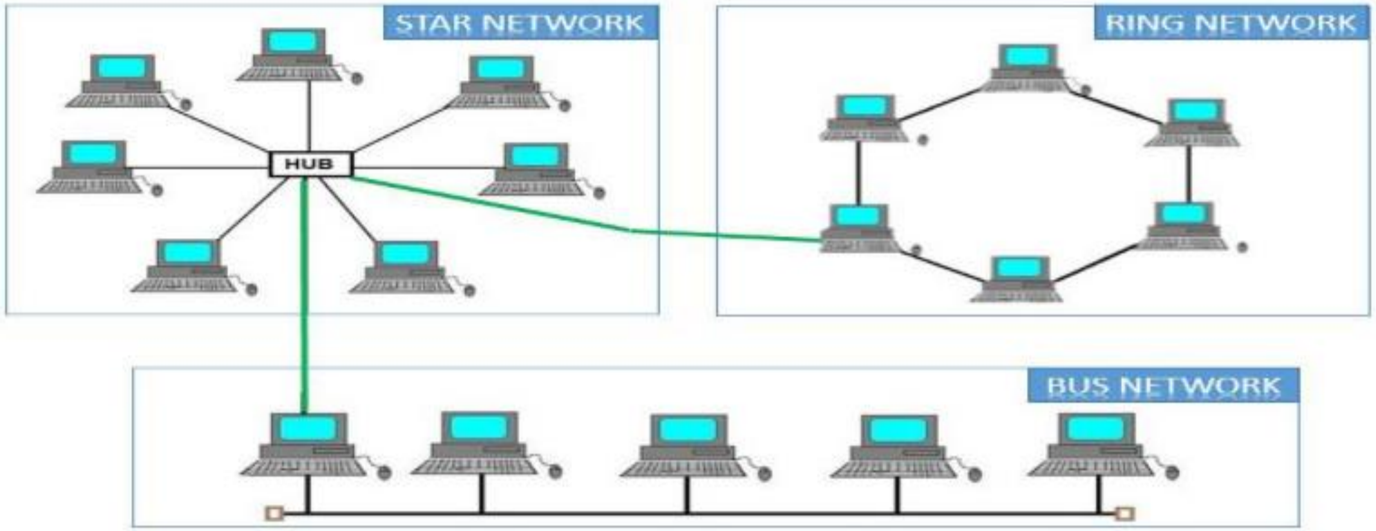


RING TOPOLOGY (contd…)

- Pros:
  - Easy to install
  - Easy to identify fault
- Cons:
  - Delay in large ring
  - Break in the ring stops all transmission



HYBRID TOPOLOGY



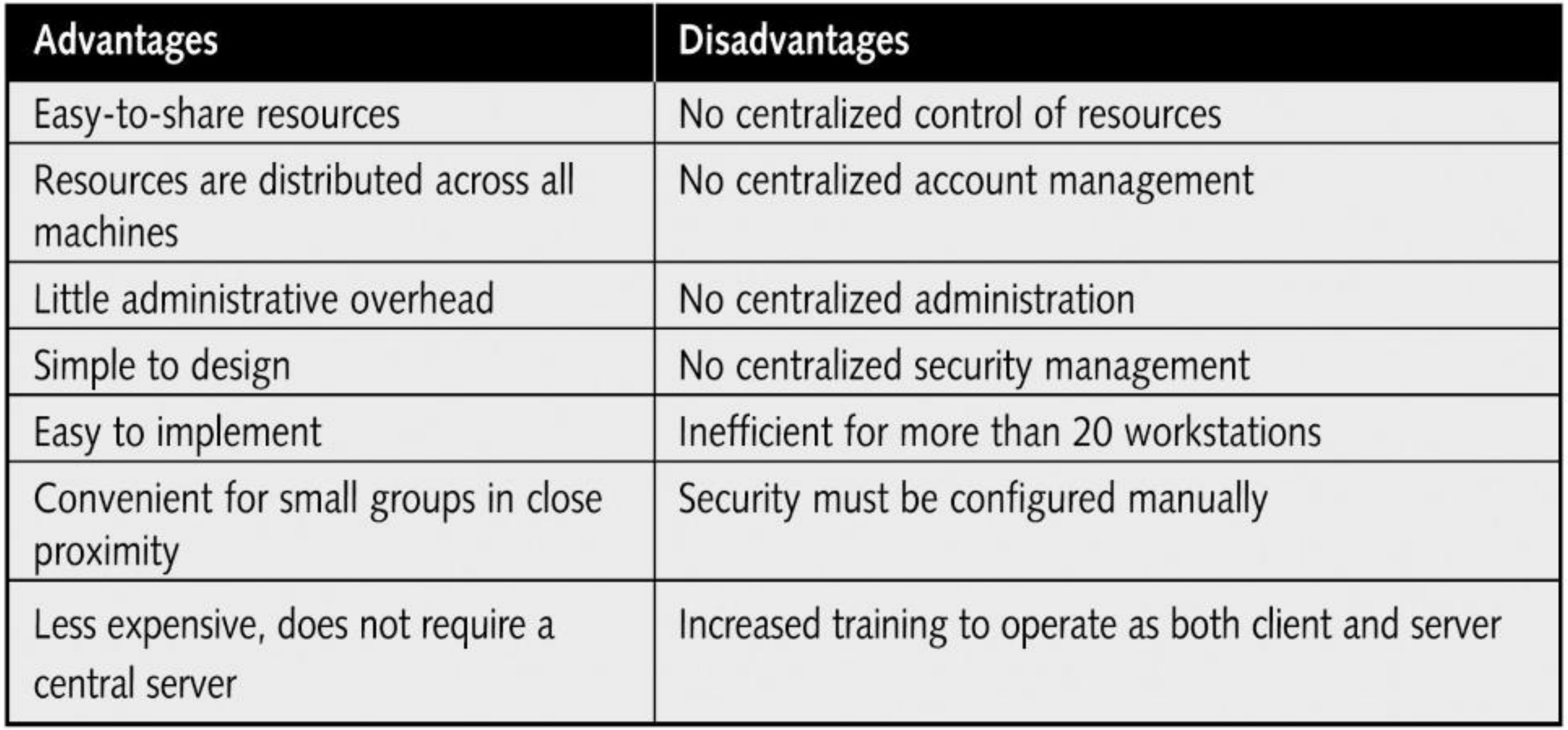
- Pros:
    - Reliable as it has far better fault tolerance
    - Effective
    - Flexible as it can be implemented for a variety of distinct network environment.
- Cons:
    - Complexity- As different topologies connect in a hybrid topology, managing the topology gets challenging.
    - Expensive

WORKGROUP MODEL

- All computers are equal
- Also known as peer-to-peer
- Each computer maintains own set of
  - Resources
  - Accounts
  - Security information

WORKGROUP MODEL (contd…)

Table 1-1 Advantages and disadvantages of workgroup networks



Advantages	Disadvantages
Easy-to-share resources	No centralized control of resources
Resources are distributed across all machines	No centralized account management
Little administrative overhead	No centralized administration
Simple to design	No centralized security management
Easy to implement	Inefficient for more than 20 workstations
Convenient for small groups in close proximity	Security must be configured manually
Less expensive, does not require a central server	Increased training to operate as both client and server

DOMAIN MODEL

- Centralizes all shared resources
- Single point of administrative and security control
- Simpler to manage from administrative and security standpoint
- Requires at least one domain controller (DC)

DOMAIN MODEL(contd…)

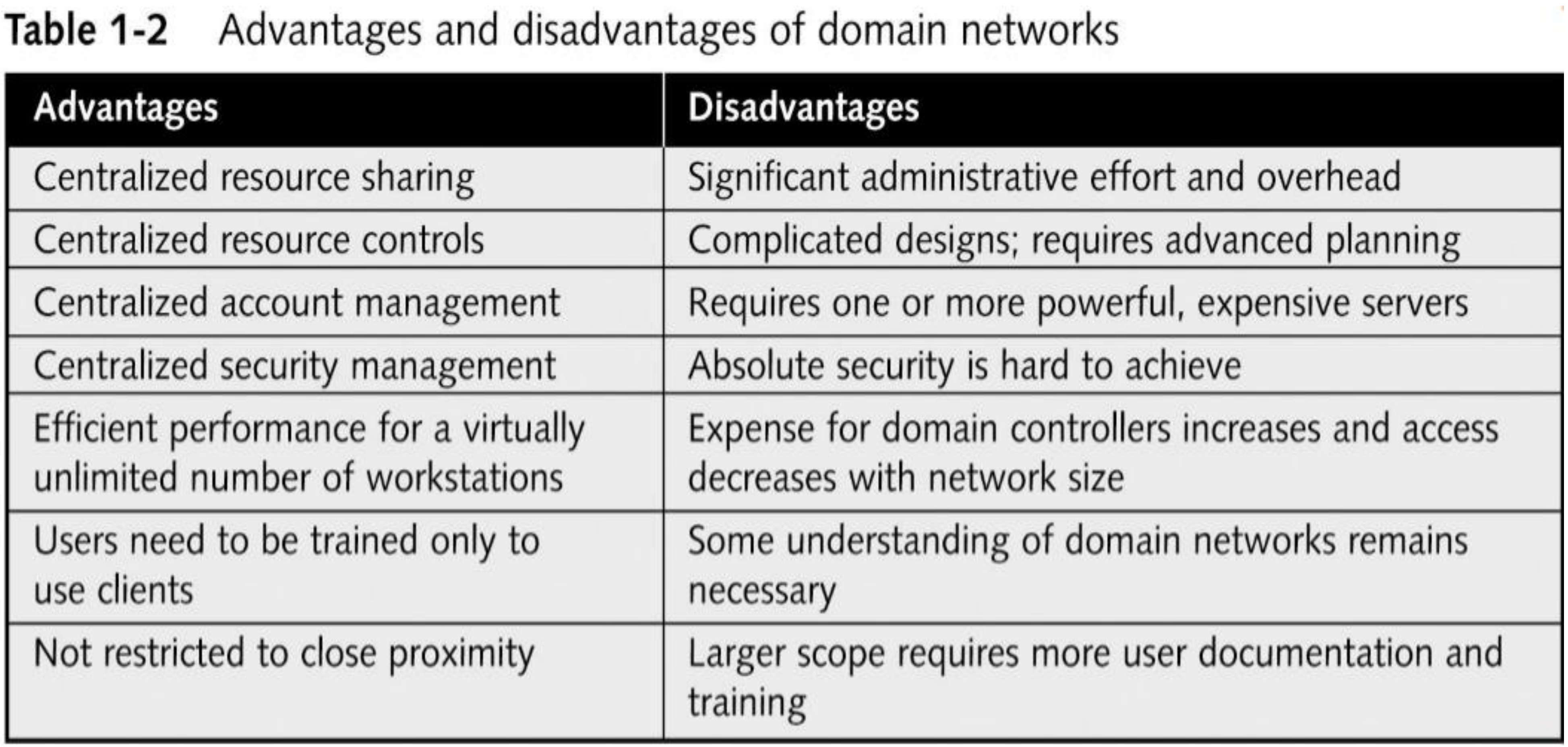


Table 1-2 Advantages and disadvantages of domain networks

Advantages	Disadvantages
Centralized resource sharing	Significant administrative effort and overhead
Centralized resource controls	Complicated designs; requires advanced planning
Centralized account management	Requires one or more powerful, expensive servers
Centralized security management	Absolute security is hard to achieve
Efficient performance for a virtually unlimited number of workstations	Expense for domain controllers increases and access decreases with network size
Users need to be trained only to use clients	Some understanding of domain networks remains necessary
Not restricted to close proximity	Larger scope requires more user documentation and training

