UNIT-I

Introduction & Physical Layer

Contents

Introduction:

- Network, Uses of Networks,
- Types of Networks
- Reference Models: TCP/IP Model, The OSI Model,
- Comparison of the OSI and TCP/IP reference model
- Architecture of Internet.

Physical Layer:

- Guided transmission media,
- Wireless transmission media,
- Switching

Introduction:

A data communications system has five components

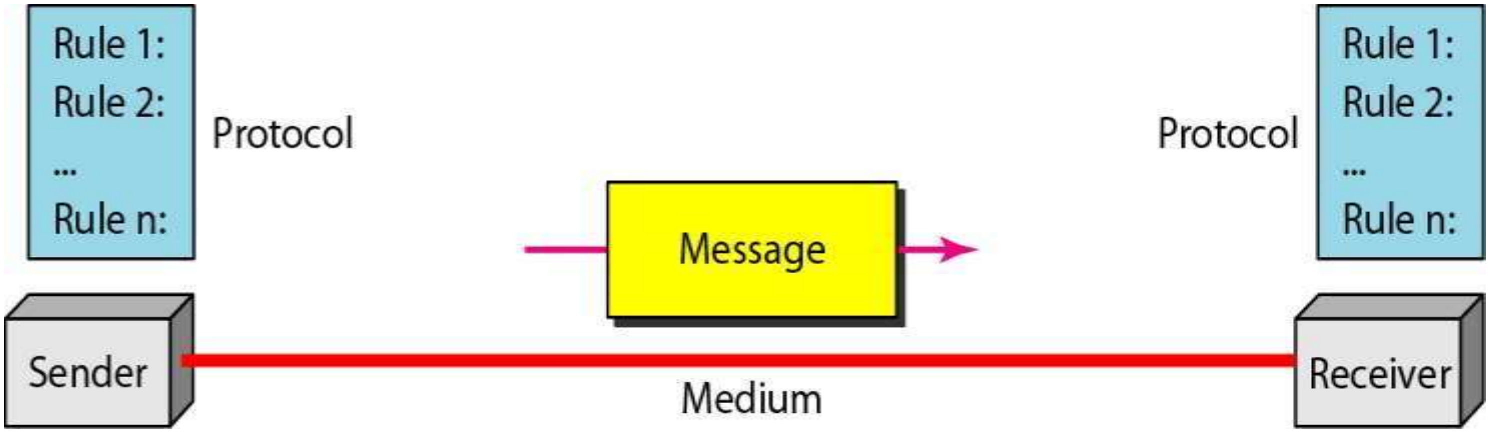
1. **Message:** Information(data) to be communicated

2. Sender

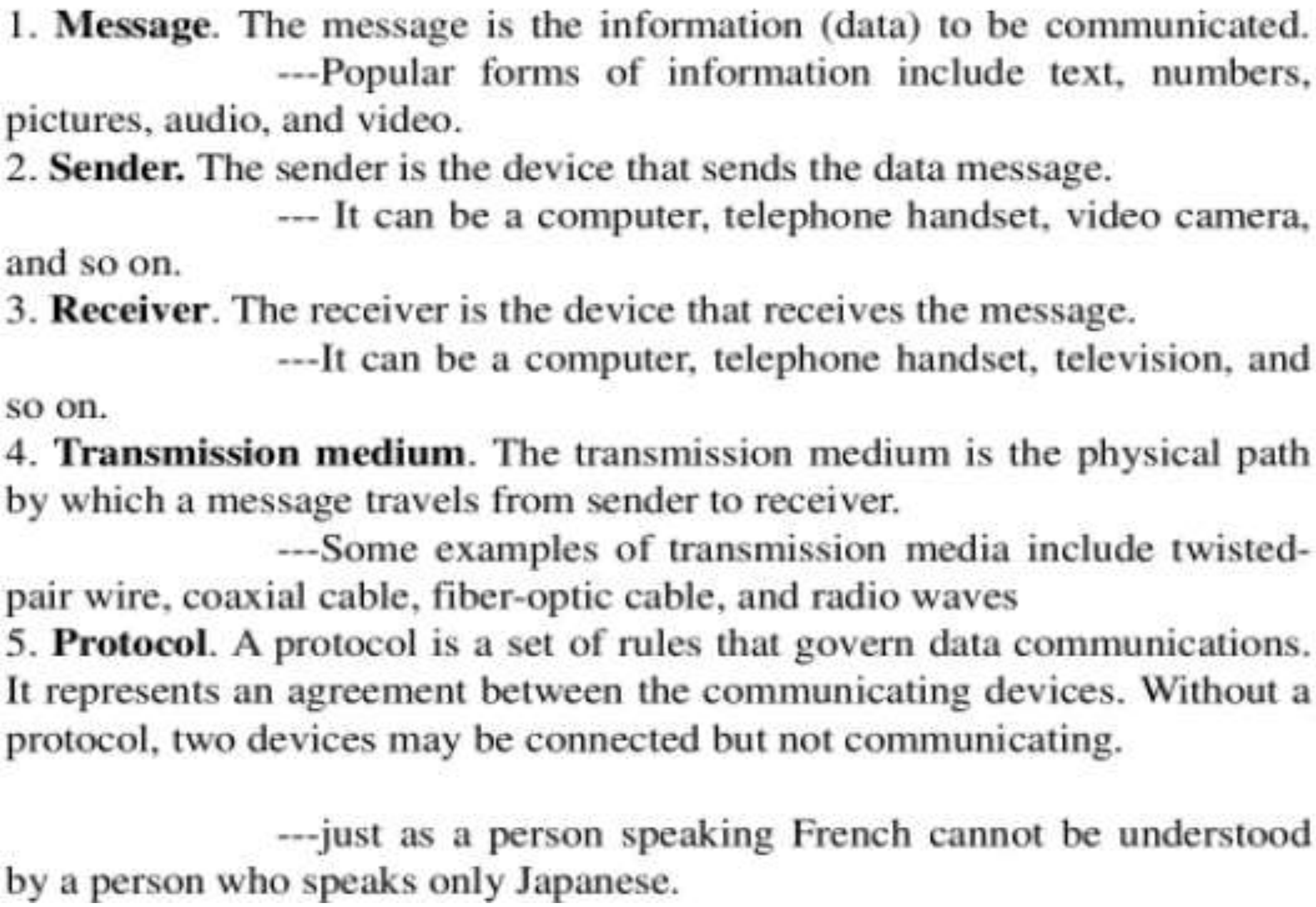
3. Receiver

4. Transmission Medium - Physical path by which a message travels

5.Protocol - A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.



Contd..



1. **Message**. The message is the information (data) to be communicated.

---Popular forms of information include text, numbers, pictures, audio, and video.

2. **Sender.** The sender is the device that sends the data message.

--- It can be a computer, telephone handset, video camera, and so on.

3. **Receiver**. The receiver is the device that receives the message.

---It can be a computer, telephone handset, television, and so on.

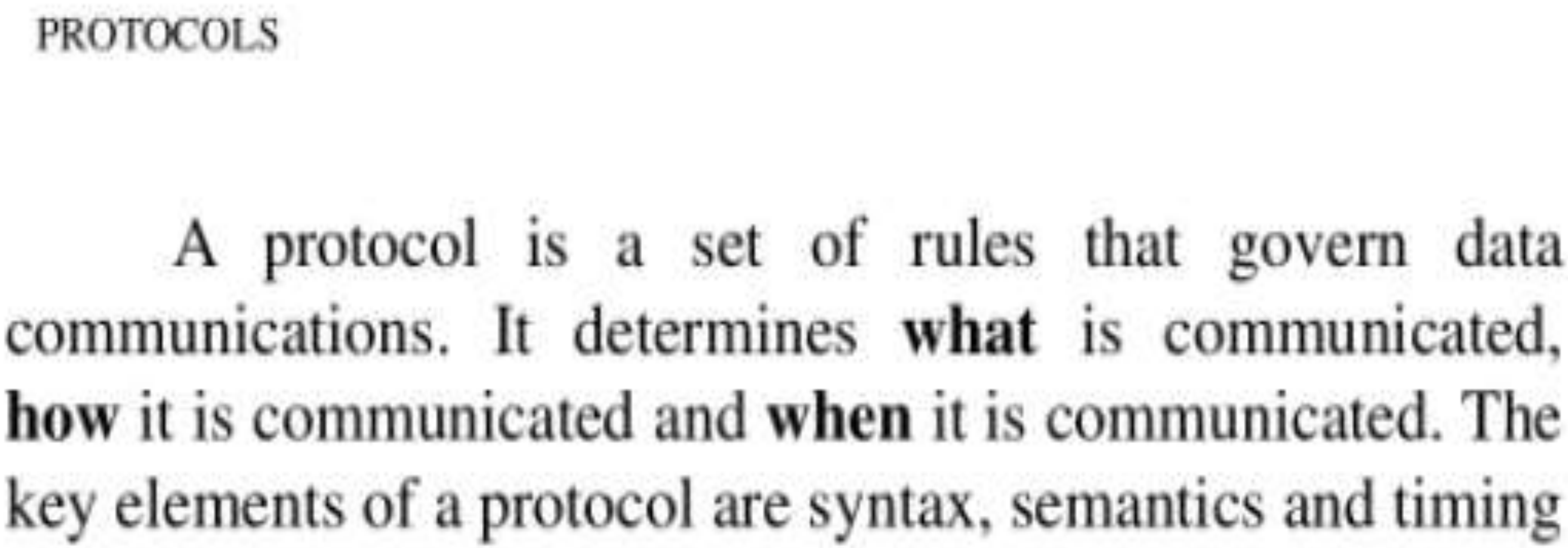
4. **Transmission medium**. The transmission medium is the physical path by which a message travels from sender to receiver.

---Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves

5. **Protocol**. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

---just as a person speaking French cannot be understood by a person who speaks only Japanese.

Contd..

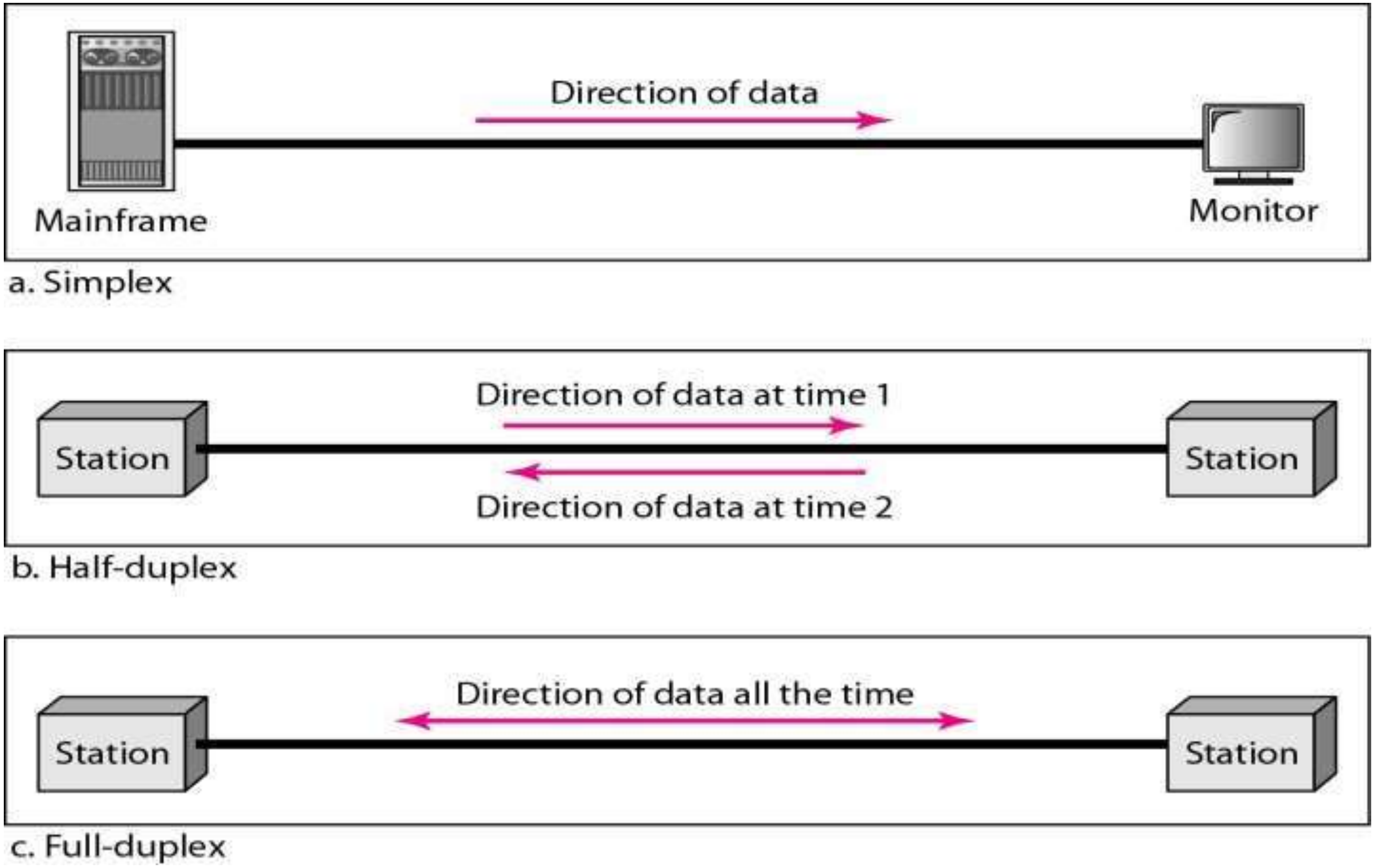


PROTOCOLS

A protocol is a set of rules that govern data communications. It determines **what** is communicated, **how** it is communicated and **when** it is communicated. The key elements of a protocol are syntax, semantics and timing

Data Flow

- Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure.


Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

a. Simplex

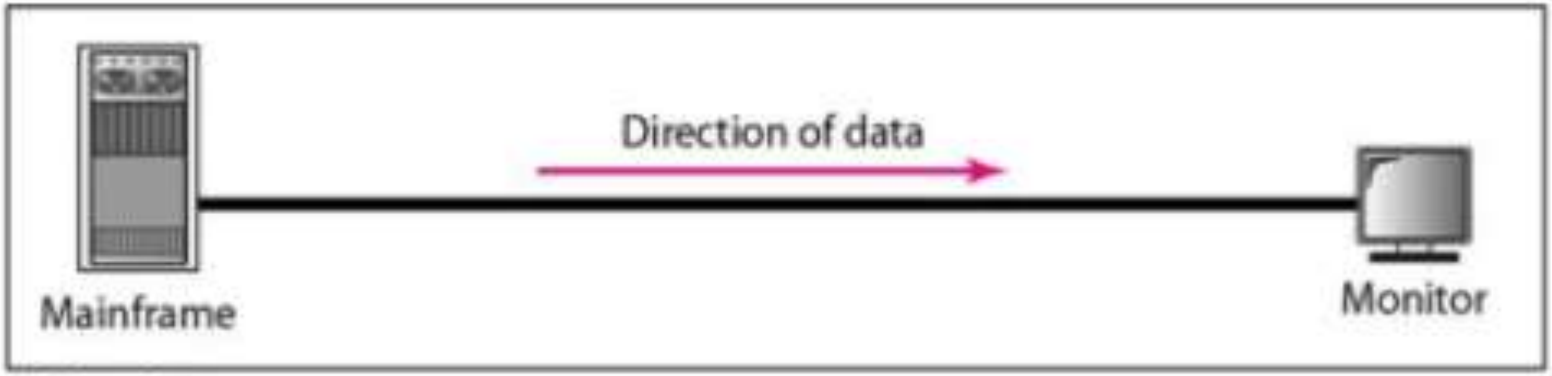
b. Half-duplex

c. Full-duplex

Simplex:

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.

Examples:- Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

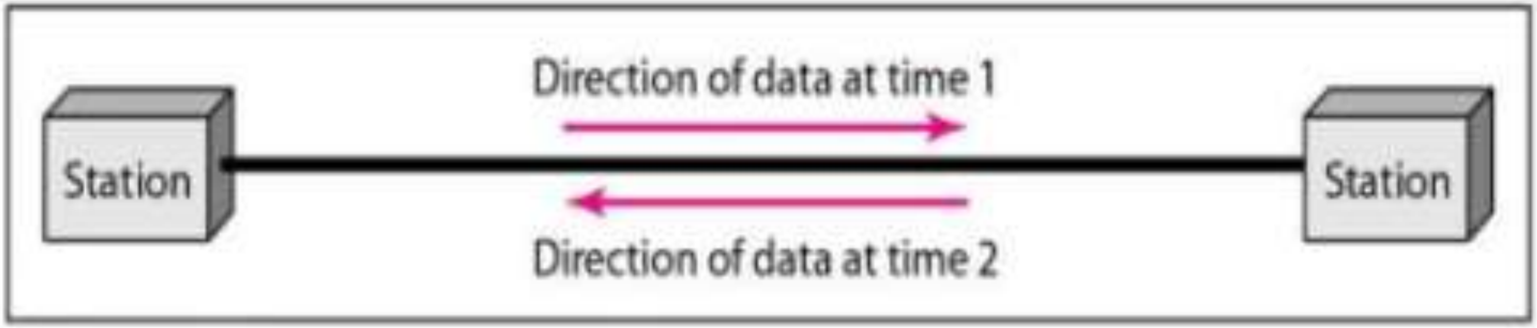


a. Simplex

Half-Duplex:

In half-duplex mode, 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.

Examples:-When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies is half-duplex systems.

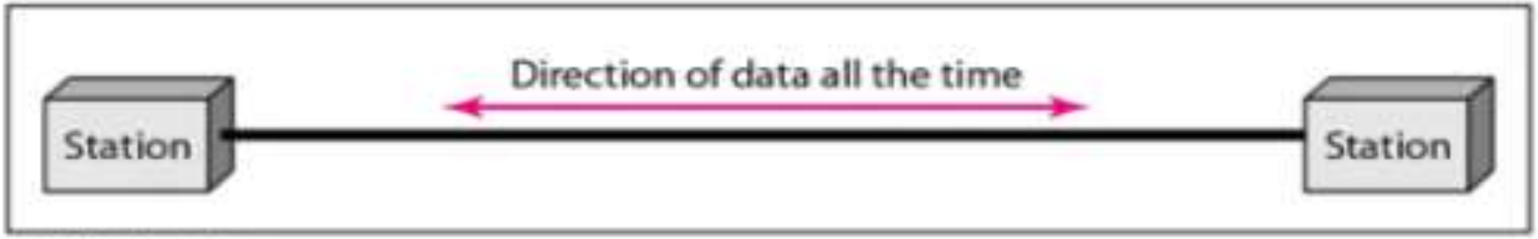


b. Half-duplex

Full-Duplex:

In full-duplex both stations can transmit and receive simultaneously. The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction.

Example:- full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.



c. Full-duplex

NETWORK

- 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

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security

- **Performance**
  - Depends on Network Elements
  - Measured in terms of Delay and Throughput
- **Reliability**
  - Measured by the frequency of failure, the time it takes a link to recover from a failure.
  - Measured in terms of availability/robustness
- **Security**
  - Protecting data from unauthorized access.
  - Implementing policies and procedures for recovery from data losses.

USES OF NETWORKS

- **Business Applications**
  - Resource sharing
  - Client-Server model.
  - Desktop sharing
  - E-commerce
  - IP telephony or Voice over IP (VoIP)

- **Home Applications**
  - peer-to-peer communication
  - person-to-person communication
  - electronic commerce
  - entertainment.(game playing,)

USES OF NETWORKS

- **Mobile Users**
  - Text messaging or texting
  - Smart phones,
  - GPS (Global Positioning System)
  - m-commerce

- **Social Issues**
  - with the good comes the bad, as this new-found freedom brings with it
    many unsolved social,)
    BOTNET ATTACK: (send spam) political, and ethical issues.

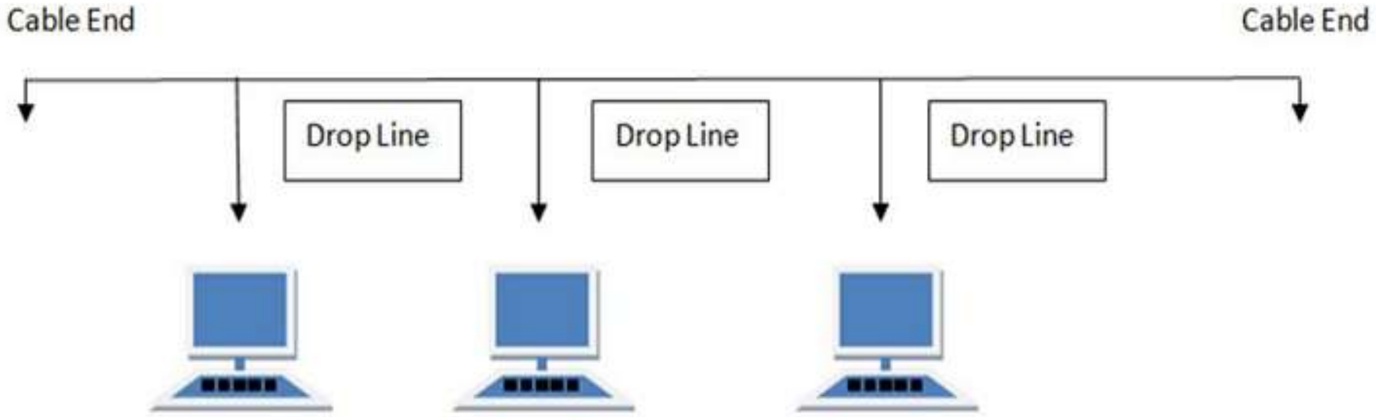
Network Topologies

- The network topology is the method for arrangement of computing devices or networking devices through which they are connected (Wired or Wireless) or Physical arrangement of various nodes in the network
- There are almost **six** types of topologies which are employed for networking of computing devices (Computers or networking devices)

- 1. Bus 2. Ring 3. Star 4. Mesh
  5. Tree 6. Hybrid

Bus Topology

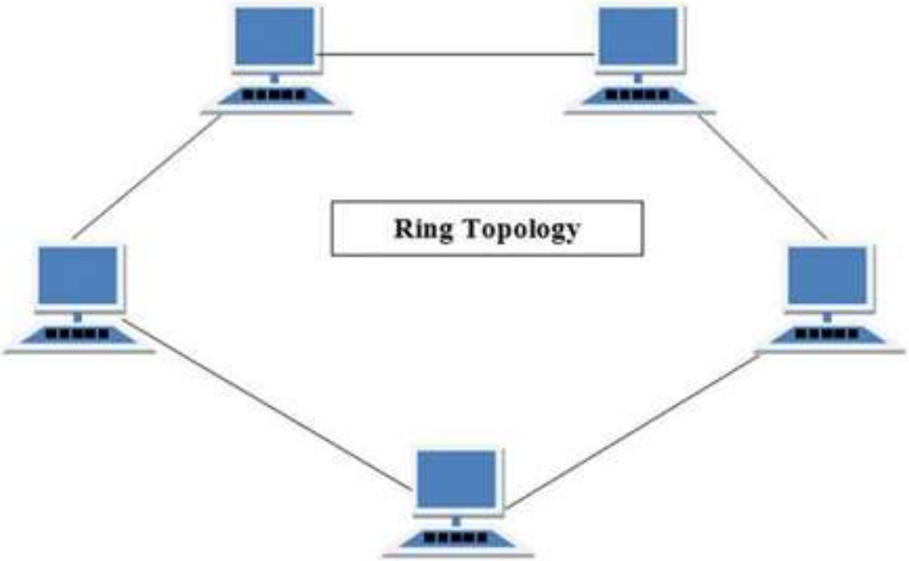
- Bus topology is a network type in which every computer and networking device is connected to single cable



- **Features**
  - Data transmission is in one direction only
  - Each device is connected to single cable
- **Advantages**
  - Cost effective (Cheap)
  - Cable required is less when compared to other topologies.
  - Easy to expand network (by joining two cables together)
- **Disadvantages**
  - When cable fails then whole network fails
  - Performance of topology decreases with increase in nodes and traffic

Ring Topology

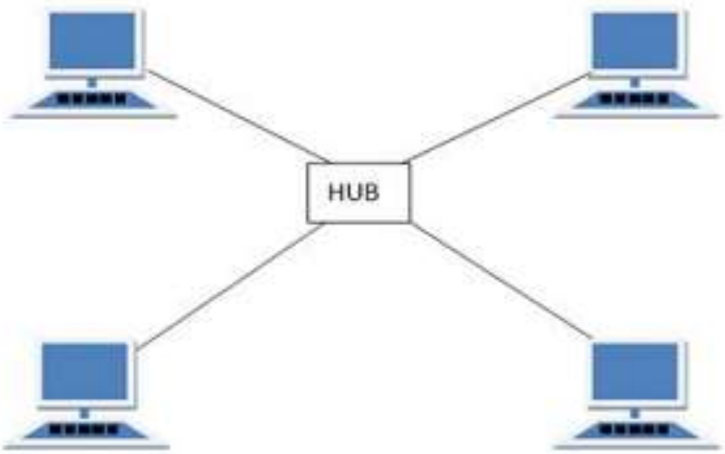
- It is called as ring topology because it forms a ring as each computer is connected to the other computer with last one connected to first.
- Ring topology has exactly two neighbors for each node



- **Features**
  - Number of repeaters are used and transmission is unidirectional
  - Data transfer is bit by bit (sequential Manner)
- **Advantages**
  - Performance of network is not effected by increase in traffic or by adding nodes as the nodes have the tokens only can participate in communication.
  - Cheap to install and expand.
- **Disadvantages**
  - Trouble shooting is difficult
  - Additions and deletions of nodes will disturb network activity.
  - Failure of one computer will disturb entire network

Star Topology

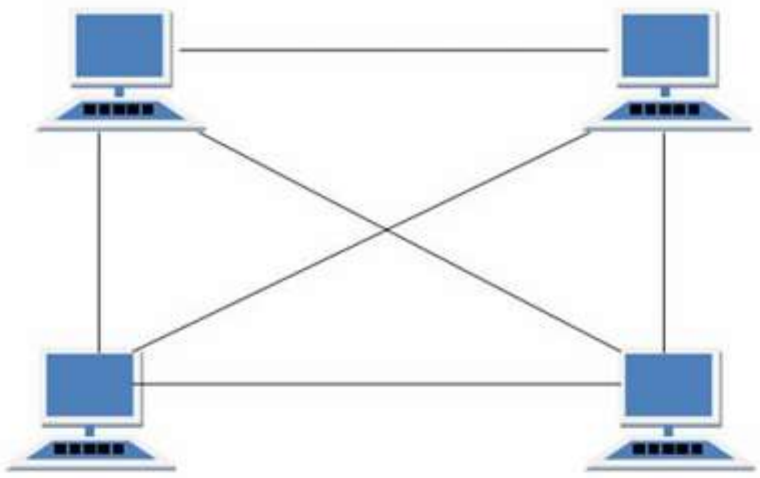
- All computers in this topology are connected to a single hub through the cable and this hub is the central node.
- All other nodes are to be connected to the central hub in the case of extending the network



- **Features**
  - Every node has its own dedicated connection to the hub.
  - Acts as repeater for data flow.
- **Advantages**
  - Hubs can be easily upgraded.
  - Easy to trouble shoot, setup and modify the network.
  - In the case of failure only failure node is effected reaming network will function smoothly.
- **Disadvantages**
  - High Cost.
  - If the hub is effected then functioning whole network is disturbed.

