

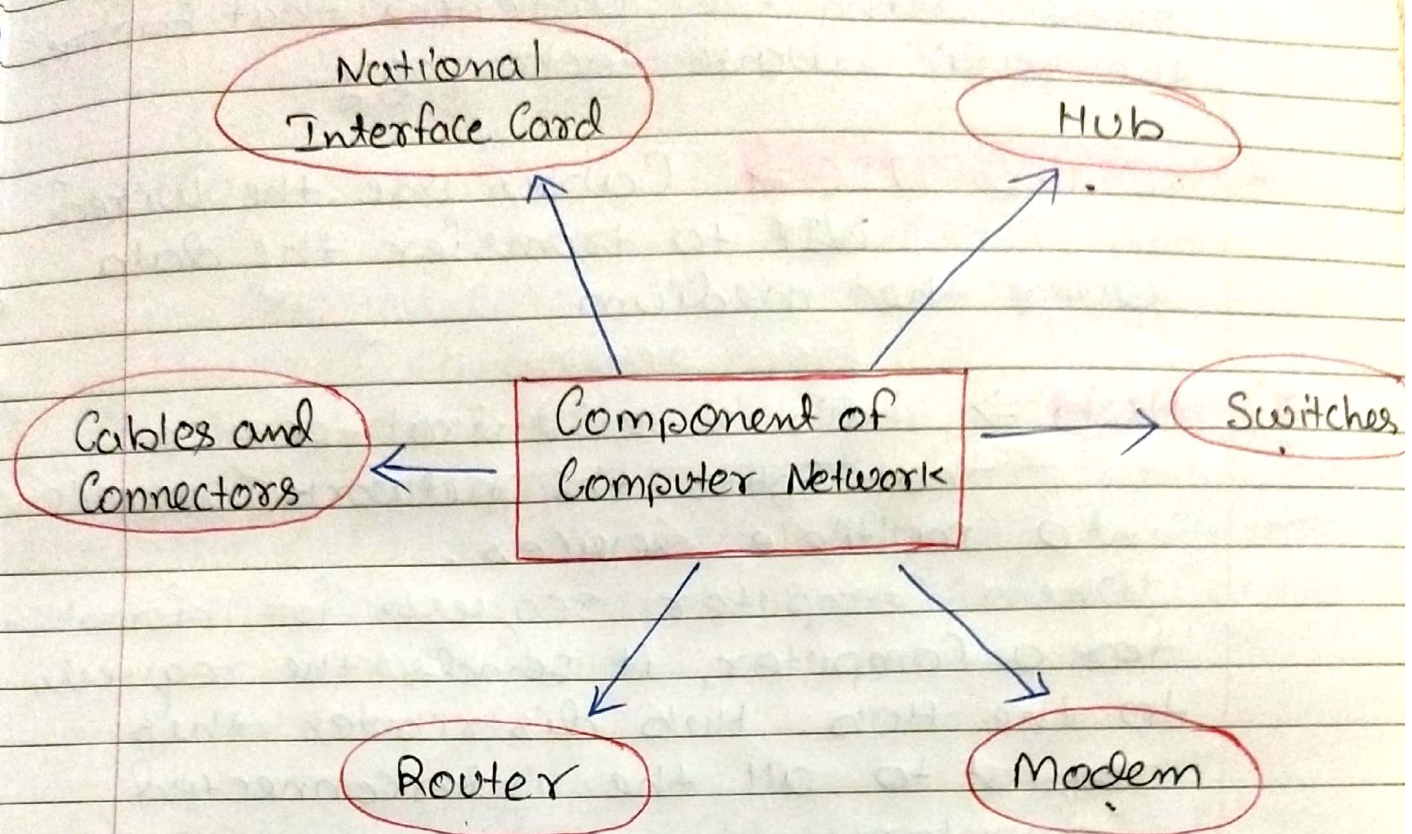
Computer Network

01

Computer Network ⇒ • Computer Network refers to interconnected computing devices that can exchange data and share resources with each other.

- Computer Network is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.
- A Computer Network is a system in which multiple computers are connected to each other to share information and resources.
- A Computer network is a set of computers sharing resources located on or provided by network nodes. The computers use common communication protocols over digital interconnections to communicate with each other.
- A Computer Network is defined as a system that connects two or more computing devices for transmitting and sharing information.

Components of Computer Network:



1) NIC (National Interface Card) ⇒

NIC is a device that helps the computer to communicate with another device.

The network interface card contains the hardware addresses, the data-link layer protocol uses this address to identify the system on the network so that it transfers the data to the correct destination.

There are two types of NIC.

1) **wireless NIC** ⇒ All the modern laptops use the wireless NIC.

in wireless NIC, a connection is made using the antenna that employs the radio wave technology.

2) **Wired NIC** $\Rightarrow$ Cables use the wired NIC to transfer the data over the medium.

2) **Hub** $\Rightarrow$ Hub is a central device that splits the network connection into multiple devices.

When computer requests for information for a computer, it sends the requests to the Hub. Hub distributes this request to all the interconnected computers.

3) **Switches** $\Rightarrow$ Switch is a networking device that groups all the devices over the network to transfer the data to another device.

A switch is better than Hub as it does not broadcast the message over the network such as it sends the message to the device for which it belongs to.

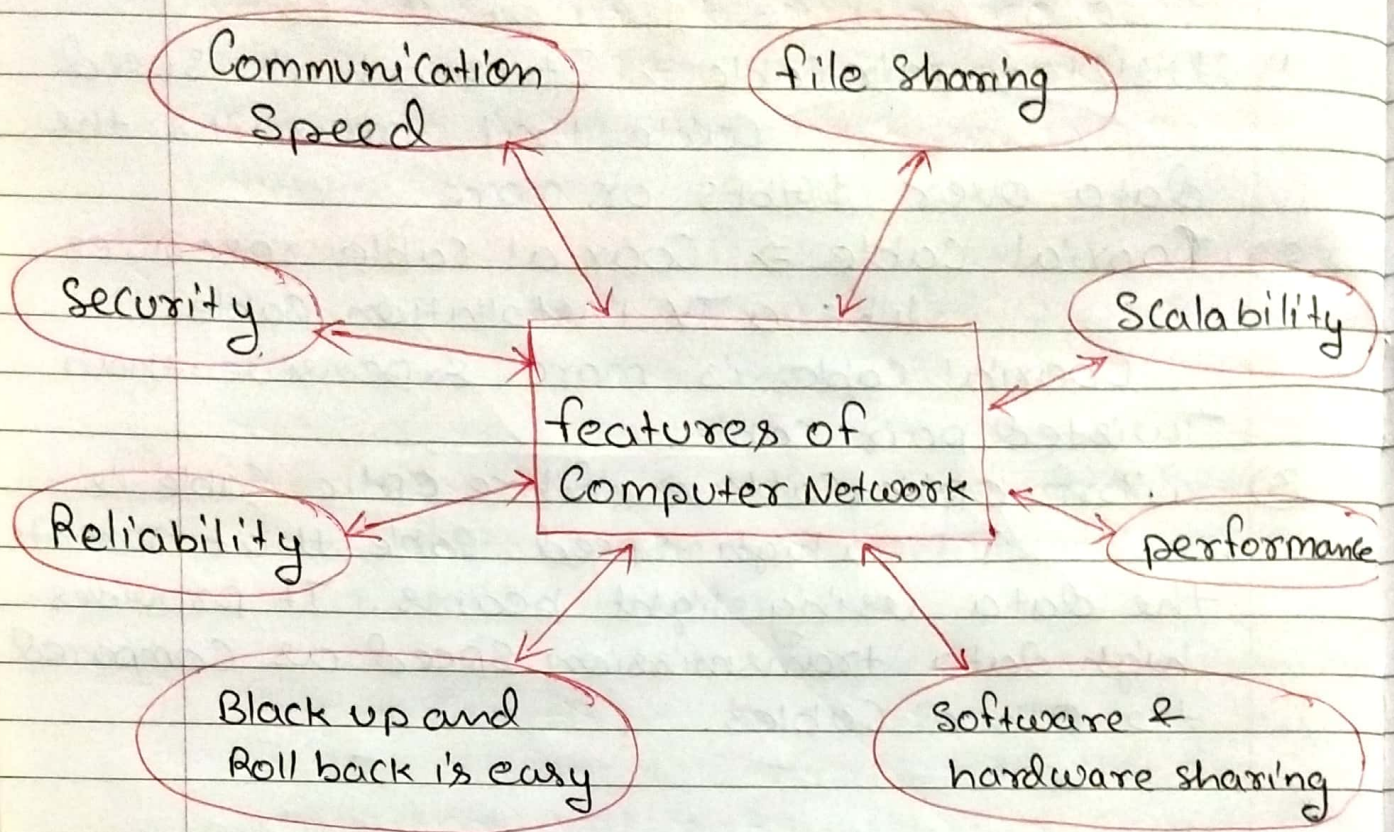
4) **Cables and Connectors** $\Rightarrow$ Cables is a transmission media that transmits the communication signals.

There are three types of Cables:

- 1) Twisted pair Cable $\Rightarrow$ It is a high-speed Cable that transmits the data over 1Gbps or more.
- 2) Coaxial Cable $\Rightarrow$ Coaxial Cable resembles like a TV installation Cable.
Coaxial Cable is more Expensive than Twisted pair Cable.
- 3) Fibre optic Cable $\Rightarrow$ Fibre optic Cable is a high-speed Cable that transmits the data using light beams. It provides high data transmission speed as compared to other Cables.
- 5) Router $\Rightarrow$ Router is a device that connects the LAN to the internet. The router is mainly used to connect the distinct networks or connect the internet to multiple Computers.
- 6) Modem $\Rightarrow$ Modem connects the Computer to the internet over the existing telephone line.
A modem is not integrated with the Computer motherboard.
A modem is a separate part on the PC slot found on the motherboard.

Features of Computer network

NO. 05



1) **Communication Speed** $\Rightarrow$ Network provides us to communicate over the network in a fast and efficient manner.

for ex $\Rightarrow$ we can do video Conferencing, email messaging etc. over the internet. The Computer network is a great way to share our knowledges and ideas.

2) **file sharing** $\Rightarrow$ One of the most important features of a Computer Network is that with their help you can easily share the files Between different Systems that are connected with each other.

through transmission media.

3) **Scalability** $\Rightarrow$ The Scalability of a Computer network simply means that we can add new nodes or components of the network easily. Any computer network must be scalable so we can extend it easily by adding new nodes. After adding new nodes to the network the speed of connection decreases which leads to a decrease in the speed of transmission of data.

4) **Performance** $\Rightarrow$ The performance of a Computer network is measured using response time and with the help of the speed of data transmission. For better performance the response time of sending and receiving data from one node to another should be minimum.

5) **Software and hardware sharing** $\Rightarrow$ We can install the application on the main server, therefore the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.

6) **Back up and Roll back is easy** $\Rightarrow$ Since the files

are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.

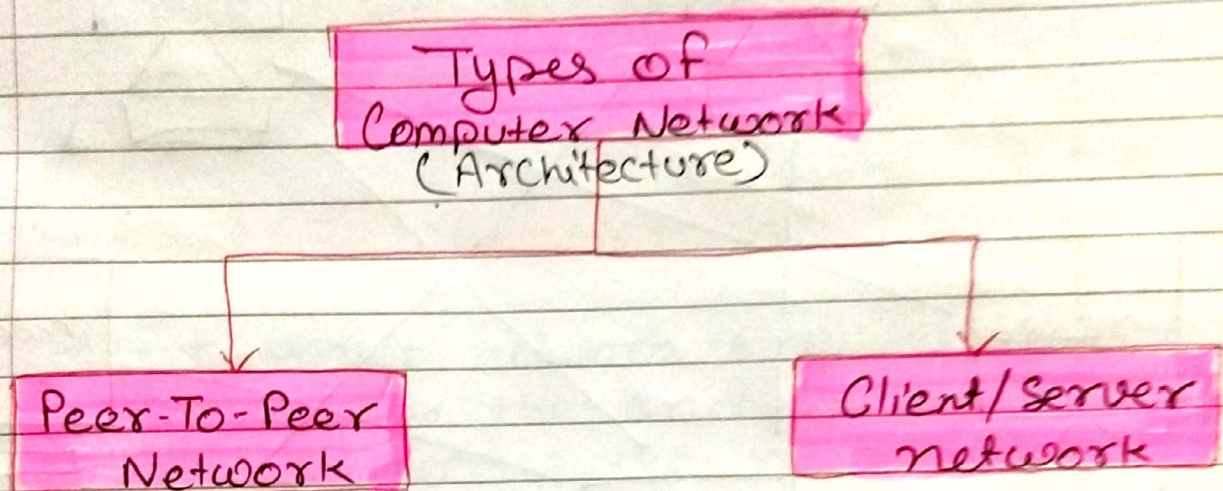
7) **Reliability** $\Rightarrow$ With the help of Computer Networks there are fewer chances for the occurrence of failure and in case if there is any failure then recovery is fast.

8) **Security** $\Rightarrow$ Security is one of the main characteristics of Computer Networks. Thus a computer network should be secure so that the data transmitting over the network should be safe from any unauthorized access. The data sent by the sending node should be received as it is at the receiving node, which simply means there should be no loss of data during the transmission of the data.

Computer Network Architecture 08

Computer Network Architecture is defined as the physical and logical design of the Software, hardware, protocols and media of transmission of data.

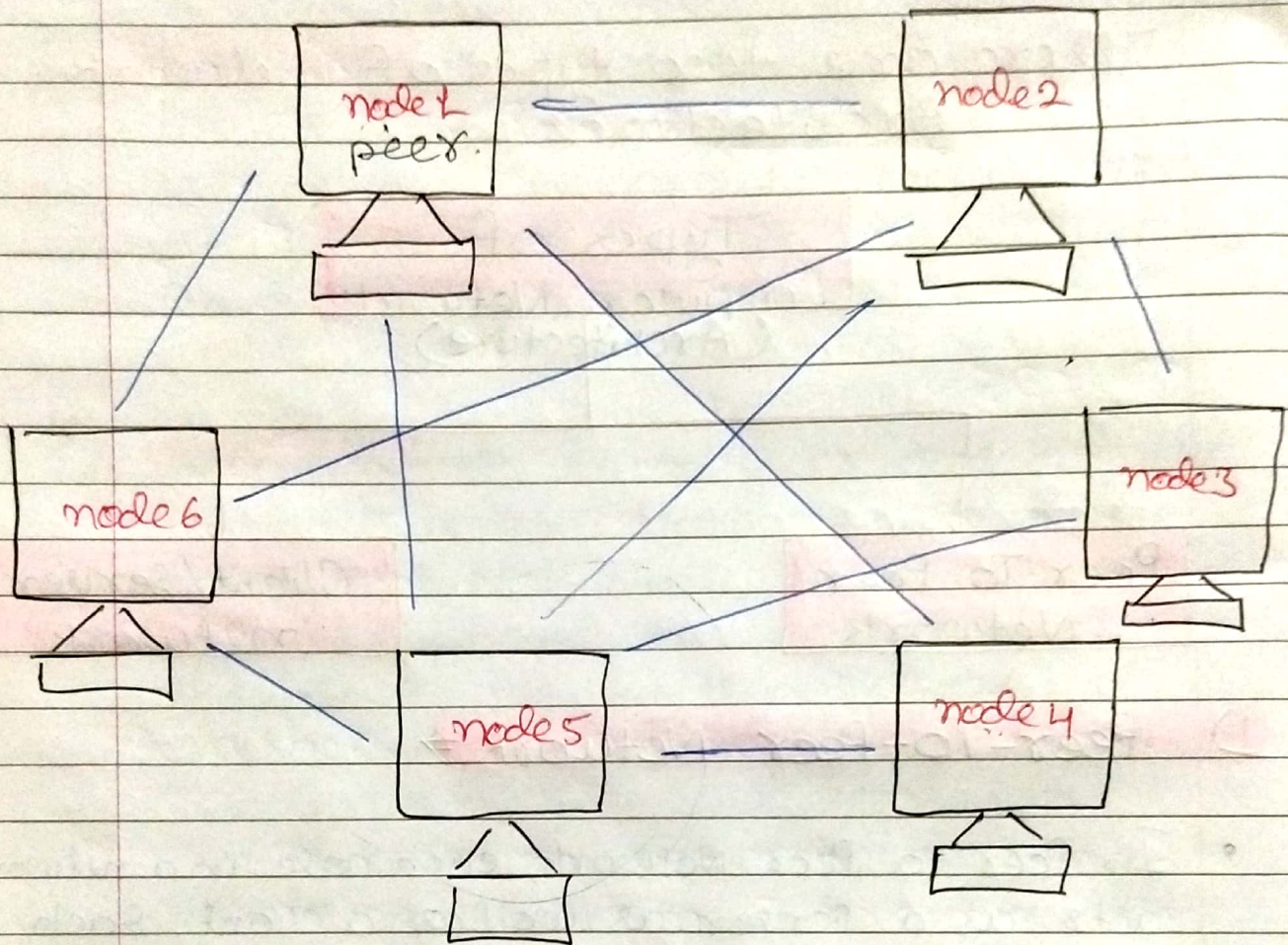
There are two types of network Architectures.



1) Peer-To-Peer Network ⇒

- In Peer to Peer Network, each node in a network acts as a server as well as a client. Each node on network is known as a peer.
- There are no dedicated servers required to provide services to the clients.
- Peer-to-Peer network is useful for small environments, usually upto 10 computers.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

- Each node is capable of requesting services and can also provide the server to other nodes.



Advantages of Peer-To-Peer Network:

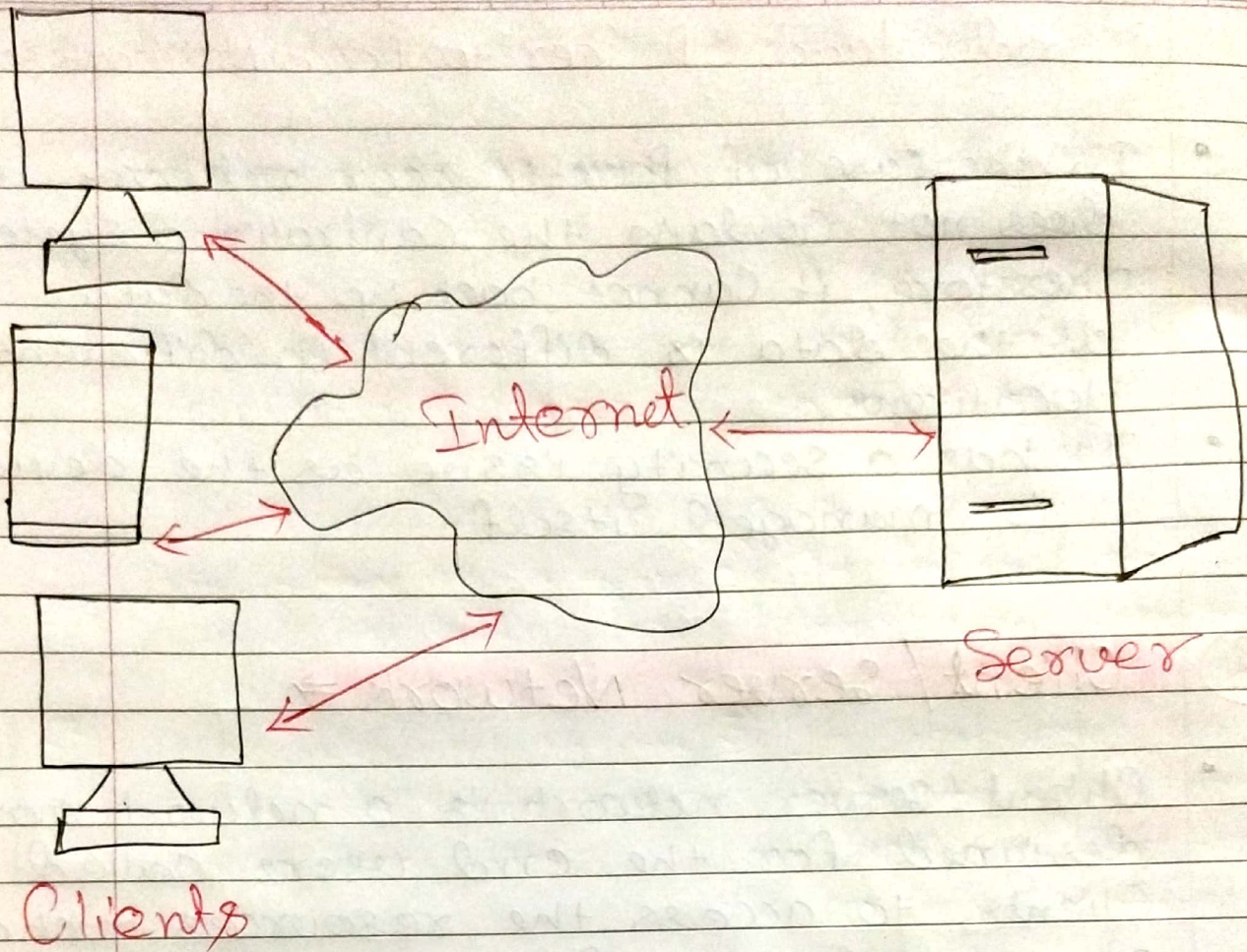
- It is less costly as it does not contain any dedicated server.
- if one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages of Peer-to-Peer Network ⇒

- In the case of Peer-to-Peer network, it does not contain the Centralized system. Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

2) Client/Server Network ⇒

- Client/server network is a network model designed for the end users called Clients, to access the resources such as songs, video etc. from a central computer known as server.
- The central controller is known as a server while all other computers in the network are called clients.
- A server performs all the major operations such as security and network management.
- All the clients communicate with each other through a server.
- Suitable for a larger network.