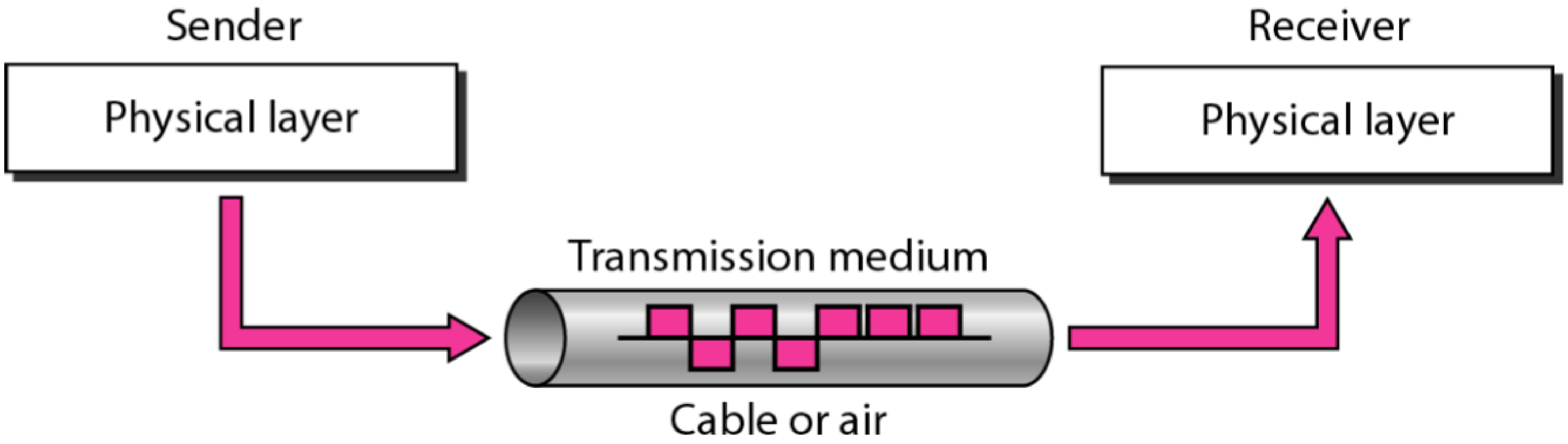
WORKGROUP Vs DOMAIN

- Workgroup
  - Peer-to-Peer Environment
    - Effective for small environments
    - Security is a problem

- Domain
  - Client/Server Environment
    - Effective for larger environments
    - Network administrator has control

TRANSMISSION MEDIA/COMMUNICATION MODES

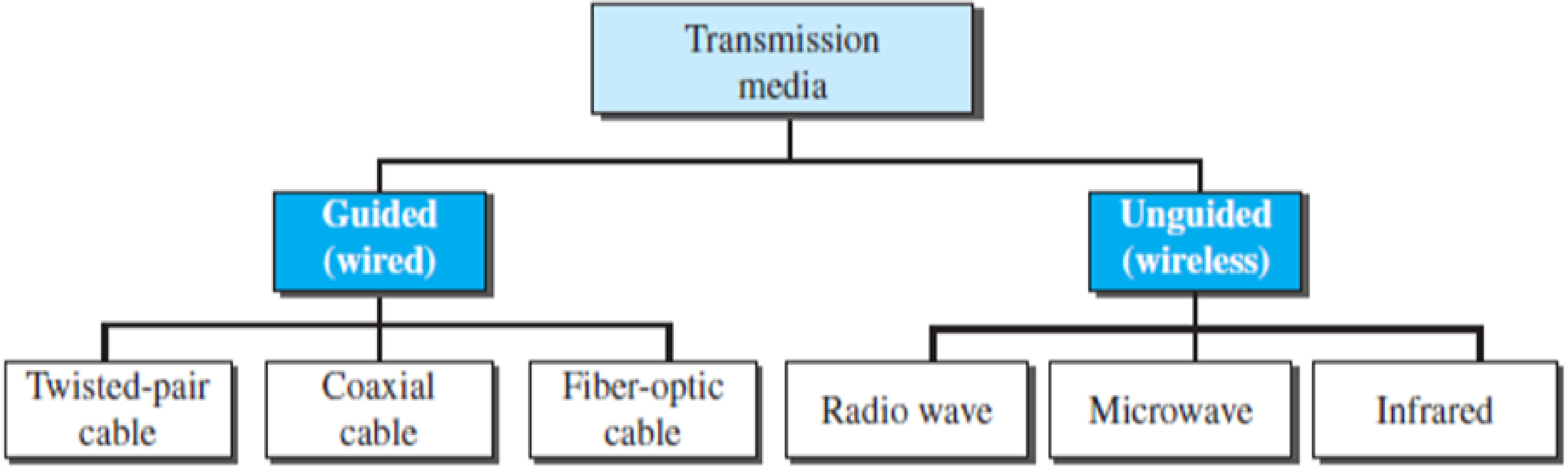
- Transmission media are located below the physical layer.
- Computers use signals to represent data.
- Signals are transmitted in form of electromagnetic energy.



TRANSMISSION MEDIA (contd…)

In telecommunications, transmission media can be divided into two broad categories: guided and unguided.

- Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable.
- Unguided medium is free space.



FACTORS TO BE CONSIDERED WHILE CHOOSING TRANSMISSION MEDIUM

- Transmission Rate
- Cost and Ease of Installation
- Resistance to Environmental Conditions
- Distances

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

- This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network.
- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown.
- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.
- In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

TWISTED PAIR CABLE (contd…)

- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e.g., one is closer and the other is farther).
- This results in a difference at the receiver. By twisting the pairs, a balance is maintained.
- Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk).
- The unwanted signals are mostly canceled out.

TWISTED PAIR CABLE (contd…)

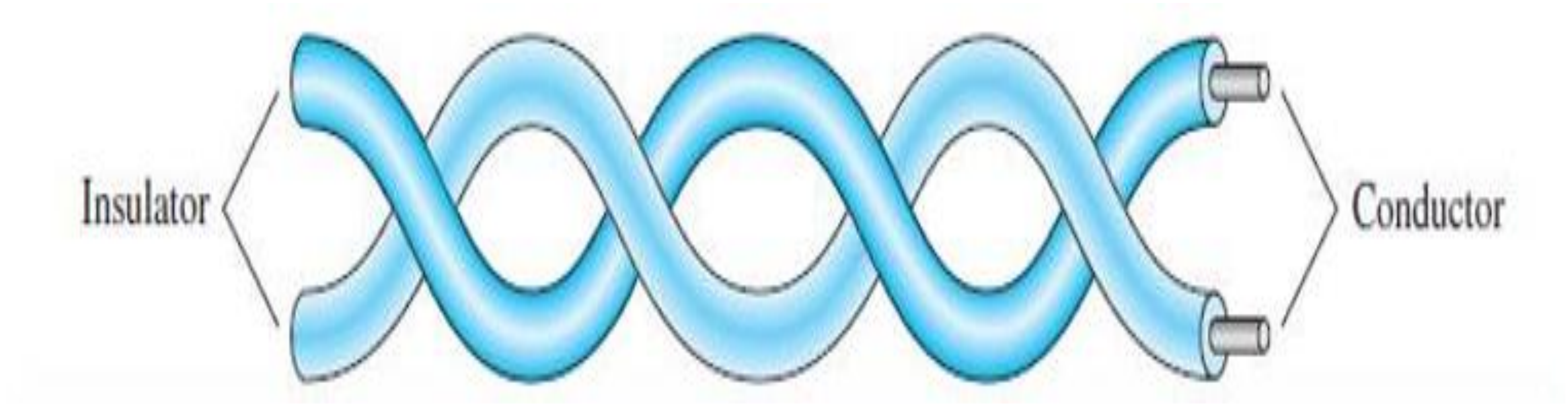
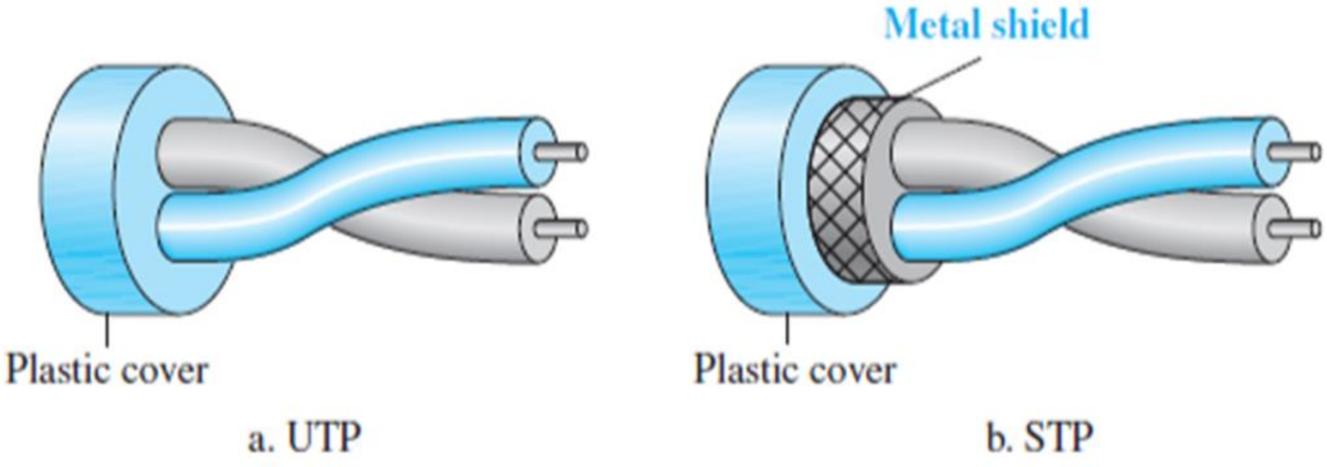


Fig. : Twisted-Pair Cable.

UTP AND STP CABLES

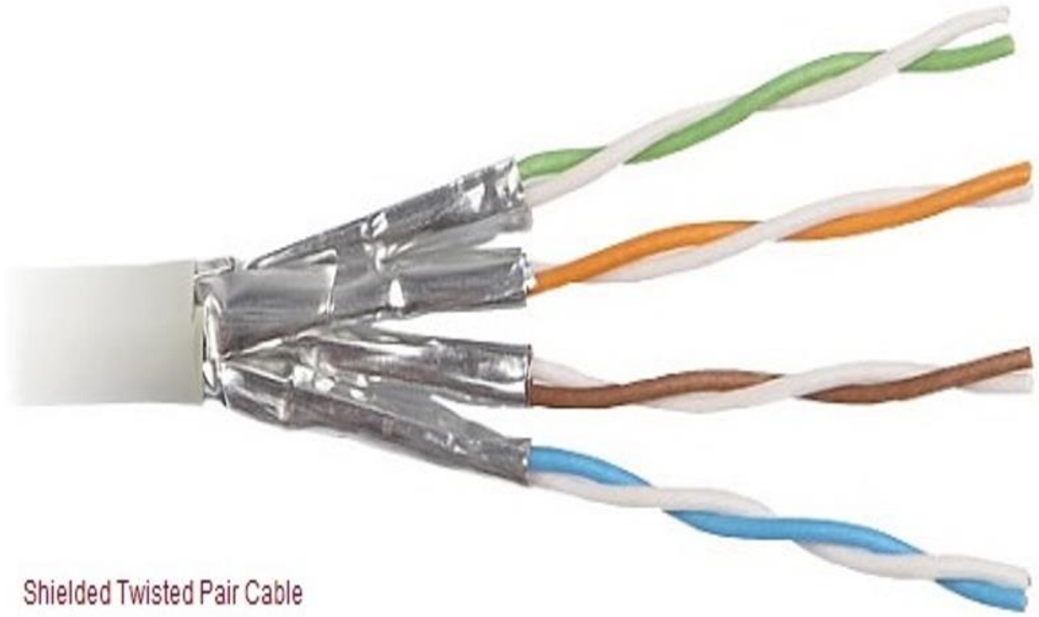
- Twisted Pair is of two types :
- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP) - STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors.