Mesh Topology

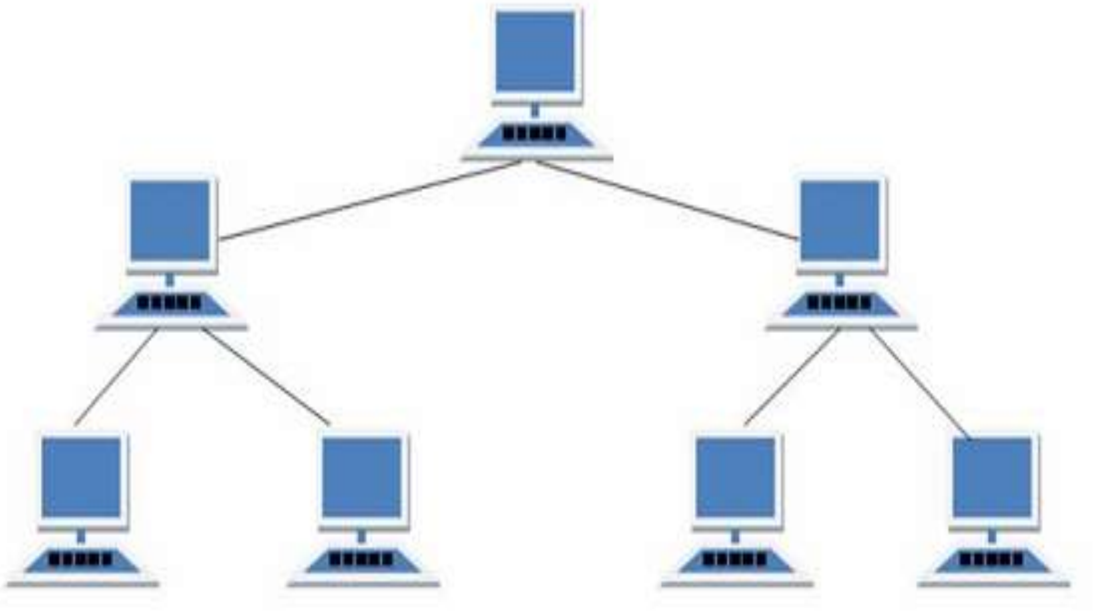
- It is a point to point connection to all other computers.
- Traffic is carried only between two nodes to which it is connected



- **Features**
  - Fully Connected
  - Robust.
- **Advantages**
  - Each connection can carry its own data.
  - Fault diagnosis is easy.
  - Provides security and privacy.
- **Disadvantages**
  - Installation and configuration is difficult.
  - Cabling cost is more.
  - Bulk wiring is required.

Tree Topology

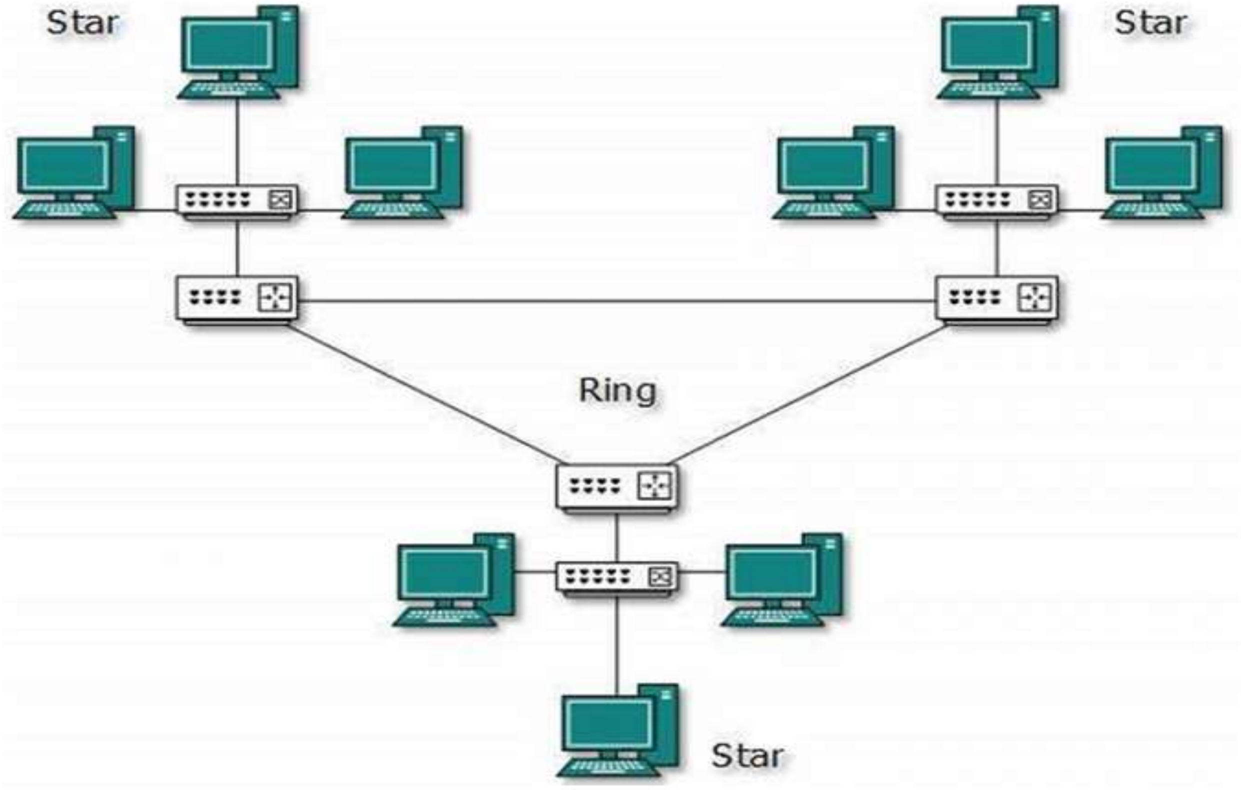
- It has a root node and all other nodes are connected to the root node forming hierarchy and it is also called as hierarchical topology.
- It should have atleast three levels for the hierarchy



- **Features**
  - Ideal if work stations are located in groups
  - Used in wide area networks.
- **Advantages**
  - Easy error detection.
  - Expansion of nodes is possible and easy.
  - Easy to maintain and manage.
- **Disadvantages**
  - Costly and heavily cabled.
  - Addition of more nodes increases difficulty in maintenance.
  - Failure of root effects all nodes in the network.

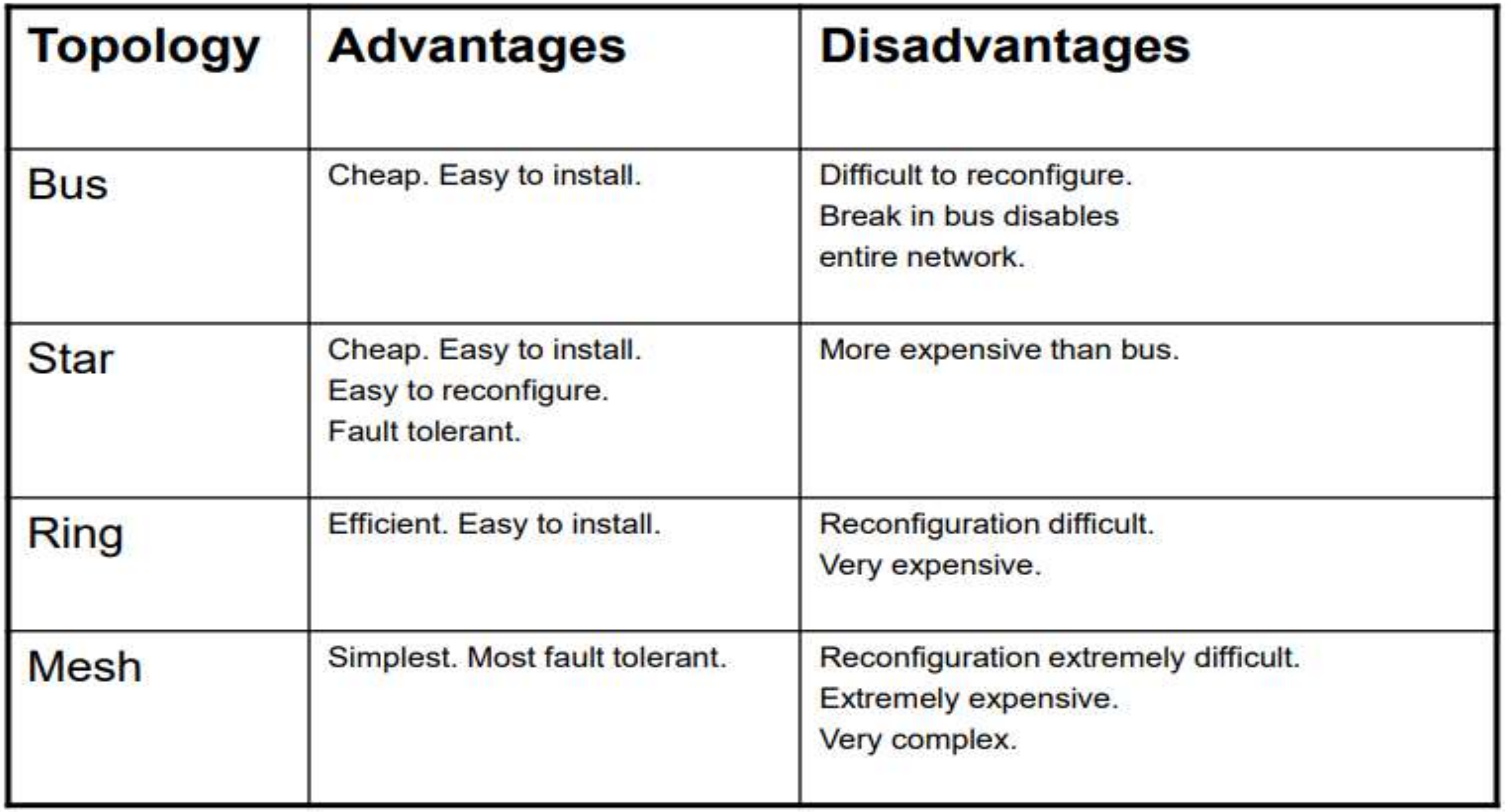
Hybrid Topology

- A network structure whose design contains more that one topology is referred as hybrid topology.



- **Features**
  - Combinations of two or more topologies
  - Inherits the advantages and disadvantages of the topologies included.
- **Advantages**
  - Reliable as error correction and trouble shooting is easy.
  - Scalable (Size can be increased and decreased easily).
- **Disadvantages**
  - Costly.
  - Complex Design.

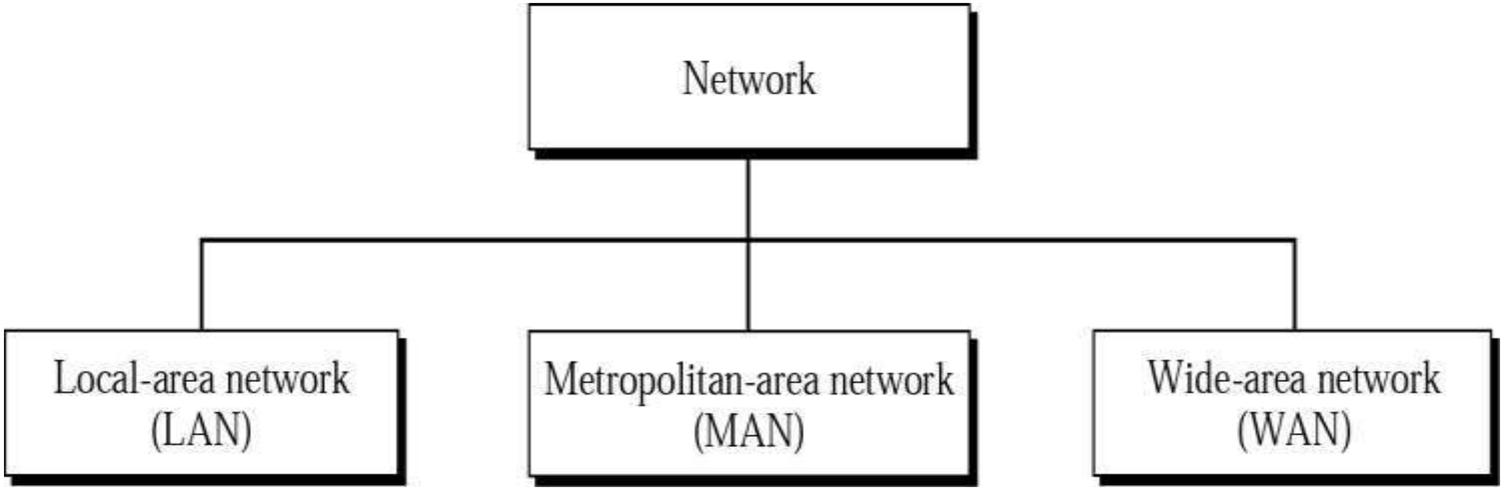
Comparison of Network Topologies



Topology	Advantages	Disadvantages
Bus	Cheap. Easy to install.	Difficult to reconfigure. Break in bus disables entire network.
Star	Cheap. Easy to install. Easy to reconfigure. Fault tolerant.	More expensive than bus.
Ring	Efficient. Easy to install.	Reconfiguration difficult. Very expensive.
Mesh	Simplest. Most fault tolerant.	Reconfiguration extremely difficult. Extremely expensive. Very complex.

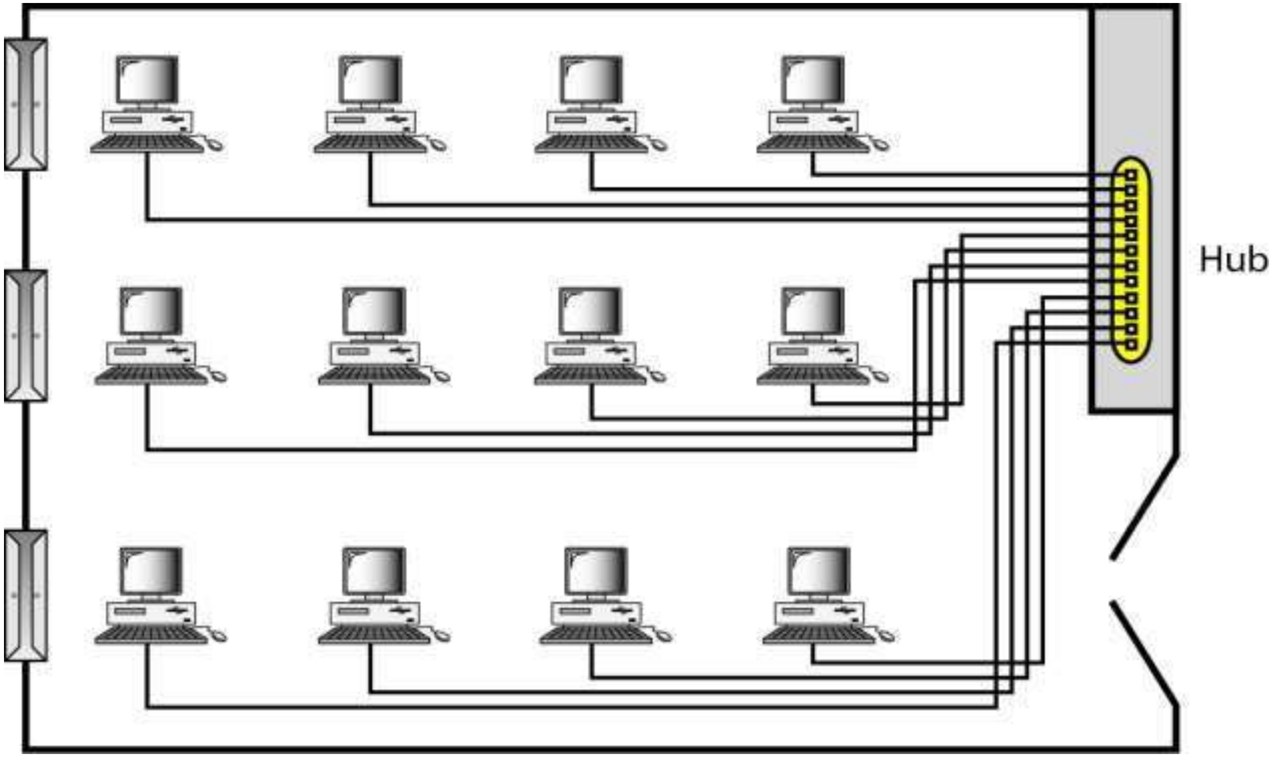
Types of Networks

The types of network are classified based upon the size, the area it covers and its physical architecture. The three primary network categories are LAN, WAN and MAN.



Local Area Networks (LANs)

- Short distances
- Designed to provide local interconnectivity

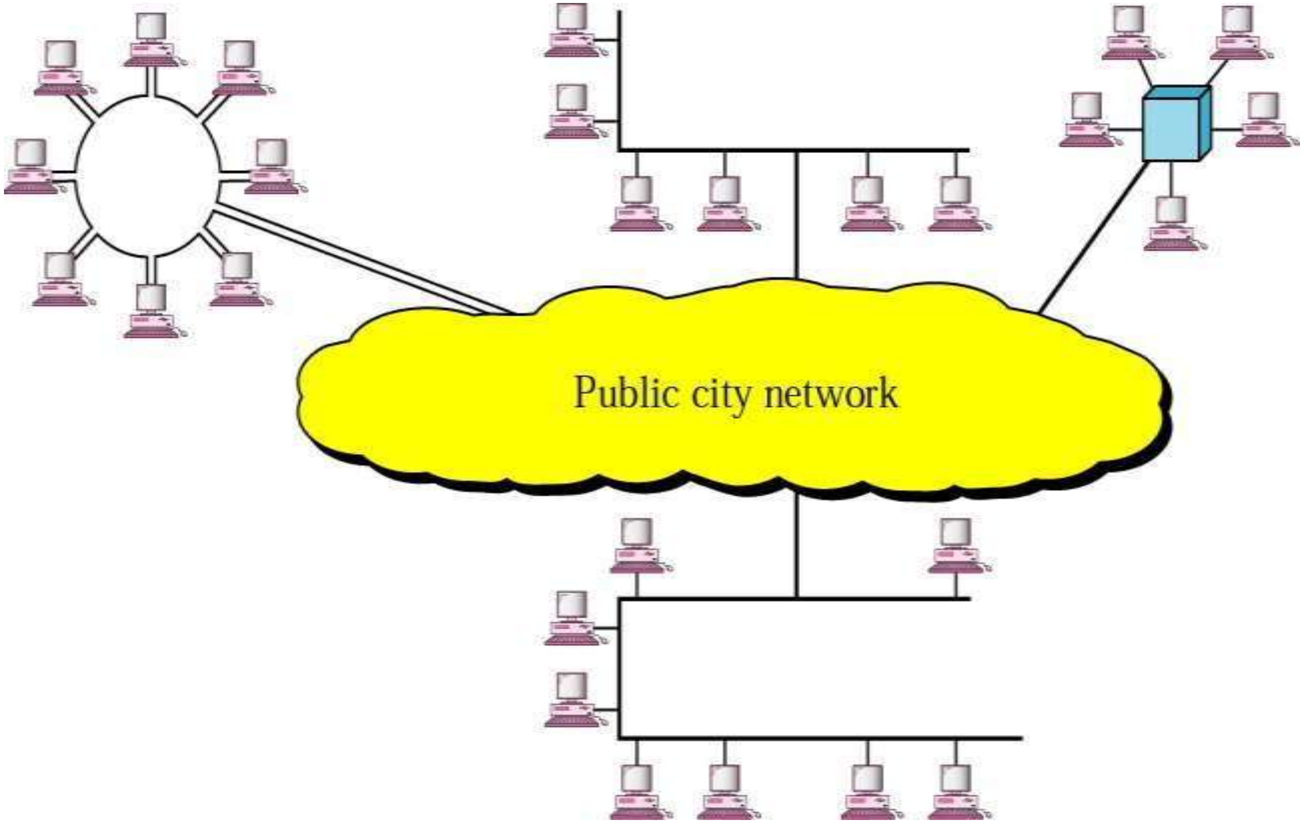


Local Area Networks (LANs)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

Metropolitan Area Networks (MANs)

- Designed to extend to an entire city
- Cable TV network, a company’s connected LAN’s



Metropolitan Area Networks (MANs)

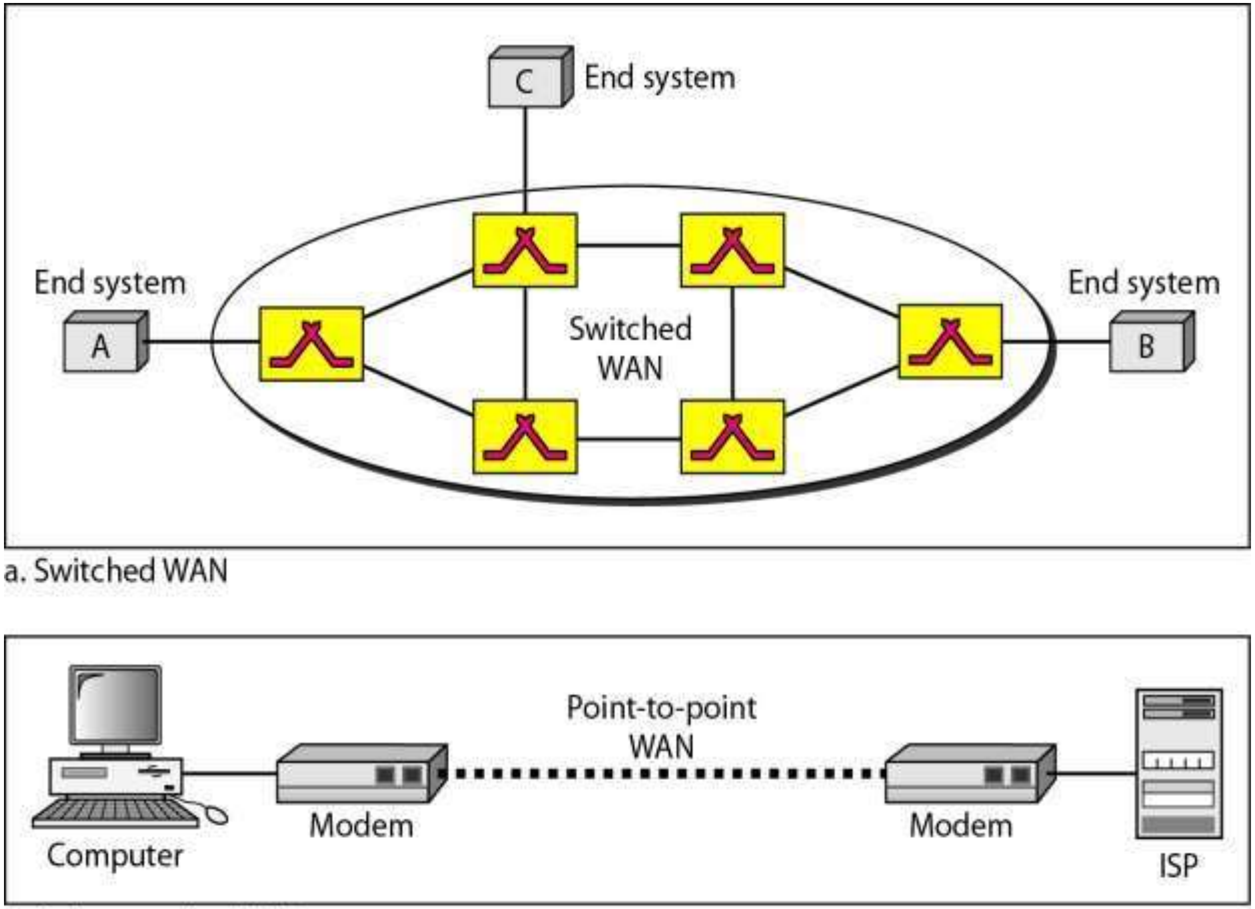
- A metropolitan area network is a network that covers areas with in the city by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).

Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

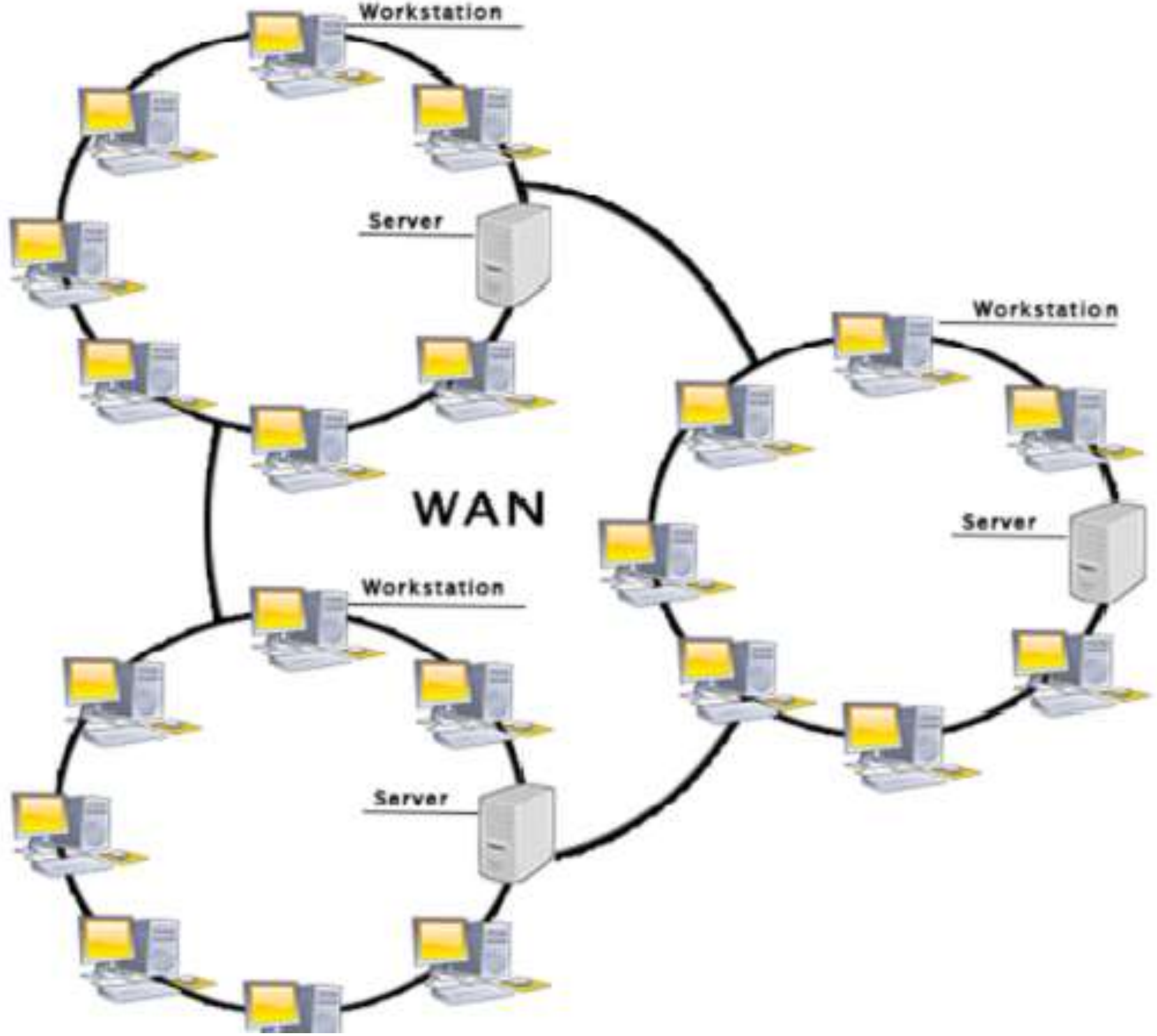
Wide Area Networks(WANs)

- Long distance transmission, e.g., a country, a continent, the world



a. Switched WAN

b. Point-to-point WAN


Workstation
Server
Workstation
WAN
Server
Workstation
Server

Wide Area Networks(WANs)

•A Wide Area Network is a network that extends over a large geographical area such as states or countries.

•A Wide Area Network is quite bigger network than the LAN.

•. A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links.

•The internet is one of the biggest WAN in the world.

•A Wide Area Network is widely used in the field of Business, government, and education.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. T.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

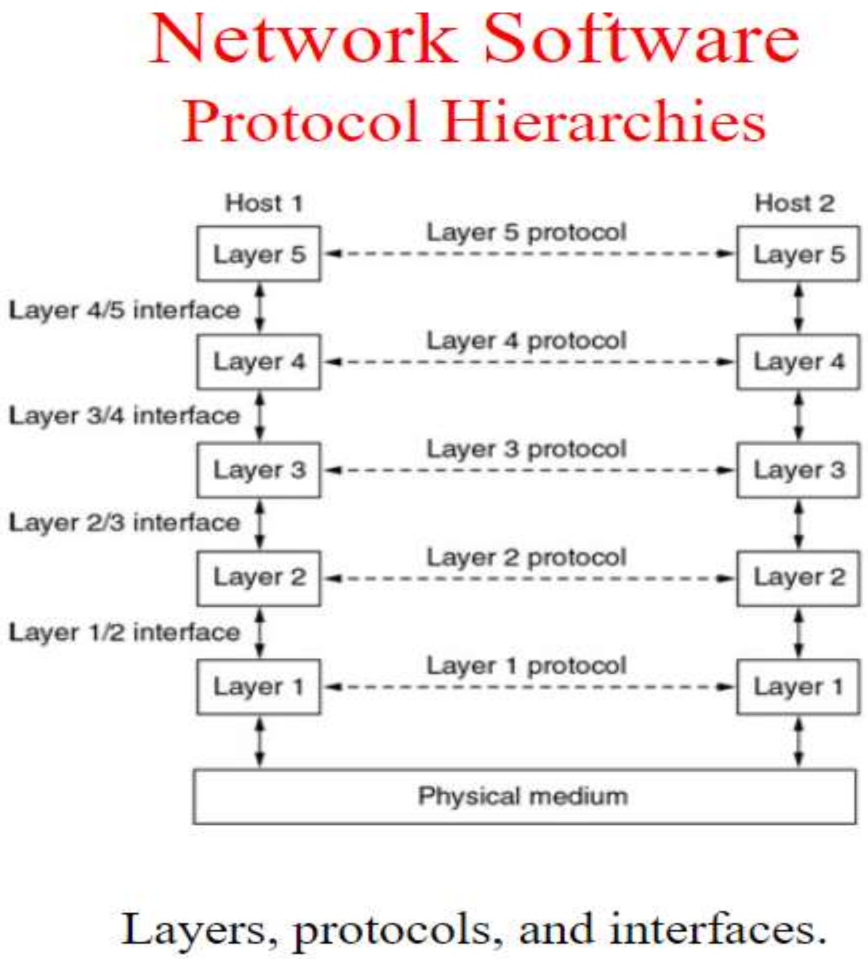
The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Network Software

- Protocol Hierarchies
- Design Issues for the Layers
- Connection-Oriented and Connectionless Services
- Service Primitives
- The Relationship of Services to Protocols

1. Protocol Hierarchies

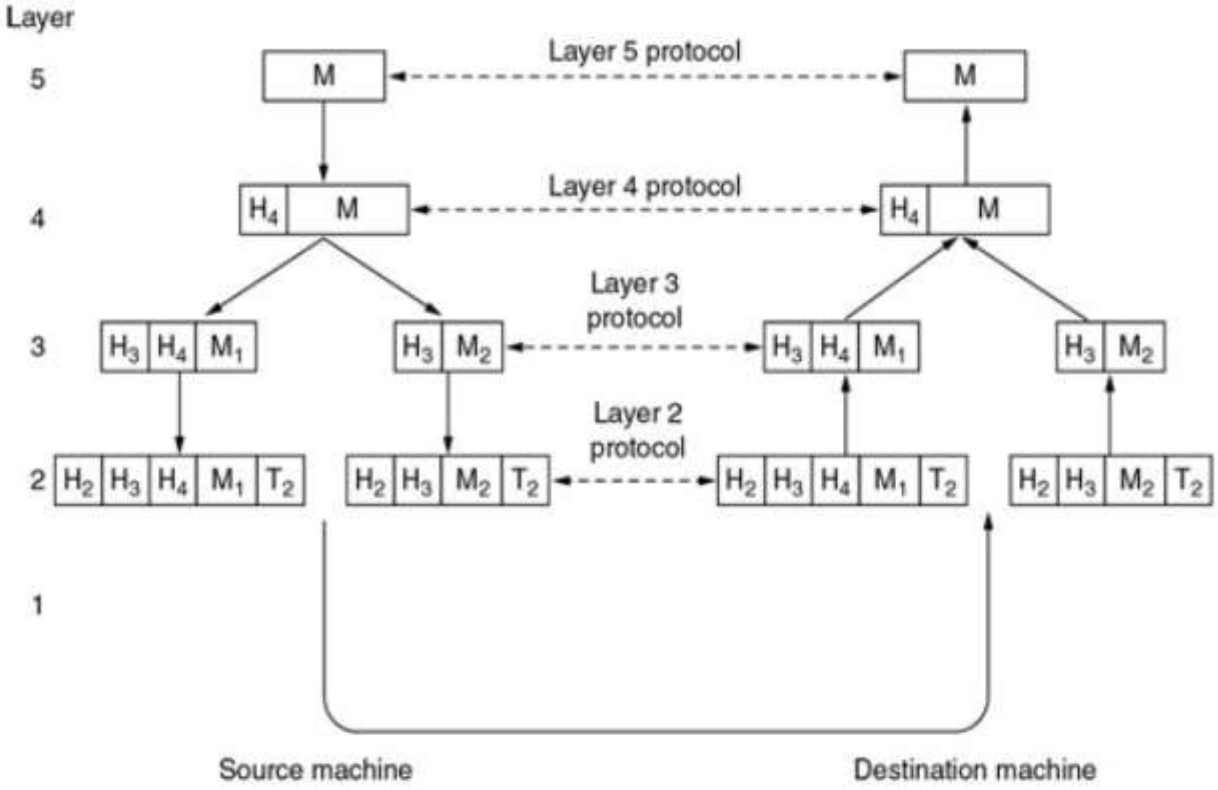


Network Software

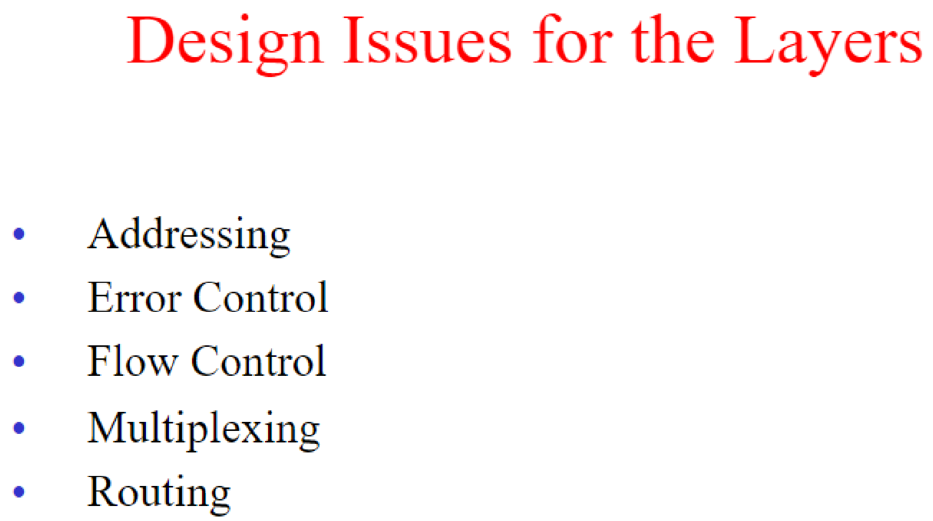
Protocol Hierarchies

Layers, protocols, and interfaces.

Protocol Hierarchies (3)



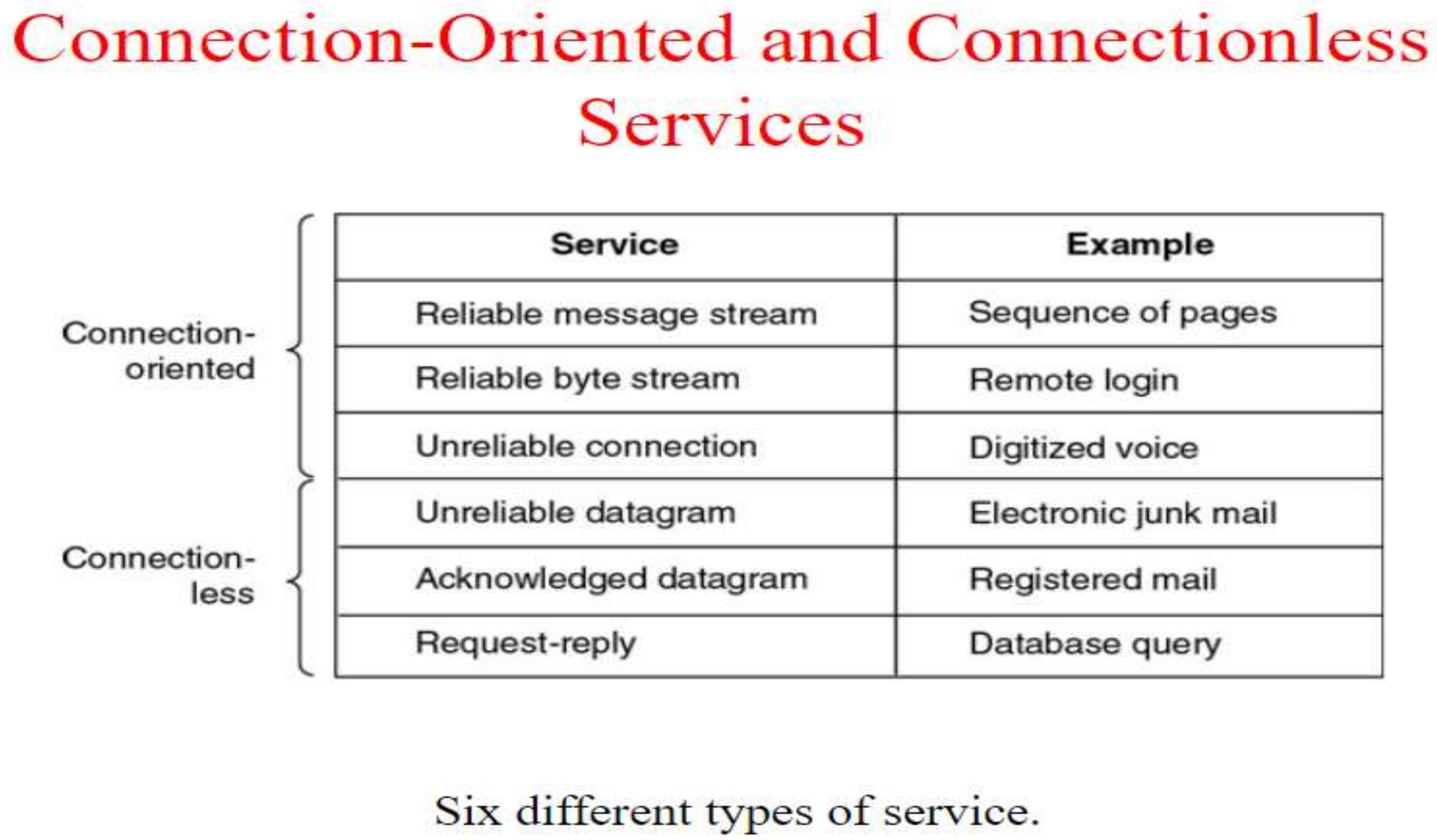
2. Design Issues for the layers



Design Issues for the Layers

- Addressing
- Error Control
- Flow Control
- Multiplexing
- Routing

3. Connection oriented & Connectionless Services

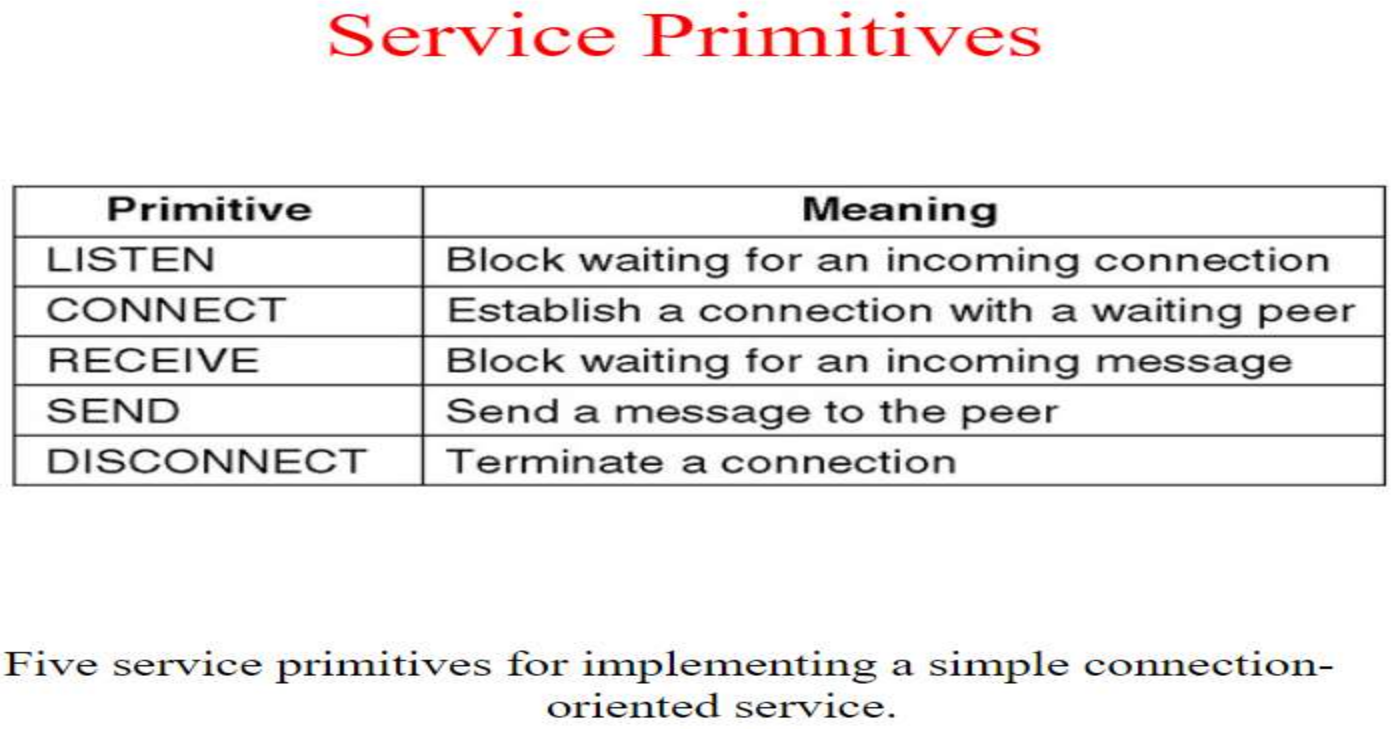


Connection-Oriented and Connectionless Services

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Six different types of service.

4. Service Primitives (Set of Operations)



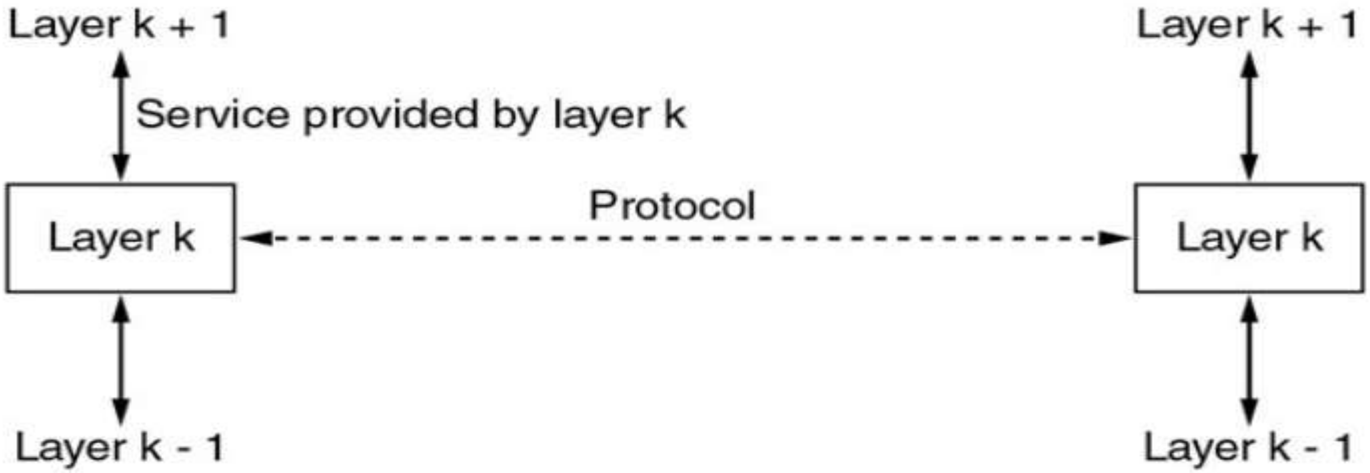
Service Primitives

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Five service primitives for implementing a simple connection-oriented service.