Advantages of Client/Server network:

- A Client/Server network contains the Centralized System. Therefore we can backup the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages of Client/Server Network:

- Client/Server network is expensive as it requires the Server with large memory.
- A server has a Network Operating System (NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

Difference between Peer-to-Peer and Client server network. 13

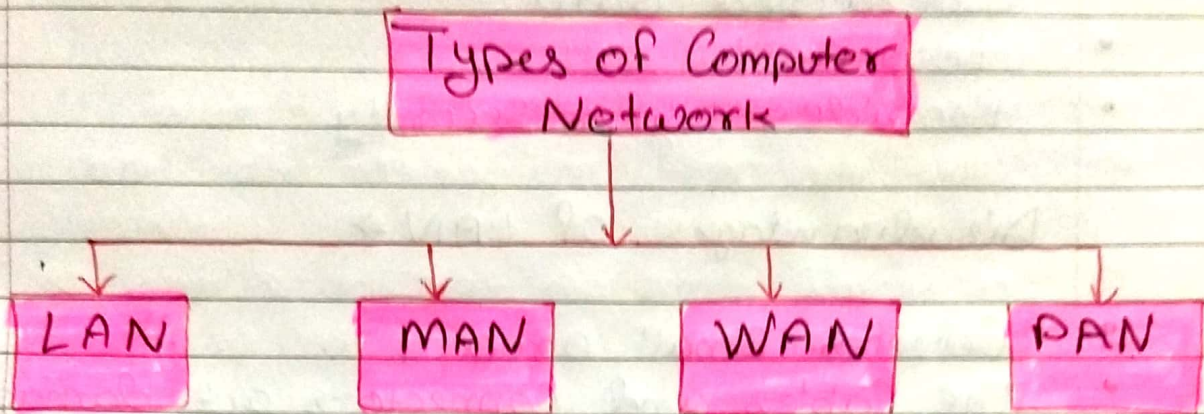
~~~~~

| Peer-to-Peer Network                                                       | Client-server Network                                                                                        |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 1) The peer-to-peer network model is distributed and decentralized nature. | 1) The Client-server network model is also distributed in nature but it is centralized.                      |
| 2) Peer-to-Peer Network focuses on connectivity.                           | 2) It focuses on information sharing.                                                                        |
| 3) In peer-to-peer Network, Clients and Server are not differentiated.     | 3) In Client-server Network, Clients and server are differentiated, specific server and clients are present. |
| 4) Peer-to-Peer Network are less stable if number of peer is increase.     | 4) Client-server Network are more stable than Peer-to-Peer Network.                                          |
| 5) Peer-to-Peer Network Each peer has its own data                         | 5) Client-server Network, Centralized server is used to store the data.                                      |
| 6) Peer-to-Peer is less expensive to implement                             | 6) Client-server network is more expensive to implement.                                                     |



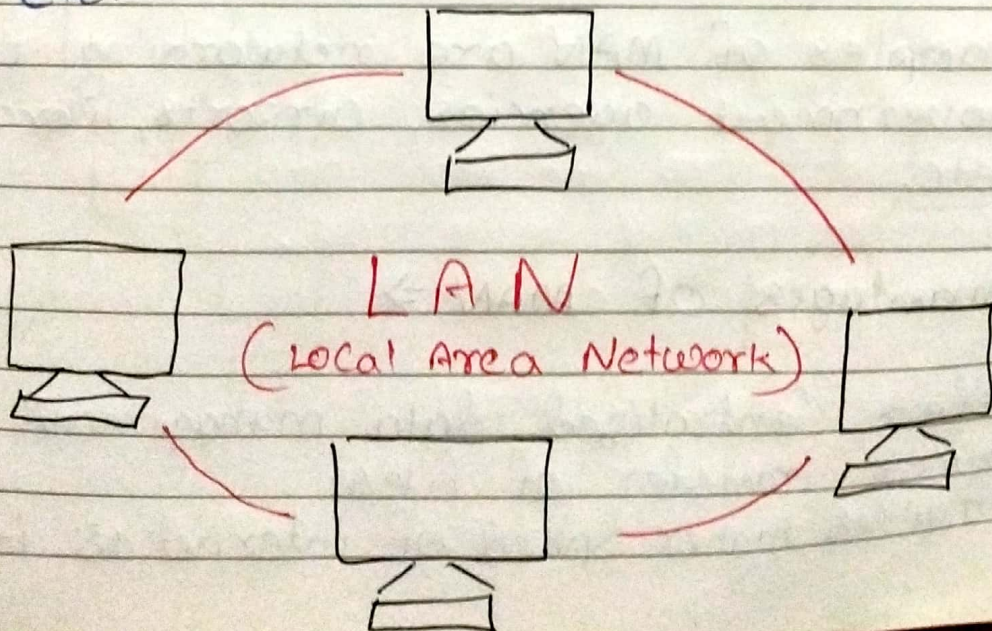
# Types of Computer Network 14

A Computer network can be categorized by their size. A Computer Network is mainly of four types:



## 1) LAN (Local Area Network) ⇒

- LAN is a group of computers connected to each other in a small area such as building, office, schools etc.
- LAN is used to connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.





## Advantages of LAN $\Rightarrow$

- High data transfer rate
- Ease of Setup
- Centralized data
- Low Cost
- Provides higher security

## Disadvantages of LAN $\Rightarrow$

- Covers small area
- The cables and connectors get damaged easily.
- Requires administrative time.

## 2) **MAN** (Metropolitan Area Network) $\Rightarrow$

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a large network.
- Examples of MAN are networking in government agencies, airports, libraries etc.

## Advantages of MAN $\Rightarrow$

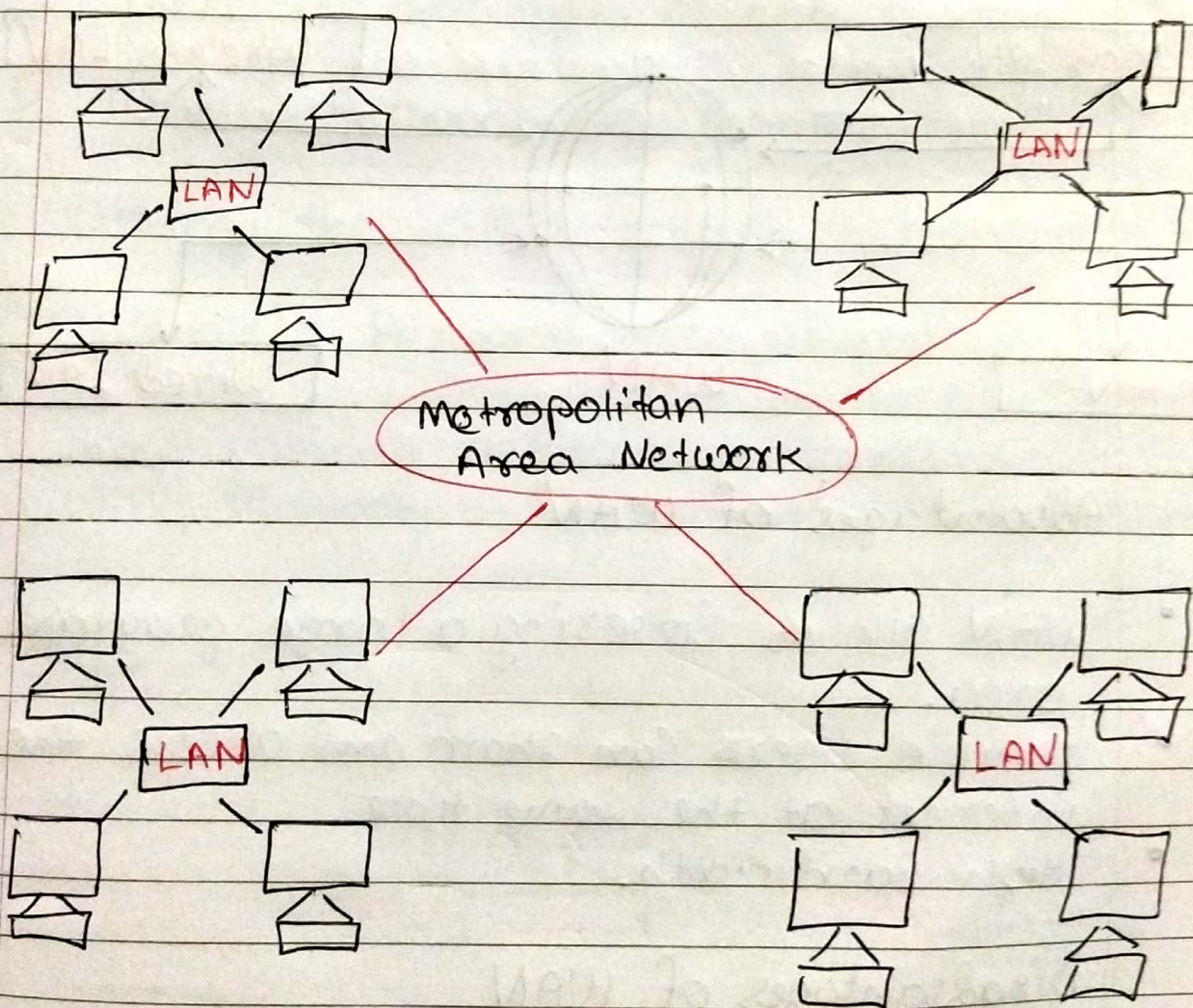
- Offers centralized data management.
- Quick transfer of files
- Provides higher speed of internet as it



Uses fiber optics.

Disadvantages of MAN  $\Rightarrow$

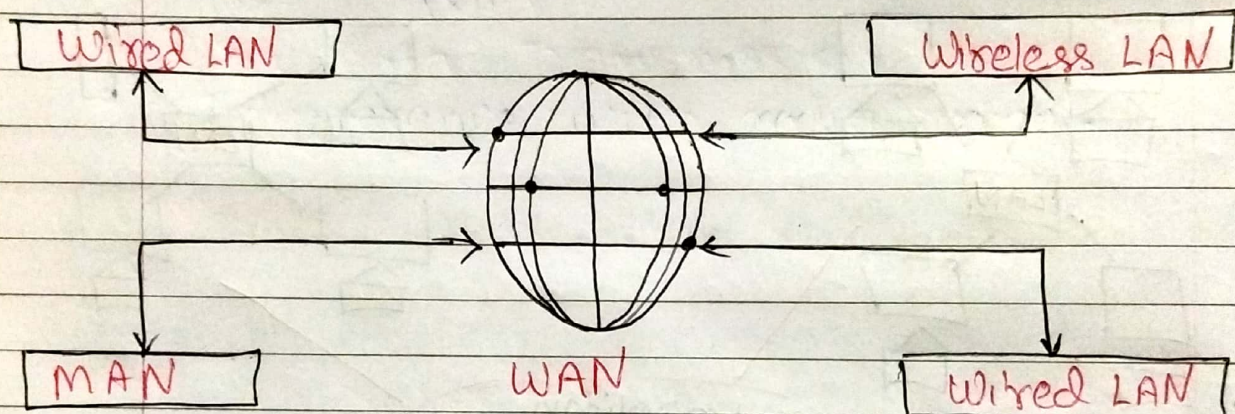
- Difficult to handle due to large network size.
- Risk of hacking
- High installation cost as it requires fiber optics.





### 3) WAN (Wide Area Network) ⇒

- WAN is a types of Computer Network that connects Computers over a Large geographical distance through a Shared Communication path.
- WAN Network Could be an interconnection between two or more LANs which are Connected through telephone lines or radio waves.



#### Advantages of WAN

- WAN allows covering a large geographical area.
- Multiple users can share and access the internet at the same time.
- High Bandwidth.

#### Disadvantages of WAN

- High initial investment cost.



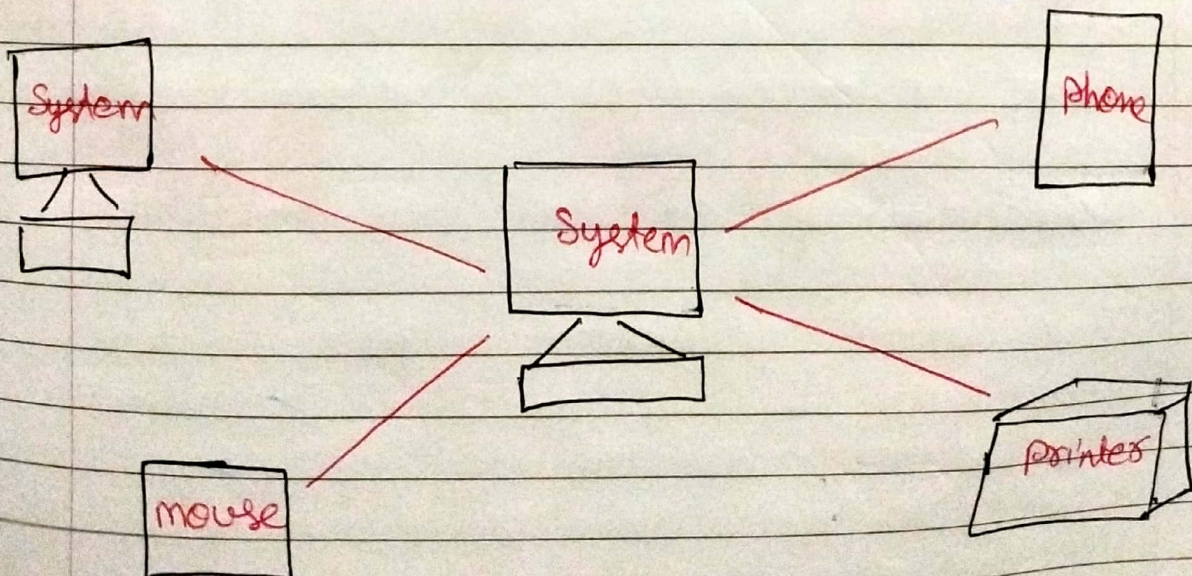
- Hard to handle as the network is vast and complex
- Less secure.

#### 4) **PAN** (Personal Area Network) $\Rightarrow$

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
  - It is the smallest and most basic type of computer network.
- There are two types of PAN

1) **Wired Personal Area Network**:  $\Rightarrow$  WPAN  
is created by using the USB.

2) **Wireless Personal Area Network**:  $\Rightarrow$  WPAN  
is developed by simply using wireless technologies such as Wifi, Bluetooth. It is a low range network.





Example of PAN are  $\Rightarrow$  USB, Computer, Bluetooth, etc.

Advantages of PAN are  $\Rightarrow$

- Less Expensive
- Confined to a small space area.
- Links to multiple devices concurrently.

Disadvantages of PAN are  $\Rightarrow$

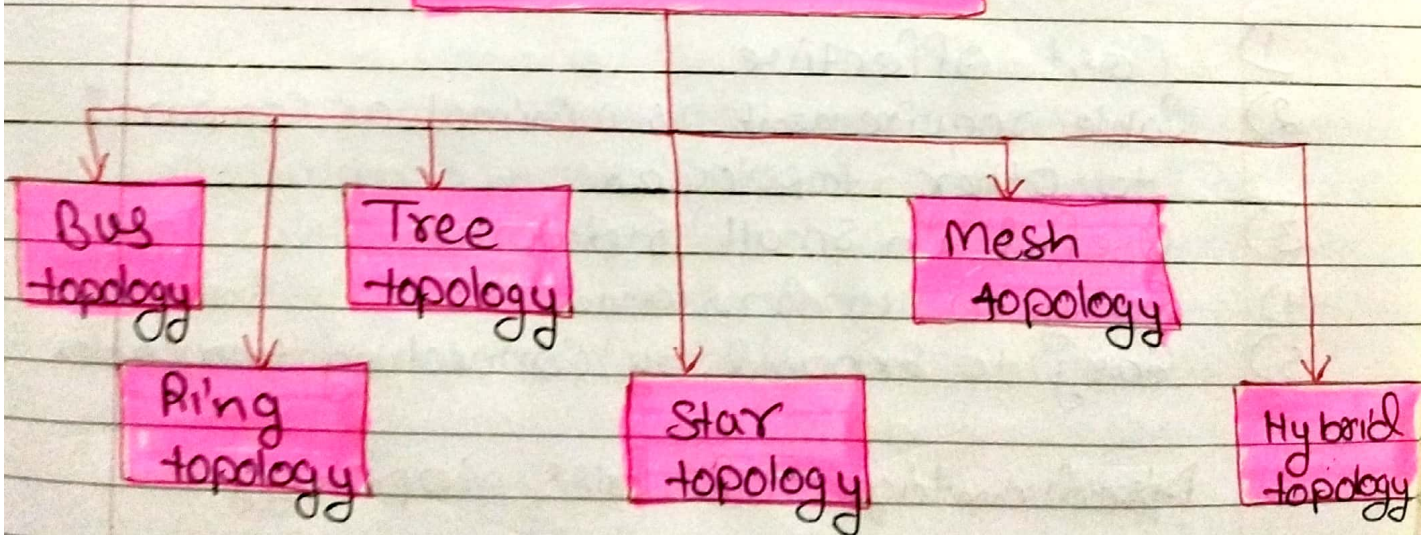
- Limited area
- Slow Data Transmission
- Interference with radio signal.



# Network Topology

- A Network Topology is the arrangement with which Computer System or network devices are connected to each other.
- The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as network topology.
- Topologies may define both physical and logical aspect of the network.  
Both logical and physical topologies could be same or different in a same network.

## Types of Network topology





## 1) Bus topology $\Rightarrow$

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- The backbone cable is considered as a "single lane" through which the message is broadcast to all the stations.
- The most common access method of the bus topology is CSMA (Carrier Sense Multiple Access).

## Advantage of Bus topology $\Rightarrow$

- 1) Cost-effective
- 2) Cable requirement is minimal as compared to other topologies
- 3) Useful in small networks
- 4) Easy to understand
- 5) Easy to expand by connecting two cables.

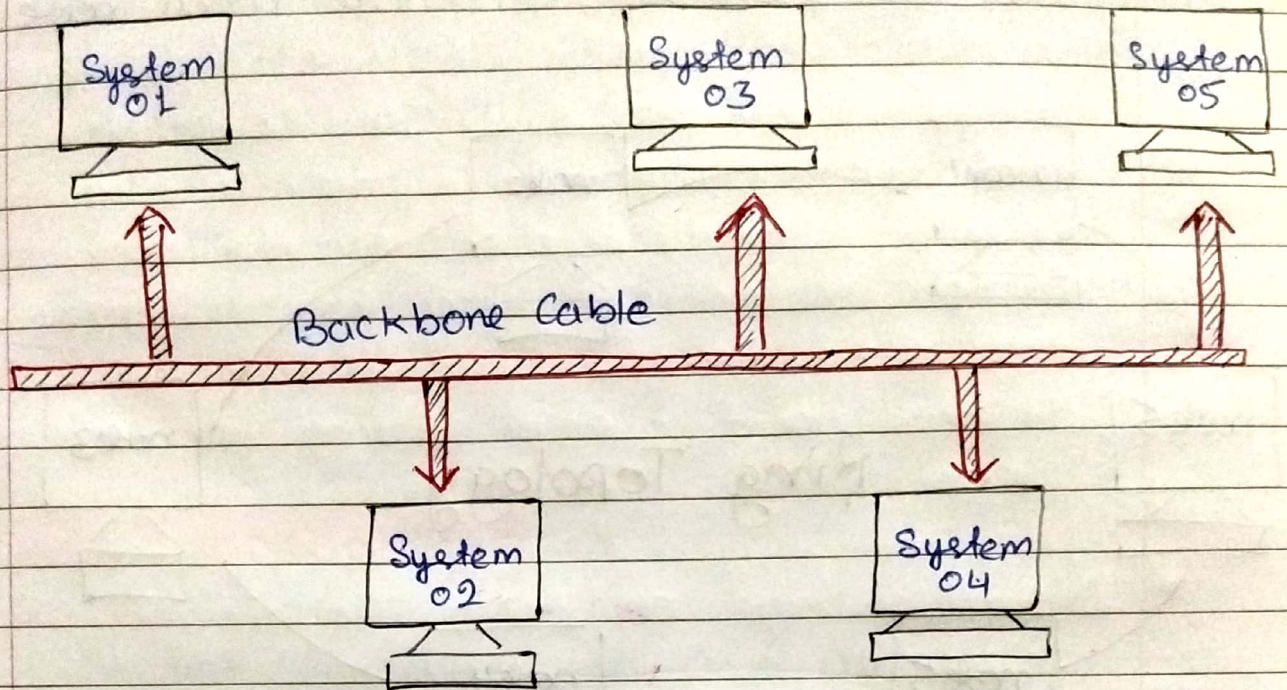
## Disadvantage of Bus topology $\Rightarrow$

- 1) The whole network fails if cables fail.
- 2) The performance of the network decreases in case network traffic is heavy or nodes are more or the cable has a



limited length.

- 3) It works slower as compared to the ring topology.

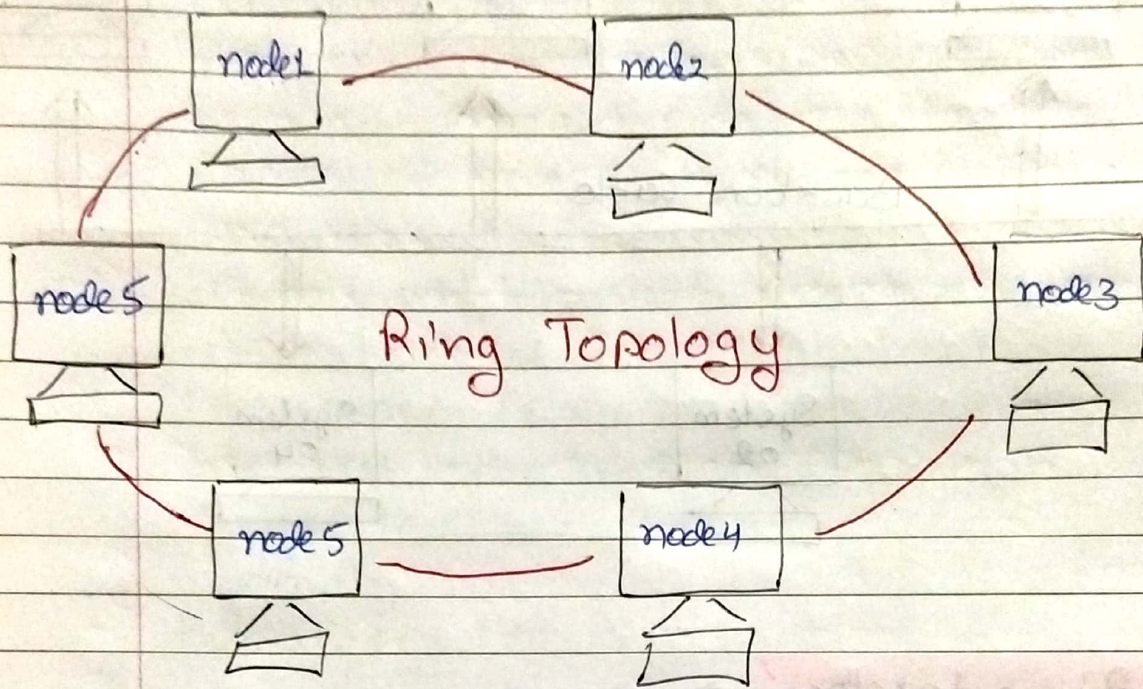


## 2) Ring topology ⇒

- It is named ring topology because it creates a ring as each computer is linked to the neighbouring computer, with the last one linked to the first, there are exactly two neighbours for each computer.
- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit it to the next node.



- Data is transmitted in a sequential manner that is bit by bit. Data transmitted, has to go through each node linked in the network, till the final node.



### Advantage of Ring Topology ⇒

- 1) Transmitting network is not affected by huge traffic or by the addition of more nodes, as only the nodes having tokens (short message) are allowed to transmit data.
- 2) Low Cost to install and expand.
- 3) It is a more reliable network because the Communication System is not dependent on the single host computer.
- 4) faulty devices can be removed from the network without bringing the network down.

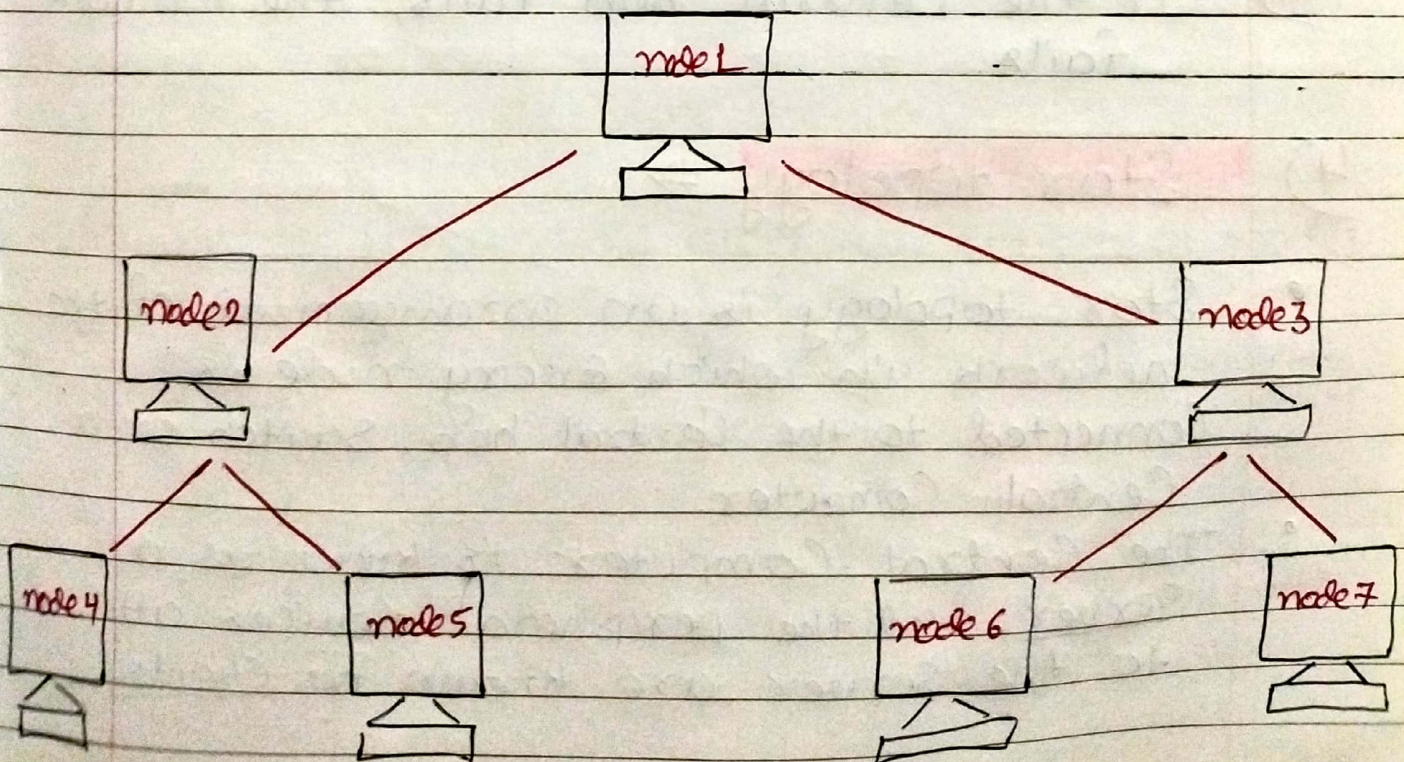


## Disadvantage of Ring topology $\Rightarrow$

- 1) Troubleshooting is not simple in a ring topology.
- 2) The addition or removal of the computers interferes with the other nodes and network activity.
- 3) The Crashing of one node affects the whole network.
- 4) Initial installation cost is high therefore not applied at low-density traffic.

## 3) Tree topology $\Rightarrow$

- It has a root node and all other nodes are linked to it "Creating a hierarchy".
- It is also called "hierarchical topology".
- It must have a minimum of three levels to the hierarchy.





- Ideal if workstations are situated in groups
- Useful in Wide Area Network.

### Advantage of Tree topology

- 1) Extension of bus and star topologies.
- 2) Expansion of nodes is possible and easy
- 3) Easily managed and maintained.
- 4) Error detection and error correction are very easy.
- 5) It has point-to-point wiring for individual segments.

### Disadvantage of tree topology

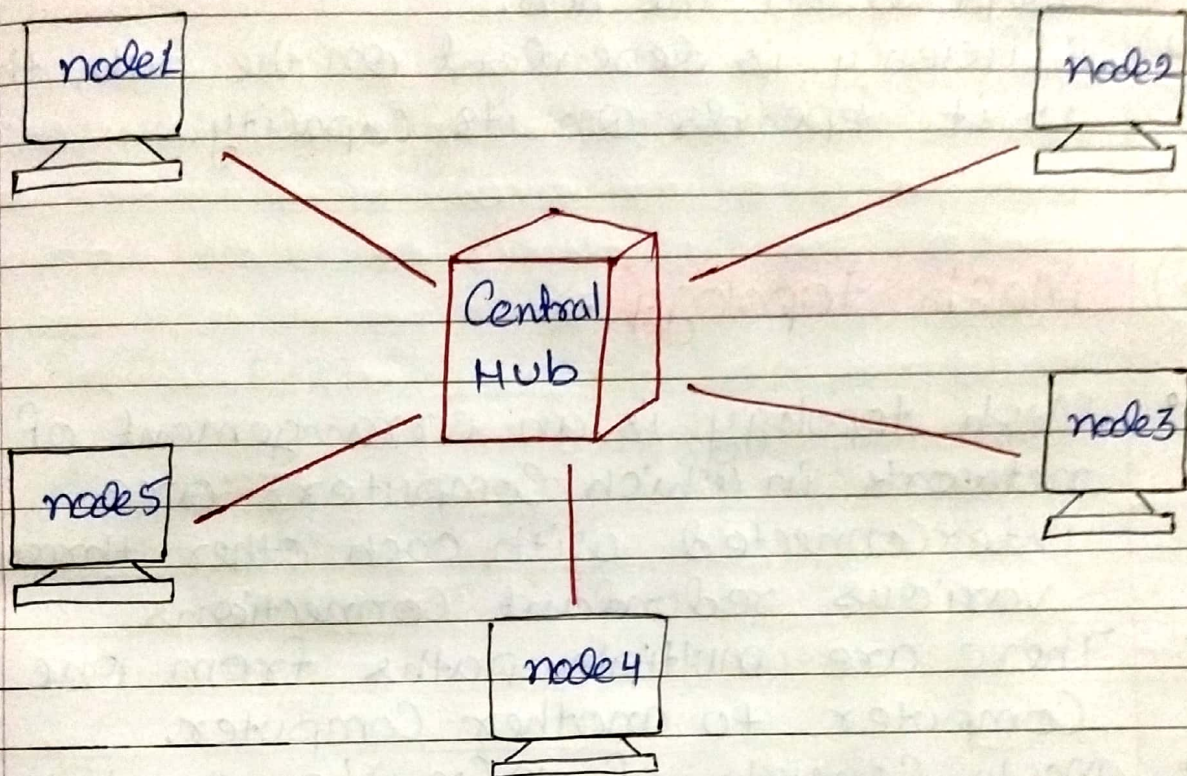
- 1) Heavily Cabled
- 2) Costly
- 3) If additional nodes are introduced, maintenance is difficult.
- 4) If the central hub fails, the network fails.

### 4) Star topology ⇒

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a Server, and the peripheral devices attached to the server are known as Clients.



- Coaxial Cable or RJ-45 Cables are used to Connect the Computers.
- Hubs or Switches are mainly used as Connection devices in a physical star topology.
- Star topology is the most popular topology in network implementation.



### Advantage of star topology

- 1) Speedy performance with less number of nodes and low network traffic.
- 2) Hub can be easily upgraded without difficulty.
- 3) Simpler to troubleshoot.
- 4) Simpler to setup and modify.
- 5) If there is a failure in one node then the failed node is only affected, and the rest of the nodes can work without any issues.

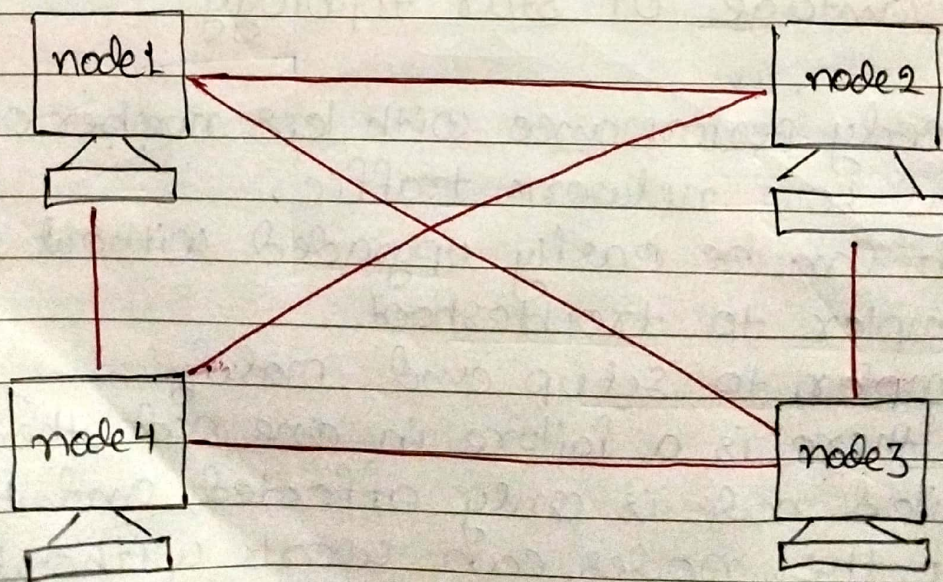


## Disadvantage of Star Topology

- 1) Expensive to install.
- 2) Expensive in usage.
- 3) If the hub crashes then the entire network is stopped because all linked nodes depend on the hub.
- 4) Efficiency is dependent on the hub, that is it depends on its capacity.

## 5) Mesh topology $\Rightarrow$

- Mesh topology is an arrangement of the network in which Computers are interconnected with each other through various redundant connections.
- There are multiple paths from one Computer to another Computer.
- Mesh consists of  $n(n-1)/2$  physical channels to link  $n$  number of devices.





## Types of Mesh topology

full Mesh  