UNSHIELDED TWISTED PAIR (UTP)

Adv:

- Ordinary telephone wire
- Cheapest
- Easiest to install
- It has high speed capacity
- 100 meter limit



Dis adv:

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

SHIELDED TWISTED PAIR (STP)

Advantages:

- Metal braid or sheathing that reduces interference
- Easy to install
- Eliminates crosstalk
- Higher capacity than unshielded twisted pair
- Increases the signaling rate

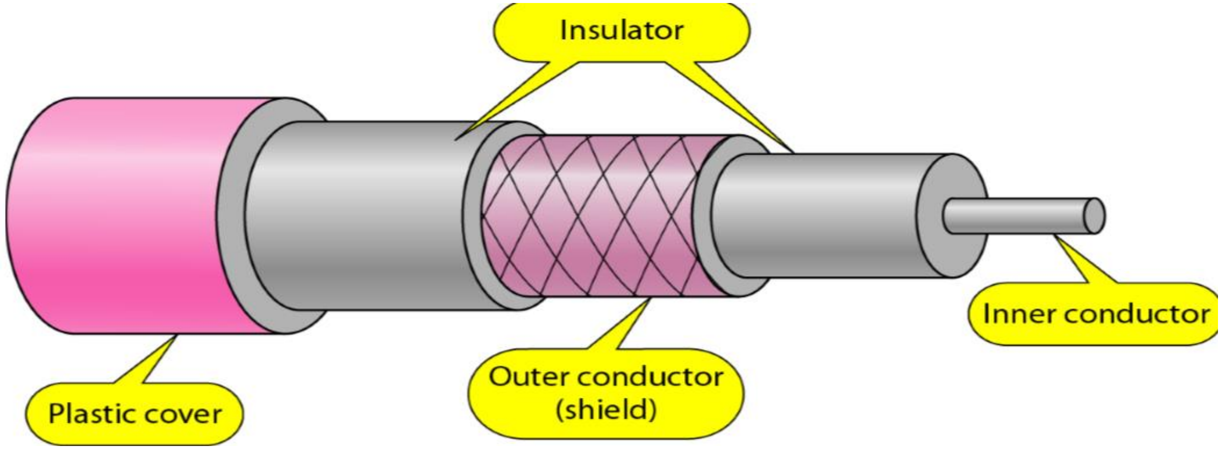
Disadvantages:

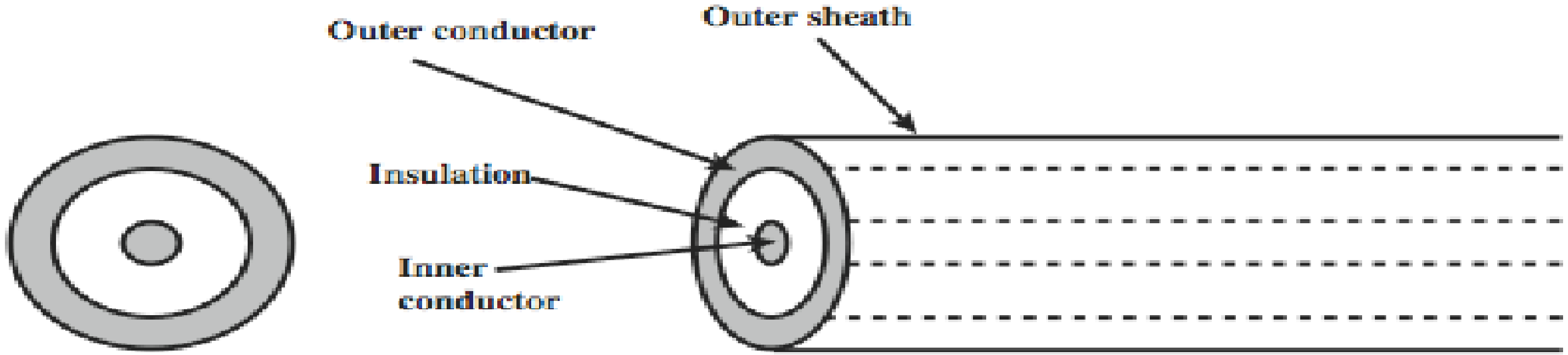
- More expensive
- Harder to handle (thick, heavy)
- Difficult to manufacture

TWISTED PAIR CABLE APPLICATIONS

- Twisted-pair cables are used in telephone lines to provide voice and data channels.
- The local loop—the line that connects subscribers to the central telephone office—commonly consists of unshielded twisted-pair cables.
- The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.
- Local-area networks, such as 10Base-T and 100Base-T, also use twisted-pair cables.

GUIDED MEDIA – COAXIAL CABLE





- Outer conductor is braided shield
- Inner conductor is solid metal
- Separated by insulating material
- Covered by padding

COAXIAL CABLE (contd…)

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently.
- Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.
- Coaxial cables are categorized by their Radio Government (RG) ratings.

TYPES OF COAXIAL CABLES

- Baseband:

Which is used for digital transmission. It is mostly used for LAN’s. Baseband transmits a single signal at a time with very high speed.

- Broadband:

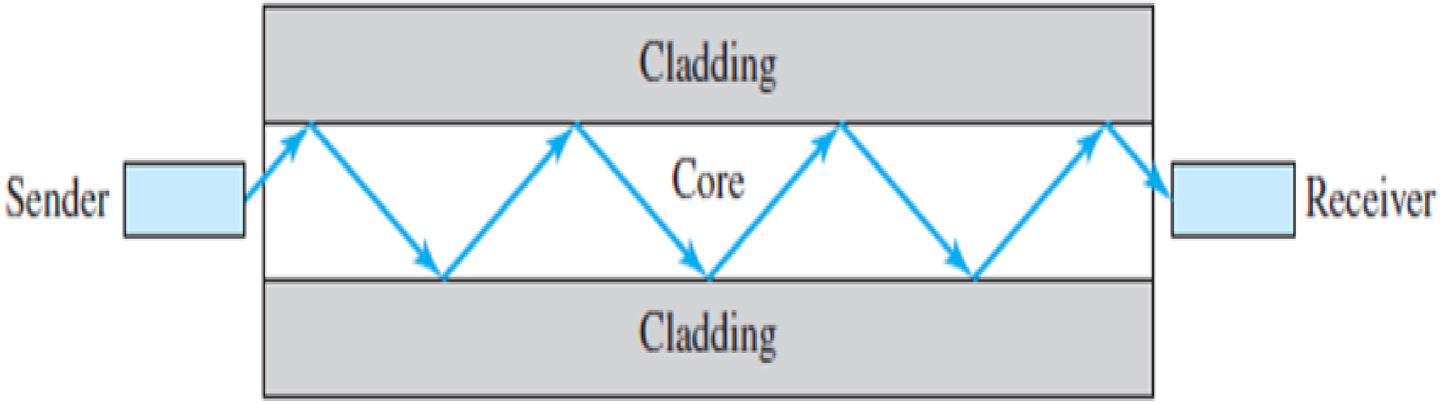
This uses analog transmission on standard cable television cabling It transmits several simultaneous signal using different frequencies.

COAXIAL CABLE (contd…)

Applications

- Analog telephone networks
- Cable TV networks
- Traditional Ethernet LAN – 10Base2, 10Base5

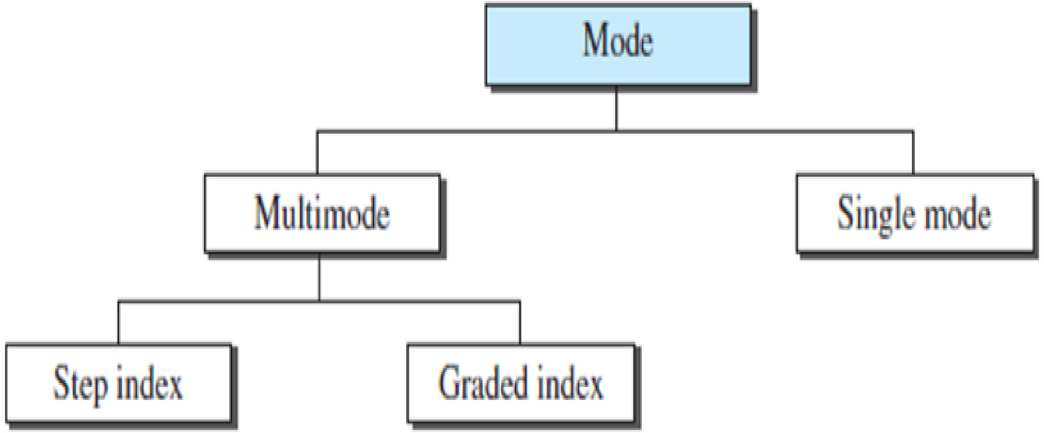
FIBER-OPTIC CABLE



- Higher bandwidth
- Less expensive
- Immune to electrical noise
- More secure – easy to notice an attempt to intercept signal
- Physical characterizes
  - Glass or plastic fibers
  - Very thin (thinner than human hair)
  - Material is light

FIBER-OPTIC CABLE (contd…)