5. Relationship of services to protocols

Services to Protocols Relationship



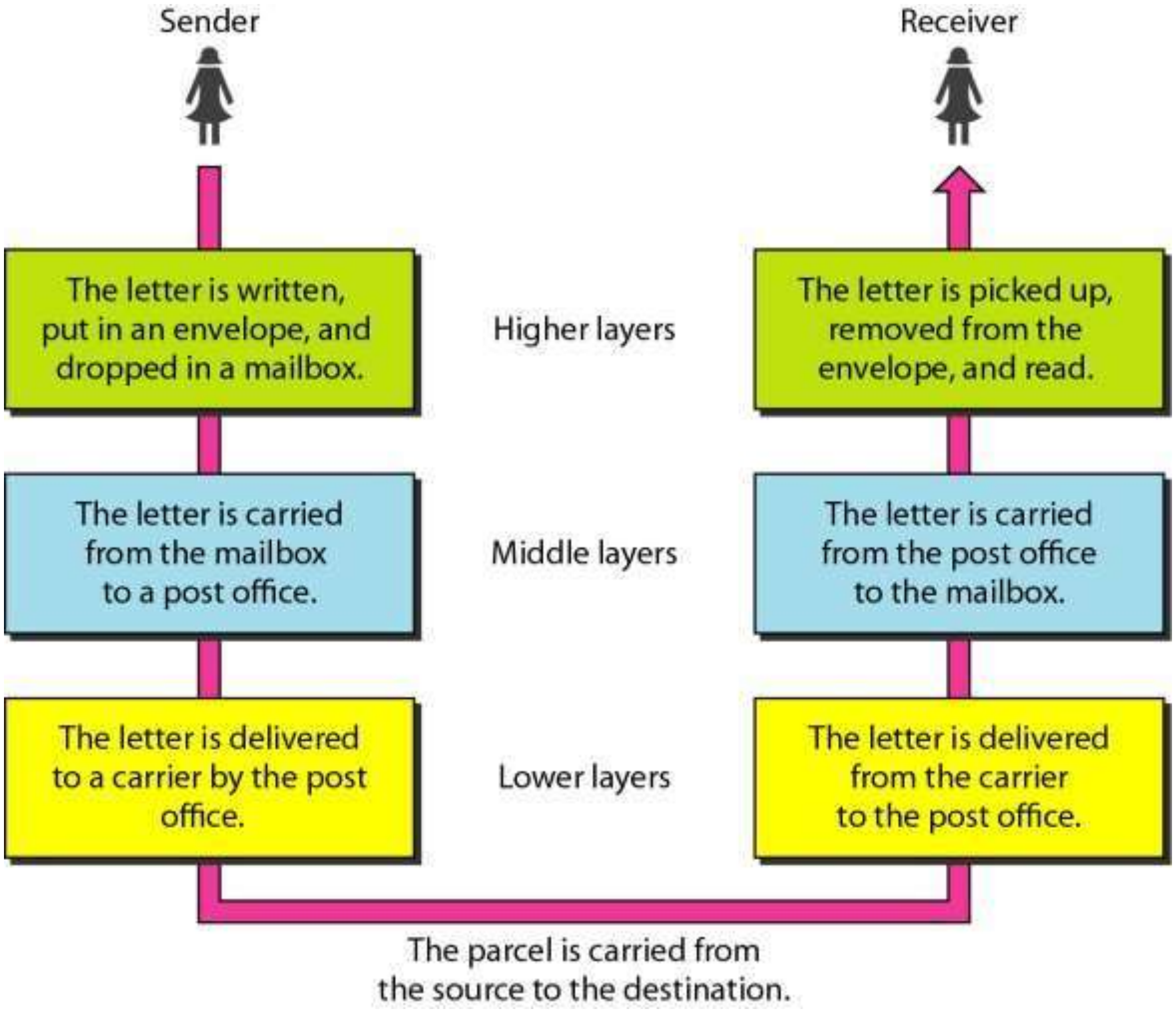
The relationship between a service and a protocol.

Reference Models : OSI Model, TCP/IP Model,

LAYERED TASKS

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office.

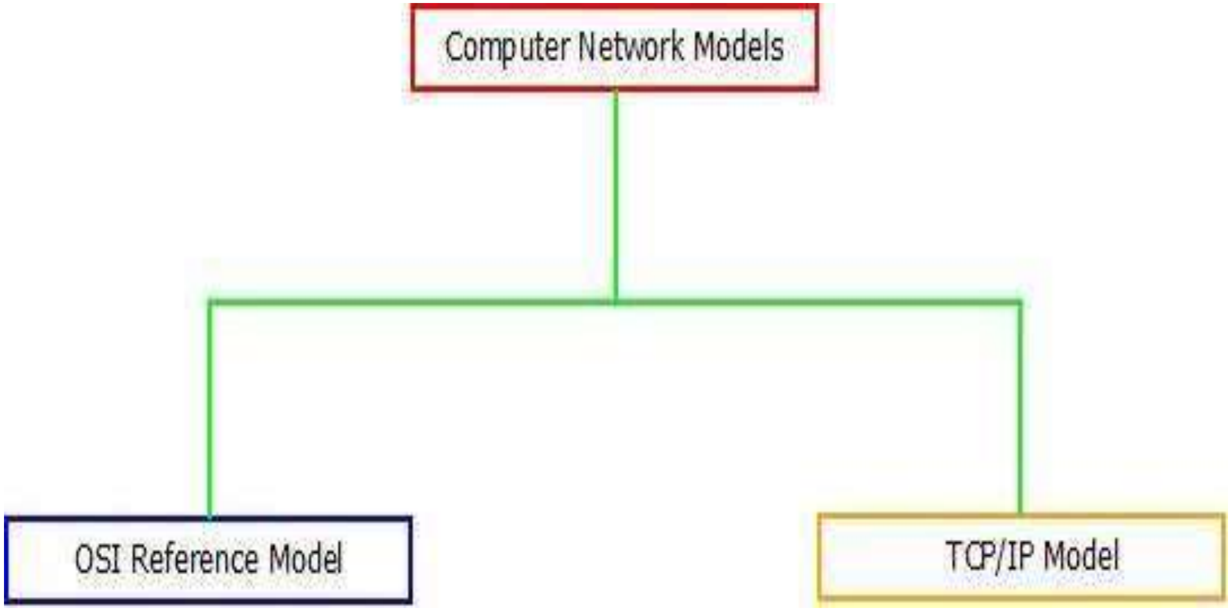
Tasks involved in sending a letter


Sender
Receiver
The letter is written, put in an envelope, and dropped in a mailbox.
Higher layers
The letter is picked up, removed from the envelope, and read.
The letter is carried from the mailbox to a post office.
Middle layers
The letter is carried from the post office to the mailbox.
The letter is delivered to a carrier by the post office.
Lower layers
The letter is delivered from the carrier to the post office.
The parcel is carried from the source to the destination.

Reference Models : OSI Model, TCP/IP Model,

- Computer network reference models are responsible for establishing a connection among the sender and receiver and transmitting the data in a smooth manner respectively.

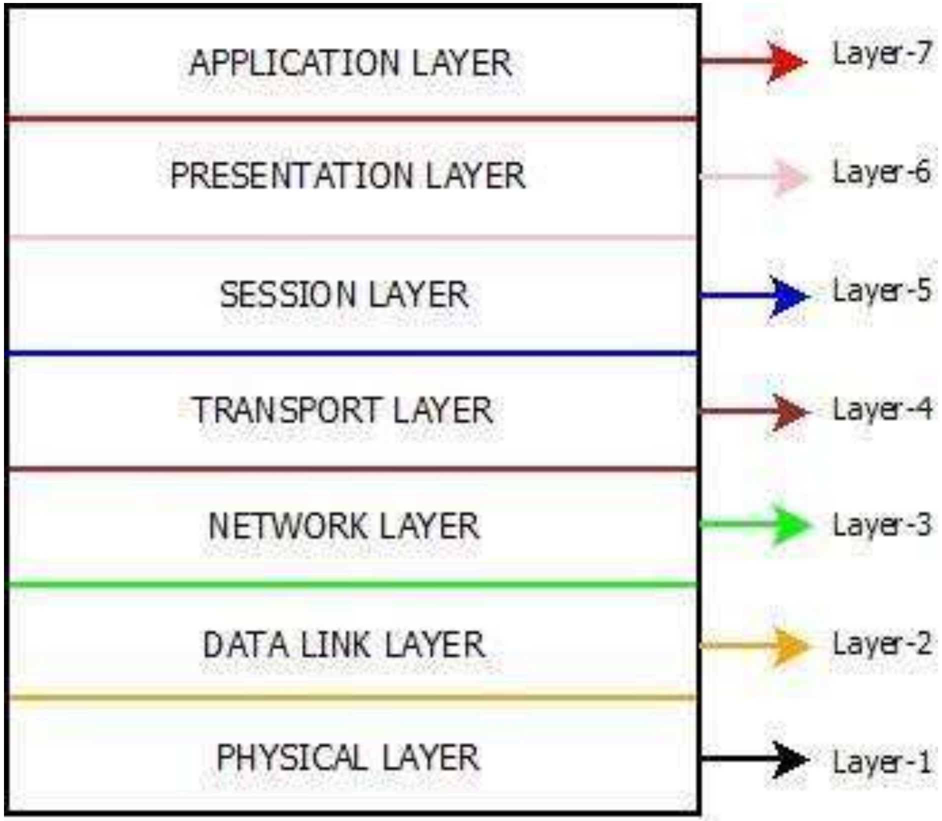
- There are two computer network models i.e. OSI Model and TCP/IP Model on which the whole data communication process relies.



OSI Reference Model

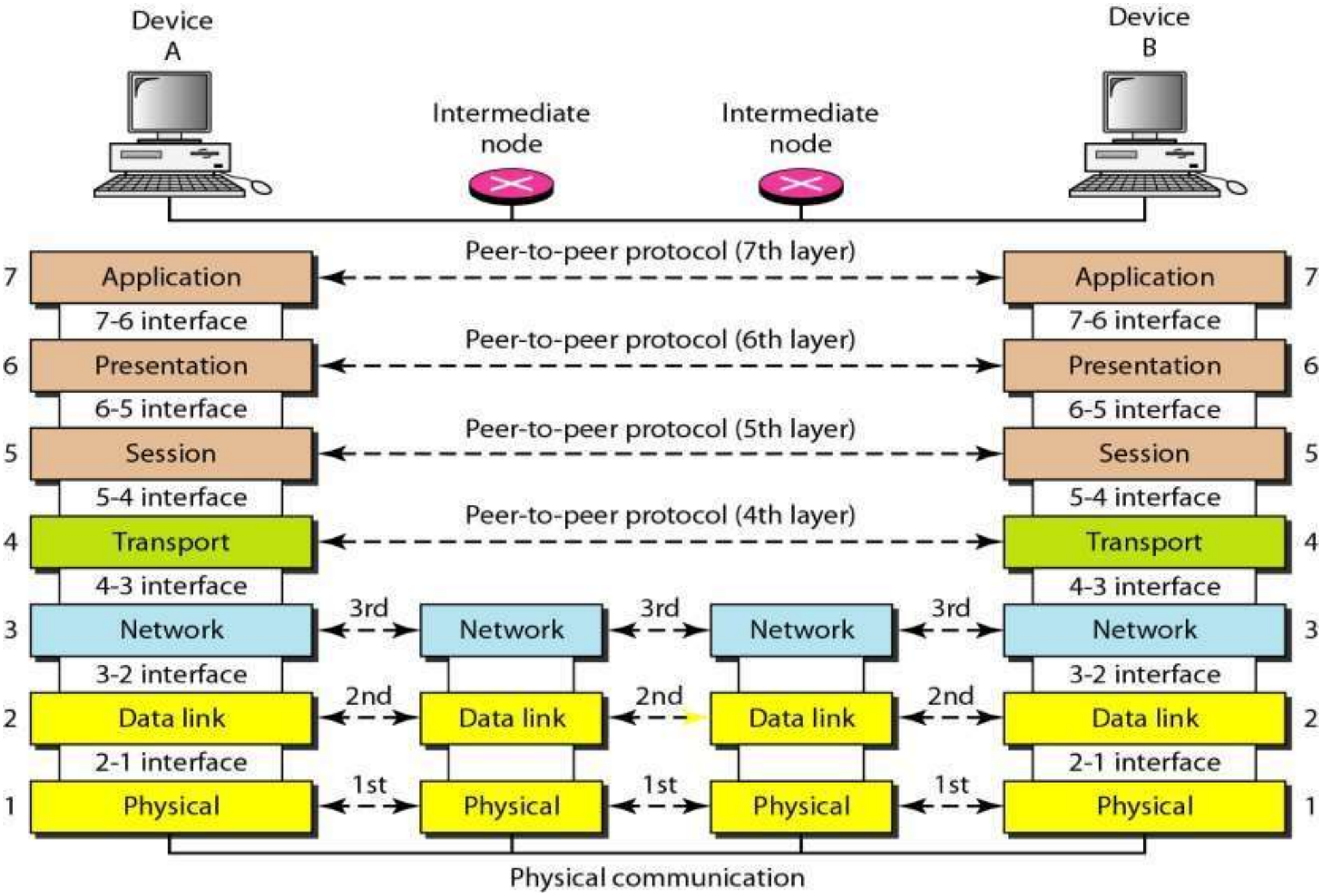
- OSI stands for Open Systems Interconnection
- Created by International Standards Organization (ISO)
- Was created as a framework and reference model to explain how different networking technologies work together and interact
- It is not a standard that networking protocols must follow
- OSI model is called as “Open Source” because of its “fit anywhere” ability. Any connection can be established using the OSI model unless and until any protocols are not used as OSI model does not support protocol establishment. It runs without the use of protocols
- Each layer has specific functions it is responsible for
- All layers work together in the correct order to move data around a network

Seven layers of the OSI model



The OSI Reference Model

Computer Network Models : Architecture And Layers of OSI Reference Model



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.

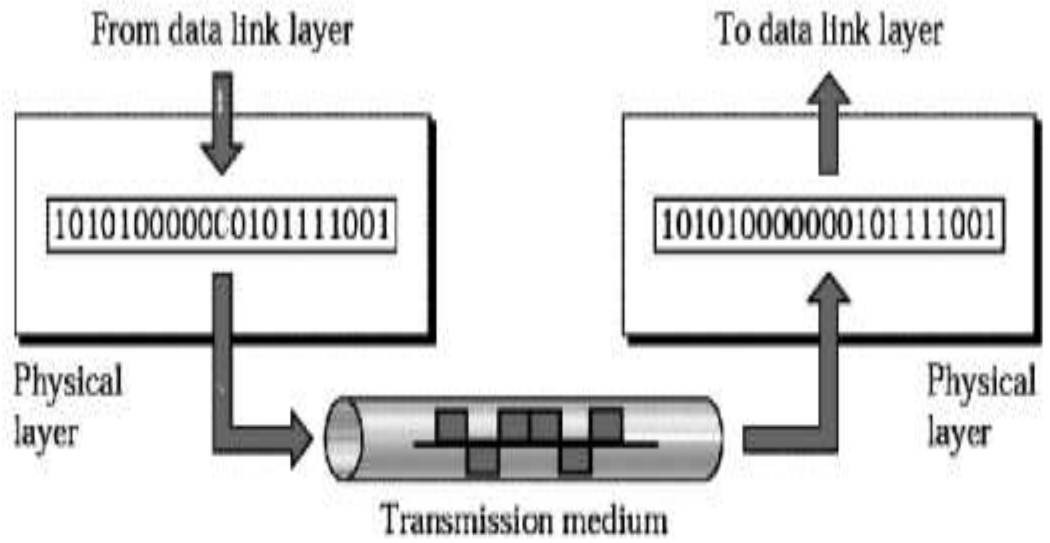
- The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next.

- 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.

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

Physical Layer (Layer 1) :

The physical layer coordinates the functions required to transmit a bit stream over a physical medium.



Physical Layer (Layer 1) :

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.

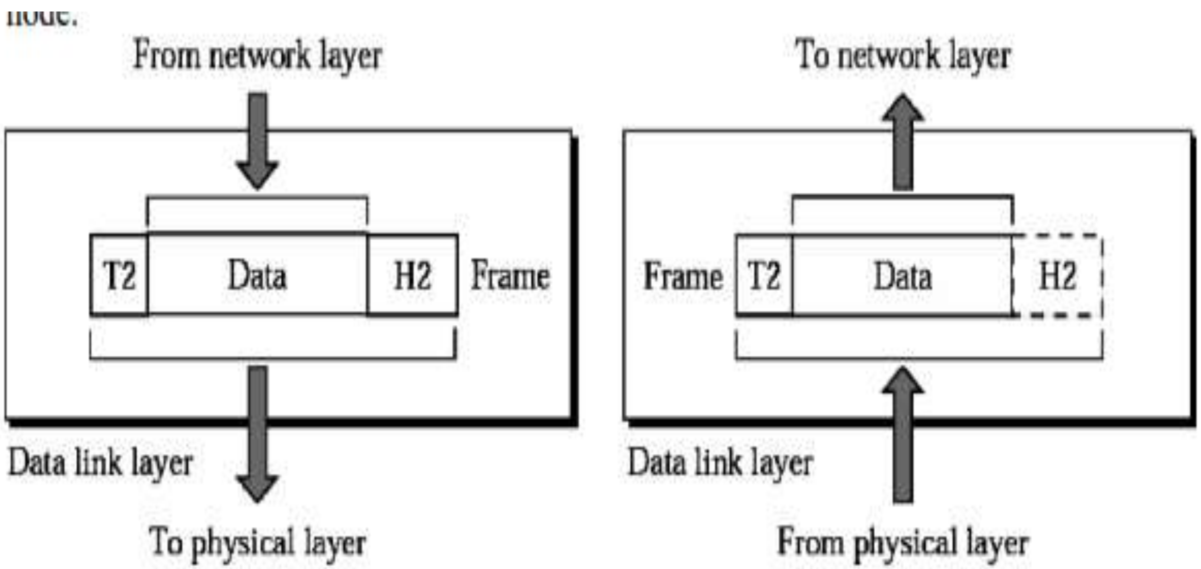
Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.

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 full-duplex.

Data Link Layer (DLL) (Layer 2) :

It is responsible for transmitting frames from one node to next node.



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.

Data Link Layer is divided into two sub layers :

- **Logical Link Control (LLC)**
- **Media Access Control (MAC)**

Data Link Layer (DLL) (Layer 2) :

Logical Link Control (LLC)

- 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.

Media Access Control (MAC)

- The Receiver’s MAC address is obtained by placing anARP(Address Resolution Protocol) request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.

The functions of the data Link layer are : - Framing, Physical addressing , Error control, Flow Control, Access control.

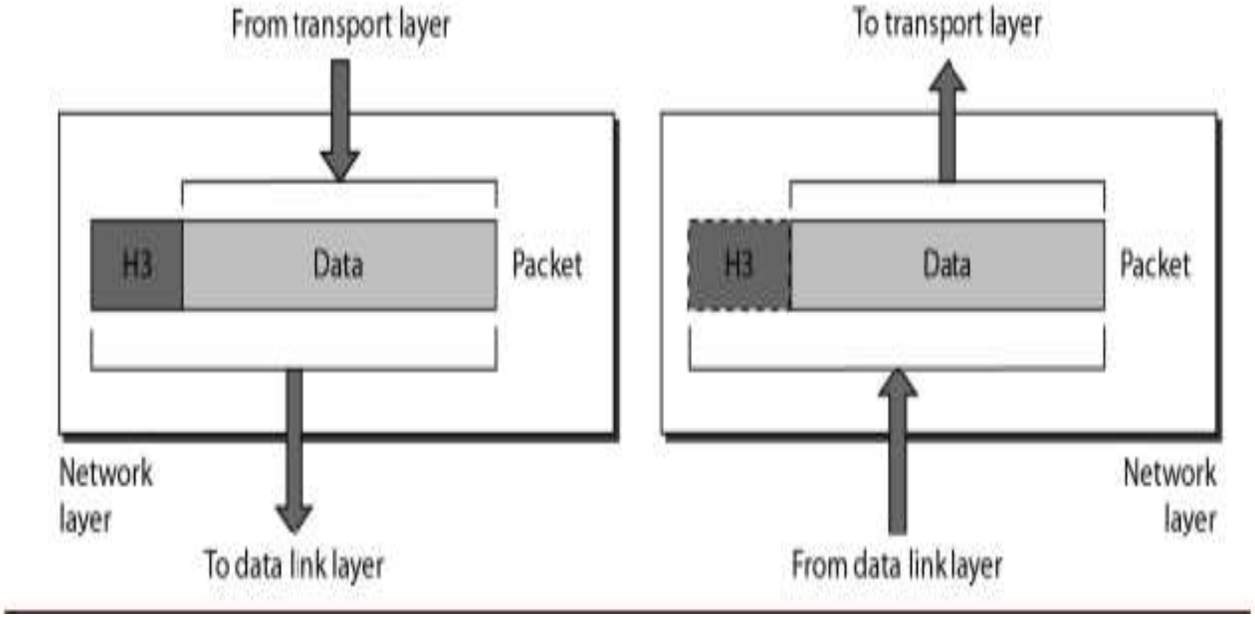
- Switch & Bridge are Data Link Layer devices.

Data Link Layer (DLL) (Layer 2) :

- **Framing** - Divides the stream of bits received into data units called frames.
- **Physical addressing** – If frames are to be distributed to different systems on the n/w , data link layer adds a header to the frame to define the sender and receiver.
- **Flow control-** If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow ctrl mechanism.
- **Error control-** Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
- **Access control -**Used to determine which device has control over the link at any given time.

Network Layer (Layer 3) :

It is mainly required, when it is necessary to send information from one network to another.



Network Layer (Layer 3) :

- Network layer works for the transmission of data from one host to the other located in different networks

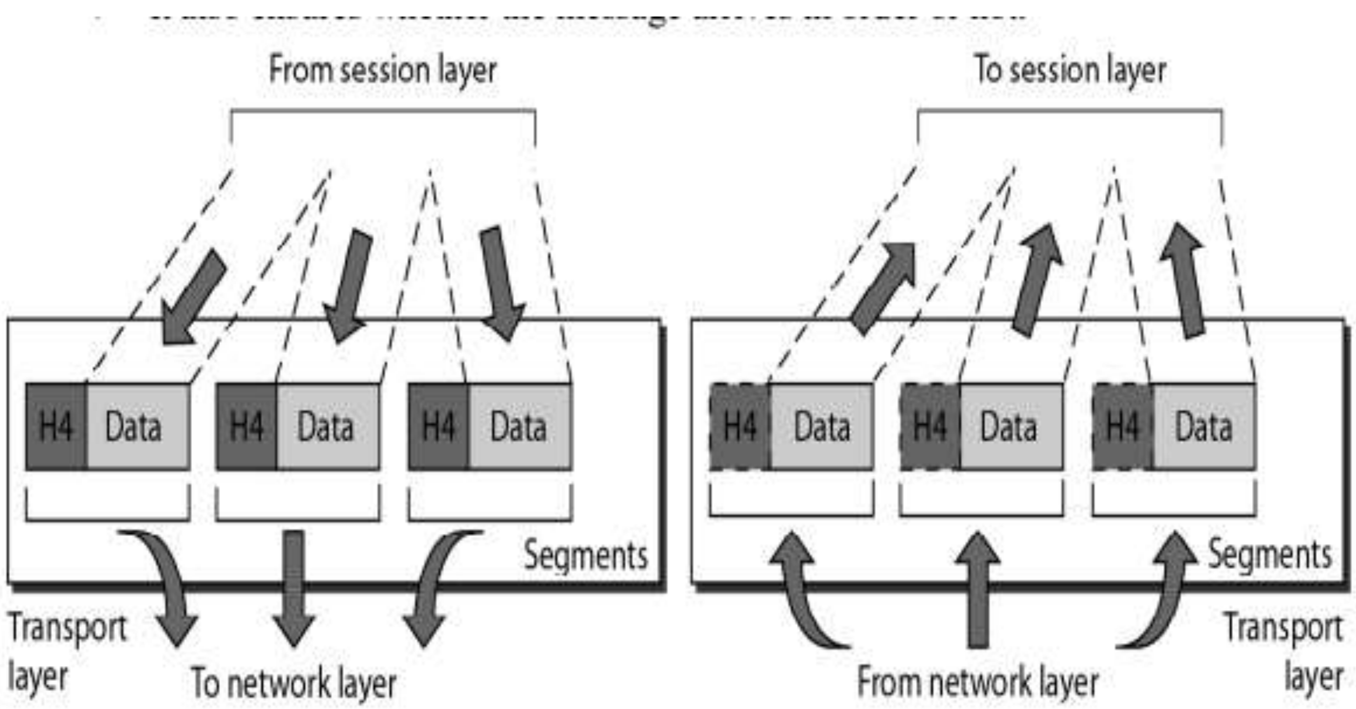
The functions of the Network layer are :

1. **Routing:–** The devices which connects various networks called routers are responsible for delivering packets to final destination. The network layer protocols determine which route is suitable from source to destination.

2.Logical Addressing: The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

* *Segment* in Network layer is referred as **Packet**.

Transport Layer(Layer 4) :



Transport Layer(Layer 4) :

- 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.

- In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address.