Topology

Partial Mesh  
Topology

- full mesh Topology  $\Rightarrow$  In a full mesh topology, Each Computer is connected to all the the Computers available in the network.
- Partial Mesh Topology  $\Rightarrow$  In a partial mesh topology, not all but certain Computers are connected to those Computers with which they Communicate frequently.

### Advantage of mesh topology $\Rightarrow$

- 1) Each Connection may carry its unique data load.
- 2) It is robust.
- 3) fault can be diagnosed easily.
- 4) Facilitates security and Privacy.

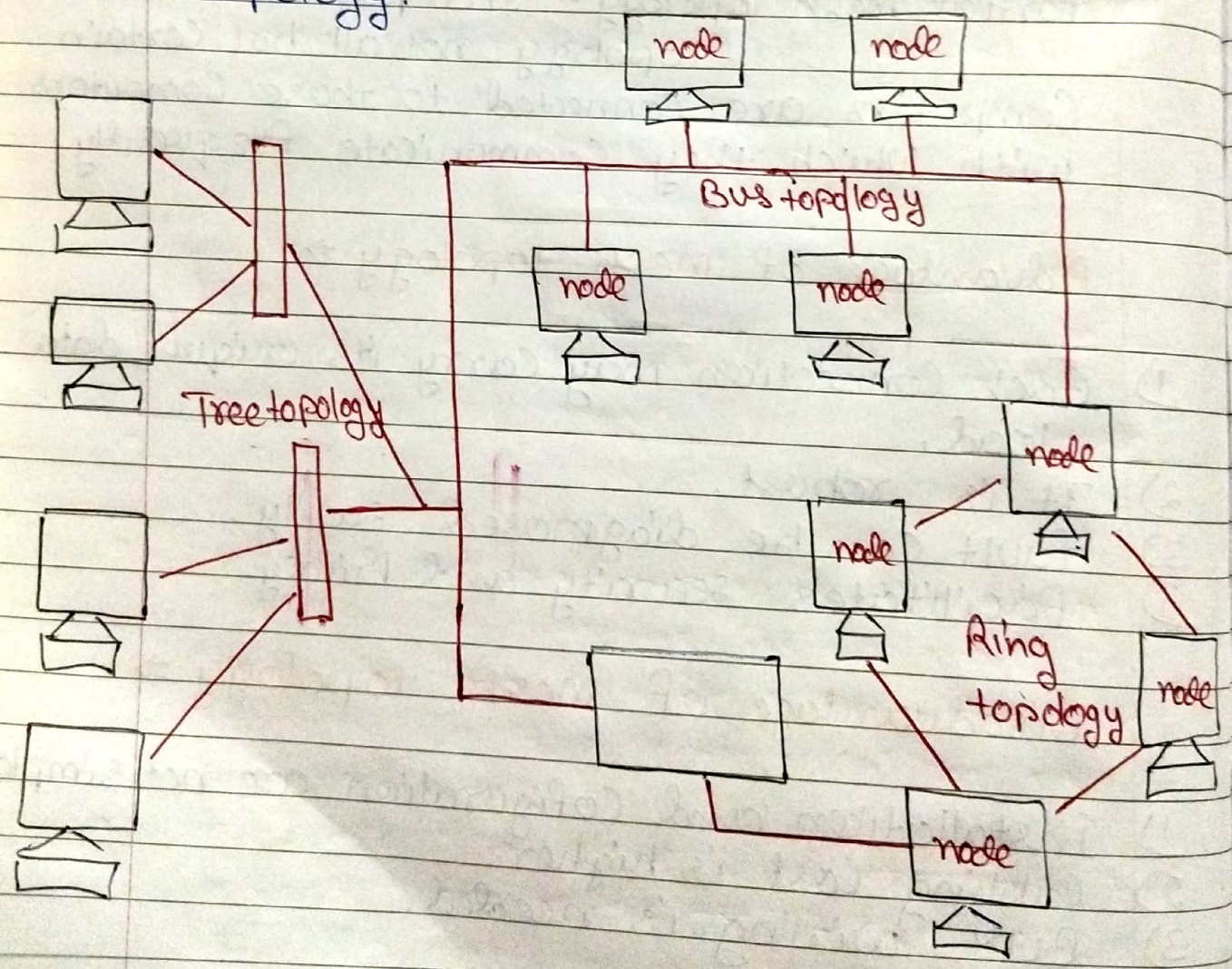
### Disadvantage of Mesh topology $\Rightarrow$

- 1) Installation and Configuration are not simple.
- 2) Cabling Cost is higher.
- 3) Bulk wiring is needed.



## 6) Hybrid topology $\Rightarrow$

- It is a combination of two or more than two topologies.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- for example  $\Rightarrow$  if in an office in some department ring topology is used and in another department in the same place, star topology is used, connecting those topologies will form a Hybrid topology.





## Advantage of Hybrid topology

- 1) Reliable because error detecting and troubleshooting are easy.
- 2) Effective
- 3) Scalable as size can be increased easily
- 4) flexible.

## Disadvantage of Hybrid Topology.

- 1) Complex in design
- 2) Costly Hub
- 3) Costly infrastructure

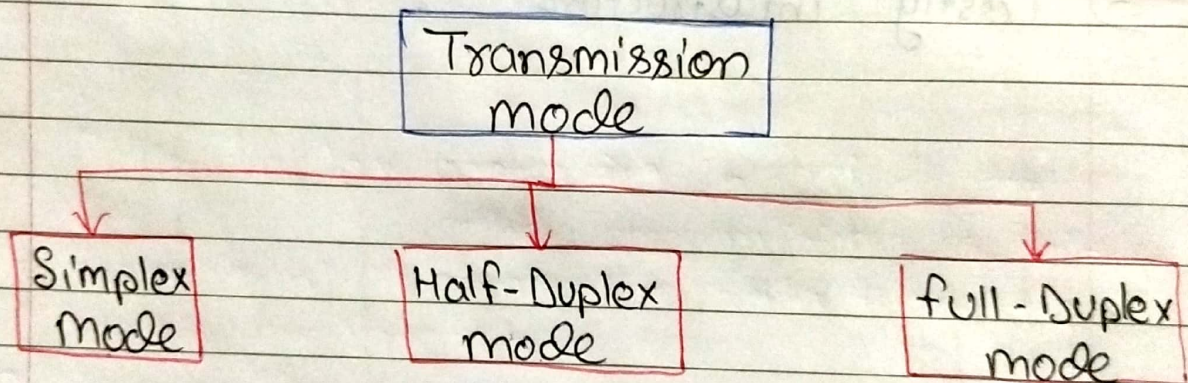


# Transmission modes

Page No: 31

- The way in which data is transmitted from one device to another device is known as transmission mode.
- Data Transmission mode defines the direction of the flow of information between two communication devices.
- The transmission mode is also known as the communication mode. These modes direct the direction of flow of information.
- The transmission mode is defined in the physical layer.

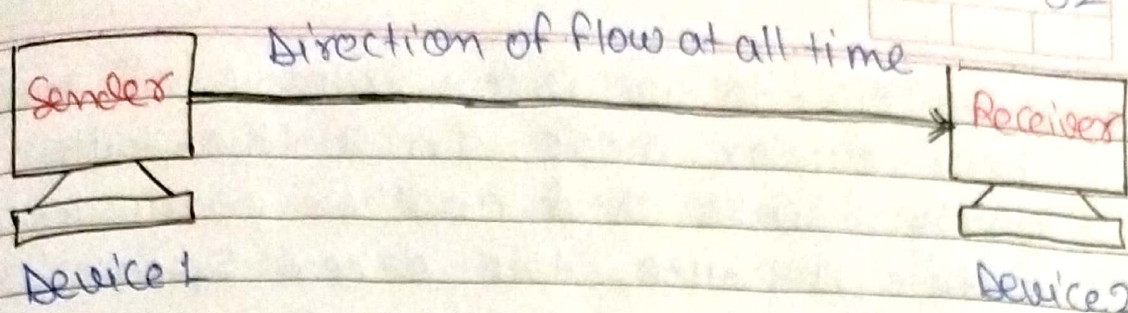
The transmission mode is divided into three categories:



Simplex Mode  $\Rightarrow$  • Simplex is the data transmission mode in which the data can flow only in one direction, i.e. the communication is unidirectional.

- A device can only send the data but cannot receive it or it can receive the data but cannot send the data.

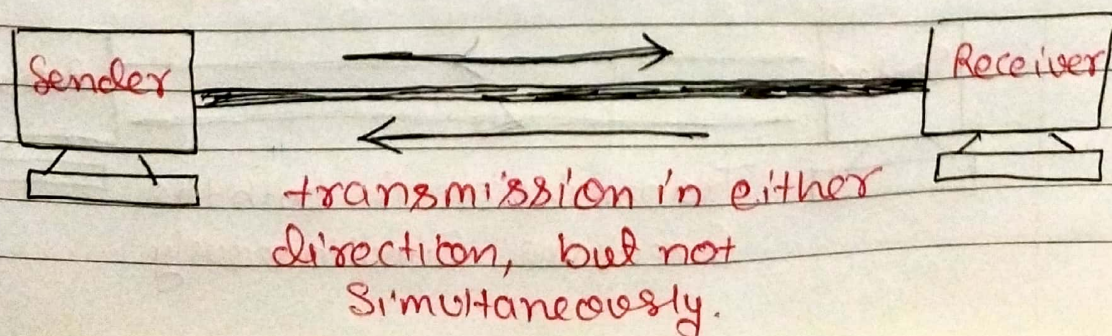




- The Simplex mode is used in the business field as in sales that do not require any corresponding reply.
- The radio station is a Simplex channel as it transmits the signal to the listeners but never allows them to transmit back.
- The main advantage of the Simplex mode is that the full capacity of the Communication channel can be utilized during transmission.
- Communication is unidirectional, so it has no inter-communication between devices.

**Half - Duplex Mode** ⇒ • In half duplex channel, direction can be reversed. Such as the station can transmit and receive the data as well.

- Message flow in both the directions, but not at the same time.
- In half-duplex mode, It is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data.

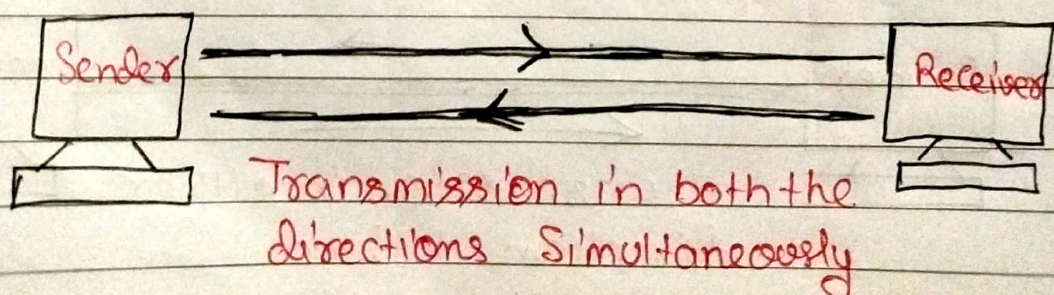




- A walkie-talkie is an example of the half-duplex mode. In walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens.
- main advantage of half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.
- One disadvantage of half-duplex mode, when one device is sending the data, then another has to wait, this causes the delay in sending the data at the right time.

Full-duplex mode  $\Rightarrow$  • In full duplex mode, the communication is bi-directional such as the data flow is in both the directions.

- Both the stations can send and receive the message simultaneously.
- full-duplex mode has two simplex channels. One channel has traffic moving in one direction, and another channel has traffic flowing in the opposite direction.





- The full-duplex mode is the fastest mode of communication between devices.
- The most common example of the full duplex mode is a telephone network. When two people are communicating with each other by a telephone line, both can talk and listen at the same time.
- Advantage of Both the stations can send and receive the data at the same time.
- Disadvantage of full-duplex if there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.



# Difference b/w Simplex, half duplex and full-duplex mode

35

| Simplex mode                                                                                             | Half-duplex mode                                                                                                     | full-duplex mode                                                                                                  |
|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| 1) the Communication is unidirectional                                                                   | 1) the Communication is bidirectional, but one at a time.                                                            | 1) The Communication is bidirectional                                                                             |
| 2) Sender and Receiver in Simplex mode, Sender can send the data but that Sender cannot receive the data | 2) Sender and Receiver in half duplex mode, Sender can send the data and also can receive the data but one at a time | 2) Sender and Receiver in full duplex mode, Sender can send the data and also can receive the data simultaneously |
| 3) Usage of one Channel for the transmission of data                                                     | 3) Usage of one Channel for the transmission of data                                                                 | 3) Usage of two channels for the transmission of data.                                                            |
| 4) Simplex utilize the maximum of a single bandwidth                                                     | 4) the half-duplex involves lesser utilization of single bandwidth at the time of transmission                       | 4) the full-duplex doubles the utilization of transmission bandwidth.                                             |
| 5) Example of Simplex mode are: keyboard and monitor                                                     | 5) Example of half duplex mode is walkie-talkies                                                                     | 5) Example of full-duplex mode is: Telephone                                                                      |

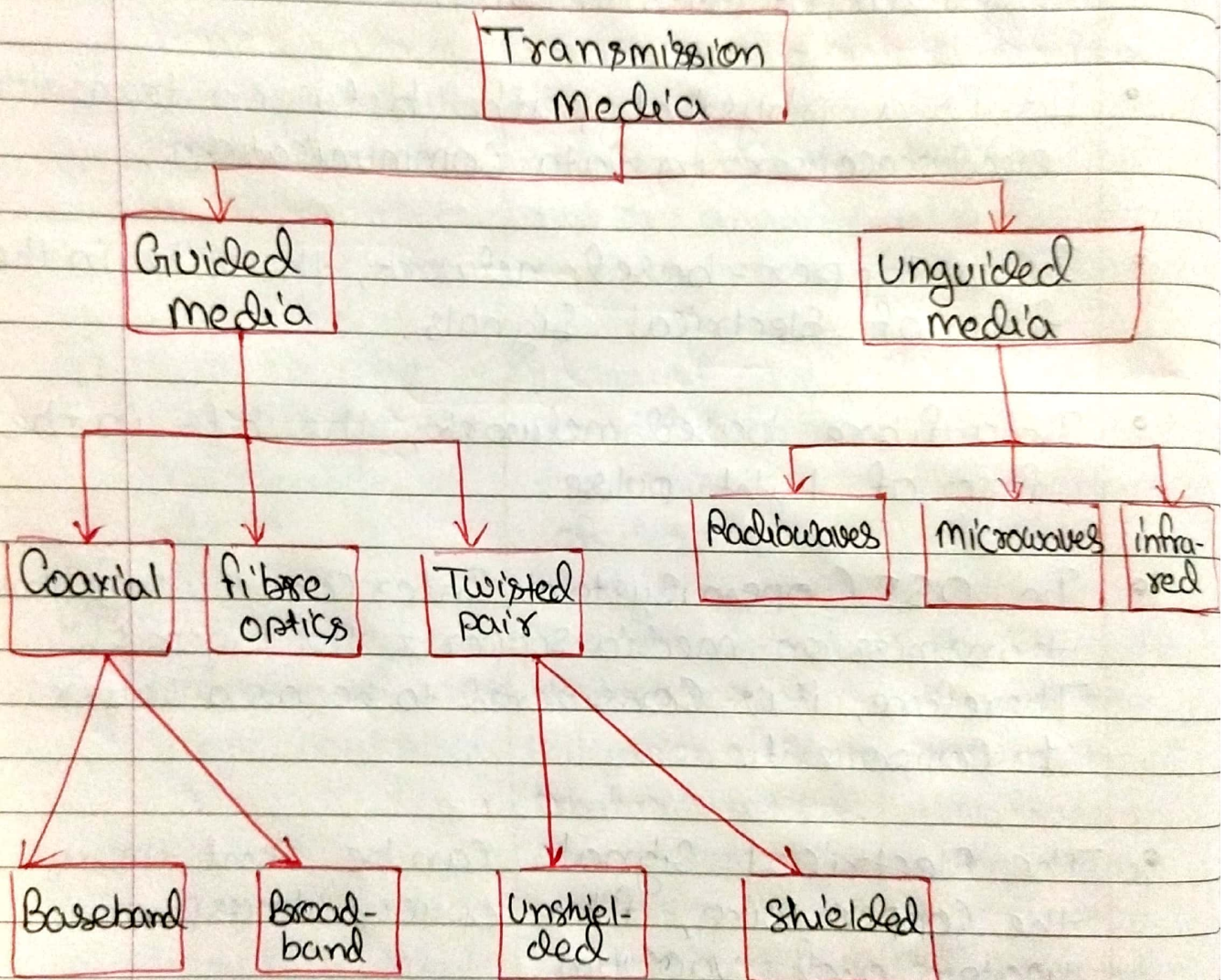


- Transmission media is a Communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through LAN.
- It is a physical path between transmitter and receiver in data communication.
- In a Copper-based network, the bits in the form of Electrical signals.
- In a fibre based network, the bits in the form of light pulse.
- In OSI (Open System Interconnection) phase transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 Component.
- The Electrical signals can be sent through the Copper wire, fibre optics, atmosphere, water and vacuum.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.



- The transmission media is available in the Lowest Layer of the OSI reference model physical layer.

## Classification of Transmission Media





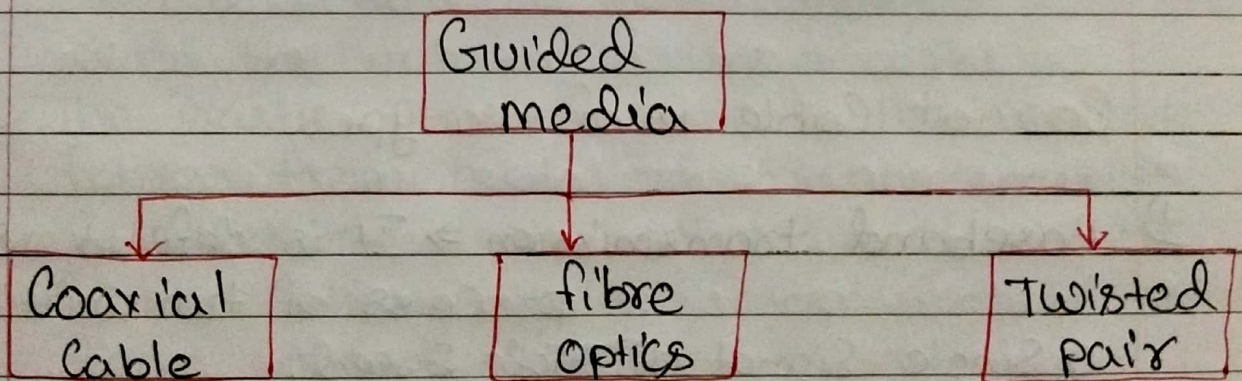
# Guided Transmission Media

Page No: 38

- Guided media are also known as wired or bounded media.
- It is defined as the physical medium through which the signals are transmitted.
- Signals being transmitted are directed and confined in a narrow pathway by using physical links.

## Feature of Guided media.

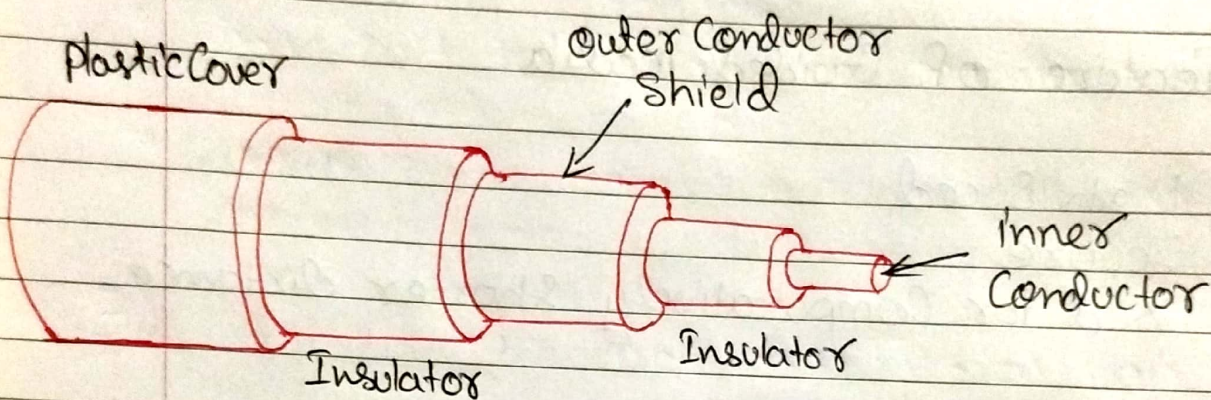
- 1) High Speed
- 2) Secure
- 3) Used for comparatively shorter distance.



- 1) Coaxial Cable ⇒ 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.



Coaxial Cable is of two types:

- 1) Baseband transmission  $\Rightarrow$  It is defined as the process of transmitting a single signal at high speed.
- 2) Broadband transmission  $\Rightarrow$  It is defined as the process of transmitting multiple signals simultaneously.

Advantages of Coaxial Cable  $\Rightarrow$

- The data can be transmitted at high speed.



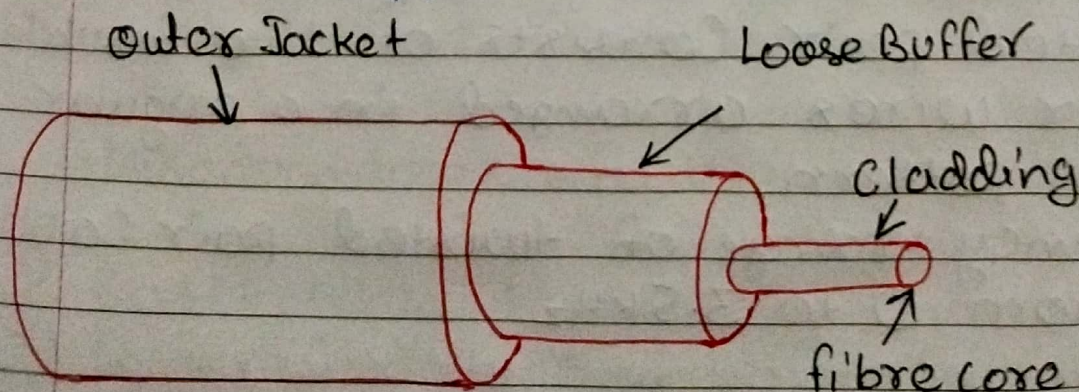
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

### Disadvantages of Coaxial Cable $\Rightarrow$

- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

2) Fibre Optics  $\Rightarrow$  • fibre optic cable is a cable that uses electrical signals for communication.

- fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other type of wiring.
- fibre optics provide faster data transmission than copper wires.





## Advantage of fibre optics $\Rightarrow$

- Increased Capacity and bandwidth
- Lightweight
- Less Signal attenuation
- Immunity to Electromagnetic interference
- Resistance to Corrosive materials.

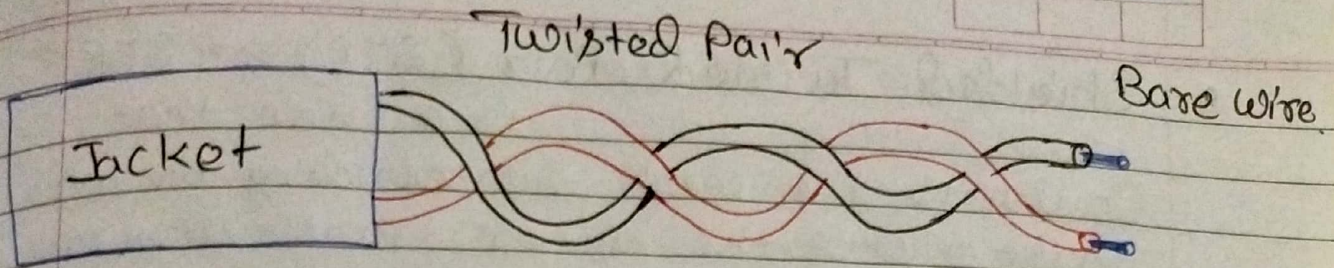
## Disadvantage of fibre optics $\Rightarrow$

- Difficult to install and maintain
- High Cost
- fragile.

3) Twisted Pair Cable  $\Rightarrow$  • 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.
- A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.
- frequency range of twisted pair cable is from 0 to 3.5 KHz.





## Types of Twisted Pair

Unshielded Twisted Pair

Shielded Twisted Pair

- Unshielded twisted Pair (UTP)  $\Rightarrow$  UTP consists of two insulated copper wires twisted around one another.
- This type of cable has the ability to block interference and does not depend on a physical shield for this purpose.