Propagation modes



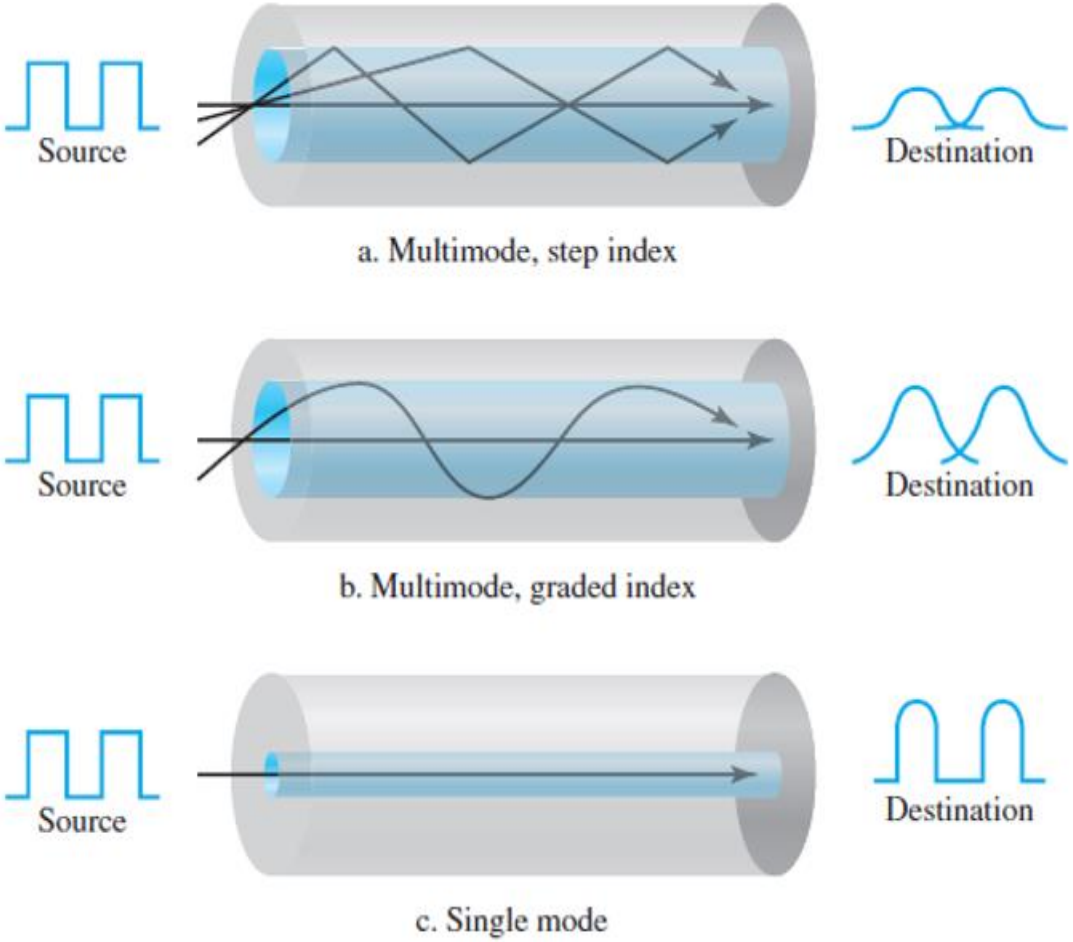
Mode

Multimode

Single mode

Step index

Graded index



a. Multimode, step index

b. Multimode, graded index

c. Single mode

FIBER-OPTIC CABLE (contd…)

- 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. Multimode graded-index fiber, decreases this distortion of the signal through the cable. The word index here refers to the index of refraction. Density is highest at the center of the core and decreases gradually to its lowest at the edge.
- 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. The single-mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density (index of refraction). The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal.

ADVANTAGES AND DISADVANTAGES OF OPTICAL FIBER

Advantages:

- Higher bandwidth
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials
- Light weight
- Greater immunity to tapping

ADVANTAGES AND DISADVANTAGES OF OPTICAL FIBER (contd…)

Disadvantages:

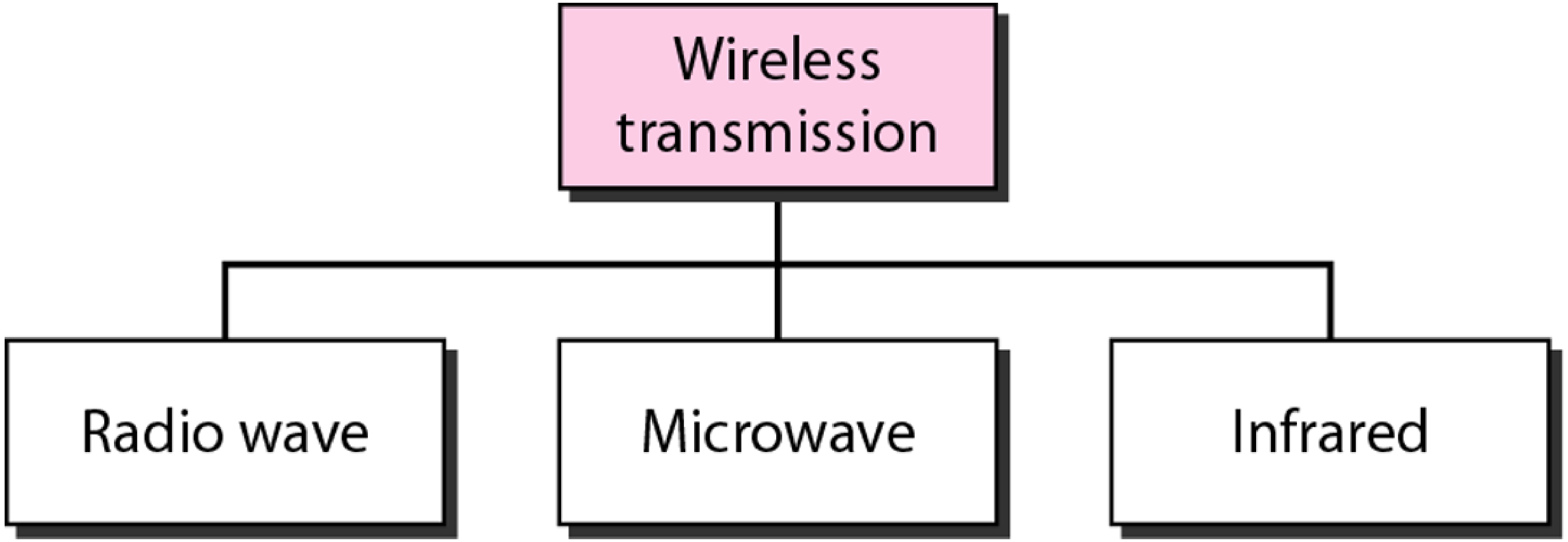
- It is expensive.
- Difficult to install.
- Maintenance is expensive and difficult

FIBER-OPTIC CABLE (contd…)

Applications:

- Backbone networks – SONET
- Cable TV – backbone
- LAN
- 100Base-FX network (Fast Ethernet)
- 1000Base-X

UNGUIDED MEDIA



UNGUIDED MEDIA (contd…)

Radio Waves

- Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves.
- Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned.

UNGUIDED MEDIA (contd…)

Microwaves

- Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.
- Microwaves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned.

UNGUIDED MEDIA (contd…)

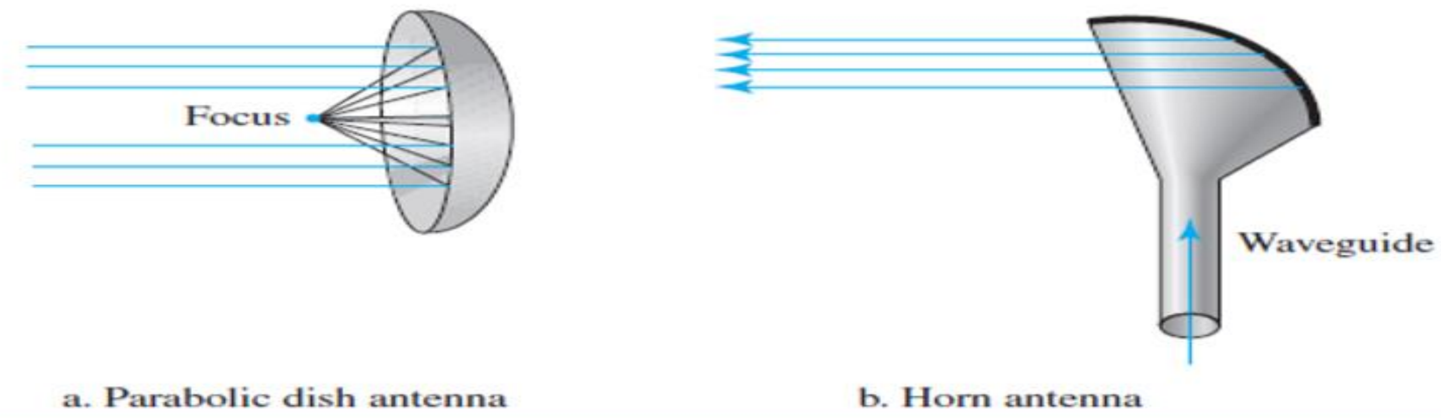
Characteristics of microwave propagation

- 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.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.
- The microwave band is relatively wide, almost 299 GHz. Therefore, wider sub-bands can be assigned, and a high data rate is possible.
- Use of certain portions of the band requires permission from authorities.

UNGUIDED MEDIA (contd…)

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

b. Horn antenna

- 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.

UNGUIDED MEDIA (contd…)

- The parabolic dish works as a funnel, catching a wide range of waves and directing them to a common point.

- Outgoing transmissions are broadcast through a horn aimed at the dish. The microwaves hit the dish and are deflected outward in a reversal of the receipt path.

- 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.

- Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

UNGUIDED MEDIA(contd…)

Infrared

- Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls.
- This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room.

Applications of infrared

- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

OSI-ISO REFERENCE MODEL

- International Organization for Standardization (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- Almost three-fourths of the countries in the world are represented in the ISO. 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.

OSI-ISO REFERENCE MODEL (contd…)