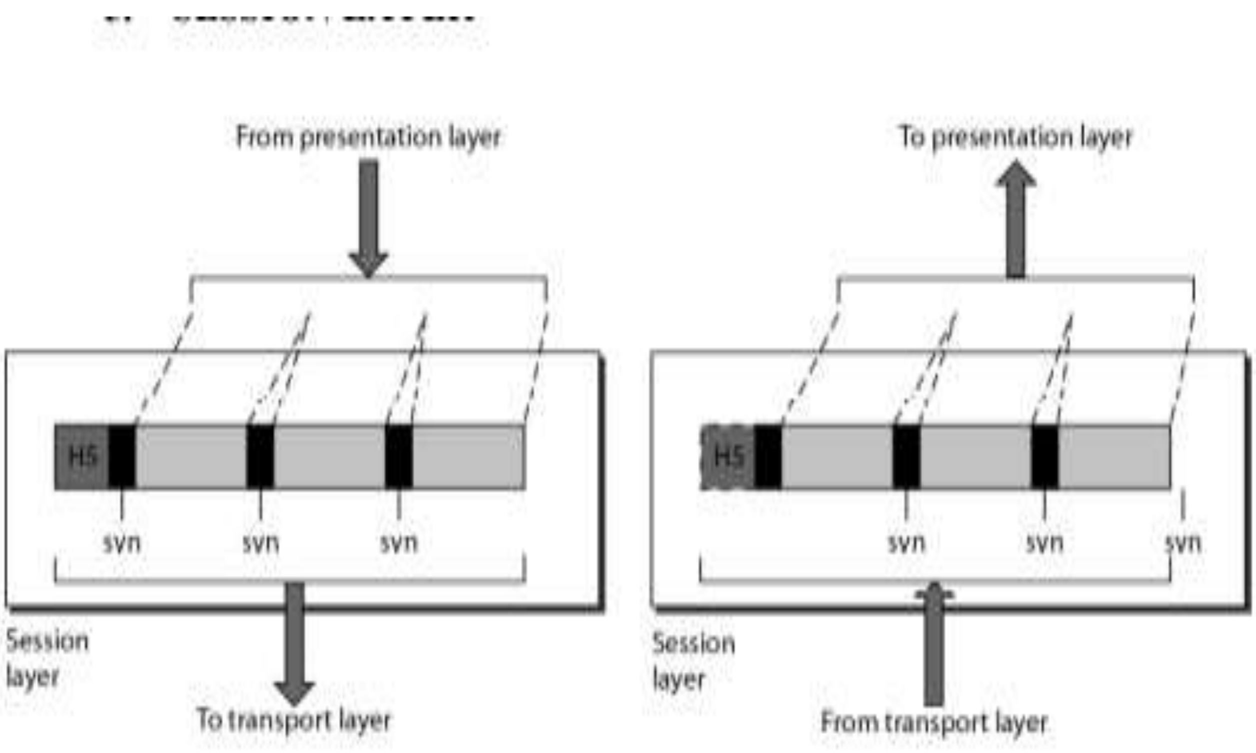
- May use a *connection-oriented protocol* such as TCP to ensure destination received segments

- May use a *connectionless protocol* such as UDP to send segments without assurance of delivery

Functions of Transport Layer(Layer 4) :

- **Port addressing** – The header in this must therefore include a address called port address. This layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.
- Connection control - This can either be connectionless or connection-oriented. The connectionless treats each segment as a individual packet and delivers to the destination. The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.
- **Flow and error control** - Similar to data link layer, but process to process take place.

Session Layer (Layer 5) :



Session Layer (Layer 5) :

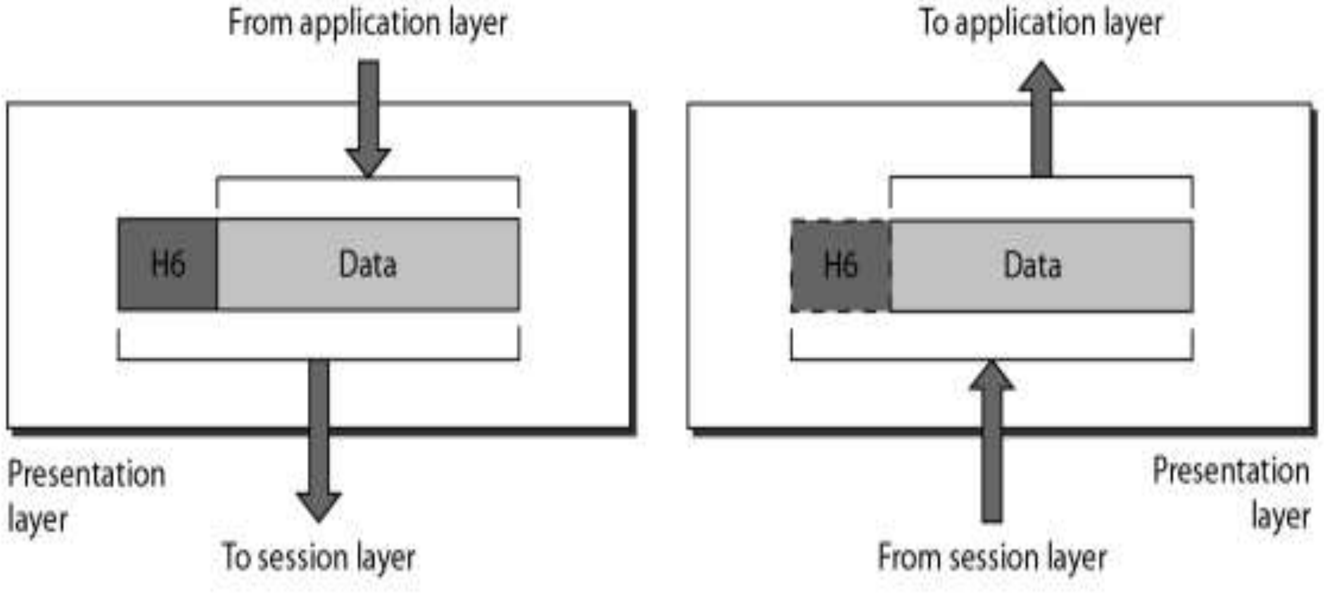
- This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
- The session layer allows two systems to start communication with each other in half-duplex or full-duplex.
- This layer allows a process to add checkpoints which are considered as synchronization points into the data.
- These synchronization point help to identify the error so that the data is re-synchronized properly and data loss is avoided

Functions of Session layer

- **Dialog control -** This session allows two systems to enter into a dialog either in half duplex or full duplex.
- **Synchronization -**This allows to add checkpoints into a stream of data.

Presentation Layer (Layer 6) :

It is concerned with the syntax and semantics of information exchanged between two systems.



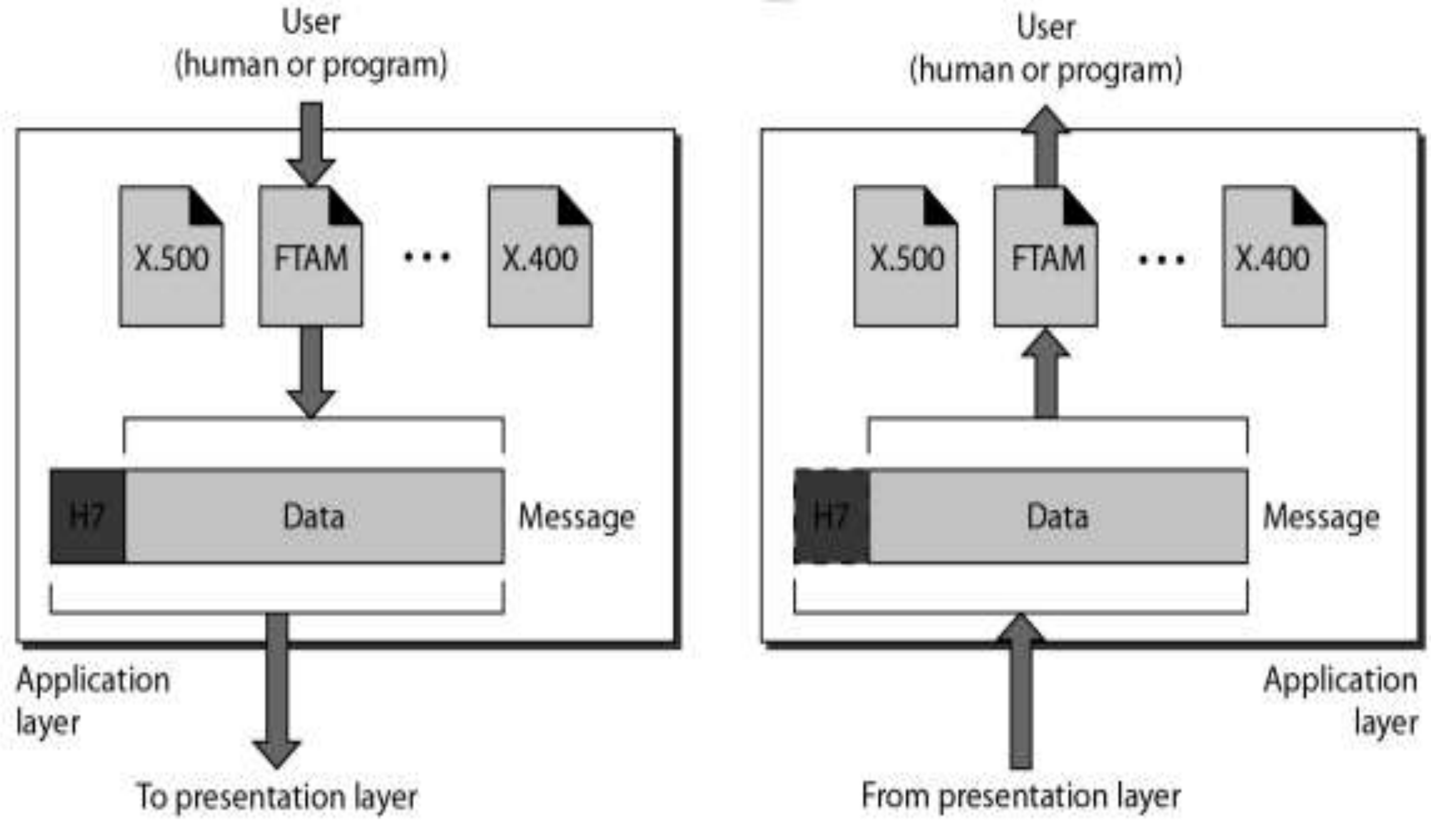
Presentation Layer (Layer 6) :

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

The functions of the presentation layer are :

- **Translation** : For example, ASCII to EBCDIC.
- **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.

Application Layer (Layer 7) :



Application Layer (Layer 7) :

- Contains all services or protocols needed by application software or operating system to communicate on the network.

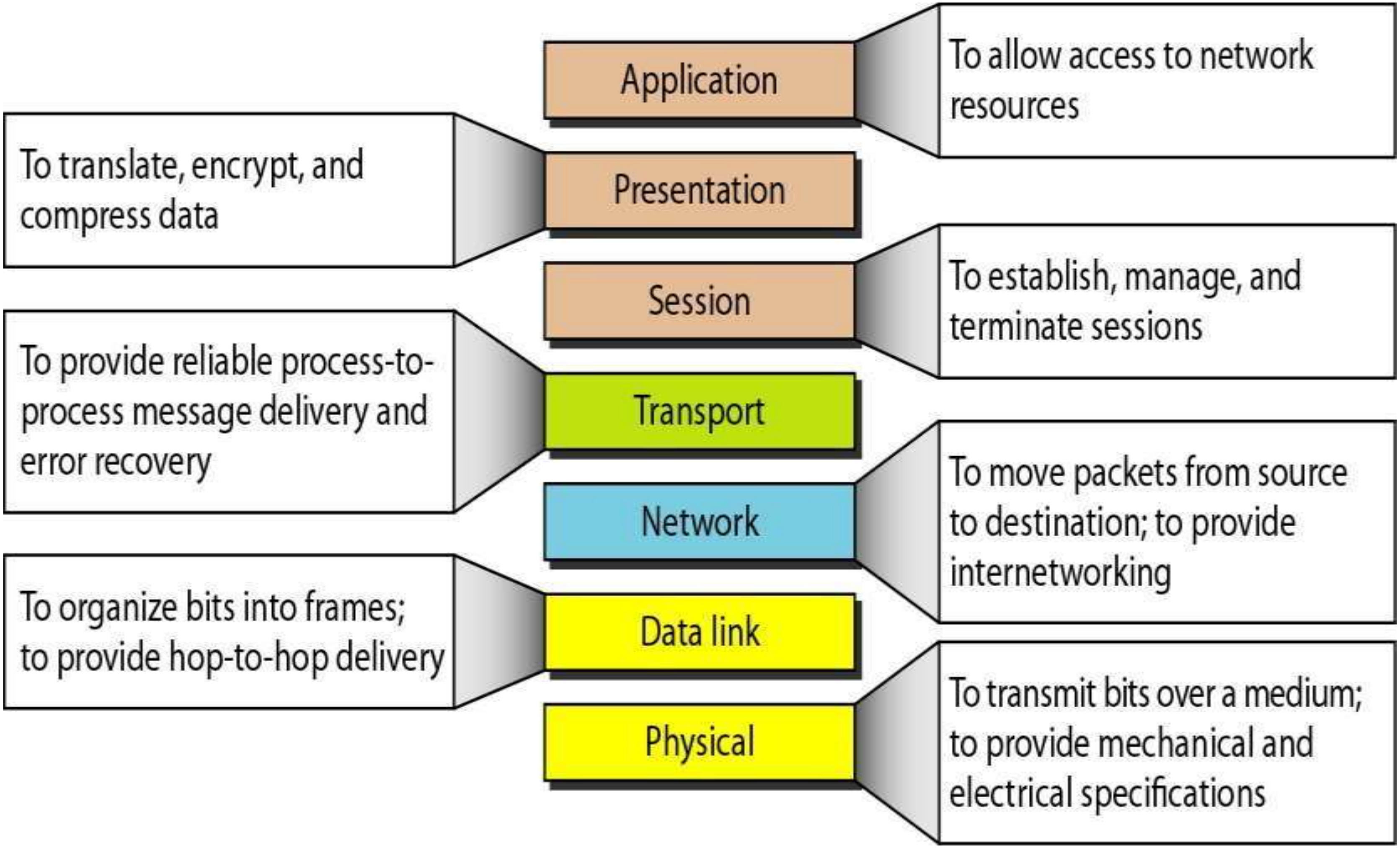
  The other responsibilities of this layer are

  - FTAM(file transfer,access,mgmt) - Allows user to access files in a remote host.
  - Mail services - Provides email forwarding and storage.
  - Directory services - Provides database sources to access information about various sources and objects
- Examples

  ○ –Firefox web browser uses HTTP (Hyper-Text Transport Protocol)

  ○ –E-mail program may use POP3 (Post Office Protocol version 3) to read e-mails and SMTP (Simple Mail Transport Protocol) to send e-mails

SUMMARY:



Application

To allow access to network resources

Presentation

To translate, encrypt, and compress data

Session

To establish, manage, and terminate sessions

Transport

To provide reliable process-to-process message delivery and error recovery

Network

To move packets from source to destination; to provide internetworking

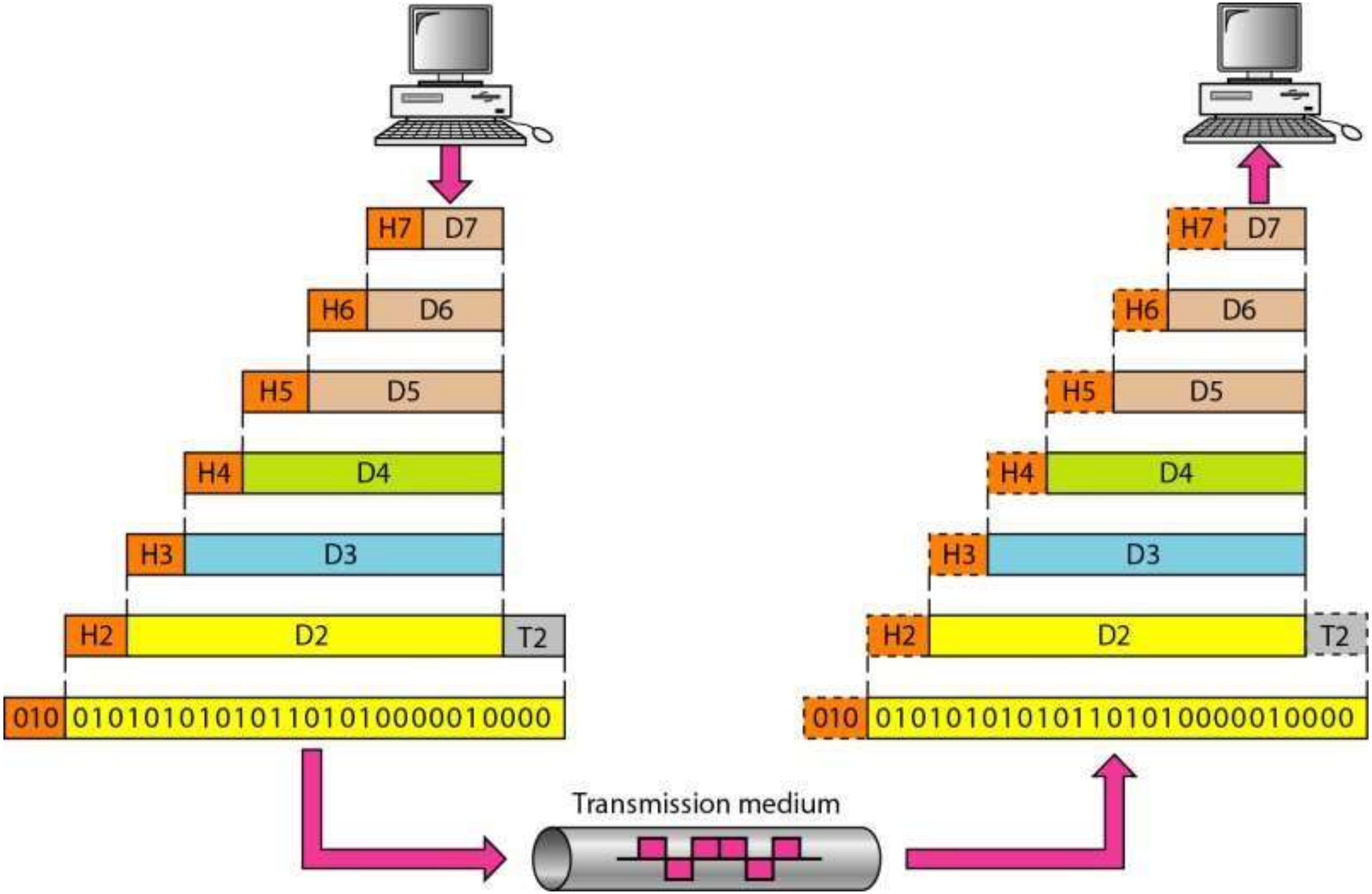
Data link

To organize bits into frames; to provide hop-to-hop delivery

Physical

To transmit bits over a medium; to provide mechanical and electrical specifications

An exchange using the OSI model



TCP/IP Model(Transmission Control Protocol/Internet Protocol)

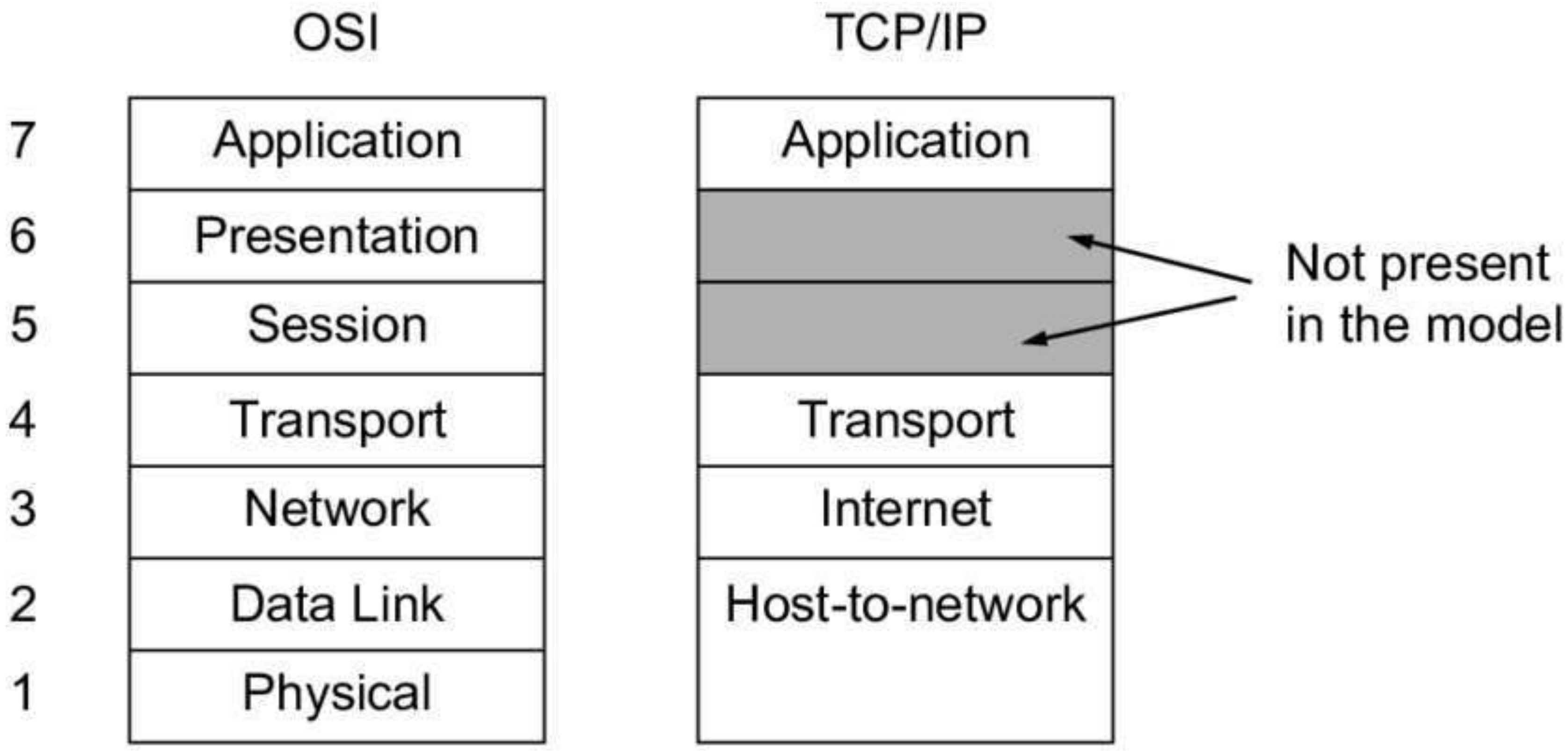
- The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.

- But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols.

- 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:

TCP/IP Model(Contd..)