- It is used for telephonic application.

### Advantages of UTP $\Rightarrow$

- 1) Least Expensive
- 2) Easy to install
- 3) High Speed Capacity.

### Disadvantages of UTP $\Rightarrow$

- 1) Susceptible to external interference.
- 2) Lower Capacity and performance in comparison to STP.
- 3) Short distance transmission due to attenuation.



- Shielded Twisted Pair (STP) ⇒ • STP is a Cable that contains the mesh surrounding the wire that allows the higher transmission rate.

### Advantages of STP

- 1) Better performance at a higher data rate in comparison to UTP.
- 2) Eliminates crosstalk.
- 3) Comparatively faster.

### Disadvantages of STP

- 1) Comparatively difficult to install and manufacture.
- 2) More expensive.
- 3) Bulky.

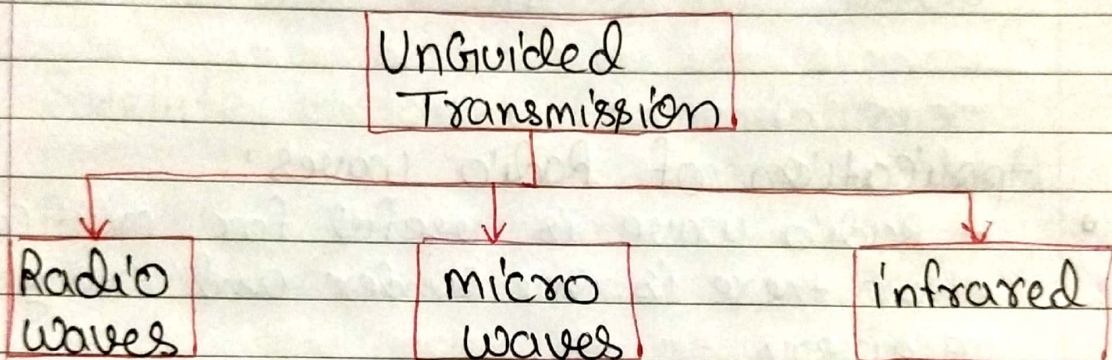


# UnGuided Transmission Media

Page No: 44

- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as Wireless transmission.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

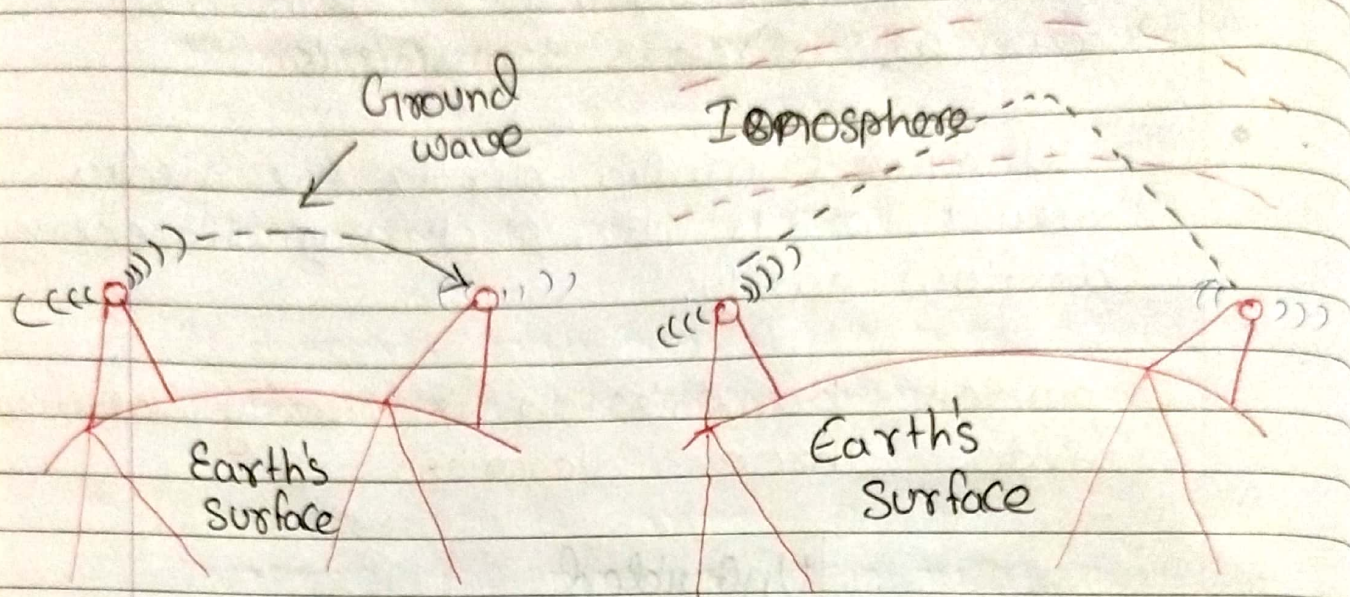


Radio waves  $\Rightarrow$  • Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.

- Radio waves are omnidirectional such as the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1Khz.
- In the case of radio waves, the sending and receiving antenna are not aligned such that the wave sent by the sending antenna can be received by any receiving antenna.



- An example of the radio wave is FM radio.



### Application of Radio waves!

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, Cordless phones are example of a radio wave.

Microwaves  $\Rightarrow$  There are two types of microwaves transmission.

- 1) Terrestrial microwaves
- 2) Satellite microwave Communication.

1) Terrestrial Microwave Transmission  $\Rightarrow$

- Terrestrial microwave transmission is a



- technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 100GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned such that the waves sent by the sending antenna are narrowly focussed.

## 2) Satellite microwave Communication $\Rightarrow$

- A Satellite is a physical object that revolves around the earth at a known height.
- Satellite Communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using Satellite Communication.

Infrared  $\Rightarrow$  • An infrared transmission is a wireless technology used for communication over short ranges.

- The frequency of the infrared is in the range from 300GHz to 400THz



- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

### Characteristics of infrared $\Rightarrow$

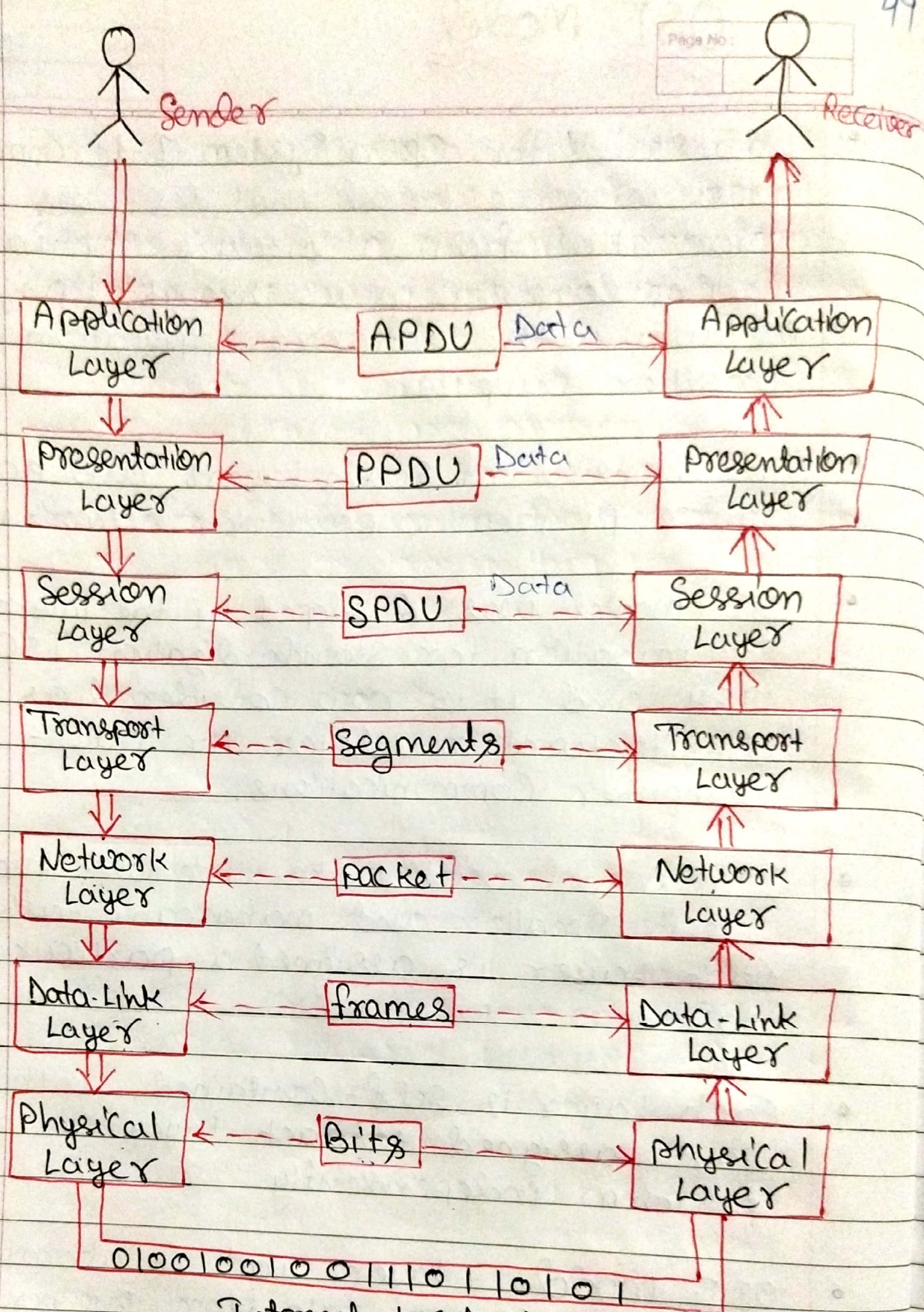
- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.



# OSI Model

- OSI stands for Open System Interconnection. It is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that the task assigned to each layer can be performed independently.
- OSI model 7 layers work collaboratively to transmit the data from one person to another across the globe.

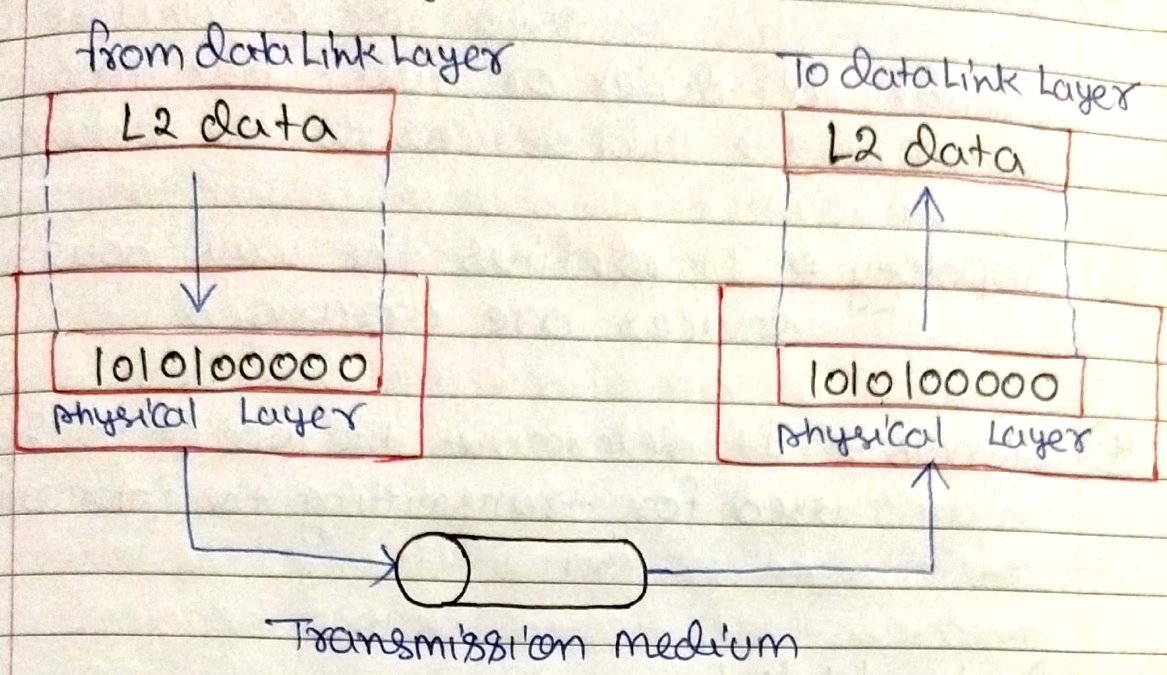




Internet, Local network,  
Long distance network etc.  
(Physical Communication)



# 1) Physical Layer ⇒



- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

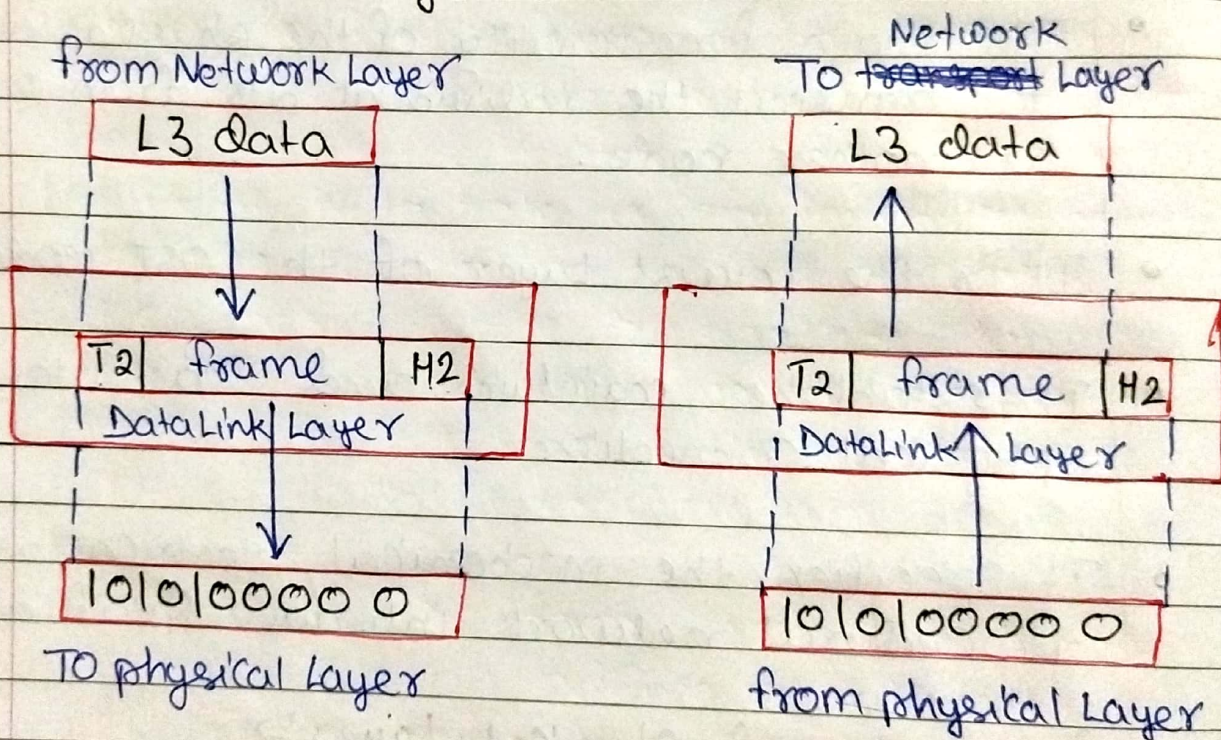
## functions of Physical Layer ⇒

- 1) Line Configuration ⇒ It defines the way how two or more devices can be connected physically.



- 2) Data transmission  $\Rightarrow$  It defines the transmission mode whether it is Simplex, half-duplex or full duplex mode between the two devices on the network.
- 3) Topology  $\Rightarrow$  It defines the way how network devices are arranged.
- 4) Signals  $\Rightarrow$  It determines the type of the signal used for transmitting the information.

## 2) Data-Link Layer $\Rightarrow$



- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.

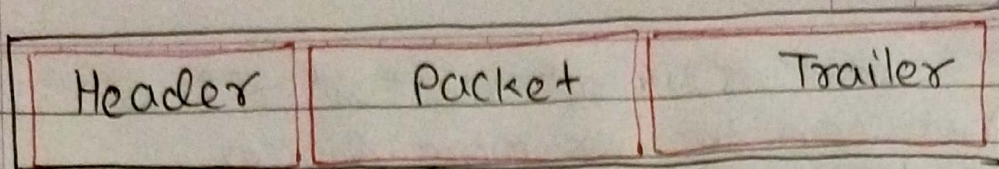


- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub layers:
  - 1) Logical Link Control Layer  $\Rightarrow$  • It is responsible for transferring the packets to the Network Layer of the receiver that is receiving.
  - It identifies the address of the network layer protocol from the header
  - It provides flow control.
- 2) Media Access Control Layer  $\Rightarrow$  • A media access control layer is a link between the Logical Link Control Layer and the network's physical layer
- It is used for transferring the packets over the network.

functions of the Data-Link layer  $\Rightarrow$

- 1) framing  $\Rightarrow$  The data link layer translates the physical's raw bit stream into packets known as frames. The data link layer adds the header and trailer to the frame.



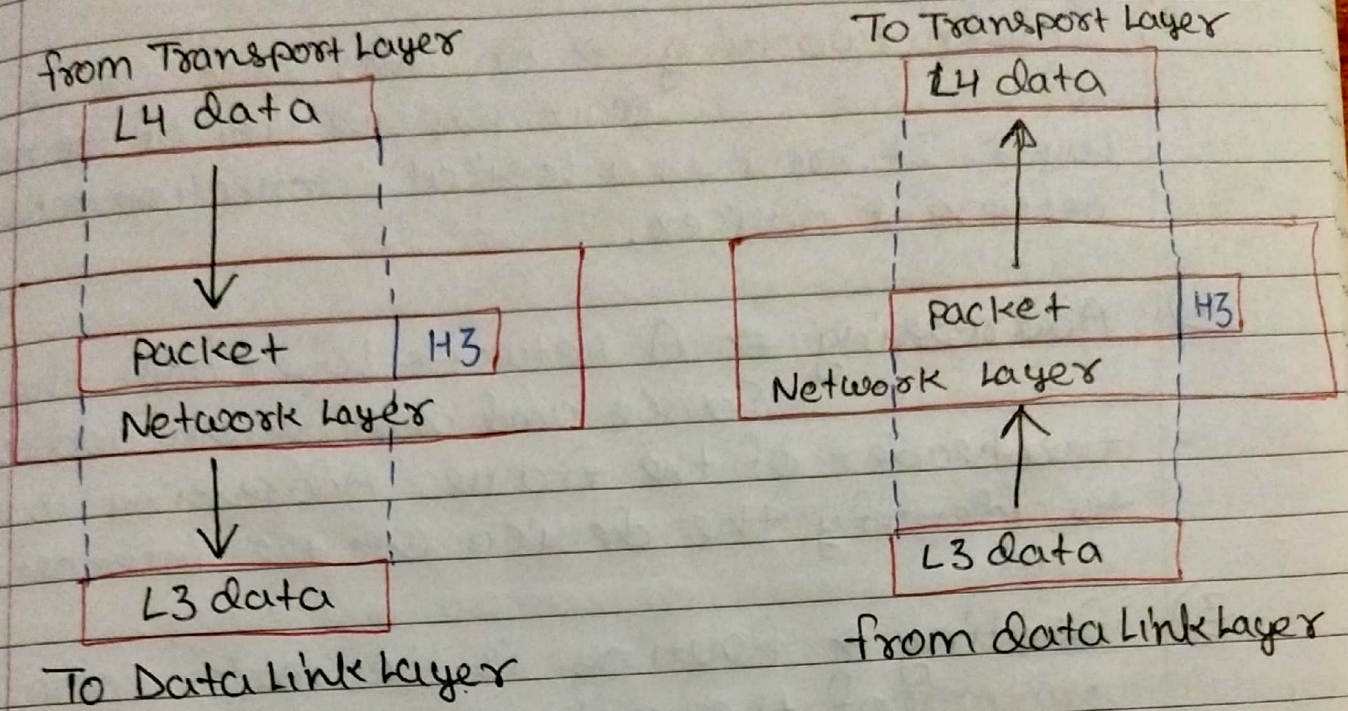


The header which is added to the frame contains the hardware destination and source address.

- 2) Physical Addressing  $\Rightarrow$  The data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- 3) flow Control  $\Rightarrow$  flow control is the main functionality of the Data-Link Layer. It is the technique through which the constant data rate is maintained on both the sides so that no data gets corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- 4) Error Control  $\Rightarrow$  Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer.
- 5) Access Control  $\Rightarrow$  When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.



### 3) Network Layer $\Rightarrow$



- It is a Layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from Source to the destination based on the network conditions, the priority of service and other factors.
- Data Link Layer is responsible for routing and forwarding the packets.
- Routers are the Layer 3 devices, they are specified in this Layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network Layer protocols. Example of protocols are IP and IPv6.

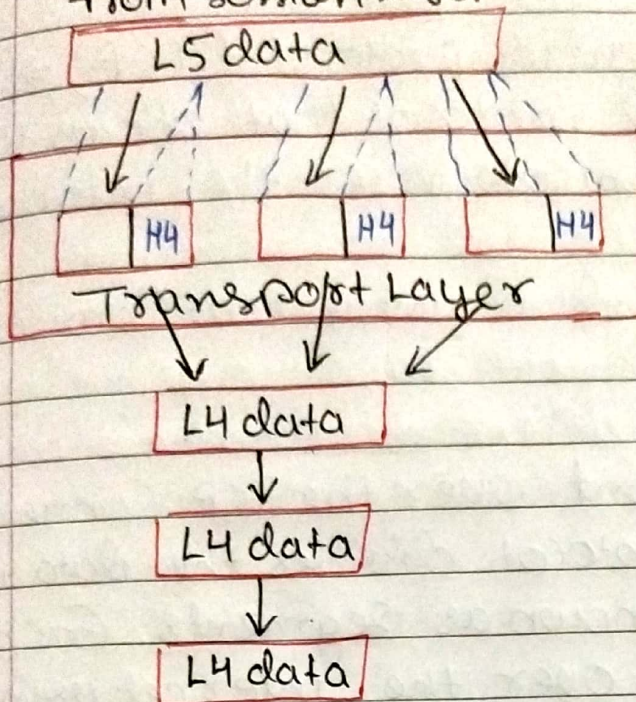


## Functions of Network Layer $\Rightarrow$

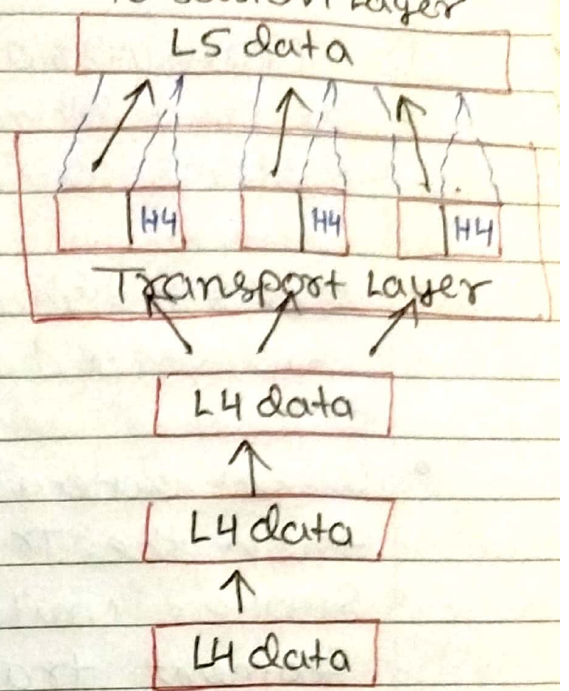
- 1) **Internetworking**  $\Rightarrow$  An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- 2) **Addressing**  $\Rightarrow$  A Network Layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- 3) **Routing**  $\Rightarrow$  Routing is the major component of the network layer, and it determines the best optimal path out of the multiple path from source to destination.
- 4) **Packetizing**  $\Rightarrow$  A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as packetizing. It is achieved by internet protocol (IP).



4) Transport Layer  $\Rightarrow$   
from Session Layer



To Session Layer



To network layer

from network layer

- The transport Layer is a Layer 4 ensure that messages are transmitted in the order in which they are send and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.



The two protocols used in this Layer are!  $\Rightarrow$

### 1) Transmission Control protocol (TCP) $\Rightarrow$

- It is a standard protocol that allows the systems to communicate over the internet.
- It establishes and maintains a connection between hosts.
- When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The TCP reorders the packets in the correct order at the receiving end.

### 2) User Datagram Protocol (UDP) $\Rightarrow$

- User Datagram protocol is a transport layer protocol.
- It is an unreliable transport protocol as in this case receiver does not send any acknowledgement when the packet is received, the sender does not wait for any acknowledgement. Therefore, this makes a protocol unreliable.



## functions of Transport Layer $\Rightarrow$

- 1) Service - point addressing  $\Rightarrow$  Computer run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one Computer to another Computer but also from one process to another process. The transport Layer adds the header that contains the address known as a Service - point address or port address. The responsibility of the network layer is to transmit the data from one Computer to another Computer and the responsibility of the transport Layer is to transmit the message to the correct process.
- 2) Segmentation and reassembly  $\Rightarrow$  When the transport Layer receives the message from the upper Layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segments.
- 3) Connection Control  $\Rightarrow$  Transport Layer provides two services Connection-oriented service and Connectionless service. A Connectionless service treats each segments as an individual packet, and they all travel in different routes to reach the destination.
- 4) flow Control  $\Rightarrow$  The transport Layer also responsible for ~~error~~ Control.  
flow

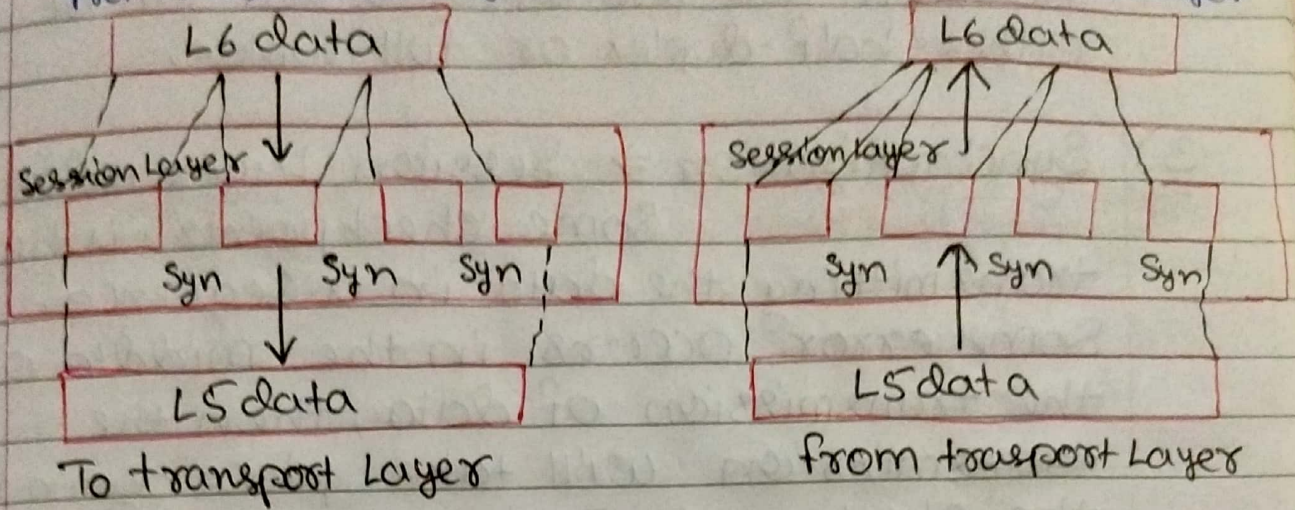


but it is performed end-to-end rather than across a single link.

- 5) Error Control  $\Rightarrow$  The transport layer is also responsible for Error Control. Error Control is performed end-to-end rather than across the single link. The sender transport layer ensure that message reach at the destination without any error.



## 5) Session Layer



- It is a Layer 3 in the OSI model.
- The Session Layer is used to establish, maintain and synchronizes the interaction between communicating devices.
- This Layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.

## functions of Session Layer:

- 1) Session establishment, maintenance and termination:  $\Rightarrow$  The Layer allows the two processes to establish, use and terminate a connection.
- 2) Dialog Control  $\Rightarrow$  Session Layer acts as a dialog controller that creates a dialog between two processes or we