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

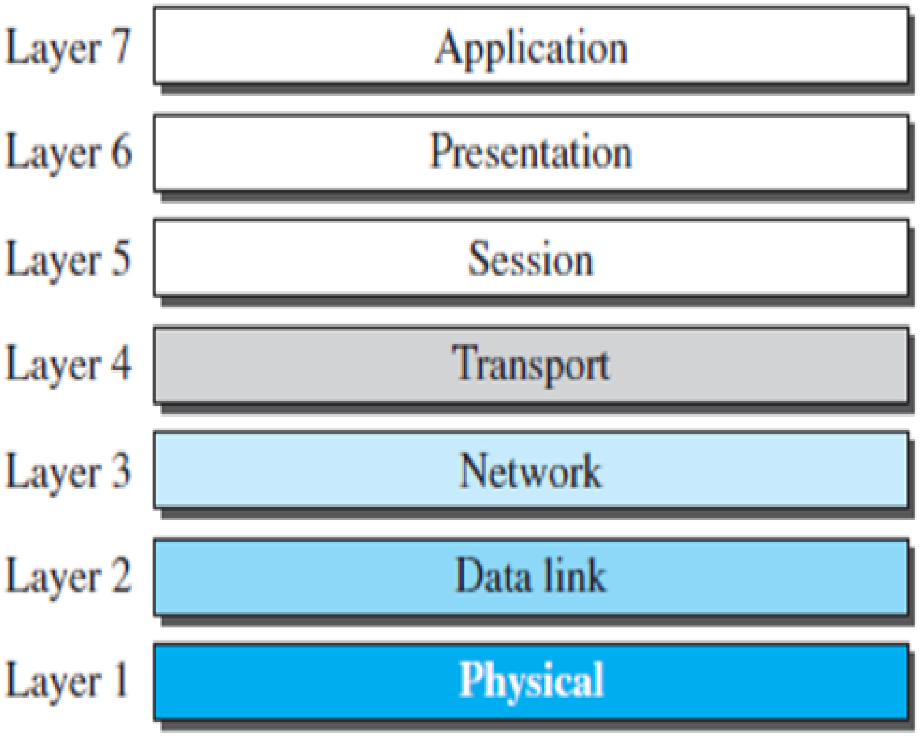


Fig. : The OSI model

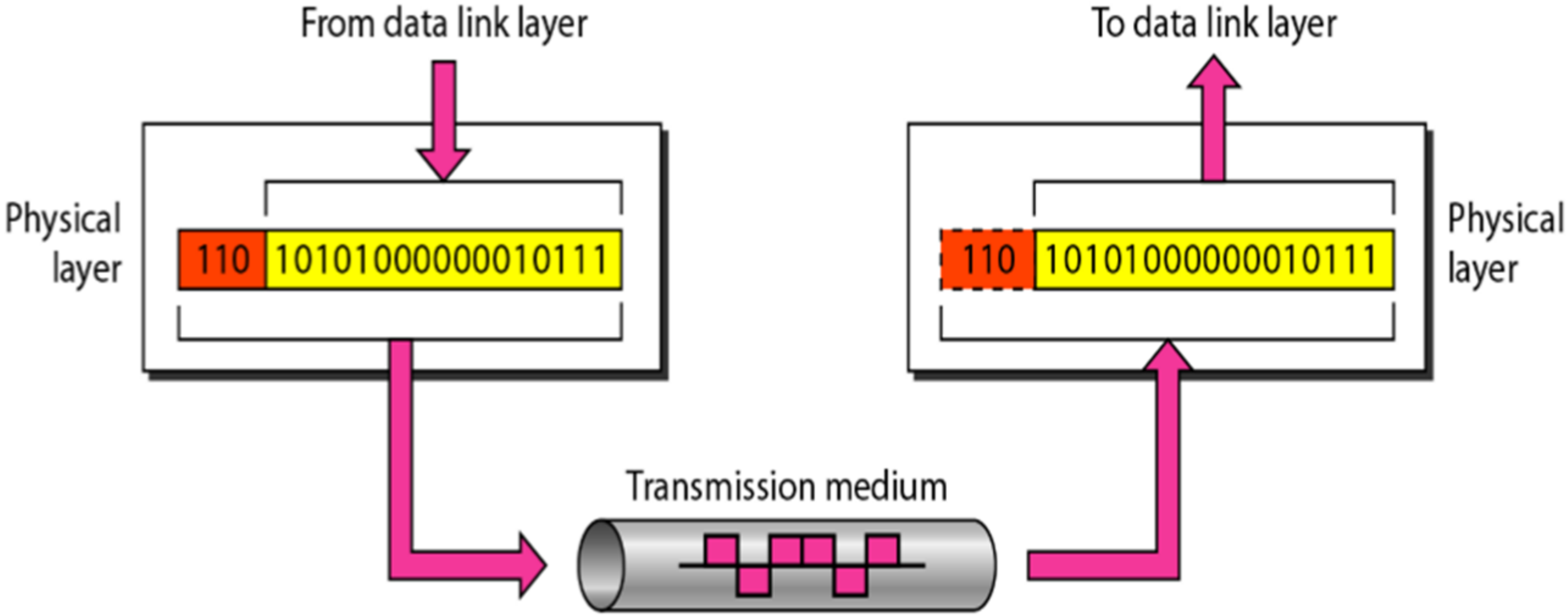
OSI-ISO REFERENCE MODEL (contd…)

Physical Layer (Layer 1)

- The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices.
- The physical layer contains information in the form of bits.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

OSI-ISO REFERENCE MODEL (contd…)

Physical Layer (Layer 1)



OSI-ISO REFERENCE MODEL (contd…)

- The functions of the physical layer are –
- Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
- Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology.

OSI-ISO REFERENCE MODEL (contd…)

The functions of the physical layer are (contd…) -

- Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology.
- Transmission mode: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and fullduplex.

Hub, Repeater, Modem, Cables are Physical Layer devices.

OSI-ISO REFERENCE MODEL (contd…)

Data Link Layer (DLL) (Layer 2)

- The data link layer is responsible for the node to node delivery of the message.
- The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

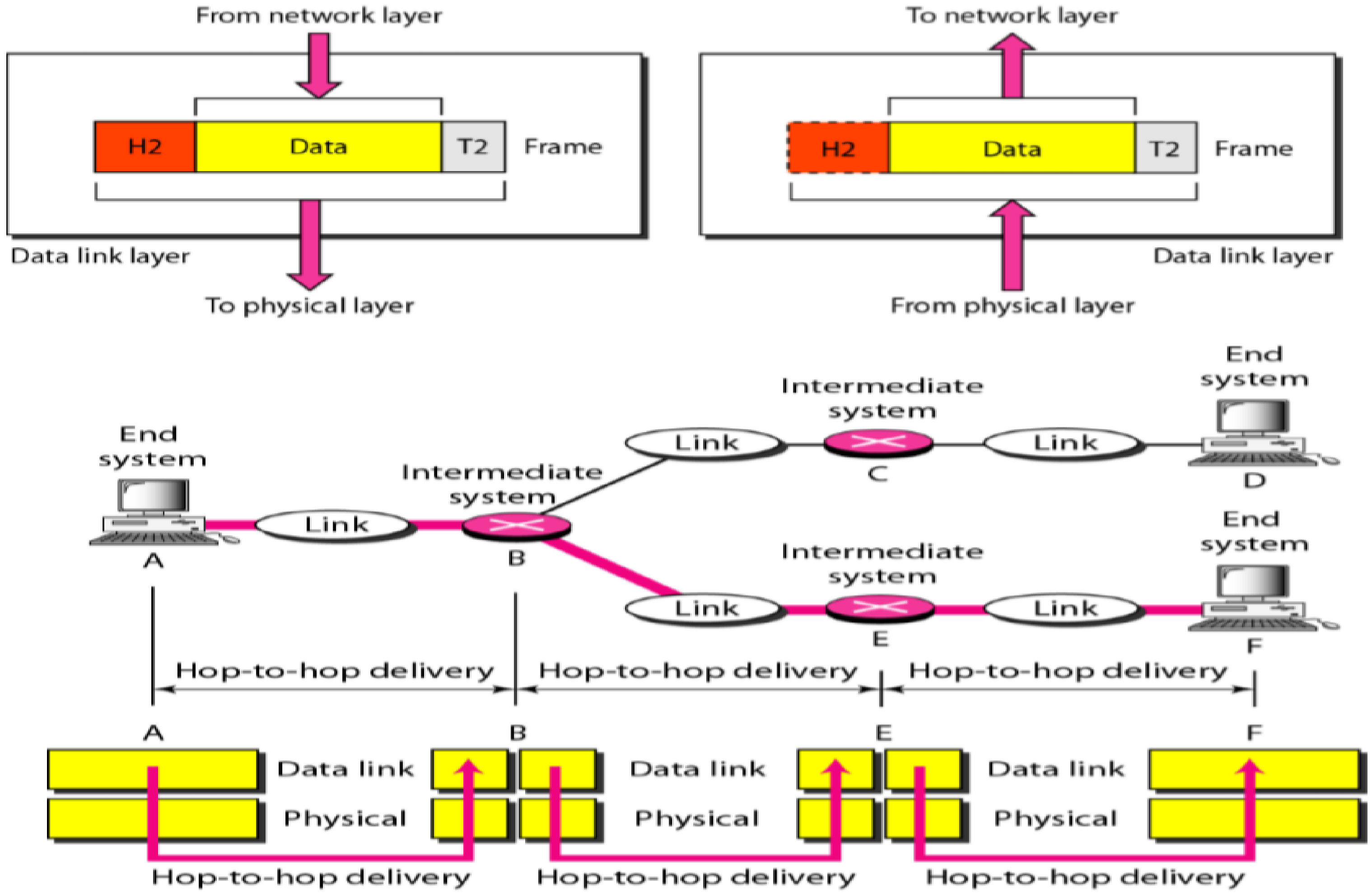
OSI-ISO REFERENCE MODEL (contd…)

Data Link Layer (DLL) (Layer 2) (contd…)

- Data Link Layer is divided into two sub layers: Logical Link Control (LLC) and Media Access Control (MAC)
- The packet received from Network layer is further divided into frames depending on the frame size of NIC (Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.
- The Receiver's MAC address is obtained by placing an ARP (Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

OSI-ISO REFERENCE MODEL (contd…)

Data Link Layer (DLL) (Layer 2) (contd…)



OSI-ISO REFERENCE MODEL (contd…)

The functions of the data Link layer are –

- Framing : It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- Physical addressing : After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
- Error control : Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- Flow Control : The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates that amount of data that can be sent before receiving acknowledgement.

OSI-ISO REFERENCE MODEL (contd…)

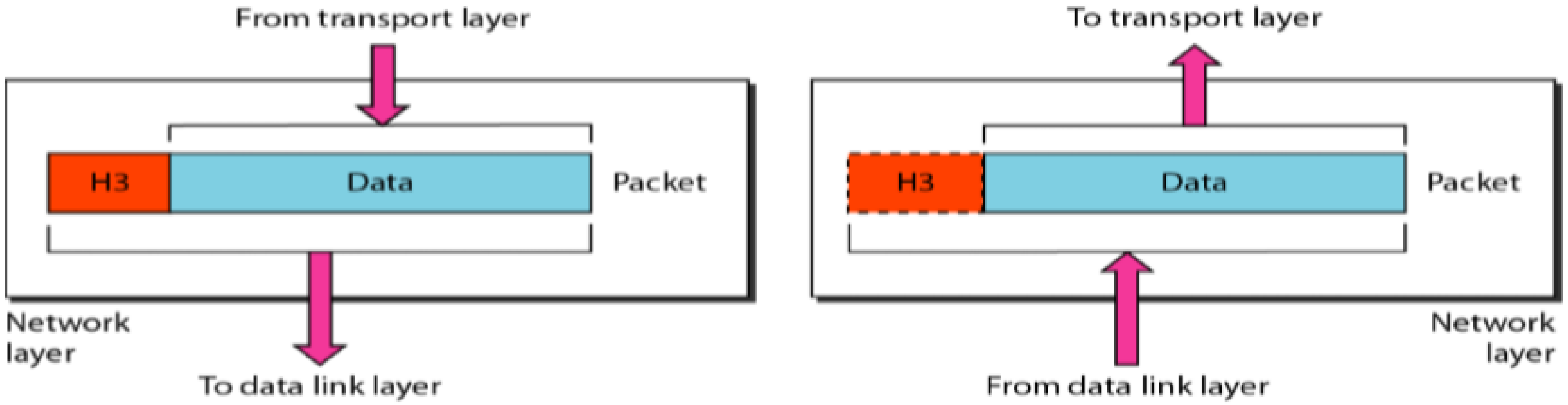
The functions of the data Link layer (contd…)

- Access control: When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.
  - Packet in Data Link layer is referred as Frame.
  - Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
  - Switch & Bridge are Data Link Layer devices.

OSI-ISO REFERENCE MODEL (contd…)

Network Layer (Layer 3)

- Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.
- The sender & receiver's IP are placed in header by network layer.