The four layers in the TCP/IP protocol suite are−

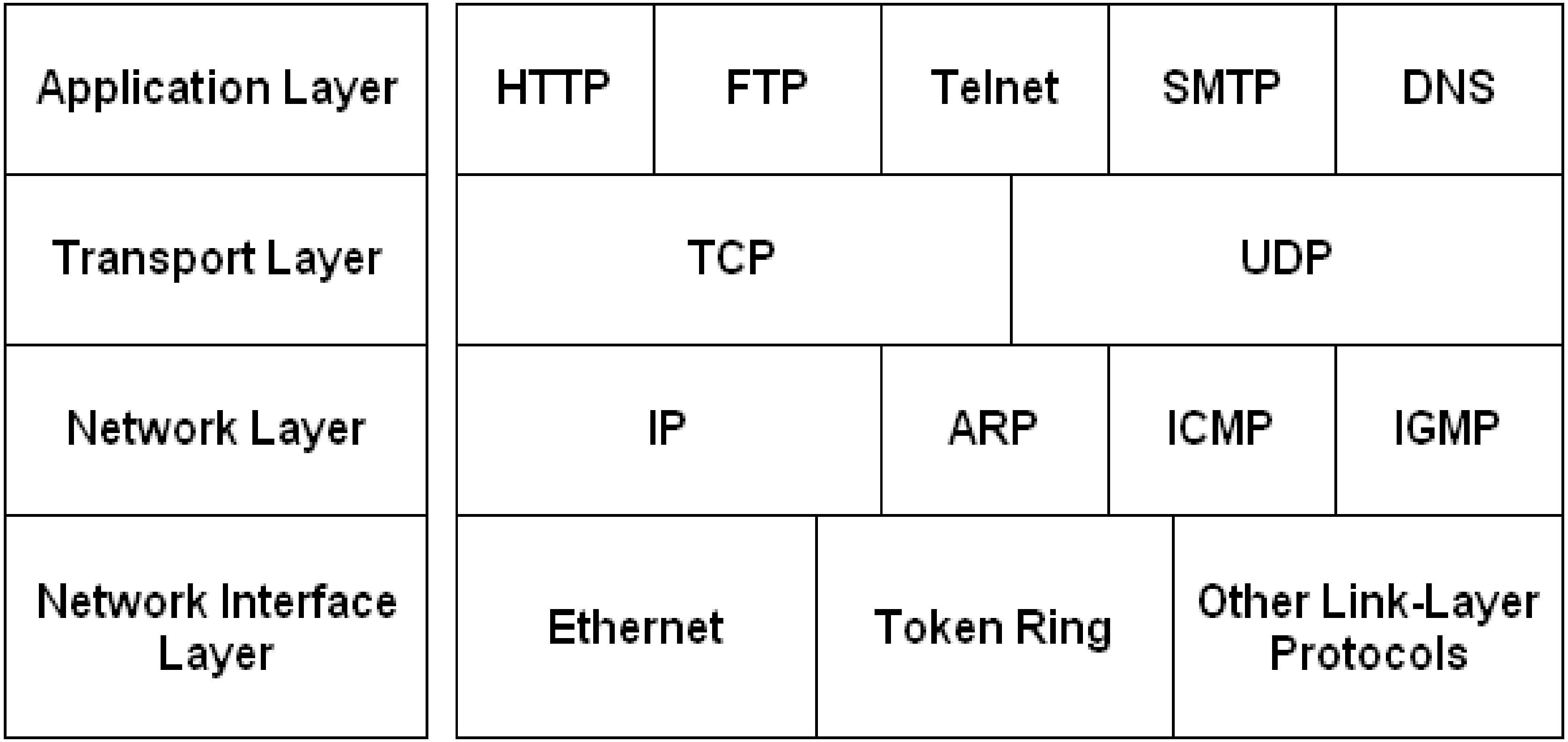


	OSI	TCP/IP
7	Application	Application
6	Presentation	▨
5	Session	▨
4	Transport	Transport
3	Network	Internet
2	Data Link	Host-to-network
1	Physical	

Not present in the model

TCP/IP Layers

TCP/IP Prototocols



Application Layer — HTTP, FTP, Telnet, SMTP, DNS

Transport Layer — TCP, UDP

Network Layer — IP, ARP, ICMP, IGMP

Network Interface Layer — Ethernet, Token Ring, Other Link-Layer Protocols

Application Layer

- Application layer protocols define the rules when implementing specific network applications
  - **FTP** – File Transfer Protocol **–** used for file transfer
  - **Telnet** – Remote terminal protocol
    - For remote login on any other computer on the network
  - **SMTP** – Simple Mail Transfer Protocol
    - used to provide e-mail services.
  - **HTTP** – Hypertext Transfer Protocol
    - For Web browsing
  - **DNS – Domain Name System**
    - The protocol that allows you to refer to other host computers by using names rather than numbers.

Transport layer

The Transport layer is where sessions are establishedand data packets are exchanged between hosts. Two core protocols are found at this layer:

- **Transmission Control Protocol (TCP):**
  Provides reliable connection oriented transmission between two hosts. TCP establishes a session between hosts, and then ensures delivery of packets between the hosts.

- **User Datagram Protocol (UDP):**
  Provides connectionless, unreliable, one-to-one **or** one-to-many delivery.

Network layer

The Network layer is where data is addressed, packaged, and routed among networks. Several important Internet protocols operate at the Network layer:

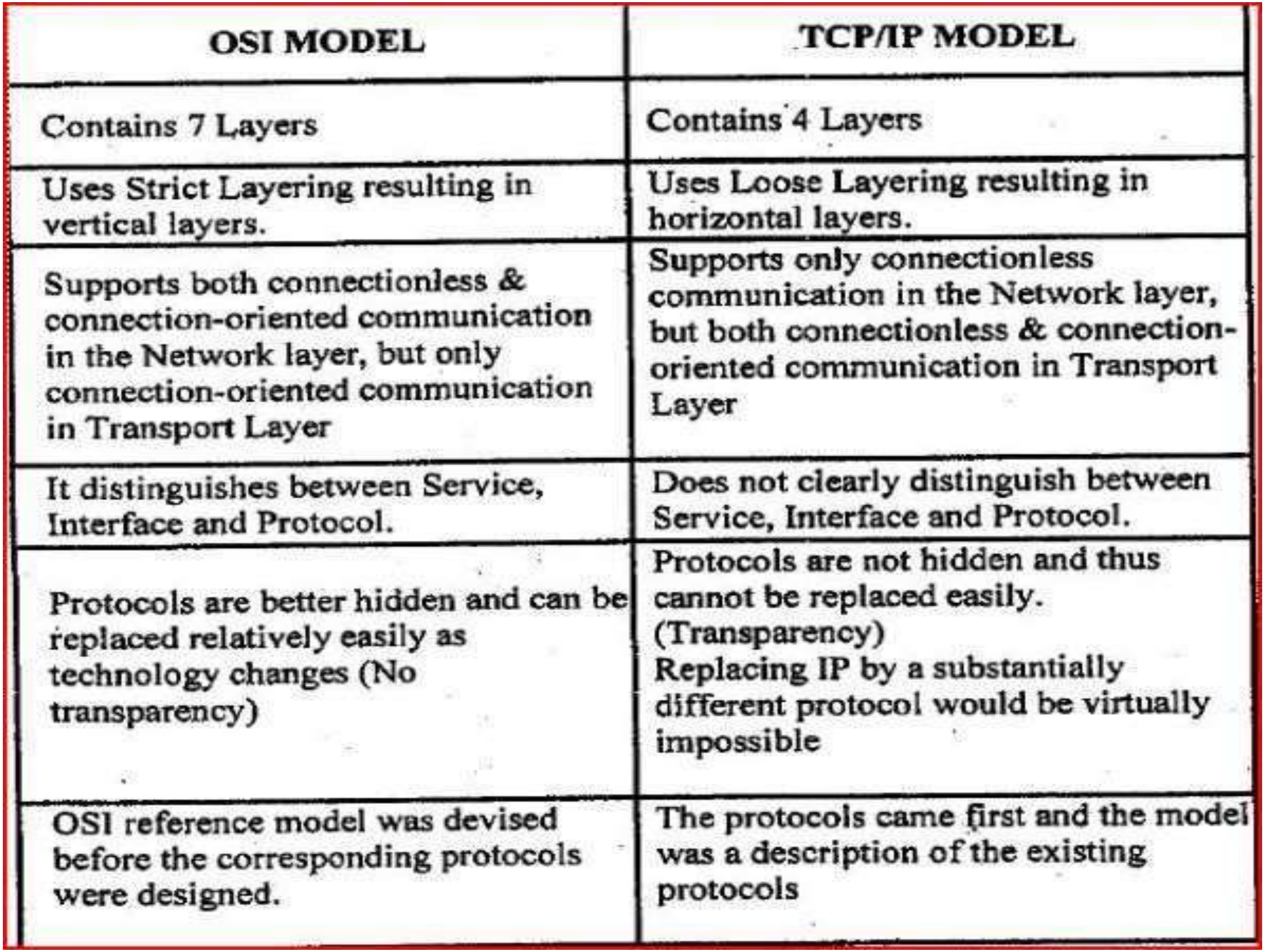
- **Internet Protocol (IP):**
  A routable protocol that uses IP addresses to deliver packets to network devices. IP is an intentionally unreliable protocol, so it does not guarantee delivery of information.

- **Address Resolution Protocol (ARP):**
  Resolves IP addresses to hardware MAC addresses.

- **Internet Control Message Protocol (ICMP):**
  Sends and receives diagnostic messages.

Network interface layer

- The lowest level of the TCP/IP architecture is the Network Interface layer. It corresponds to the OSI's Physical and Data Link layers.
- You can use many different TCP/IP protocols at the Network Interface layer, including Ethernet and Token Ring for local area networks and protocols such as X.25, Frame Relay, and ATM for wide area networks.



OSI MODEL	TCP/IP MODEL
Contains 7 Layers	Contains 4 Layers
Uses Strict Layering resulting in vertical layers.	Uses Loose Layering resulting in horizontal layers.
Supports both connectionless & connection-oriented communication in the Network layer, but only connection-oriented communication in Transport Layer	Supports only connectionless communication in the Network layer, but both connectionless & connection-oriented communication in Transport Layer
It distinguishes between Service, Interface and Protocol.	Does not clearly distinguish between Service, Interface and Protocol.
Protocols are better hidden and can be replaced relatively easily as technology changes (No transparency)	Protocols are not hidden and thus cannot be replaced easily. (Transparency) Replacing IP by a substantially different protocol would be virtually impossible
OSI reference model was devised before the corresponding protocols were designed.	The protocols came first and the model was a description of the existing protocols

Physical Layer

1. Transmission Media

What is Transmission Media ?

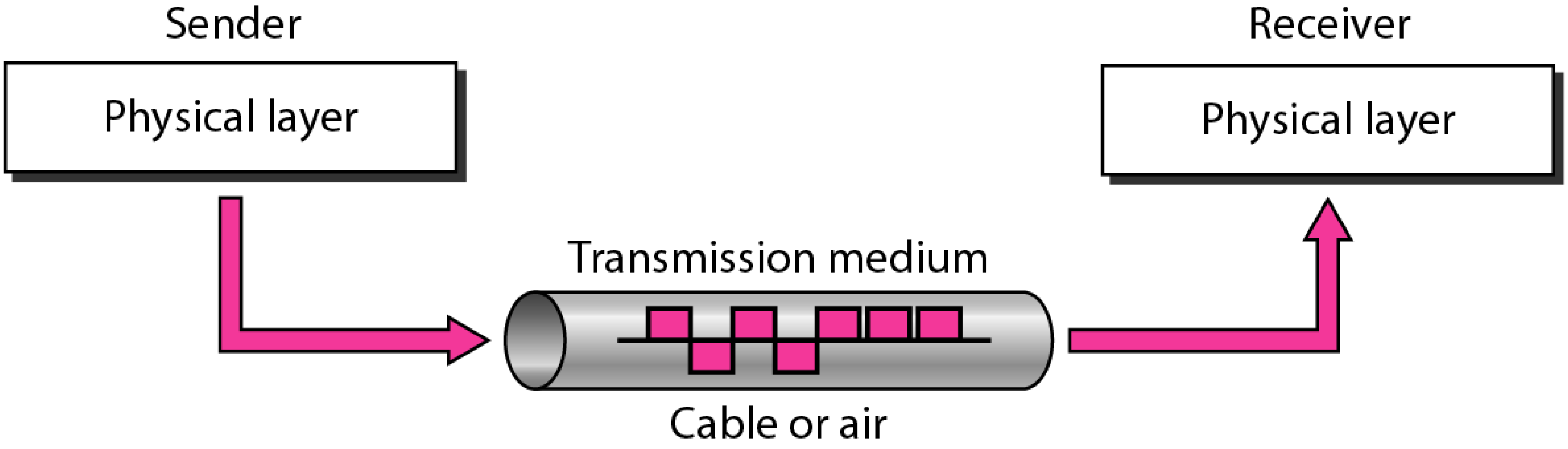
In data communication,

- A transmission medium can be broadly defined as anything that can carry information from a source to a destination.

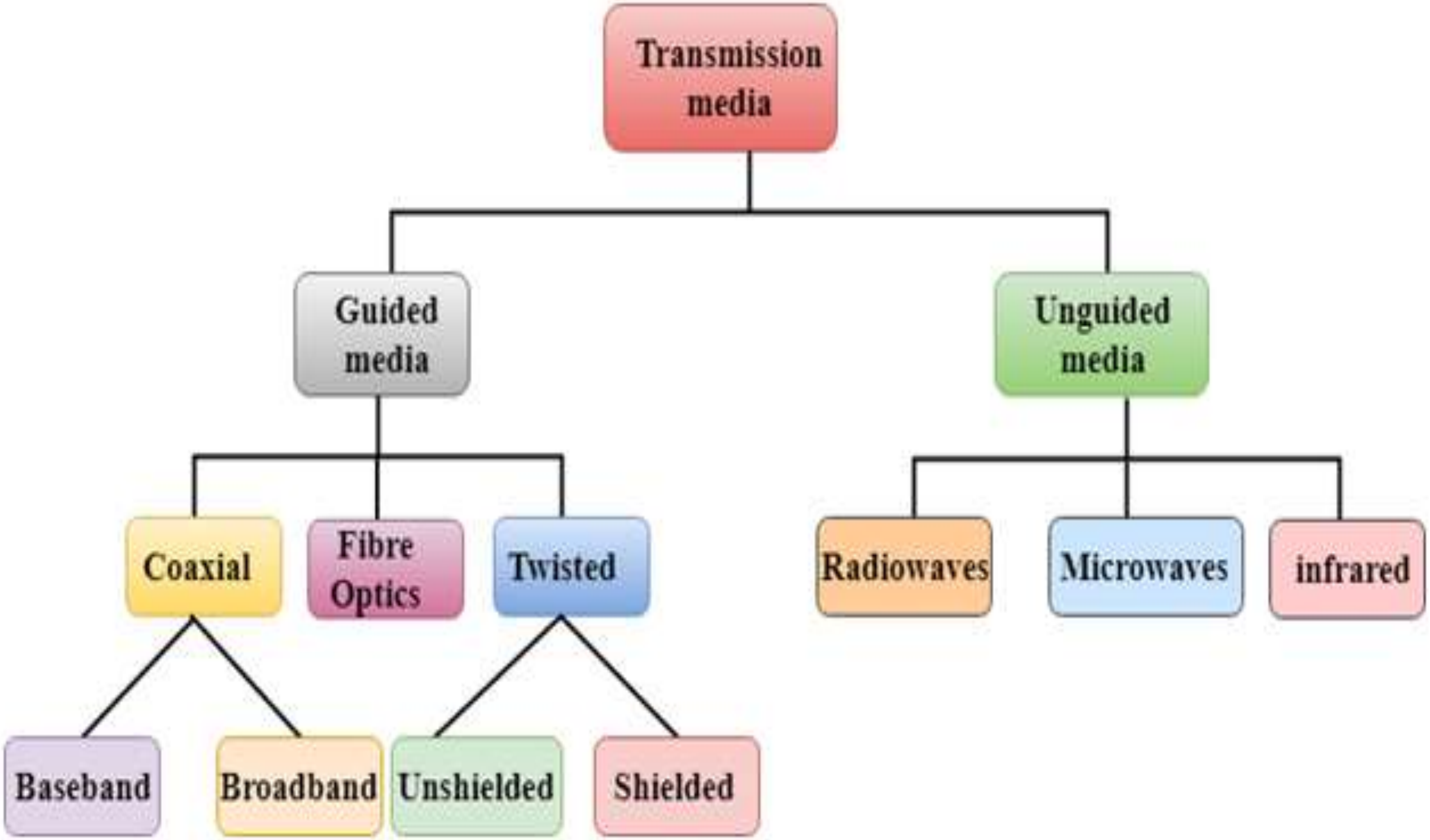
- We use different types of cables or waves to transmit data.

•Data is transmitted normally through electrical or electromagnetic signals.

- Transmission media are located below the physical layer



Classification of Transmissionmedia

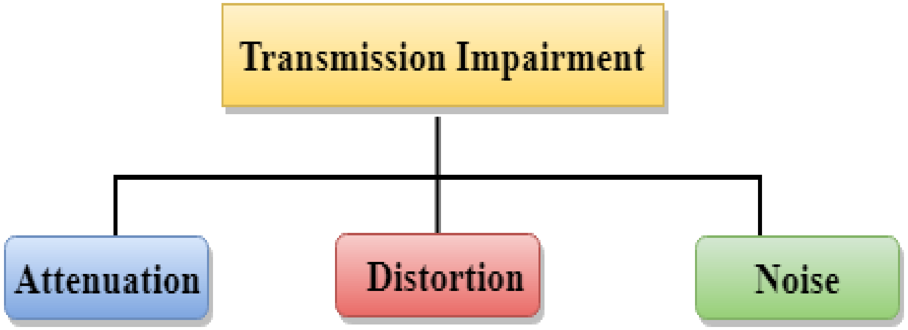


Contd..

Some factors need to be considered for designing the transmission media are:

- **Bandwidth:** the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

Causes Of Transmission Impairment:



- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Guided Media

- It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.
- Types Of Guided media:

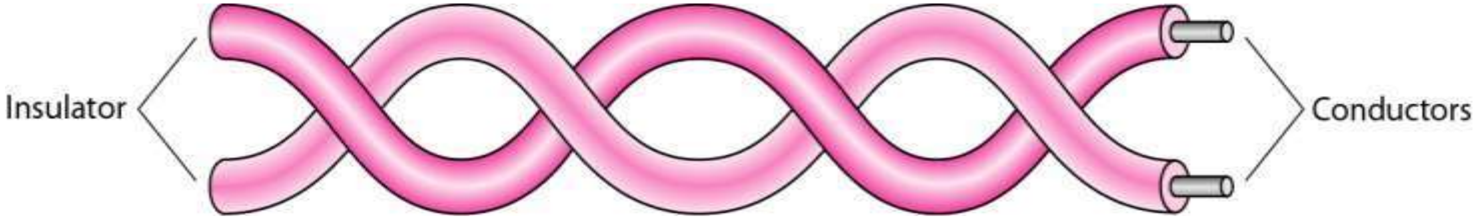
1. Twisted pair cable:

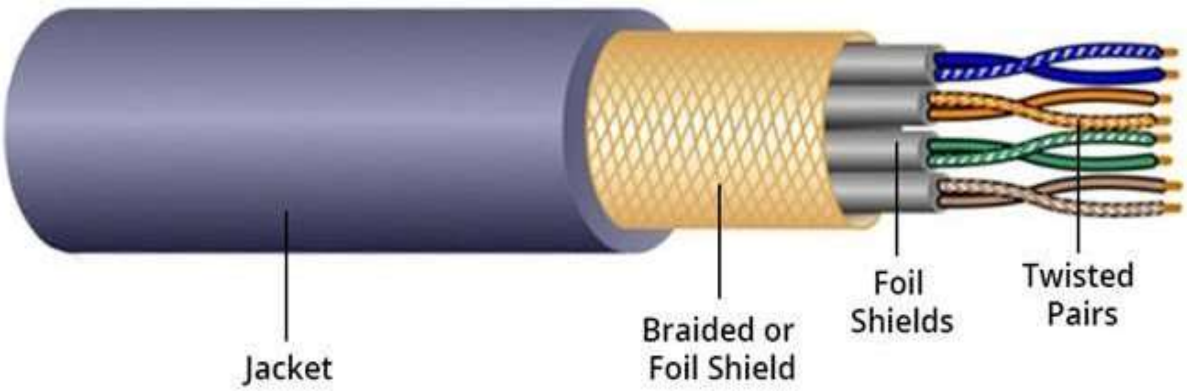
- Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.
- A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.
- The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.

1.Twisted-pair cable

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

- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference.





Twisted-pair cable(contd.)

Advantages:

- Cheap
- Easy to work with

Disadvantages:

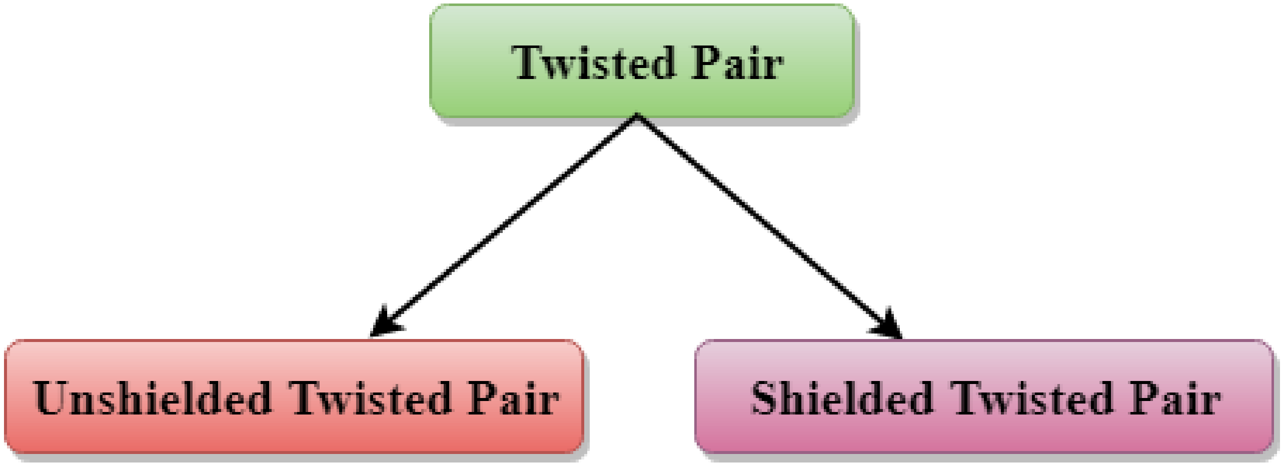
- Low data rate
- Short range

Applications

- Very common medium
- Can be use in telephone network
- Connection Within the buildings
- For local area networks (LAN)

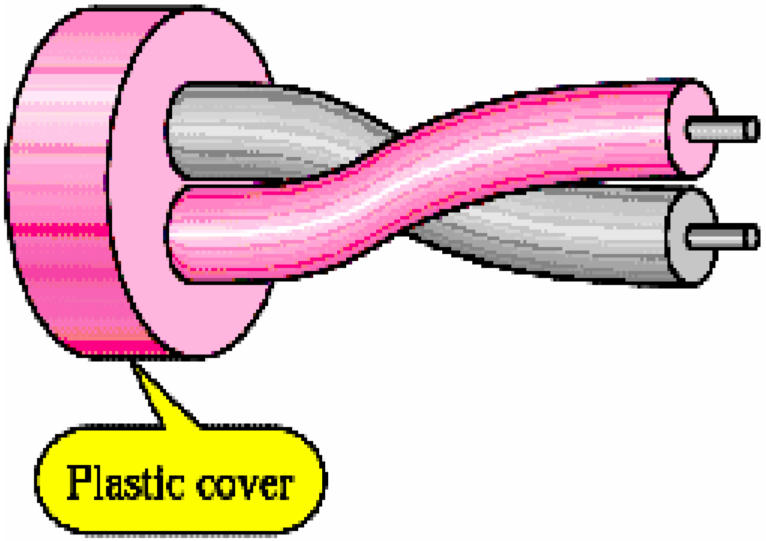
Contd..

Types of Twisted pair:

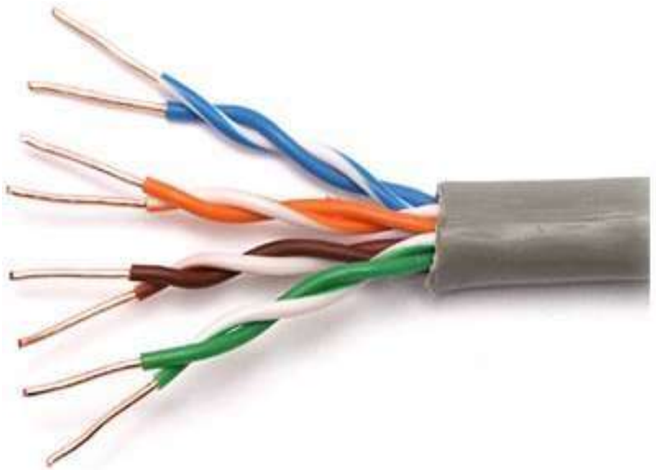


i). Unshielded Twisted-Pair Cable

- The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP).
- Pair of unshielded wires wound around each other
- Easy to install



a. UTP



i). Unshielded Twisted-Pair Cable

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support up to 4Mbps and it is suitable for voice data communication.
- **Category 3:** It can support up to 16Mbps.
- **Category 4:** It can support up to 20Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support up to 200Mbps and it is used in local area network.