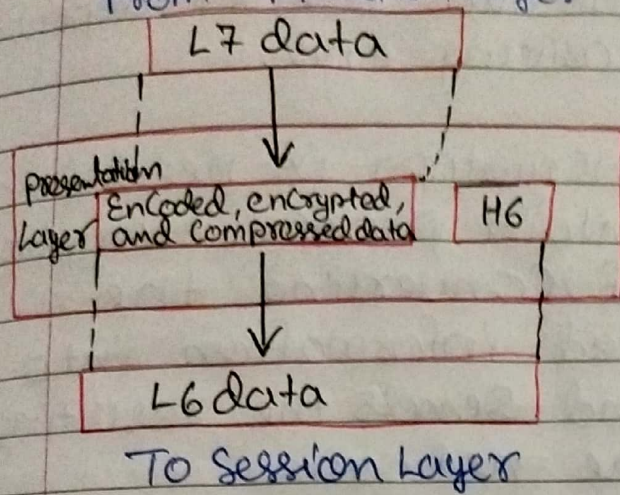
Can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

- 3) Synchronization  $\Rightarrow$  Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

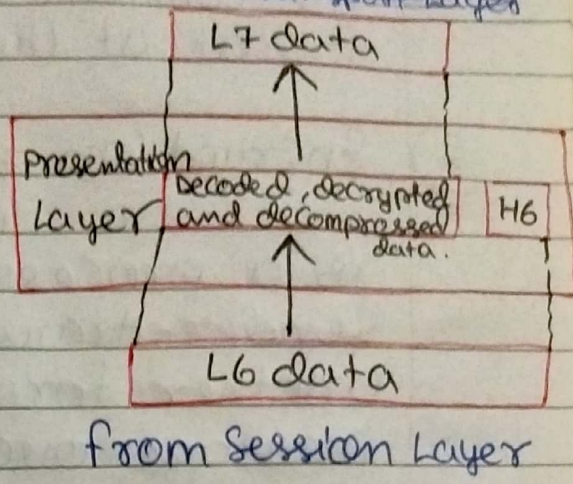
msg  $\rightarrow$  Hello P.T  
 Key  $\begin{array}{r} +3 \\ \hline \text{KHOO R} \end{array}$  Encode C.T  
 $\begin{array}{r} -3 \\ \hline \text{HELLO} \end{array} \rightarrow \text{u}$



## 6) Presentation Layer from Application Layer



## Application Layer To Transport Layer



- A Presentation Layer is mainly concerned with the Syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This Layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation Layer is also known as the Syntax Layer.

## functions of Presentation Layer ⇒

- 1) Translation ⇒ The processes in two systems exchange the information in the form of character string, number and so on. It converts the data from sender-dependent



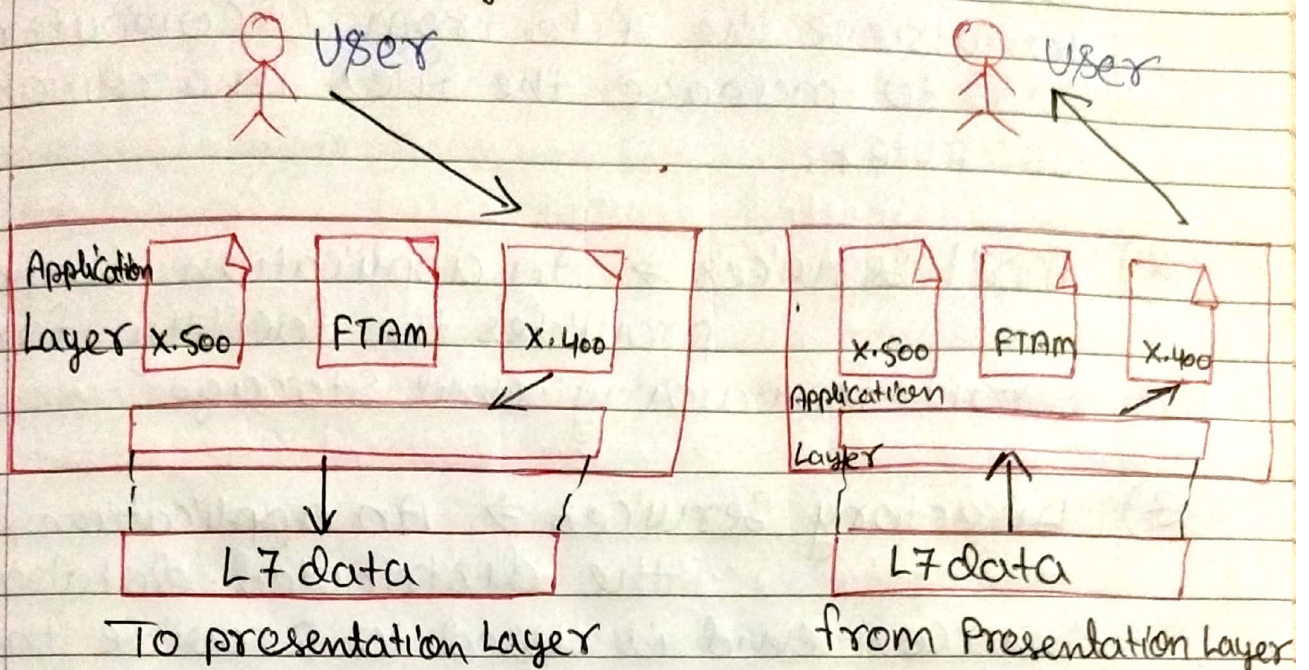
format into a Common format and changes the Common format into receiver-dependent format at the receiving end.

2) Encryption  $\Rightarrow$  Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.

3) Compression  $\Rightarrow$  Data Compression is a process of compressing the data, such that it reduce the no. of bits to be transmitted. Data Compression is very important in multimedia such as text, audio, video.



## 7) Application Layer ⇒



- An application Layer serves as a window for users and application process to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application Layer is not an application, but it performs the application layer function.
- This layer provides the network services to the end-users.

## function of Application Layer ⇒

- 1) file transfer, access, and management (FTAM) ⇒  
An application layer allows a user



to access the files in a remote Computer,  
to retrieve the file from a Computer  
and to manage the files in a remote  
Computer.

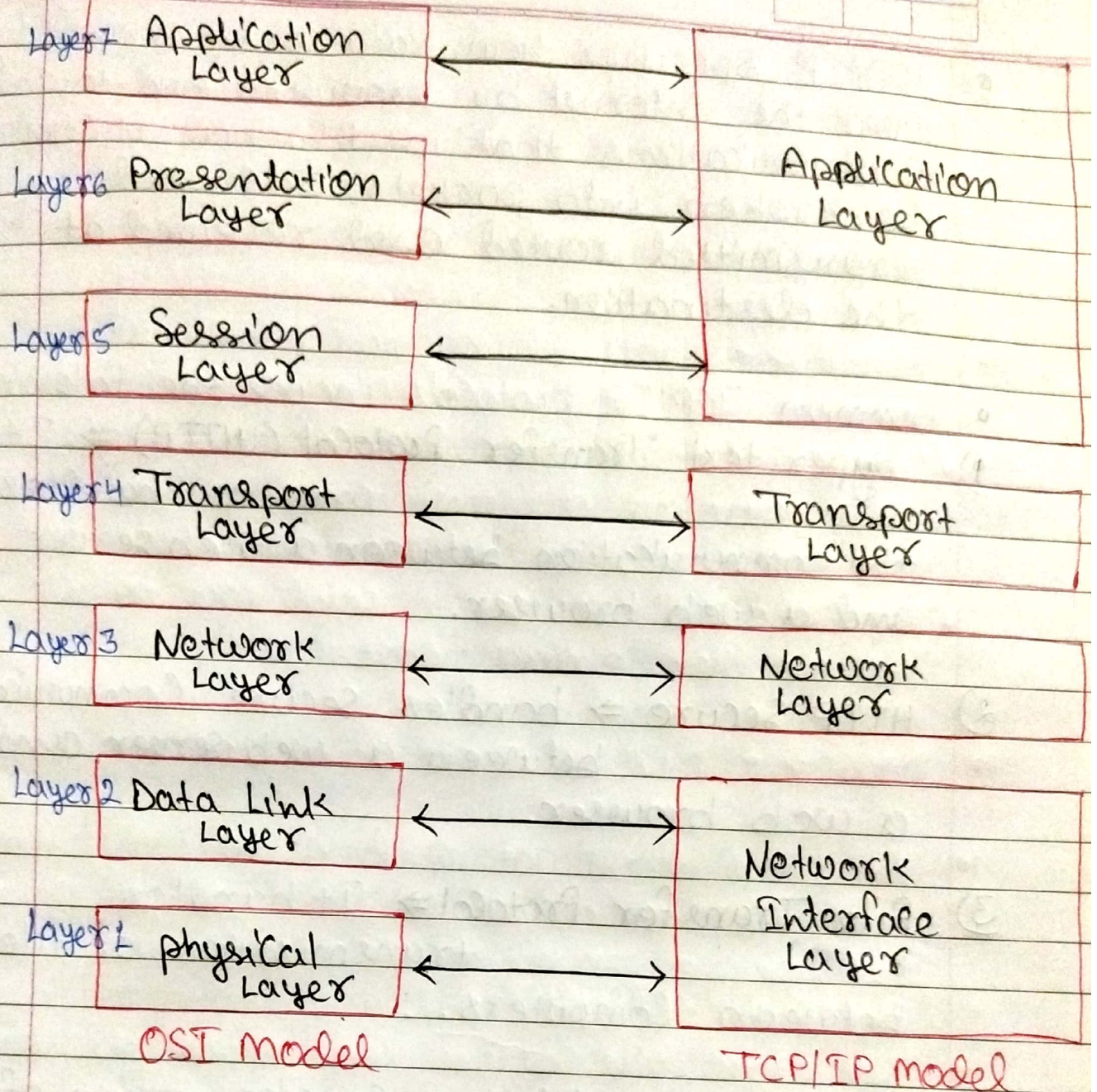
2) Mail services  $\Rightarrow$  An application Layer  
provides the facility for  
email forwarding and storage.

3) Directory Services  $\Rightarrow$  An application provides  
the distributed database  
sources and is used to provide that  
global information about various objects.



# TCP/IP Model

Page No: 66



- TCP/IP Stands for Transmission Control Protocol/ Internet Protocol and is a suite of Communication protocols used to interconnect network devices on the internet.
- TCP/IP is also used as a Communication protocol in a private Computer network (an internet and Extranet).



- TCP/IP Specifies how data is exchanged over the internet by providing end-to-end Communications that identify how it should be broken into packets, addressed, transmitted routed and received at the destination.
- Common TCP/IP protocols include the following:
  - 1) Hyper text Transfer Protocol (HTTP)  $\Rightarrow$  It handles the communication between a web server and a web browser.
  - 2) HTTP Secure  $\Rightarrow$  handles secure Communication between a web server and a web browser.
  - 3) File Transfer Protocol  $\Rightarrow$  It handles transmission of files between Computers.
- 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:
  - 1) Application Layer / process
  - 2) Transport Layer / Host-to-Host
  - 3) Internet Layer / Network Layer
  - 4) Network Interface / Link Layer



## 1) Application Layer $\Rightarrow$

- 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.
- Example of the application layer is an application such as file transfer, email, remote login etc.

## function and protocols of Application layer $\Rightarrow$

|              |      |      |        |     |      |
|--------------|------|------|--------|-----|------|
| Application  |      |      |        |     |      |
| Presentation | SMTP | FTP  | TELNET | DNS | SNMP |
| Session      |      | HTTP |        |     |      |

- **HTTP  $\Rightarrow$**  • This protocol allows us to access the data over the world wide web.
- It transfer the data in the form of plain text, audio, video.
- It is known as a hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.



- **SNMP** ⇒ • SNMP stands for Simple Network Management Protocol.
  - It is a framework used for managing the devices on the internet by using the TCP/IP protocol Suite.
- **SMTP** ⇒ • SMTP stands for Simple mail Transfer protocol.
  - The TCP/IP protocol that support the e-mail is known as a Simple mail transfer protocol.
  - This protocol is used to send the data to another e-mail address.
- **DNS** ⇒ • DNS stands for Domain Name System
  - 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.
- **TELNET** ⇒ • It stands for Terminal Network or teletype Network Protocol.
  - It establishes the Connection between the Local Computer and remote Computer in such a way that the local terminal appears to be a terminal at the remote System.

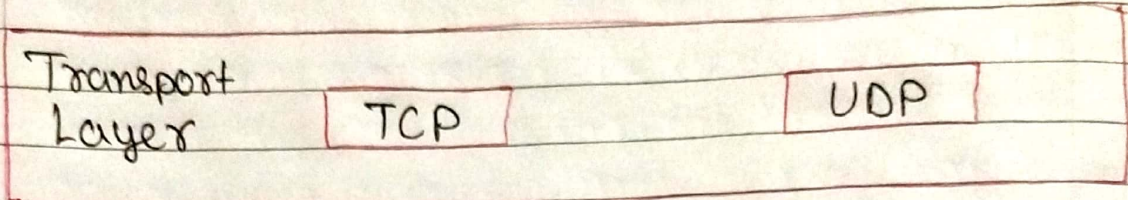


- **FTP** ⇒ • FTP stands for file transfer Protocol.
- FTP is a standard internet protocol used for transmitting the files from one Computer to another Computer.



## 2) Transport Layer $\Rightarrow$

- 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.

### # User Datagram Protocol (UDP) $\Rightarrow$

- It provides connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the error but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged. ICMP (Internet Control Message Protocol)

$\Rightarrow$  UDP consists of the following fields:

Source port address  $\Rightarrow$  The source port address is the address of the

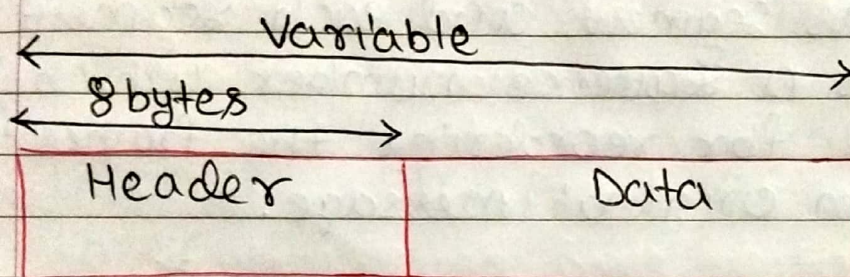


application program that has Created the message.

Destination port address  $\Rightarrow$  The destination port address is the address of the application program that receives the message.

Total Length  $\Rightarrow$  It defines the total no. of bytes of the user datagram in bytes.

Checksum  $\Rightarrow$  The Checksum is a 16-bit field used in error detection.



Header format

|                               |                                    |
|-------------------------------|------------------------------------|
| Source port<br>address 16 bit | Destination port<br>address 16 bit |
| Total length 16<br>bits       | Checksum<br>16 bits                |

## # Transmission Control Protocol (TCP) $\Rightarrow$

- 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.

- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, 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 segments, 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.



### 3) Internet Layer $\Rightarrow$

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

Internet  
Layer

ICMP

IGMP

IP

ARP

RARP

IP  $\Rightarrow$  Internet Protocol

ARP  $\Rightarrow$  Address Resolution Protocol

ICMP  $\Rightarrow$  Internet Control Message Protocol

IGMP  $\Rightarrow$  Internet Group Management Protocol

RARP  $\Rightarrow$  Reverse Address Resolution Protocol.

following are the protocols used in this layer are:  $\Rightarrow$

- 1) IP Protocol  $\Rightarrow$  IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.



Following are the responsibilities of this protocol:

- **IP addressing**  $\Rightarrow$  this protocol implements Logical host addresses known as IP address.
- **Host-to-host Communication**  $\Rightarrow$  It determines the path through which the data is to be transmitted.
- **Data Encapsulation and formatting**  $\Rightarrow$  An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely. It encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly**  $\Rightarrow$  the limit imposed on the size of the IP datagram by data link layer protocol is known as maximum Transmission Unit (MTU).  
If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network.
- **Routing**  $\Rightarrow$  When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly.



## 2) ARP Protocol $\Rightarrow$

- ARP stands for 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  $\Rightarrow$  When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
- ARP reply  $\Rightarrow$  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.

## 3) ICMP Protocol $\Rightarrow$

- ICMP stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.



- A datagram travels from router-to-router until it reaches its destination.
- An ICMP protocol mainly uses two terms:  
ICMP test  $\Rightarrow$  ICMP test is used to test whether the destination is reachable or not.  
ICMP Reply  $\Rightarrow$  ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the address of the source and destination but not of the router that it is passed to.



#### 4) Network Interface (Access) Layer $\Rightarrow$

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



## Difference between OSI and TCP/IP model

| OSI Model                                                                                                                                               | TCP/IP Model                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| 1) OSI stands for open System Interconnection                                                                                                           | 1) TCP/IP implies Transmission Control Protocol / Internet Protocol.                                                                     |