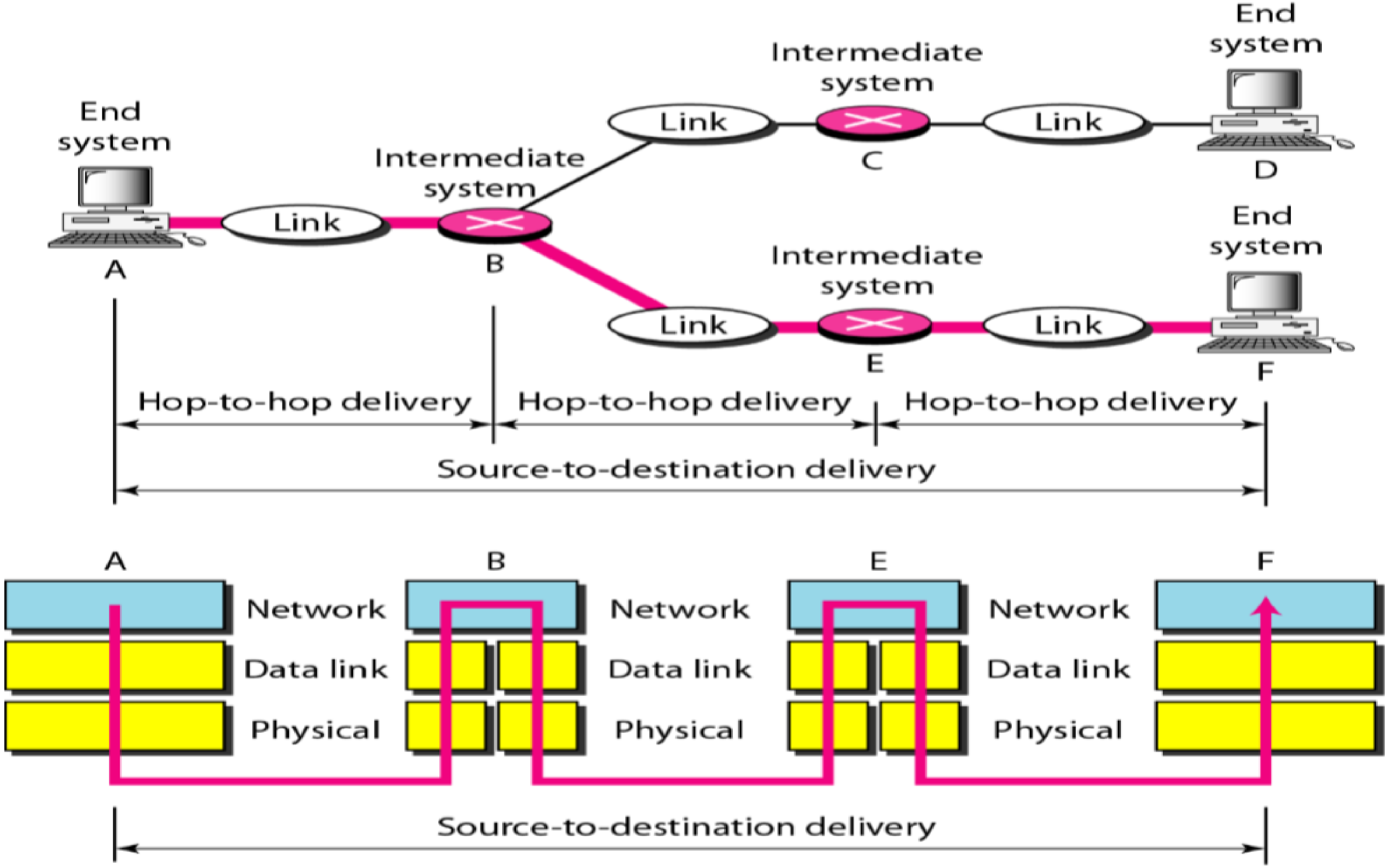
OSI-ISO REFERENCE MODEL (contd…)

The functions of the Network layer are -

- Routing: The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
- Logical Addressing: In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

OSI-ISO REFERENCE MODEL (contd…)

Network Layer (Layer 3)



OSI-ISO REFERENCE MODEL (contd…)

Transport Layer (Layer 4)

- Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments.
- It is responsible for the End to End delivery of the complete message.
- Transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

OSI-ISO REFERENCE MODEL (contd…)

Transport Layer (Layer 4)

At sender's side -

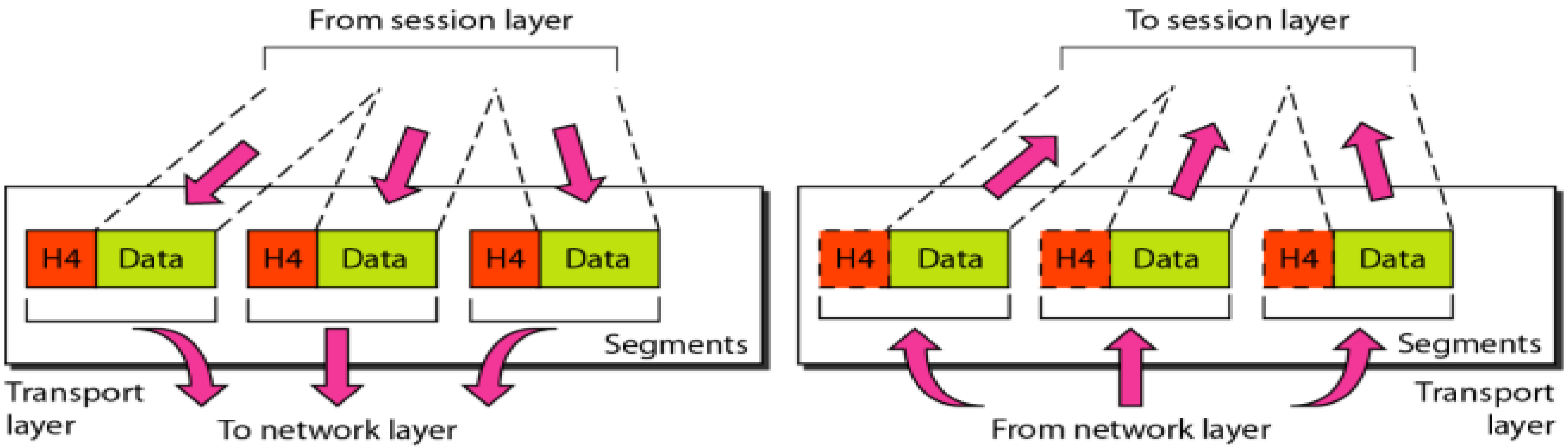
- Transport layer receives the formatted data from the upper layers, performs Segmentation and also implements Flow & Error control to ensure proper data transmission.
- It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

OSI-ISO REFERENCE MODEL (contd…)

Transport Layer (Layer 4)

At receiver’s side -

- Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application.
- It also performs sequencing and reassembling of the segmented data.



OSI-ISO REFERENCE MODEL (contd…)

Functions of the Transport Layer (Layer 4)

Segmentation and Reassembly -

- This layer accepts the message from the (session) layer, breaks the message into smaller units. Each of the segment produced has a header associated with it.
- The transport layer at the destination station reassembles the message.

Service Point Addressing -

- In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address.
- Thus, by specifying this address, transport layer makes sure that the message is delivered to the correct process.

OSI-ISO REFERENCE MODEL (contd…)

Session Layer (Layer 5)

- This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
- The functions of the session layer are:
  - Session establishment, maintenance and termination: The layer allows the two processes to establish, use and terminate a connection.

OSI-ISO REFERENCE MODEL (contd…)

Session Layer (Layer 5) (contd…)

Synchronization -

- This layer allows a process to add checkpoints which are considered as synchronization points into the data.

- These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.

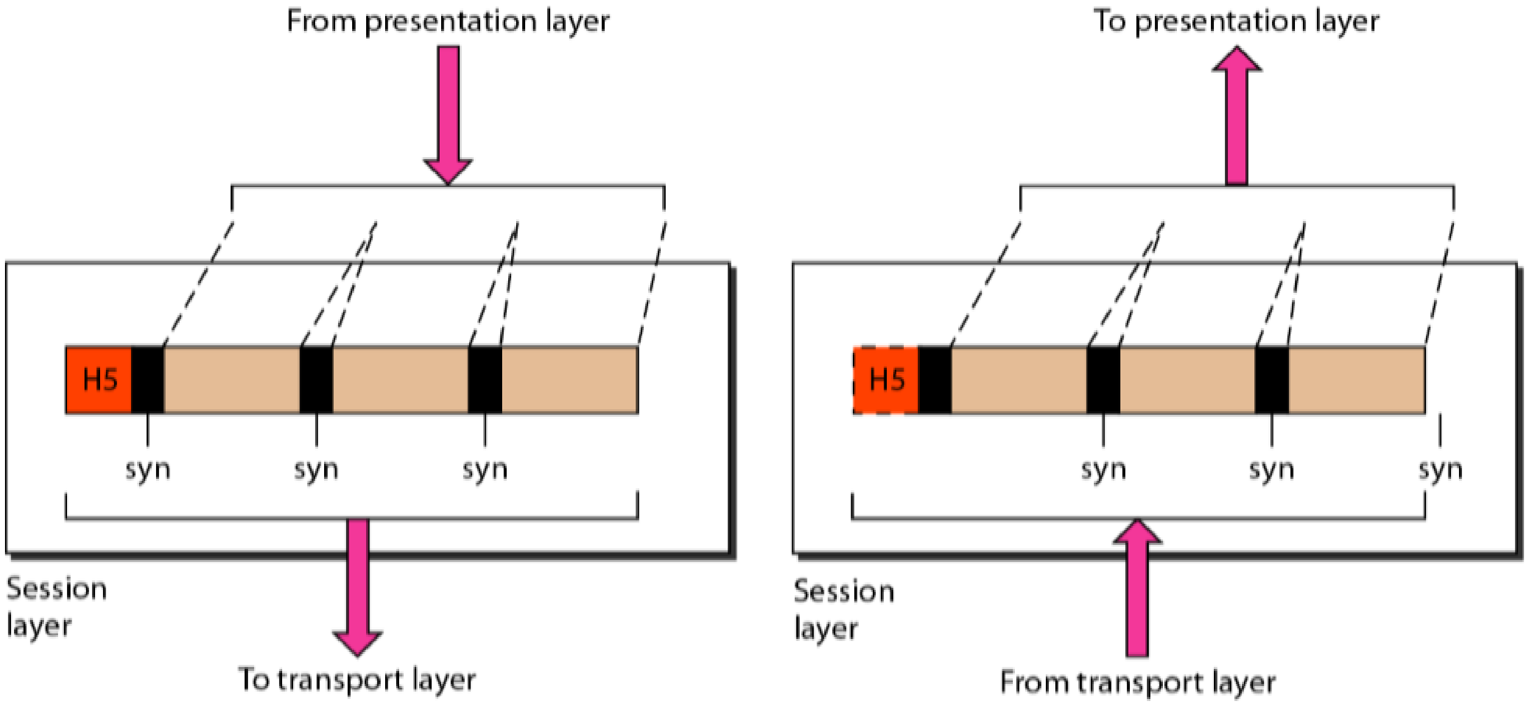
Dialog Controller -

- The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

OSI-ISO REFERENCE MODEL (contd…)

Session Layer (Layer 5) (contd…)

- All the below 3 layers (including Session Layer) are integrated as a single layer in TCP/IP model as “Application Layer”.