Contd..

advantages Of Unshielded Twisted Pair:

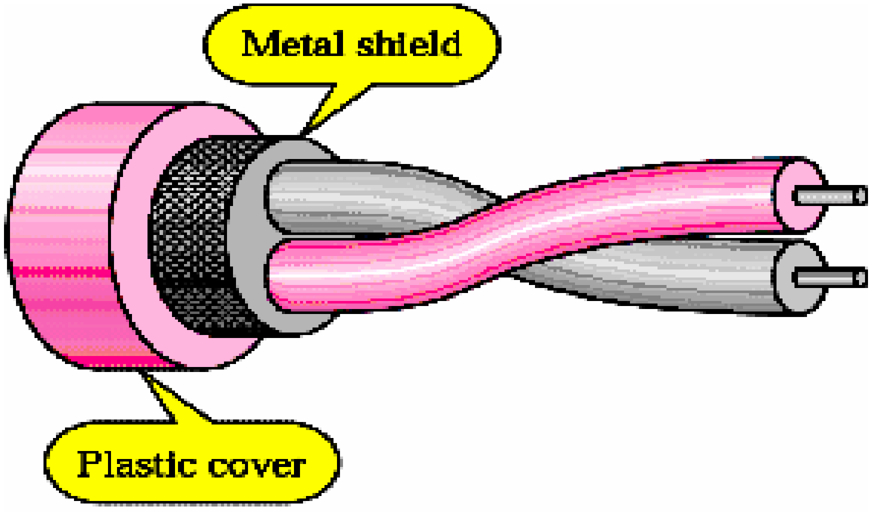
- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

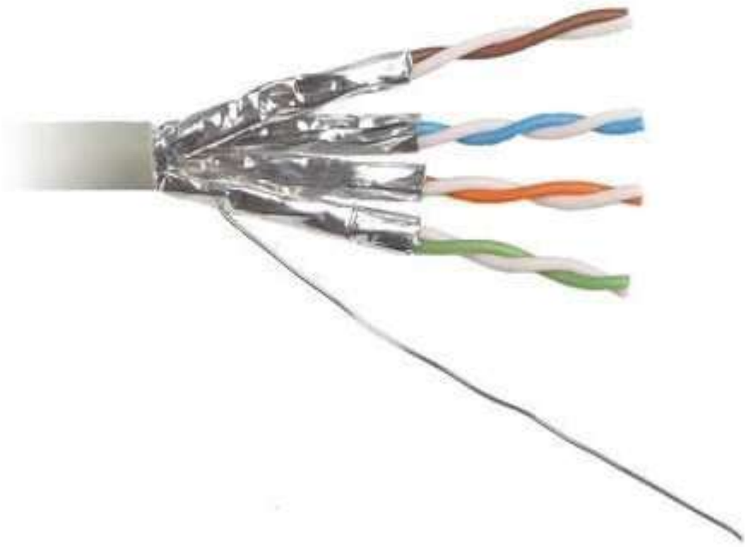
- This cable can only be used for shorter distances because of attenuation.

ii). Shielded Twisted Pair(STP)

- STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors.
- A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.
- Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.



b. STP



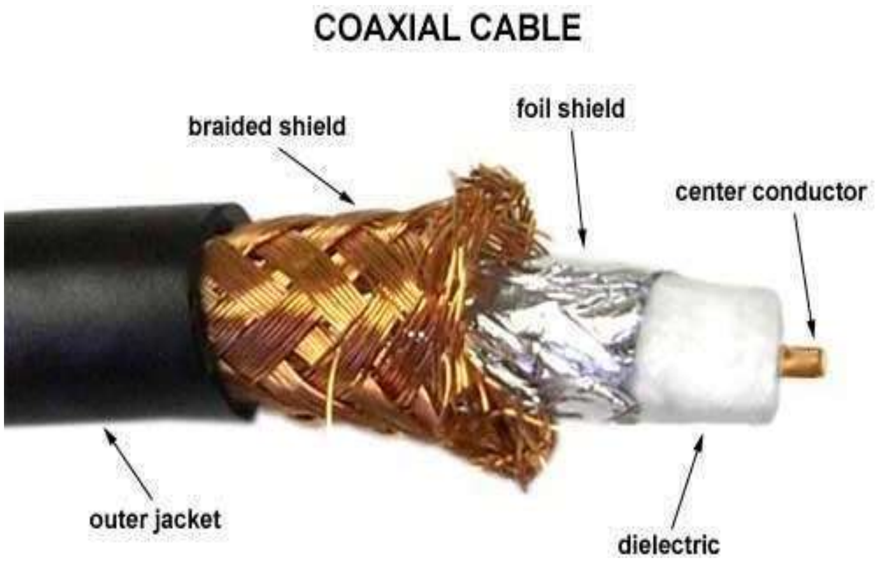
Contd..

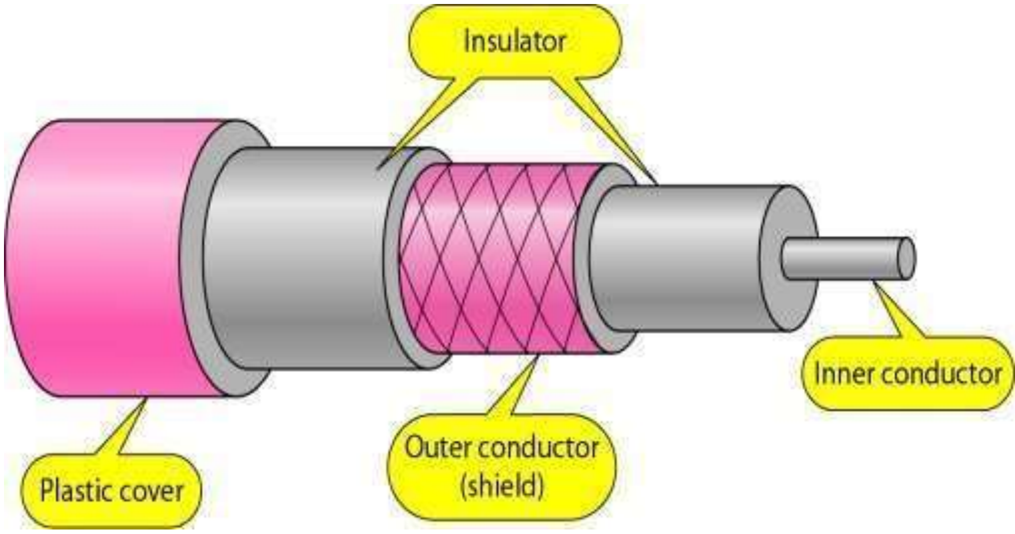
Characteristics Of Shielded Twisted Pair:

- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.
- **Disadvantages**
- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

2. Coaxial Cable

- Coaxial cable (or *coax)* carries signals of higher frequency ranges than those in twisted pair cable.
- Inner conductor is a solid wire
- Outer conductor serves as a shield against noise and a second conductor



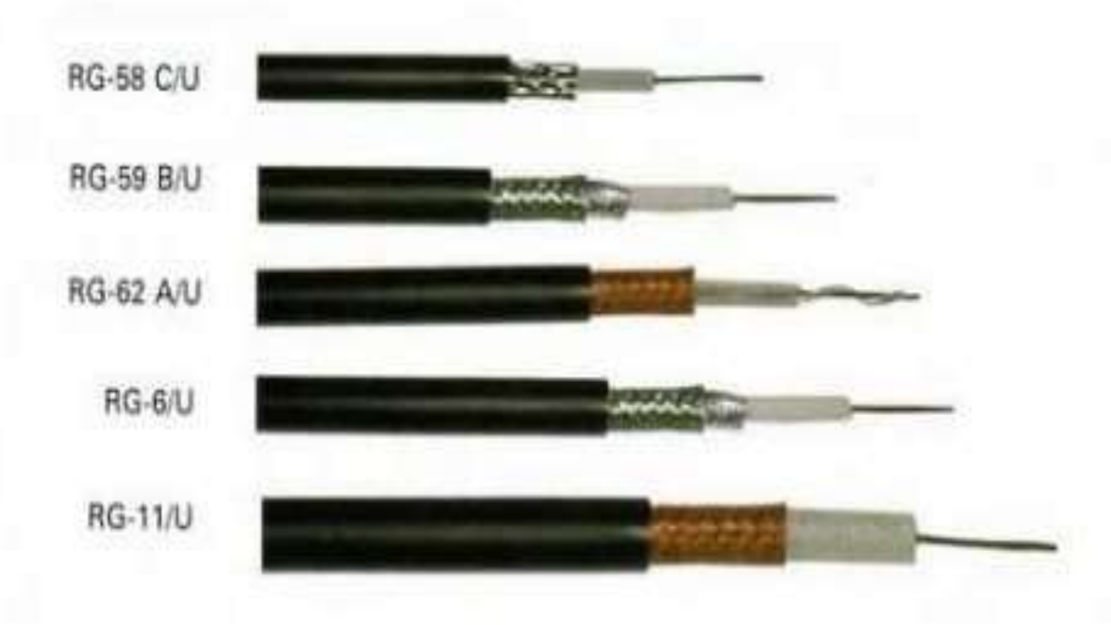


Contd..

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).

Categories of coaxial cables

Category	Use
RG-6	Cable TV, Internet
RG-59	CCTV
RG-11	HDTV



Coaxial Cable Applications

- Long distance telephone transmission
- Can carry 10,000 voice calls simultaneously
- Short distance computer systems links - Local area networks

ADVANTAGES

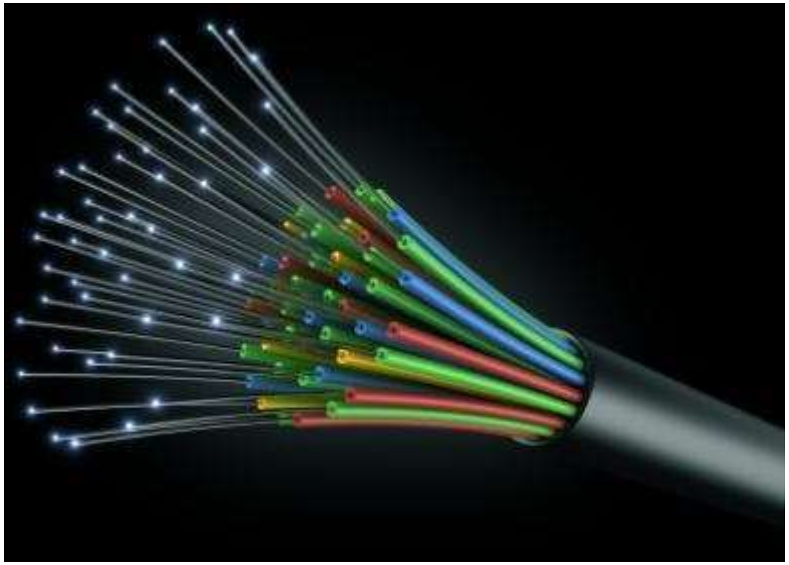
- Easy to wire
- Easy to expand

DISADVANTAGES

- 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

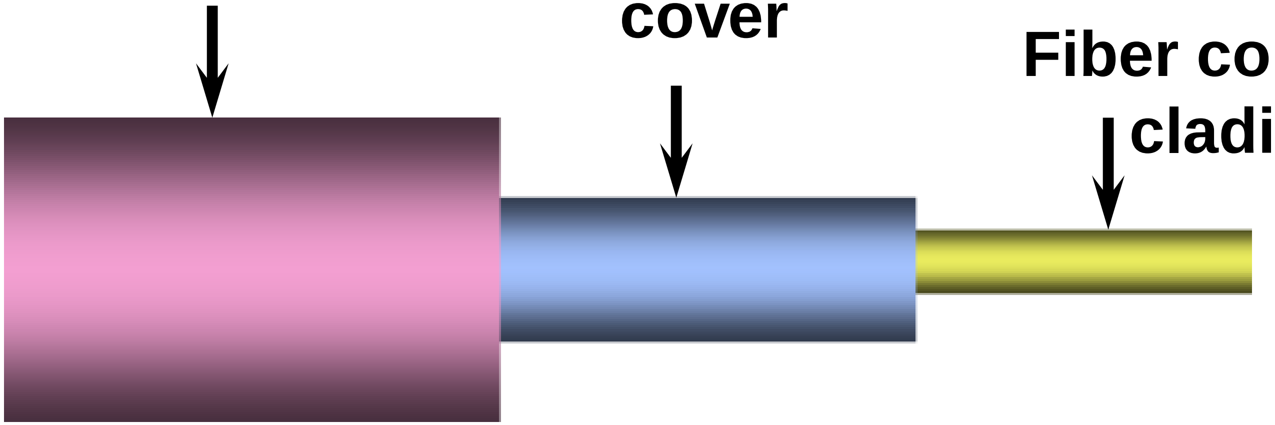
Fiber-Optic Cable

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. Light travels in a straight line as long as it is moving through a single uniform substance.
- If a ray of light traveling through one substance suddenly enters another substance(of a different density), the ray changes direction.



Optical Fiber

- **consists of three concentric sections**



plastic jacket

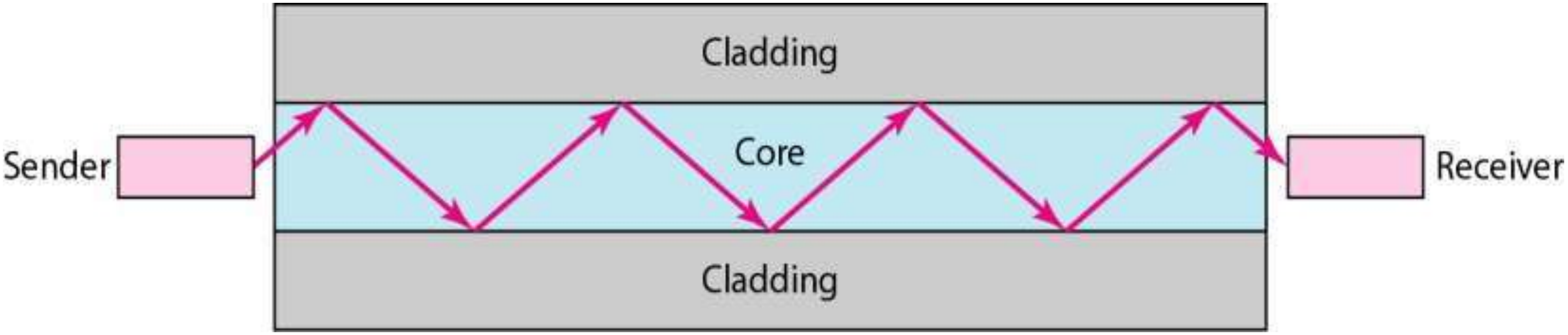
glass or plastic cover

Fiber core and cladding

- Core: consists of one or more very thin strands or fibers made of glass or plastic
- Each fiber is surrounded by its own cladding, a glass or plastic coating that has optical properties different from the core
- Jacket: a plastic or other material acts as a layer to protect against moisture, crushing, and other environmental dangers.

Fiber-Optic Cable(Contd.)

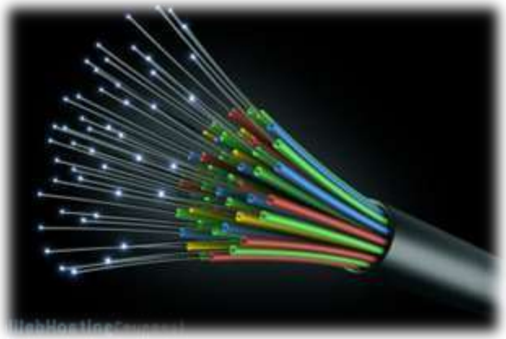
- Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- An optical fiber cable has a cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket(outer part of the cable).



Areas of Application

- **Telecommunications**
- **Local Area Networks**
- **Cable TV**
- **CCTV**
- **Medical Education**

Optical Fiber Disadvantages

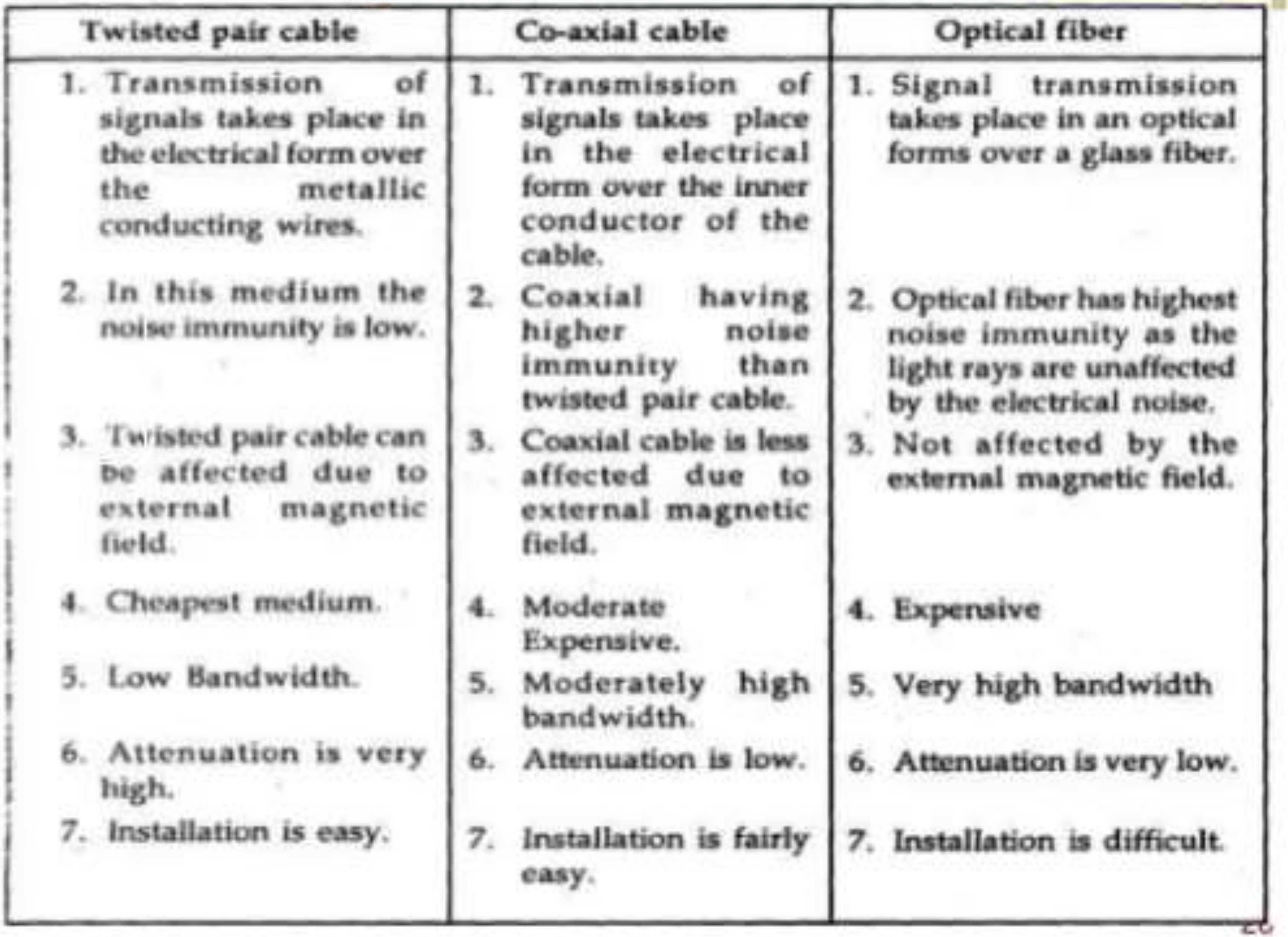


- Installation and maintenance need expertise
- Only Unidirectional light propagation, two fibers are needed for bidirectional
- Much more expensive

Optical Fiber Advantages

Greater capacity and Lower attenuation (signal loss)

- Example: Data rates at 100 Gbps
- Smaller size & light weight
- A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.
- Highly Secure(no light leaking)

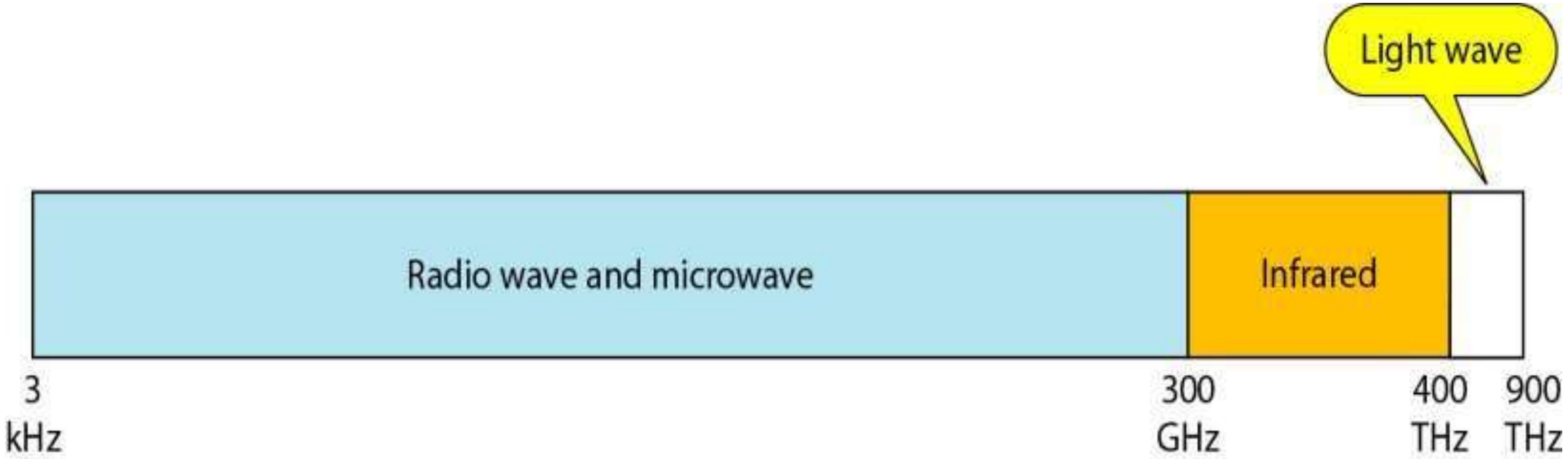


Twisted pair cable	Co-axial cable	Optical fiber
1. Transmission of signals takes place in the electrical form over the metallic conducting wires.	1. Transmission of signals takes place in the electrical form over the inner conductor of the cable.	1. Signal transmission takes place in an optical forms over a glass fiber.
2. In this medium the noise immunity is low.	2. Coaxial having higher noise immunity than twisted pair cable.	2. Optical fiber has highest noise immunity as the light rays are unaffected by the electrical noise.
3. Twisted pair cable can be affected due to external magnetic field.	3. Coaxial cable is less affected due to external magnetic field.	3. Not affected by the external magnetic field.
4. Cheapest medium.	4. Moderate Expensive.	4. Expensive
5. Low Bandwidth.	5. Moderately high bandwidth.	5. Very high bandwidth
6. Attenuation is very high.	6. Attenuation is low.	6. Attenuation is very low.
7. Installation is easy.	7. Installation is fairly easy.	7. Installation is difficult.

UNGUIDED MEDIA: WIRELESS

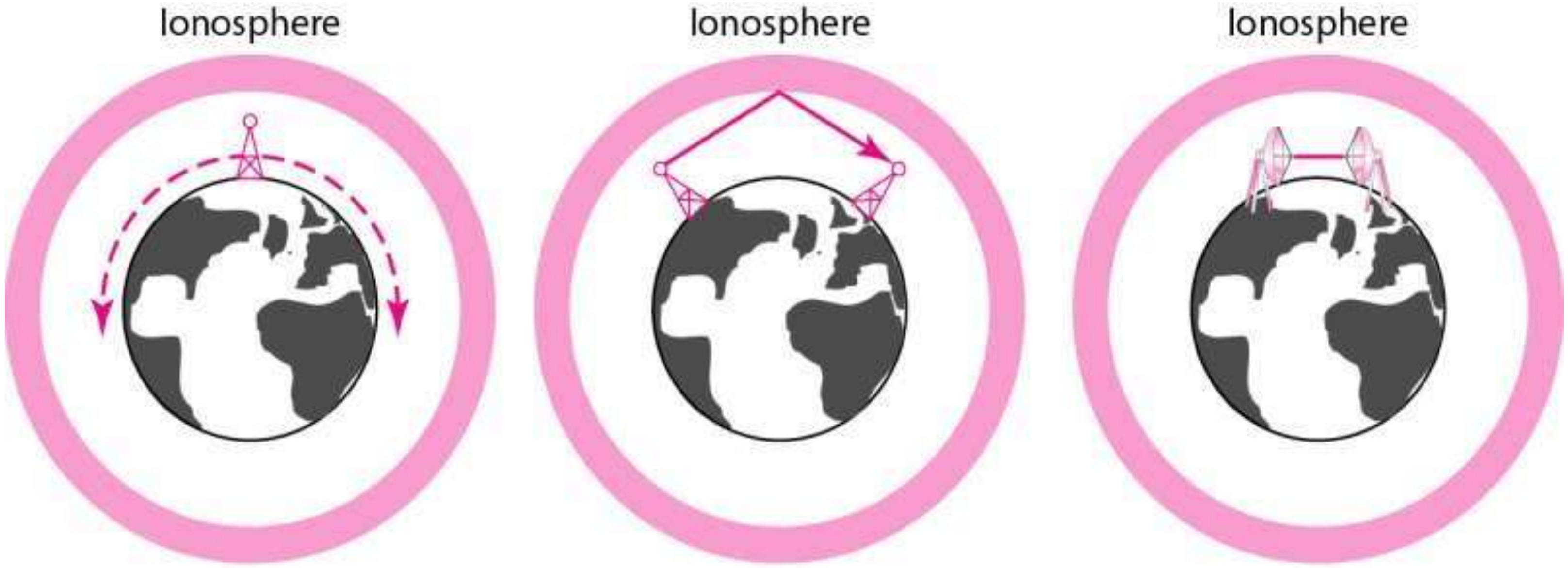
•Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.