| 2) The OSI model was developed by ISO (International Standard Organization) in 1984.                                                                    | 2) The TCP/IP model was developed by ARPANET (Advanced Research Project Agency Network) in 1982.                                         |
| 3) It Consists of 7 Layers: Starting from the bottom they are the Physical, data link, Network, Transport, Session, Presentation and Application Layer. | 3) It Consists of 4 Layers: Starting from the bottom they are the Network Interface, Internet, Transport and Application Layer.          |
| 4) The OSI model follows a vertical approach.                                                                                                           | 4) The TCP/IP model follows a horizontal approach.                                                                                       |
| 5) In the OSI model, the transport layer provides a guarantee for the delivery of the packets.                                                          | 5) In TCP/IP transport Layer does not provide the surety for the delivery of packets. But Still, we can say that It is a reliable model. |



## OSI model

- 6) In the OSI model, the Physical Layer and data Link Layer are separate Layer.
- 7) In OSI model, the Session and presentation Layers are separated such as both the Layers are different.

## TCP/IP model

- 6) In TCP/IP, physical and data Link Layers are merged as a single network Layer.
- 7) In this model, the Session and presentation Layer are not different layers. Both Layers are included in the application Layer.



# Data link layer

The Data Link Layer is the second layer of the OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model. Its primary function is to ensure reliable and efficient communication between devices over a physical transmission medium, such as a cable or a wireless connection

## **Key functions and responsibilities of the data link layer include**

- Framing: Breaking data into frames for transmission and reassembling them at the receiving end.
- Physical Addressing: Assigning unique physical addresses (MAC addresses) to devices for identification.
- Error Detection and Correction: Implementing error detection mechanisms like CRC (Cyclic Redundancy Check) to ensure data integrity.
- Flow Control: Managing the flow of data between devices to prevent congestion and ensure smooth transmission.
- Media Access Control: Controlling access to the physical transmission medium to avoid data collisions

## **Common challenges and issues associated with the data link layer include**

**Collision:** In shared media networks, collisions can occur when multiple devices attempt to transmit data simultaneously, leading to data loss and network congestion.

**Error Handling:** While error detection mechanisms like CRC are in place, errors can still occur during data transmission, leading to corrupted frames and potential data loss.

**Addressing:** Managing and assigning MAC addresses efficiently can become complex, especially in large networks, leading to address conflicts and misconfigurations

**Security Concerns:** Without proper security measures, data transmitted at the data link layer can be unauthorized access.



# Framing

Framing in the data link layer refers to the process of breaking up the stream of data received from the network layer into manageable units called frames for transmission over the physical medium. These frames include not only the data itself but also control information necessary for the successful delivery of the data. Framing is crucial for ensuring that data can be reliably transmitted and received between devices on a network

## Here's an overview of the framing process

1. **Dividing Data into Frames:** The data link layer receives data from the network layer in the form of a continuous stream of bits. To transmit this data over the network, it must be divided into discrete units called frames. Frames typically consist of a header, data payload, and trailer.
2. **Adding Header:** The header of the frame contains essential control information, such as source and destination addresses, frame sequence numbers (for sequence control), and other protocol-specific information. This header provides the necessary details for proper routing and delivery of the frame.
3. **Adding Trailer:** The trailer of the frame typically contains error detection codes, such as CRC (Cyclic Redundancy Check), which are used to ensure data integrity during transmission. By adding error detection codes, the data link layer can detect and possibly correct errors that may occur during transmission.
4. **Transmitting Frames:** Once the frame is constructed, it is transmitted over the physical medium to the destination device. The physical layer is responsible for the actual transmission of the frame across the network medium.
5. **Receiving Frames:** At the receiving end, the frame is received from the physical medium. The data link layer then extracts the header and trailer from the received frame, verifies the integrity of the data using error detection codes, and delivers the data payload to the network layer for further processing.

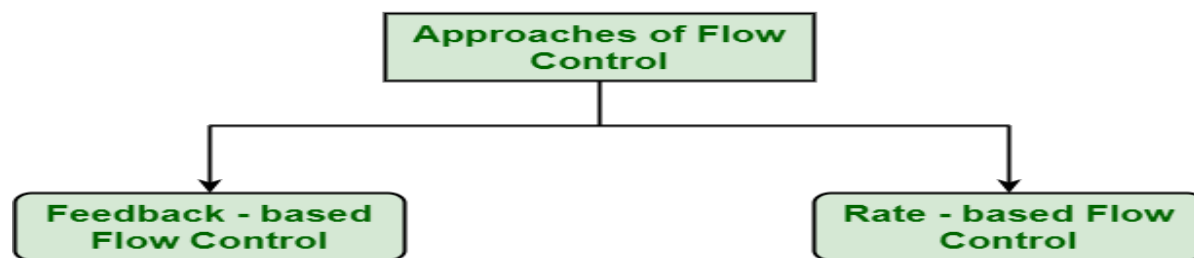


## **Flow Control issues at data link layer**

Flow control is [design issue at Data Link Layer](#). It is a technique that generally observes the proper flow of data from sender to receiver. It is very essential because it is possible for sender to transmit data or information at very fast rate and hence receiver can receive this information and process it.

This can happen only if receiver has very high load of traffic as compared to sender, or if receiver has power of processing less as compared to sender. Flow control is basically a technique that gives permission to two of stations that are working and processing at different speeds to just communicate with one another. Flow control in Data Link Layer simply restricts and coordinates number of frames or amount of data sender can send just before it waits for an acknowledgement from receiver

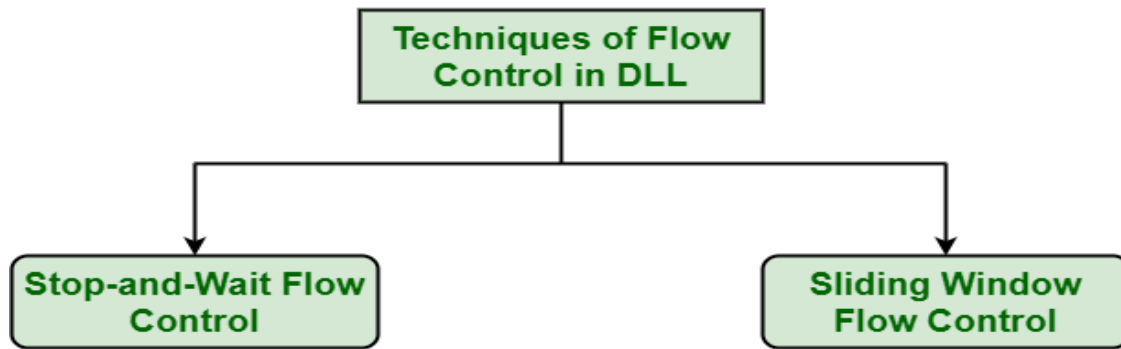
### **Flow control can be broadly classified into two categories**



- **Feedback based Flow Control** : In these protocols, the sender sends frames after it has received acknowledgments from the user. This is used in the data link layer.
- **Rate – based Flow Control** : In this control technique, usually when sender sends or transfer data at faster speed to receiver and receiver is not being able to receive data at the speed, then mechanism known as built-in mechanism in protocol will just limit or restricts overall rate at which data or information is being transferred or transmitted by sender without any feedback or acknowledgement from receiver.

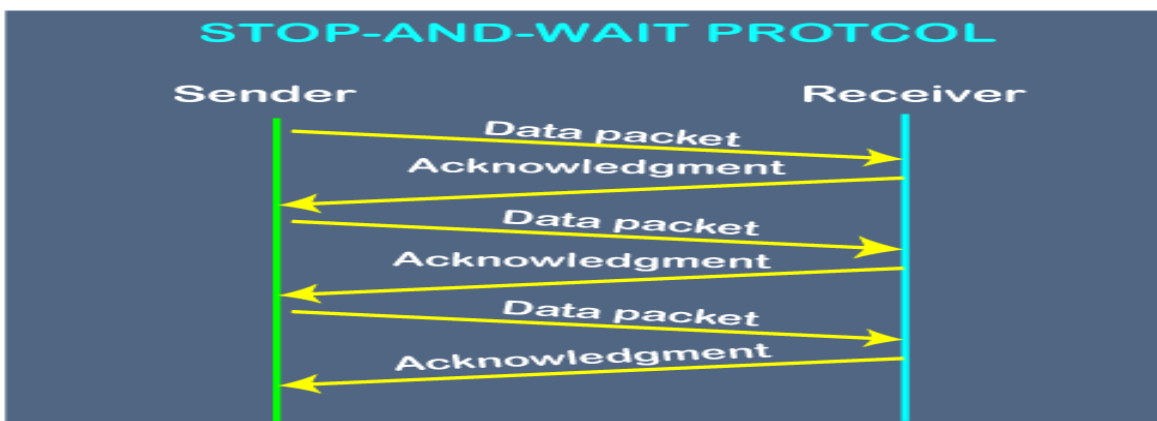
**Techniques of Flow Control in Data Link Layer** : There are basically two types of techniques being developed to control the flow of data





### Stop-and-Wait Flow Control:

- The sender sends a frame and waits for acknowledgment.
- Once the receiver receives the frame, it sends an acknowledgment frame back to the sender.
- On receiving the acknowledgment frame, the sender understands that the receiver is ready to accept the next frame. So it sends the next frame in queue
- When acknowledgment is received, then only sender will send or transfer the next frame. This process is continued until sender transmits EOT (End of Transmission) frame. In this method, only one of frames can be in transmission at a time



### Advantages –

- This method is very easiest and simple and each of the frames is checked and acknowledged well.
- This method is also very accurate

### Disadvantages –

- This method is very slow.
- In this, only one packet or frame can be sent at a time.
- It is very inefficient and makes the transmission process very slow



### **Sliding Window Flow Control:**

This protocol improves the efficiency of stop and wait protocol by allowing multiple frames to be transmitted before receiving an acknowledgment

- Both the sender and the receiver has finite sized buffers called windows. The sender and the receiver agrees upon the number of frames to be sent based upon the buffer size.

The sender sends multiple frames in a sequence, without waiting for acknowledgment. When its sending window is filled, it waits for acknowledgment. On receiving acknowledgment, it advances the window and transmits the next frames, according to the number of acknowledgments received

### **Advantages –**

- It performs much better than stop-and-wait flow control.
- This method increases efficiency.
- Multiples frames can be sent one after another.

### **Disadvantages –**

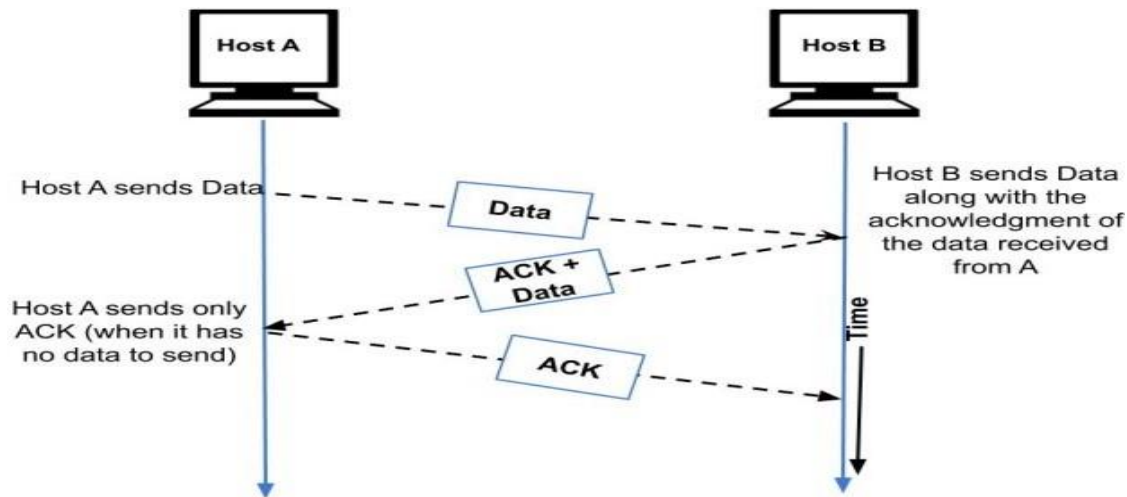
- The main issue is complexity at the sender and receiver due to the transferring of multiple frames.
- The receiver might receive data frames or packets out the sequence

## **Piggybacking and Sliding Window Protocol**

Piggybacking is a process of attaching the acknowledgment with the data packet to be sent

Suppose there is two-way communication between two devices A and B. When the data frame is sent by A to B, then device B will not send the acknowledgment to A until B does not have the next frame to transmit. And the delayed acknowledgment is sent by the B with the data frame. The method of attaching the delayed acknowledgment with sending the data frame is known as piggybacking.