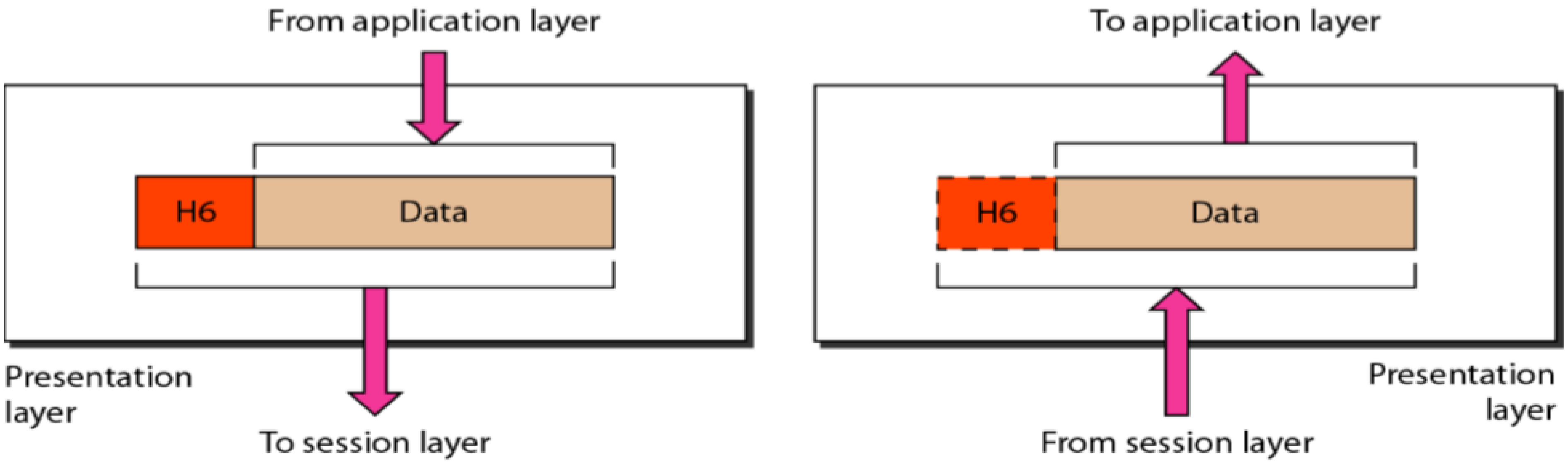


- Implementation of these 3 layers is done by the network application itself. These are also known as Upper Layers or Software Layers.

OSI-ISO REFERENCE MODEL (contd…)

Presentation Layer (Layer 6)

- Presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.



OSI-ISO REFERENCE MODEL (contd…)

Presentation Layer (Layer 6) (contd…)

Encryption/ Decryption -

- Data encryption translates the data into another form or code.
- The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

Compression -

- Reduces the number of bits that need to be transmitted on the network.

OSI-ISO REFERENCE MODEL (contd…)

Application Layer (Layer 7)

- At the very top of the OSI Reference Model stack of layers, we find Application layer (is also called as Desktop Layer).
- These applications produce the data, which has to be transferred over the network.
- This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
- Ex: Application – Browsers, Skype Messenger etc.

OSI-ISO REFERENCE MODEL (contd…)

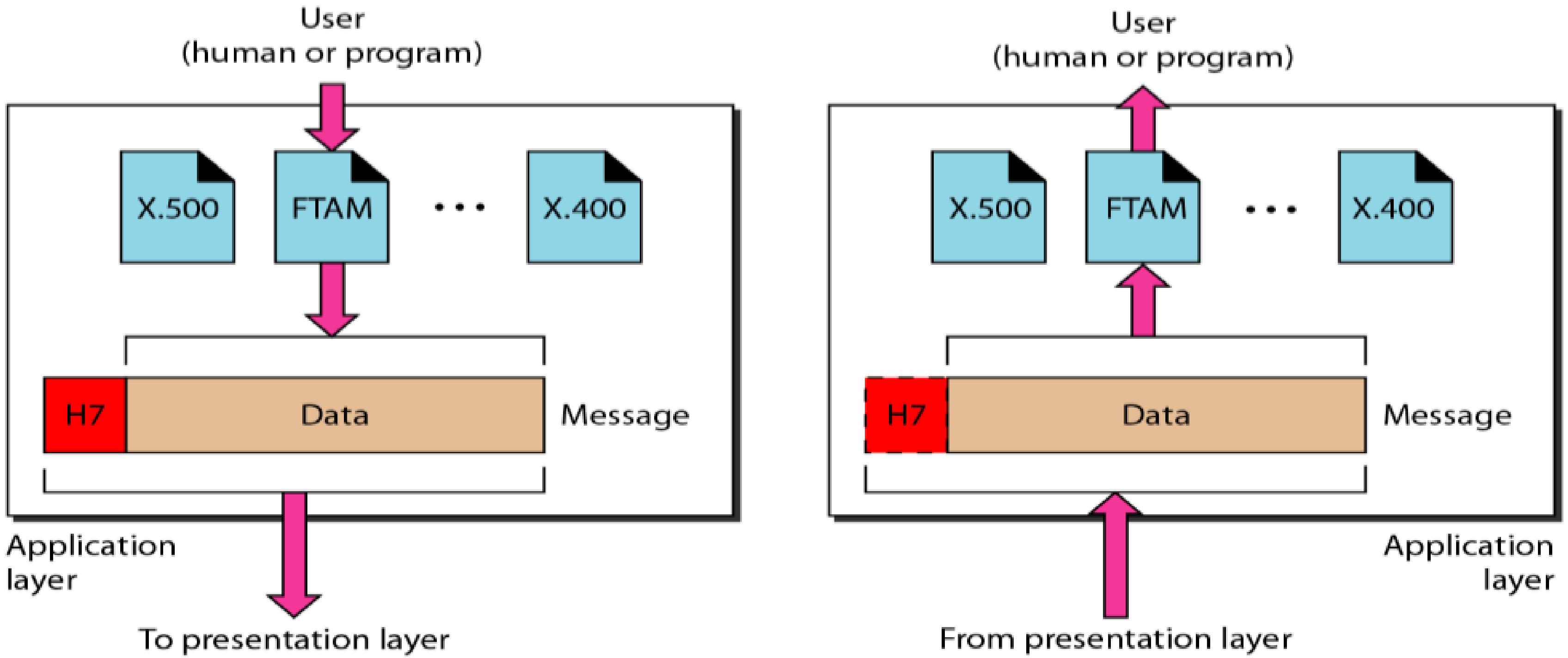


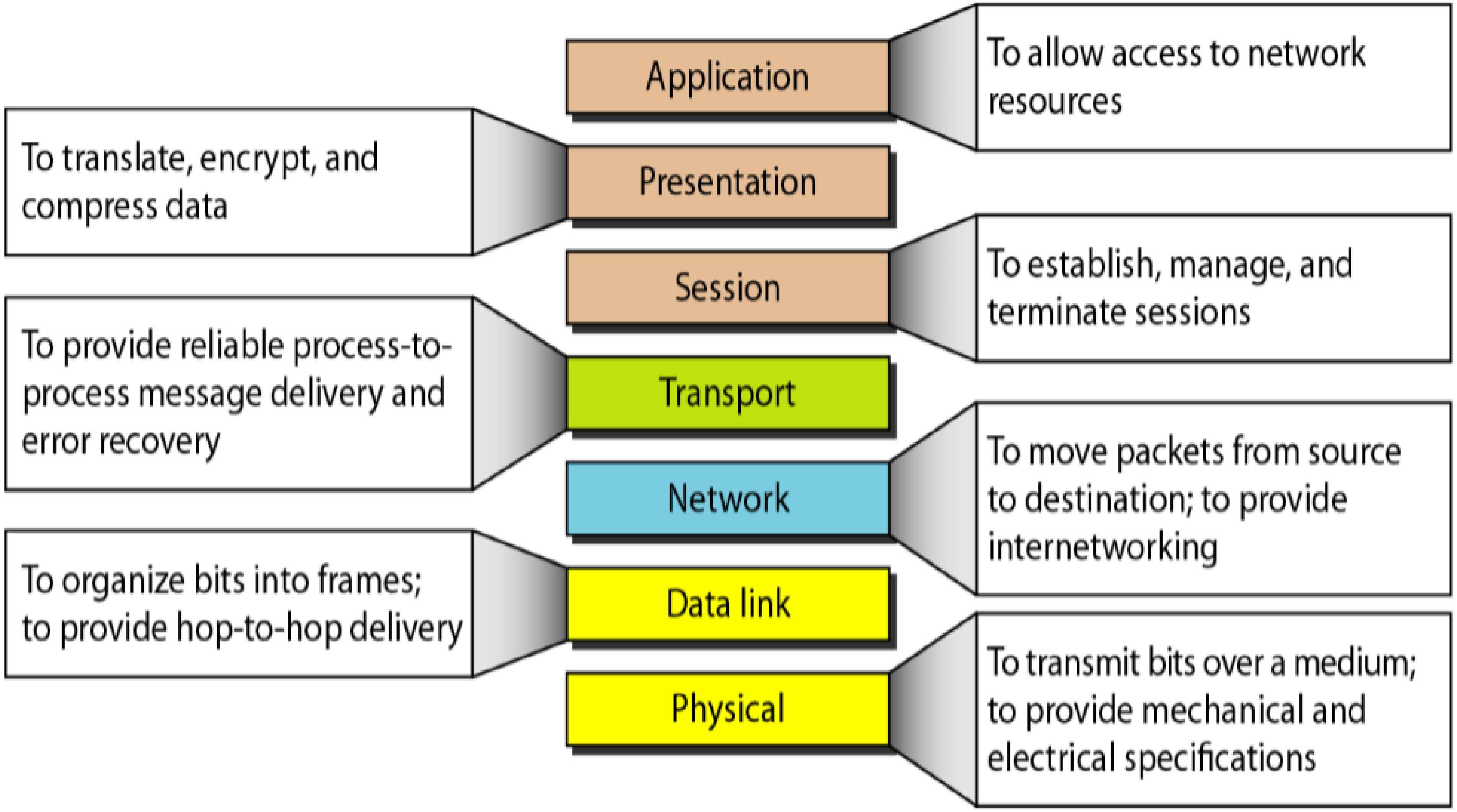
Fig.: Application Layer (Layer 7).

OSI-ISO REFERENCE MODEL (contd…)

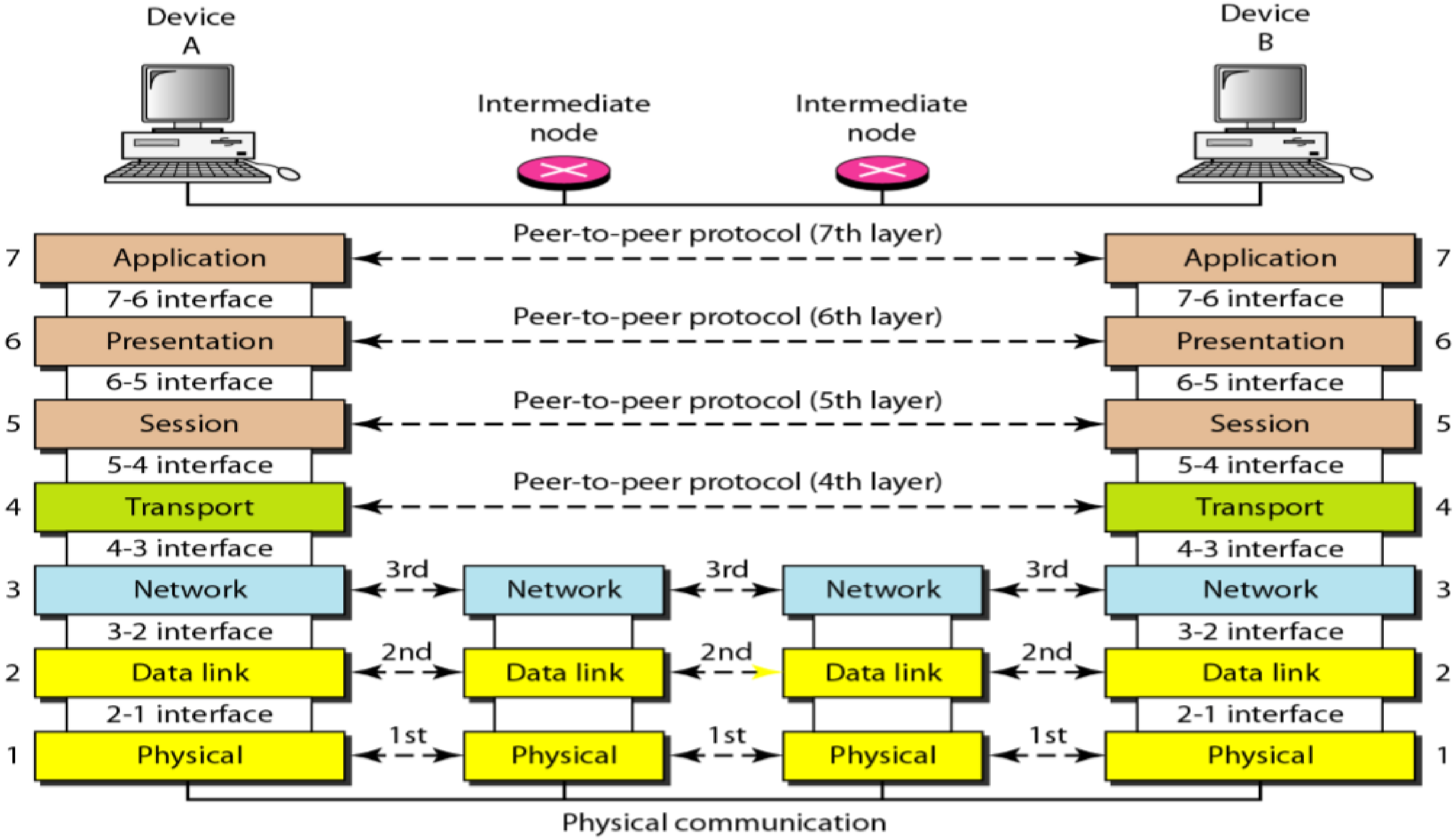
The functions of the Application layer –