1. **Radio Waves**
2. **Microwaves**
3. **Infrared**



UNGUIDED MEDIA: WIRELESS

Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation, as shown in Figure



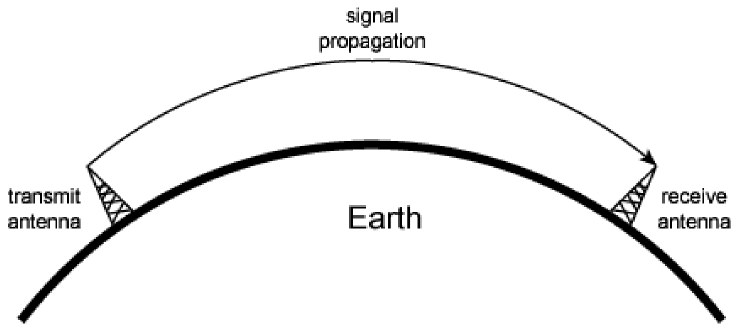
Ground propagation
(below 2 MHz)

Sky propagation
(2–30 MHz)

Line-of-sight propagation
(above 30 MHz)

Ground propagation:

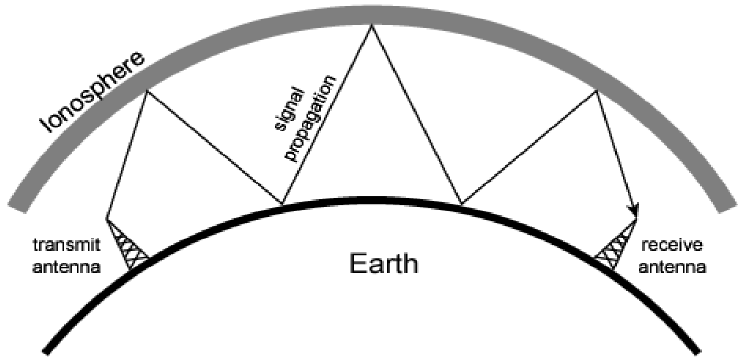
- Radio waves travel through the lowest portion of the atmosphere
- Touching the earth.



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

Sky propagation:

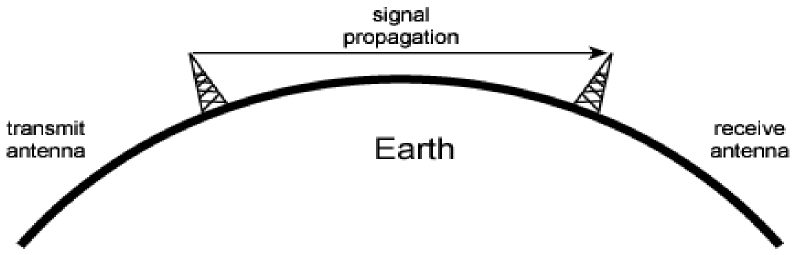
- Radio waves radiate to the ionosphere then they are reflected back to earth.



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

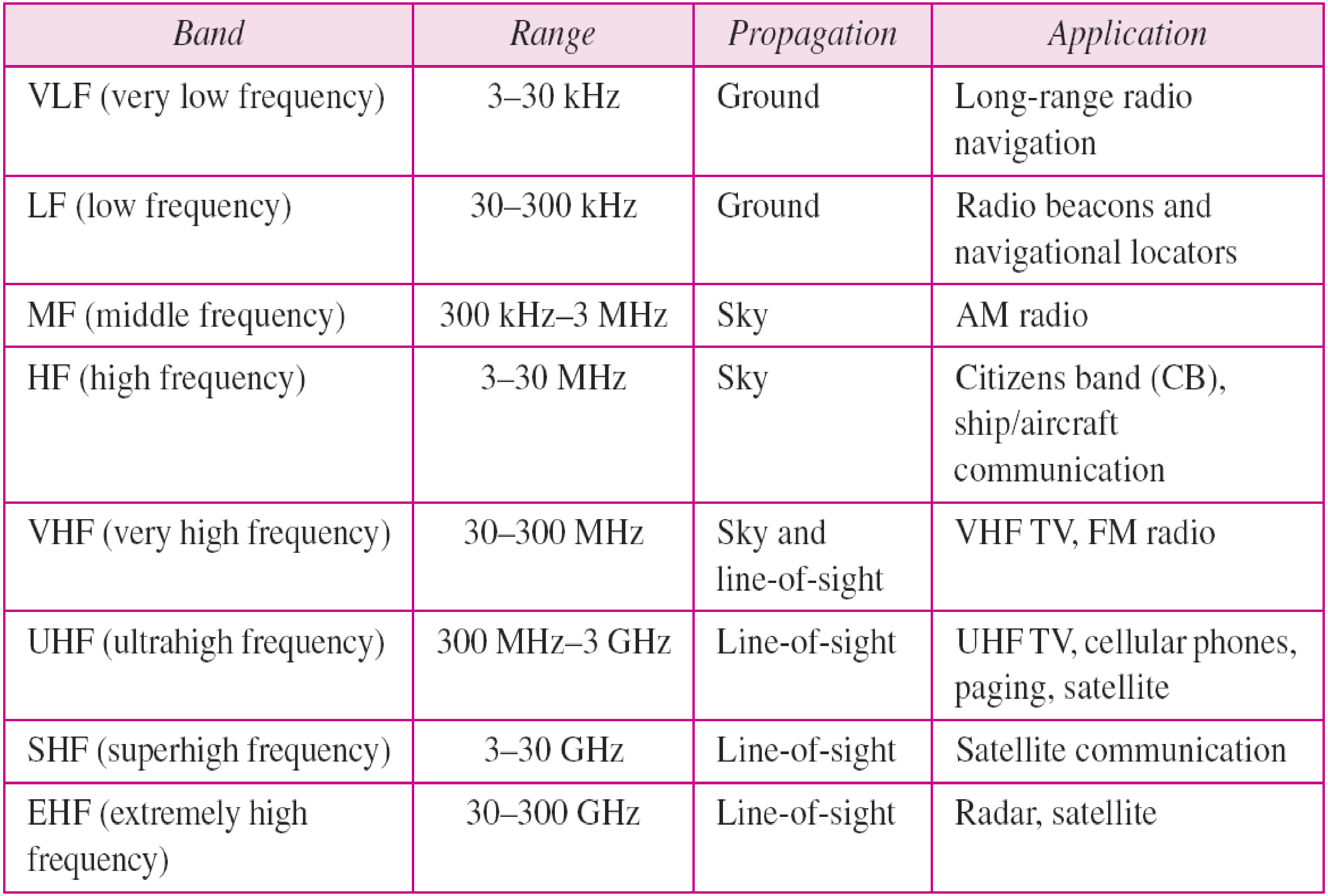
Line-of-Sight Propagation:

- In straight lines directly from antenna to antenna.



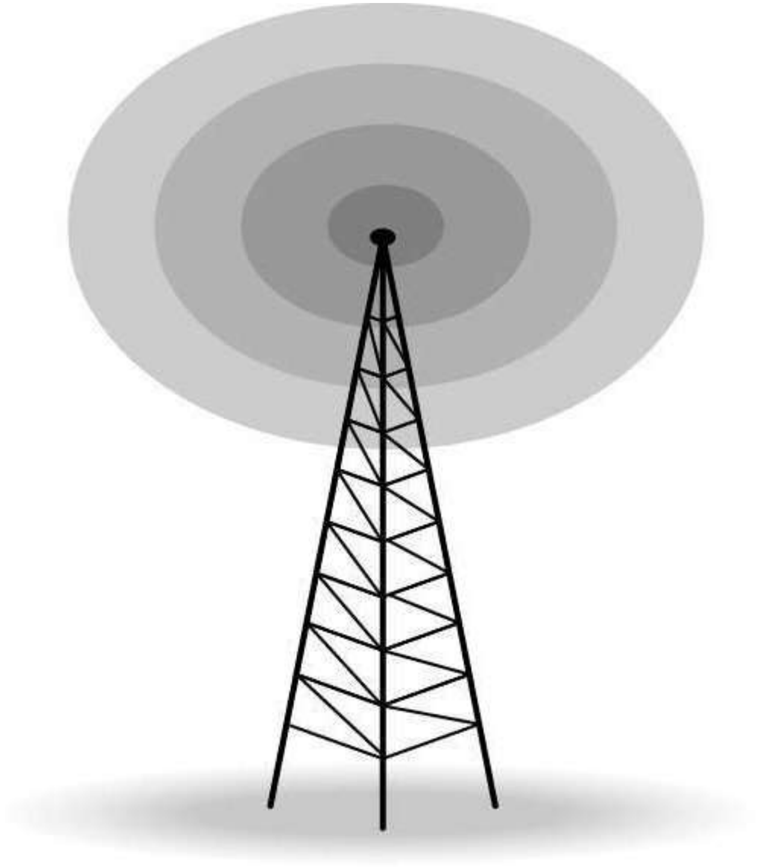
(c) Line-of-sight (LOS) propagation (above 30 MHz)

UNGUIDED MEDIA: WIRELESS



Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3–30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30–300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz–3 MHz	Sky	AM radio
HF (high frequency)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3–30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30–300 GHz	Line-of-sight	Radar, satellite

Unguided Media – Radio Waves



- **Omnidirectional Antenna**
- **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.**

Infrared

- Frequencies between 300 GHz to 400 THz.
- Used for short-range communication
- Example: Night Vision Camera,Remote control, File sharing between two phones, Communication between a PC and peripheral device,

Micro waves Transmission

- Microwaves are unidirectional
- Micro waves electromagnetic waves having frequency between 1 GHZ and 300 GHZ.
- 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), GPS

ARPANET

- **ARPANET** stands for **Advanced Research Projects Agency NET**.
- ARPANET was first network which consisted of distributed control.
- It was basically beginning of Internet with use of these technologies.
- It was designed with a basic idea in mind that was to communicate with scientific users among an institute or university.

History of ARPANET :

- ARPANET was introduced in the year 1969 by Advanced Research Projects Agency (ARPA) of US Department of Defense.
- It was established using a bunch of PCs at various colleges and sharing of information and messages was done.
- In the year 1980, ARPANET was handed over to different military network, Defense Data Network.

Characteristics of ARPANET :

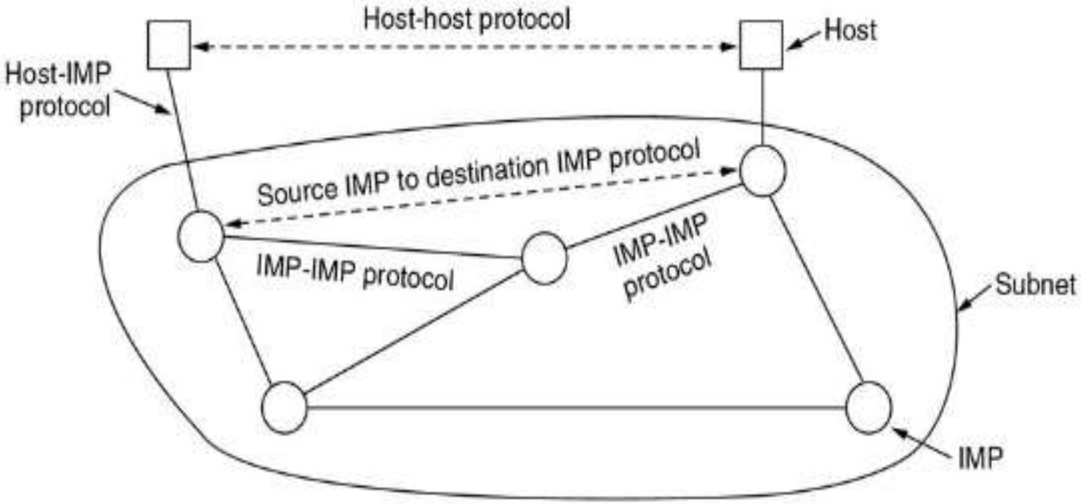
1.It is basically a type of WAN.

2.It used concept of Packet Switching Network.

3.It used Interface Message Processors(IMPs) for sub-netting.

4.ARPANETs software was split into two parts- a host and a subnet.

ARPANET Architecture



The original ARPANET design.

Advantages of ARPANET :

- ARPANET was designed to service even in a Nuclear Attack.
- It was used for collaborations through E-mails.
- It created an advancement in transfer of important files and data of defense.

Limitations of ARPANET :

- Increased number of LAN connections resulted in difficulty handling.
- It was unable to cope-up with advancement in technology.

History of Internet

- More than 100 countries use the Internet. Millions of people are users. Yet this extraordinary communication system only came into being in 1969.

- In the mid-1960s, mainframe computers in research organizations were standalone devices. Computers from different manufacturers were unable to communicate with one another.

- The Advanced Research Projects Agency(ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort

- In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas . The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an interface message processor (IMP).

- Each IMP had to be able to communicate with other IMPs as well as with its own attached host. By 1969, ARPANET was a reality.

- Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the Network Control Protocol (NCP) provided communication between the hosts.

INTERNET

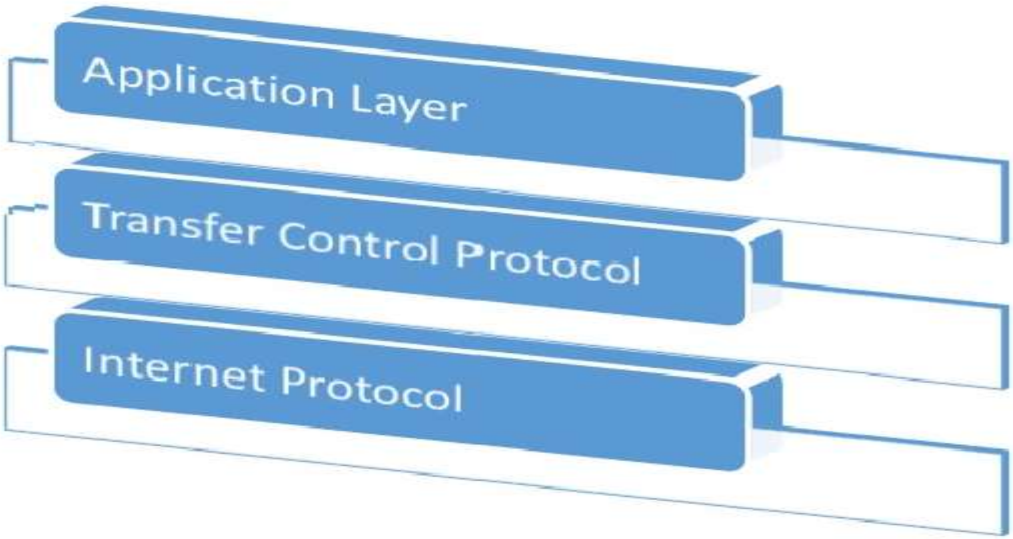
- Internet is called the network of networks. It is a global communication system that links together thousands of individual networks.
- In other words, internet is a collection of interlinked computer networks, connected by copper wires, fiber-optic cables, wireless connections, etc.
- As a result, a computer can virtually connect to other computers in any network. These connections allow users to interchange messages, to communicate in real time (getting instant messages and responses), to share data and programs and to access limitless information.

Basics of Internet Architecture

- Internet architecture is a meta-network, which refers to a congregation of thousands of distinct networks interacting with a common protocol. In simple terms, it is referred as an internetwork that is connected using protocols. Protocol used is TCP/IP.
- protocol connects any two networks that differ in hardware, software and design.
- TCP/IP provides end to end transmission, i.e., each and every node on one network has the ability to communicate with any other node on the network.

Layers of Internet Architecture

- Internet architecture consists of three layers.



IP:(Internet protocol)

- In order to communicate, we need our data to be encapsulated as Internet Protocol (IP) packets. These IP packets travel across number of hosts in a network through routing to reach the destination. However IP does not support error detection and error recovery, and is incapable of detecting loss of packets.

Contd..

TCP

- TCP stands for "Transmission Control Protocol". It provides end to end transmission of data, i.e., from source to destination. It is a very complex protocol as it supports recovery of lost packets.

Application Protocol

- Third layer in internet architecture is the application layer which has different protocols on which the internet services are built. Some of the examples of internet services include email (SMTP facilitates email feature), file transfer (FTP facilitates file transfer feature), etc

THE INTERNET TODAY

- The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations.

- It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed.

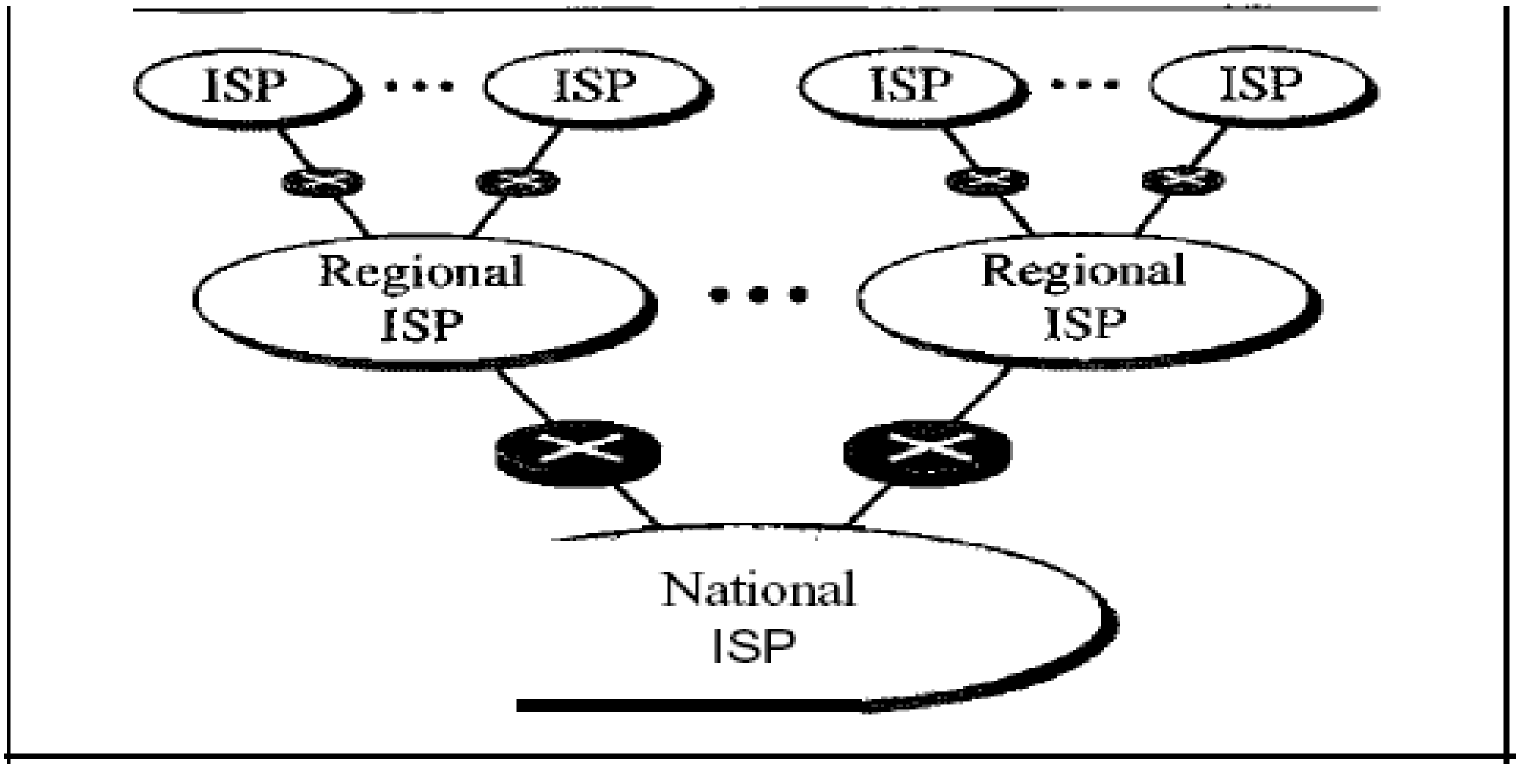
- Today most end users who want Internet connection use the services of Internet service providers (ISPs). There are international service providers, national service providers, regional service providers, and local service providers.

- In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internetting Projec1

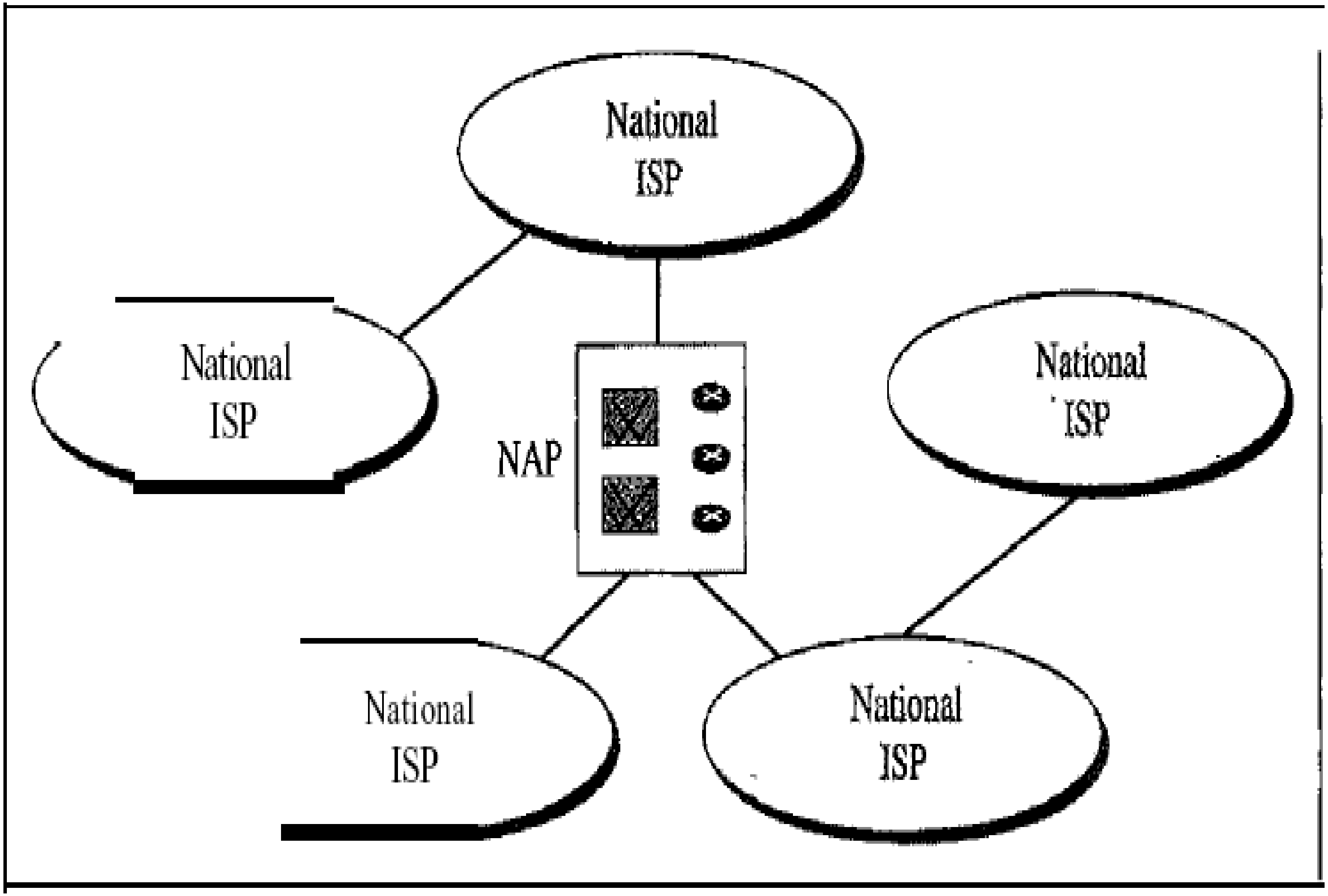
- Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end- to-end delivery of packets. This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

- Shortly thereafter, authorities made a decision to split TCP into two protocols: Transmission Control Protocol (TCP) and Internetworking Protocol (lP). IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCPIIP.

- The Internet today is run by private companies, not the government. Below figure shows a conceptual (not geographic) view of the Internet.



a. Structure of a national ISP



b. Interconnection of national ISPs