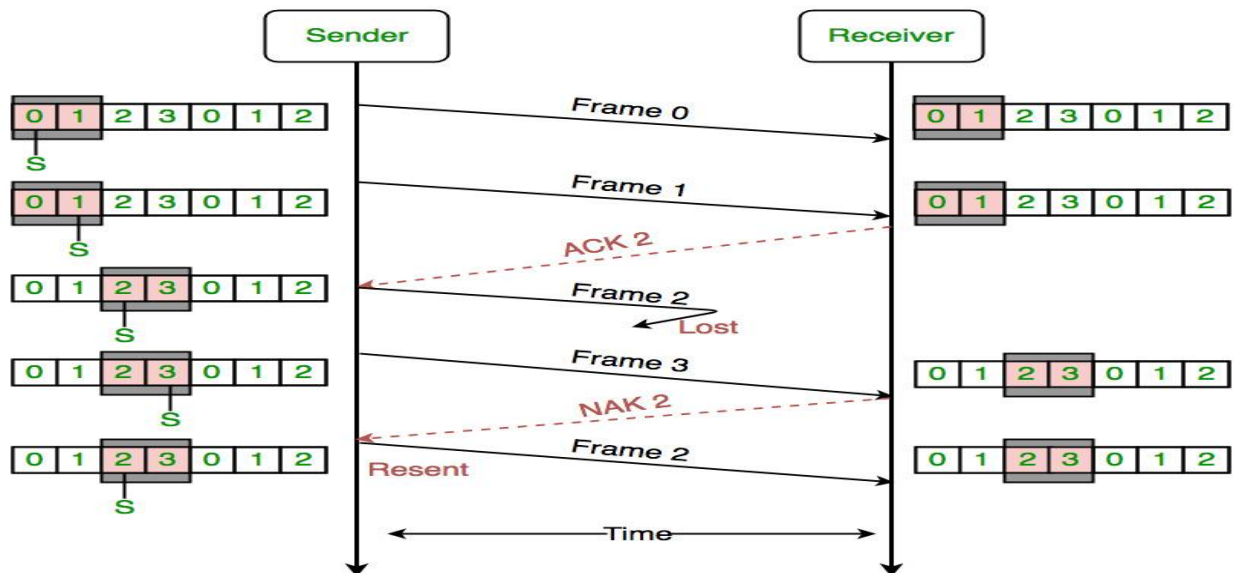




## Sliding Window Protocol

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in [TCP \(Transmission Control Protocol\)](#).

In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number

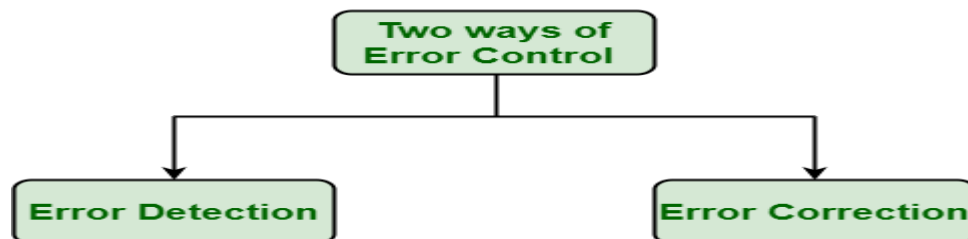




## Error Control issues at data link layer

Error control in data link layer is the process of detecting and correcting data frames that have been corrupted or lost during transmission

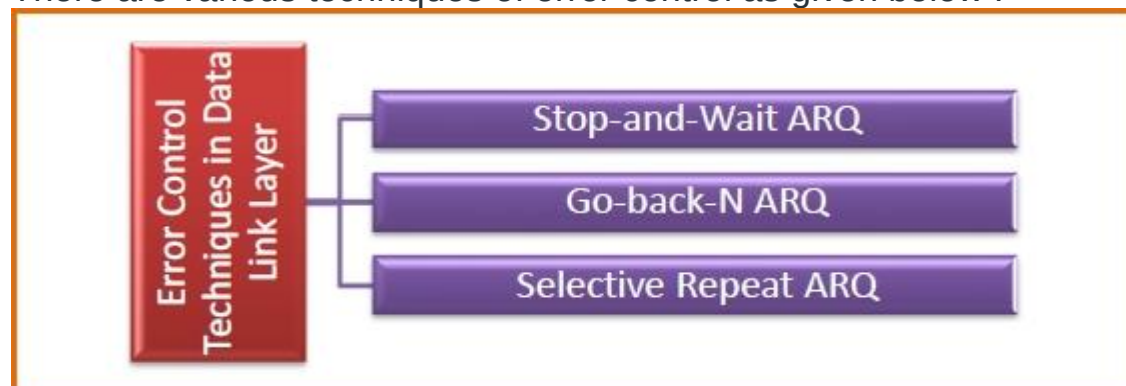
Error control is basically process in data link layer of detecting or identifying and re-transmitting data frames that might be lost or corrupted during transmission. In both of these cases, receiver or destination does not receive correct data frame and sender or source does not even know anything about any such loss regarding data frames.



**Error Detection** : Error detection, as the name suggests, simply means detection or identification of errors. These errors may occur due to noise or any other impairments during transmission from transmitter to the receiver

2. **Error Correction** : Error correction, as the name suggests, simply means correction or solving or fixing of errors. It simply means reconstruction and rehabilitation of original data that is error-free. But error correction method is very costly and very hard.

There are various techniques of error control as given below :





## **Stop and Wait ARQ**

This protocol involves the following transitions –

- A timeout counter is maintained by the sender, which is started when a frame is sent.
- If the sender receives acknowledgment of the sent frame within time, the sender is confirmed about successful delivery of the frame. It then transmits the next frame in queue.
- If the sender does not receive the acknowledgment within time, the sender assumes that either the frame or its acknowledgment is lost in transit. It then retransmits the frame.
- If the sender receives a negative acknowledgment, the sender retransmits the frame.

- **Go-Back-N ARQ**

The working principle of this protocol is –

- The sender has buffers called sending window.
- The sender sends multiple frames based upon the sending-window size, without receiving the acknowledgment of the previous ones.
- The receiver receives frames one by one. It keeps track of incoming frame's sequence number and sends the corresponding acknowledgment frames.
- After the sender has sent all the frames in window, it checks up to what sequence number it has received positive acknowledgment.
- If the sender has received positive acknowledgment for all the frames, it sends next set of frames.
- If sender receives NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

- **Selective Repeat ARQ**

- Both the sender and the receiver have buffers called sending window and receiving window respectively.
- The sender sends multiple frames based upon the sending-window size, without receiving the acknowledgment of the previous ones.
- The receiver also receives multiple frames within the receiving window size.
- The receiver keeps track of incoming frame's sequence numbers, buffers the frames in memory.
- It sends ACK for all successfully received frames and sends NACK for only frames which are missing or damaged.
- The sender in this case, sends only packet for which NACK is received.



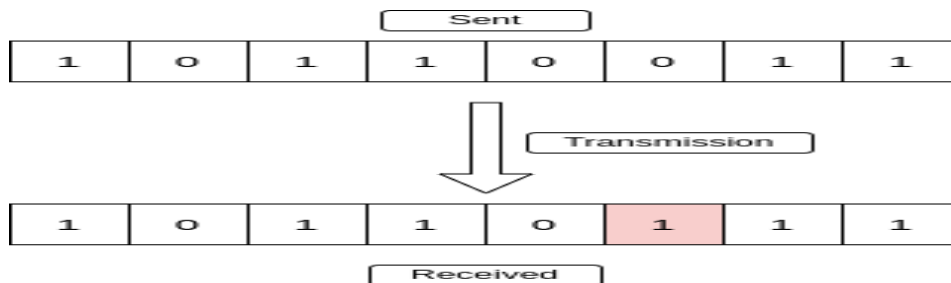
## Error Detection Method and Error Correction Method

**Error** is a condition when the receiver's information does not match the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits traveling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

### Types of Errors

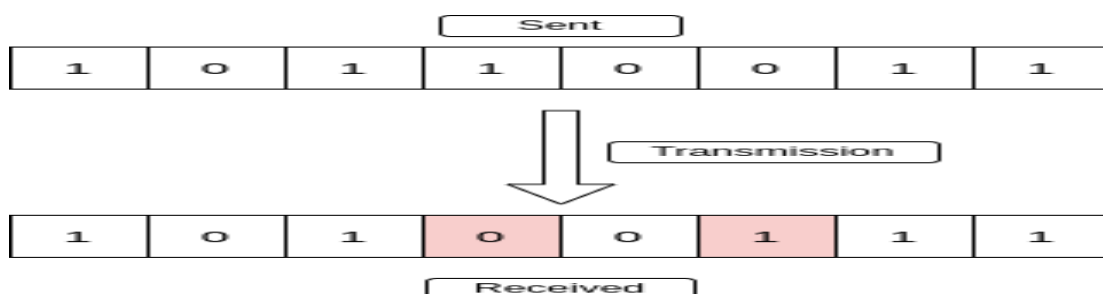
#### Single-Bit Error

A single-bit error refers to a type of data transmission error that occurs when one bit (i.e., a single binary digit) of a transmitted data unit is altered during transmission, resulting in an incorrect or corrupted data unit.



#### Multiple-Bit Error

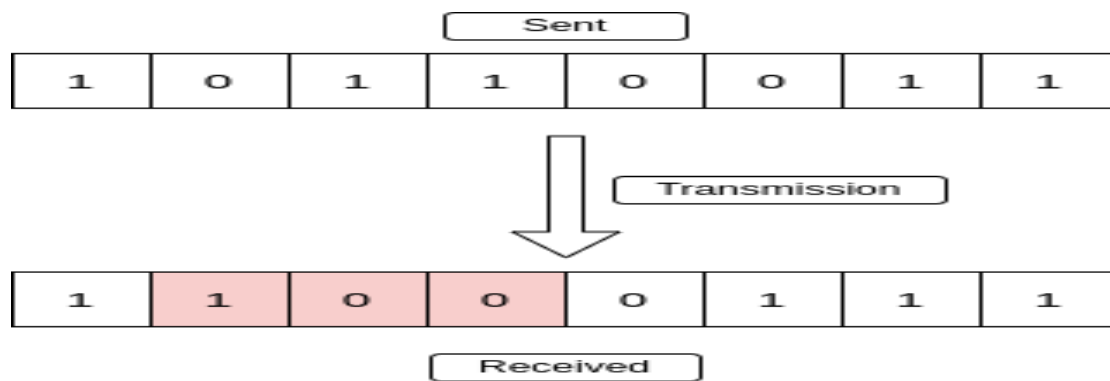
A multiple-bit error is an error type that arises when more than one bit in a data transmission is affected



#### Burst Error

When several consecutive bits are flipped mistakenly in digital transmission, it creates a burst error. This error causes a sequence of consecutive incorrect values.

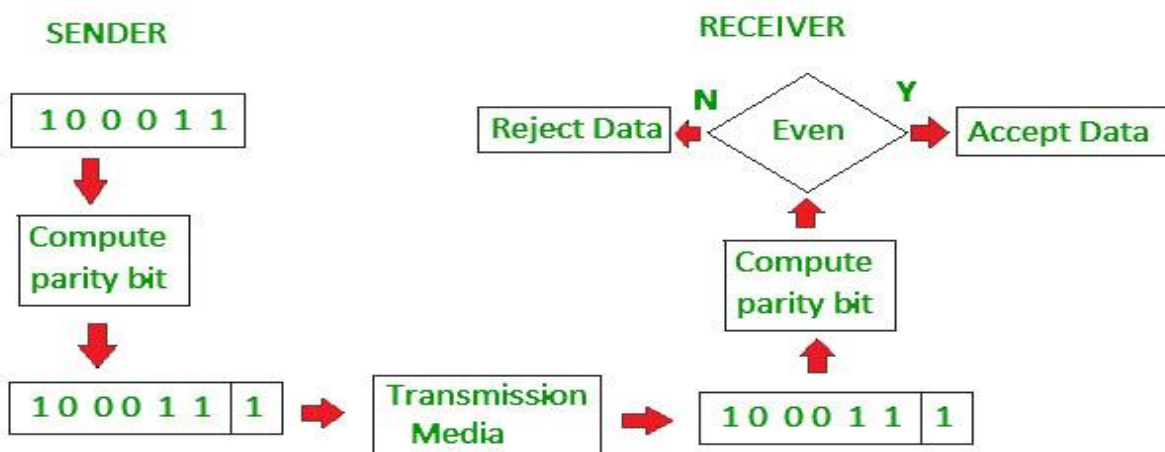




## Error Detection Methods

**Simple Parity Check:** Simple-bit parity is a simple error detection method that involves adding an extra bit to a data transmission. It works as:

- 1 is added to the block if it contains an odd number of 1's, and
- 0 is added if it contains an even number of 1's



## Two-dimensional Parity Check

Two-dimensional Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end, these are compared with the parity bits calculated on the received data.



### Original Data

|          |          |          |          |
|----------|----------|----------|----------|
| 10011001 | 11100010 | 00100100 | 10000100 |
|----------|----------|----------|----------|

### Row parities

|                 |   |
|-----------------|---|
| 1 0 0 1 1 0 0 1 | 0 |
| 1 1 1 0 0 0 1 0 | 0 |
| 0 0 1 0 0 1 0 0 | 0 |
| 1 0 0 0 0 1 0 0 | 0 |
| 1 1 0 1 1 0 1 1 | 0 |

### Column parities



|           |           |           |           |           |
|-----------|-----------|-----------|-----------|-----------|
| 100110010 | 111000100 | 001001000 | 100001000 | 110110110 |
|-----------|-----------|-----------|-----------|-----------|

### Data to be sent

## Checksum:

Checksum error detection is a method used to identify errors in transmitted data. The process involves dividing the data into equally sized segments and using a 1's complement to calculate the sum of these segments. The calculated sum is then sent along with the data to the receiver. At the receiver's end, the same process is repeated and if all zeroes are obtained in the sum, it means that the data is correct

### Original Data

|          |          |          |          |
|----------|----------|----------|----------|
| 10011001 | 11100010 | 00100100 | 10000100 |
|----------|----------|----------|----------|

k=4, m=8

### Sender

|           |           |
|-----------|-----------|
| 1         | 10011001  |
| 2         | 11100010  |
|           | 101111011 |
|           | 1         |
|           | 01111100  |
| 3         | 00100100  |
|           | 10100000  |
| 4         | 10000100  |
|           | 100100100 |
|           | 1         |
| Sum:      | 00100101  |
| Checksum: | 11011010  |

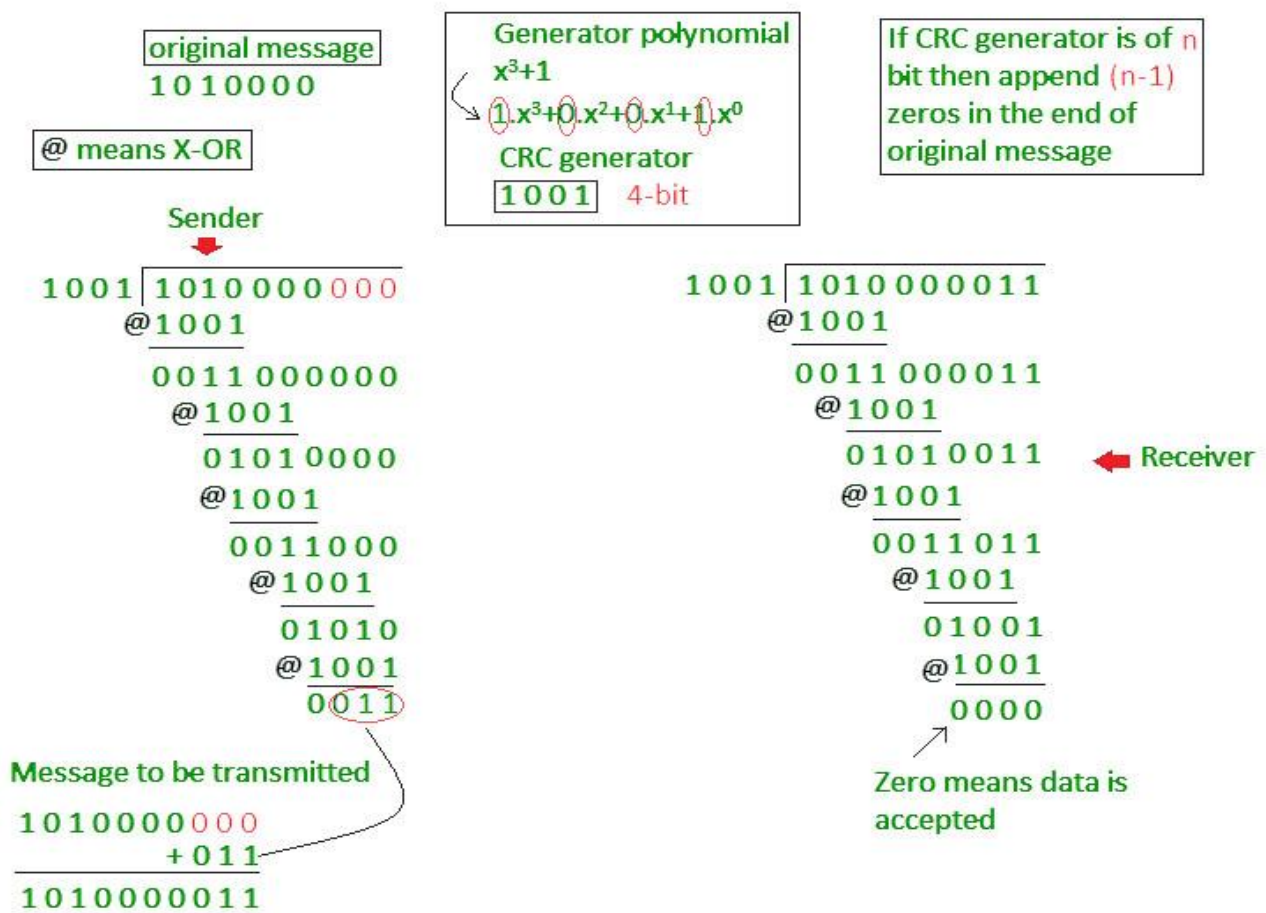
### Receiver

|             |             |
|-------------|-------------|
| 1           | 10011001    |
| 2           | 11100010    |
|             | 101111011   |
|             | 1           |
|             | 01111100    |
| 3           | 00100100    |
|             | 10100000    |
| 4           | 10000100    |
|             | 100100100   |
|             | 1           |
|             | 00100101    |
|             | 11011010    |
| Sum:        | 11111111    |
| Complement: | 00000000    |
| Conclusion: | Accept Data |



## Cyclic Redundancy Check (CRC)

- Unlike the checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of the data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.





## **Error Correction:**

In the digital world, error correction can be done in two ways

**Backward Error Correction:** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit

**Forward Error Correction:** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

**Hamming Code is also error correction method to used**

## **Data Link Layer Protocol: HDLC, PPP**

HDLC (High-Level Data Link Control):

HDLC is a bit-oriented synchronous data link layer protocol. It provides both connection-oriented and connectionless service options for data transmission over point-to-point and multipoint links. HDLC is widely used in various networking technologies, including synchronous serial communication links, ISDN (Integrated Services Digital Network), and frame relay

### **Features of HDLC**

- Error detection and correction: HDLC uses error detection and correction mechanisms such as CRCs and acknowledgments to ensure the integrity of the transmitted data.
- Full-duplex communication: HDLC supports full-duplex communication, which allows data to be transmitted in both directions simultaneously.
- Multiplexing: HDLC supports multiplexing, which enables multiple data streams to be transmitted over a single communication channel

## **PPP (Point to Point Protocol)**

PPP is a widely used data link layer protocol for establishing a direct connection between two nodes over a serial link.



- Authentication: PPP includes authentication mechanisms such as Password Authentication Protocol (PAP) and to ensure secure communication.
- Error detection and correction: PPP uses error detection and correction mechanisms such as CRCs and acknowledgments to ensure the integrity of the transmitted data.
- Network layer protocol independence: PPP is independent of the network layer protocol being used, making it compatible with various network protocols.
- Multilink support: PPP supports multilink connections, which allow multiple physical connections to be combined to increase the data transmission rate

note:formate of ppp and hdlc