- Network Virtual Terminal
- FTAM-File transfer access and management
- Mail Services
- Directory Services

SUMMARY OF ISO/OSI REFERENCE MODEL


Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

The interaction between layers in the OSI model



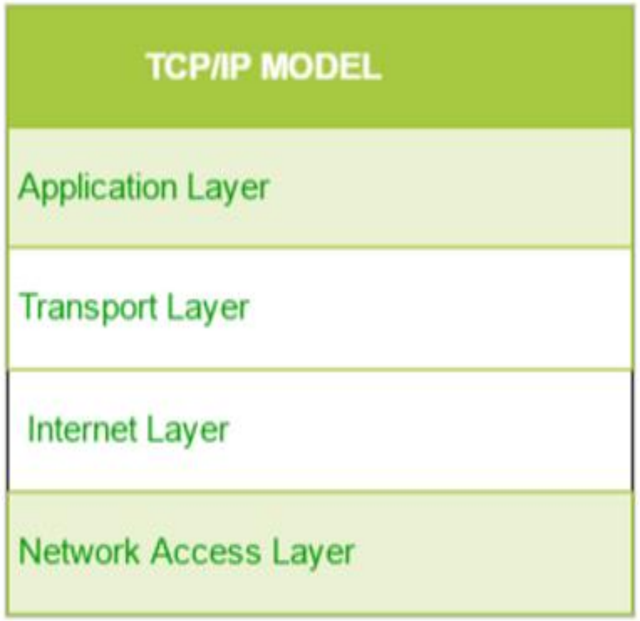
TCP/IP Model

- TCP/IP model was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol.

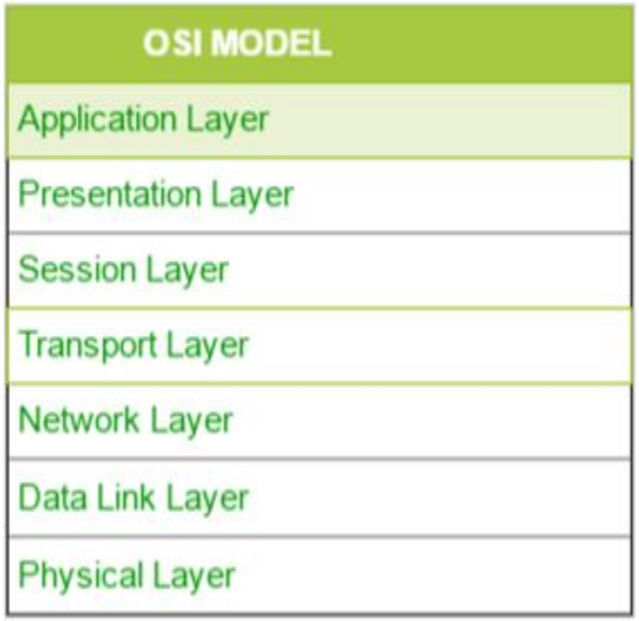
- The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.

- The layers are:
    - Process/Application Layer
    - Host-to-Host/Transport Layer
    - Internet Layer
    - Network Access/Link Layer

TCP/IP Model (contd…)



TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer



OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

TCP/IP Model (contd…)

1. Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.

- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.

- It defines how the data should be sent physically through the network.

- This layer is mainly responsible for the transmission of the data between two devices on the same network.

- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.

- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

TCP/IP Model (contd…)

2. Internet Layer

- An internet layer (also known as the network layer) is the second layer of the TCP/IP model.

- The main responsibility of the internet layer is to send the packets from any network and they arrive at the destination irrespective of the route they take.

- The protocols used in this layer are:

➢IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

TCP/IP Model (contd…)

Responsibilities of IP protocol

- IP Addressing
- Host-to-host communication
- Data Encapsulation and Formatting
- Fragmentation and Reassembly
- Routing

TCP/IP Model (contd…)

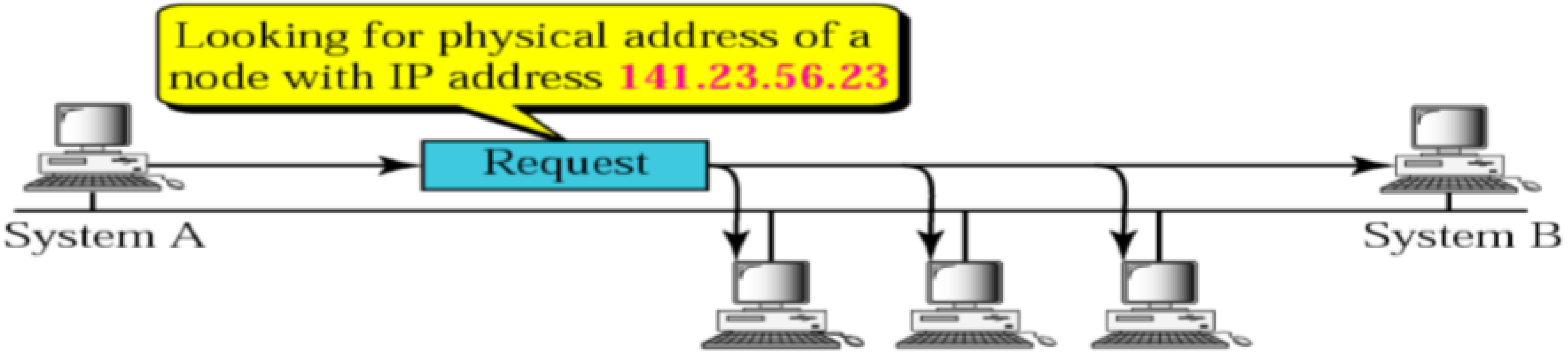
- ARP Protocol: Address Resolution Protocol(ARP) is a network layer protocol which is used to find the physical address from the IP address.

The two terms are mainly associated with the ARP Protocol:

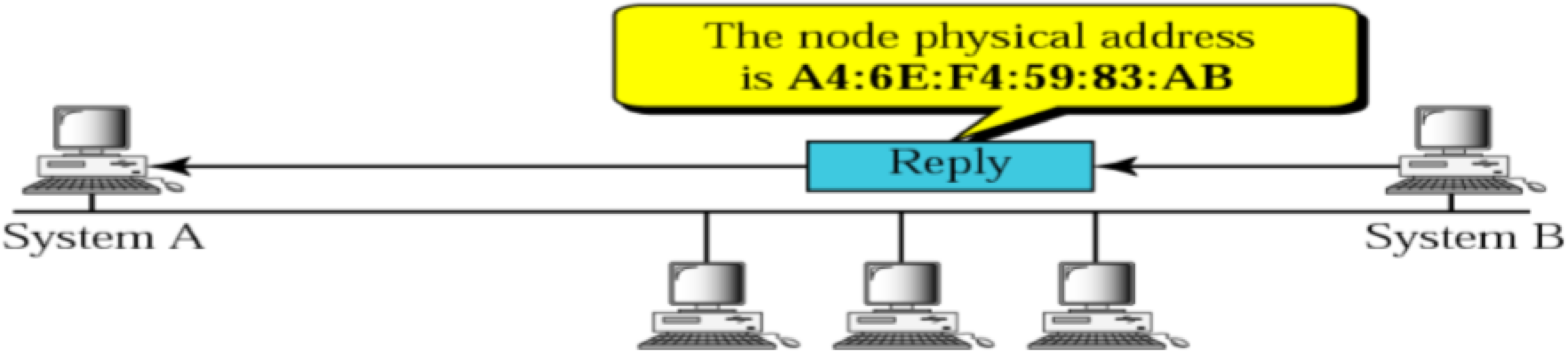
- ARP request: When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.

- ARP reply: Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header.

TCP/IP Model (contd…)


Looking for physical address of a node with IP address 141.23.56.23
Request
System A
System B

a. ARP request is broadcast



b. ARP reply is unicast

TCP/IP Model (contd…)

How ARP Works

- When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address.
- The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine.
- If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it.

TCP/IP Model (contd…)

How ARP Works (contd…)

- A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.
- There is a Reverse ARP (RARP) for host machines that don't know their IP address. RARP enables them to request their IP address from the gateway's ARP cache.

TCP/IP Model (contd…)

➢ICMP Protocol: Internet Control Message Protocol(ICMP) is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.

An ICMP protocol mainly uses two terms:

- ICMP Test: ICMP Test is used to test whether the destination is reachable or not.
- ICMP Reply: ICMP Reply is used to check whether the destination device is responding or not.

TCP/IP Model (contd…)

3. Transport Layer

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- The two protocols used in the transport layer are User Datagram protocol and Transmission control protocol.

TCP/IP Model (contd…)

➢ User Datagram Protocol (UDP)

- It provides connectionless service and end-to-end delivery of transmission.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
- UDP consists of the following fields:

○ Source port address: It is the address of the application program that has created the message.

○ Destination port address: It is the address of the application program that receives the message.

○ Total length: The total number of bytes of the user datagram in bytes.

○ Checksum: The checksum is a 16-bit field used in error detection.

○ UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

TCP/IP Model (contd…)

➢ Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver and it is active for the duration of the transmission.
- It ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

TCP/IP Model (contd…)

4. Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.

TCP/IP Model (contd…)

The main protocols used in the application layer are:

- Hypertext transfer protocol (HTTP) 0allows us to access the data over the World Wide Web. It transfers the data in the form of plain text, audio, video.
- Simple Network Management Protocol (SNMP) is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- Simple mail transfer protocol (SMTP) supports the e-mail (i.e. is used to send the data to another e-mail address.)

TCP/IP Model (contd…)

The main protocols used in the application layer (contd…)

- Domain Name System(DNS): An IP address is used to identify the connection of a host to the internet uniquely. But people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

- File Transfer Protocol(FTP) is a standard internet protocol used for transmitting the files from one computer to another computer

THANK YOU