## **Elearning.reb.rw website**

### **Definition of LAN Architecture:**

A Local Area Network (LAN) architecture is the overall design of a computers network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building. The LAN architecture consists of three levels: Physical, Media Access Control (MAC) and Logical Link Control (LLC).

- The LLC provides connection management, if needed.
- The Media Access Control (MAC) is a set of rules for accessing high speed physical links and for transferring data frames from one computer to another in a network.
- The Physical level deals mainly with actual transmission and reception of bits over the transmission medium

### **Definition of standard:**

Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers in guaranteeing national and international interoperability of data and telecommunications technology and processes. With Ethernet technologies, different types of standards have been so far used in networks.

The different Ethernet technologies used in wired networks to connect computers are given in the following table. The choice of one or another type depends on the size of networks and the quantity of data to exchange

### **IEEE Full Form**

IEEE stands for Institute of Electrical and Electronics Engineers. It is a professional association with a nonprofit organization with its headquarter in New York in the United States of America



| IEEE Standard | Description                                                                             |
|---------------|-----------------------------------------------------------------------------------------|
| IEEE 802      | For LAN/MAN networks                                                                    |
| IEEE 802.1    | Standards for LAN/MAN management and bridging and remote media access control bridging. |
| IEEE 802.2    | For Logical Link Control connectivity.                                                  |
| IEEE 802.3    | Standards for <a href="#">CSMA/CD</a> .                                                 |
| IEEE 802.4    | Standards for the token passing bus access                                              |
| IEEE 802.11   | For WiFi or Wireless Networking                                                         |

| Name                        | IEEE Standard | Data Rate | Media Type                               | Maximum Distance                                | Advantages                                                     |
|-----------------------------|---------------|-----------|------------------------------------------|-------------------------------------------------|----------------------------------------------------------------|
| Ethernet                    | 802.3         | 10 Mbps   | 10Base-T                                 | 100 meters                                      | Low cost components<br>Easy to install<br>Easy to troubleshoot |
| Fast Ethernet/<br>100Base-T | 802.3u        | 100 Mbps  | 100Base-TX<br>100Base-FX                 | 100 meters<br>2000 meters                       | It is the most popular and cheapest Ethernet                   |
| Gigabit Ethernet/<br>GigE   | 802.3z        | 1000 Mbps | 1000Base-T<br>1000Base-SX<br>1000Base-LX | 100 meters<br>275/550 meters<br>550/5000 meters | Gigabit Ethernet is ten times faster than Fast Ethernet        |

As your Choise (thing)

## 10BASE-F

10BASE-F is a generic term for the family of 10 Mbit/s Ethernet standards using fiber optic cable. In 10BASE-F, the 10 represents its maximum throughput of 10 Mbit/s, BASE indicates its use of base band transmission, and F indicates that it



relies on medium of fiber-optic cable. In fact, there are at least three different kinds of 10BASE-F. All require two strands of 62.5/125 µm multimode fiber. One strand is used for data transmission and one strand is used for reception, making 10BASE-F a full-duplex technology.

The 10BASE-F variants include **10BASE-FL**, **10BASE-FB** and **10BASE-FP**. Of these only **10BASE-FL** experienced widespread use. All 10BASE-F variants deliver 10 Mbit/s over a fiber pair. These 10 Mbit/s standards have been largely replaced by faster Fast Ethernet, Gigabit Ethernet and 100 Gigabit Ethernet standards

### Media access control, MAC address

**MAC Addresses** are unique **48-bit** hardware numbers of a computer that are embedded into a network card (known as a [Network Interface Card](#)) during manufacturing. The MAC Address is also known as the [Physical Address](#) of a network device. In the IEEE 802 standard,

Mac address is unique and permanent address for all electronics and networking device

### MAC ADDRESS FORMATE

1. MM:MM:MM:SS:SS:SS:
2. MM-MM-MM-SS-SS-SS
3. MMM.MMM.SSS.SSS

Example:3C:D9:2B:6F:2B:9C

The First 6 digits (say 3C:D9:2B) of the MAC Address identify the manufacturer, called the OUI (**Organizational Unique Identifier**)

The rightmost six digits represent **Network Interface CARD**, which is assigned by the manufacturer.

TYPES MAC(unicast,multicast,broadcast)

### **ALOHA Protocol in computer network**

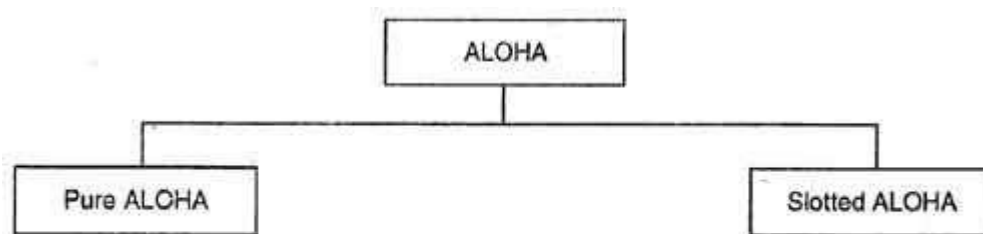
**ALOHA** is a multiple access protocol for transmission of data via a shared network channel. It operates in the medium access control sublayer (MAC sublayer) of the [open systems interconnection](#) (OSI) model. Using this



protocol, several data streams originating from multiple nodes are transferred through a multi-point transmission channel

**Note:** In **ALOHA**, each node or station transmits a frame without trying to detect whether the transmission channel is idle or busy. If the channel is idle, then the frames will be successfully transmitted. If two frames attempt to occupy the channel simultaneously, collision of frames will occur and the frames will be discarded. These stations may choose to retransmit the corrupted frames repeatedly until successful transmission occurs

### Versions of ALOHA Protocols



Types of ALOHA

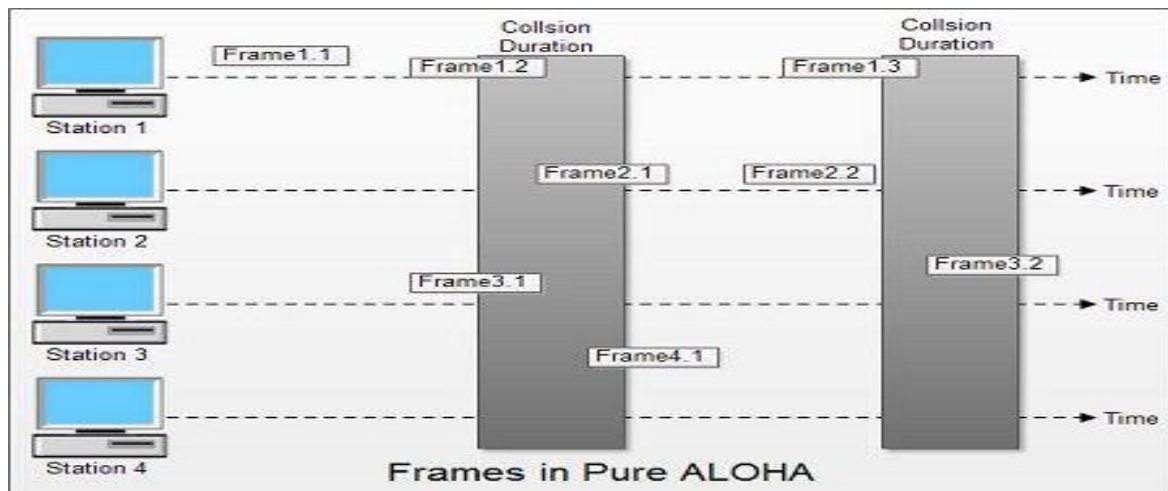
### Pure ALOHA

In pure ALOHA, the time of transmission is continuous. Whenever a station has an available frame, it sends the frame. If there is collision and the frame is destroyed, the sender waits for a random amount of time before retransmitting it.

- In pure ALOHA, the stations transmit frames whenever they have data to send.
- When two or more stations transmit simultaneously, there is collision and the frames are destroyed.
- In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
- If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.
- If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.
- Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before re-sending its frame. This randomness will help avoid more collisions.



- Figure shows an example of frame collisions in pure ALOHA



**Note:** In fig there are four stations that contend with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed

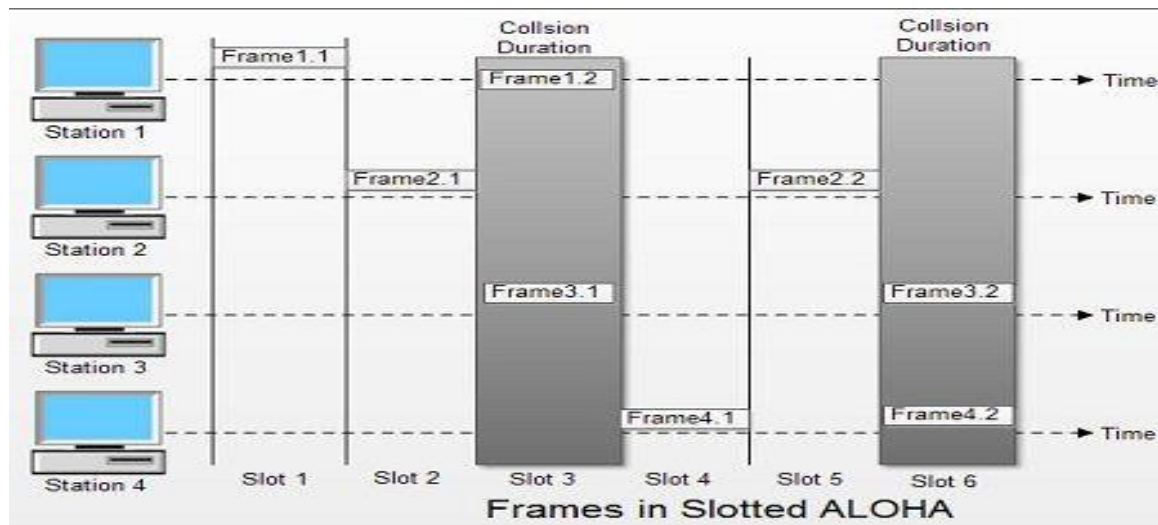
Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged.

## **Slotted ALOHA**

Slotted ALOHA reduces the number of collisions and doubles the capacity of pure ALOHA. The shared channel is divided into a number of discrete time intervals called slots. A station can transmit only at the beginning of each slot. However, there can still be collisions if more than one station tries to transmit at the beginning of the same time slot

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot





- In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.* it misses the time slot then the station has to wait until the beginning of the next time slot.
- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.
- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

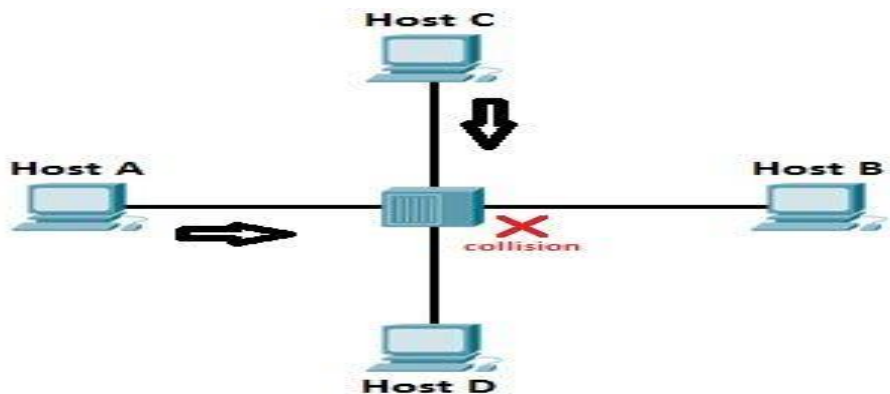
## Ethernet:

Ethernet is a family of computer networking technologies commonly used in local area networks, metropolitan area networks and wide area networks. Ethernet cable is one of the most popular forms of network cable used in wired networks. They connect devices together within a local area network like PCs, routers and switches. A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps). Ethernet uses CSMA/CD (Carrier Sense multiple Access with Collision Detection)



## Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

In a LAN, computers transmit data to each other. Normally, there is order to follow so that two computers can not send data at the same time while they are using the same route. When it happens that two computers send messages at the same time, there is what we call data collision. Therefore, a data collision occurs when two or more computers send data at the same time. When this happens, each computer stops data transmission and waits to resend it when the cable is free. Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a set of rules determining how network devices respond to a collision



In the topology above we have a hub network. Host A is trying to communicate with host B. Host A “senses” the wire and decides to send packets. But, in the same time, host C sends its packets to host D and the collision occurs. The sending devices (host A and host C) detect the collision and resend the packet after a random period of time.

## Algorithms

The algorithm of CSMA/CD is:

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits until the channel becomes idle.
- If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
- If a collision is detected, the station starts the collision resolution algorithm.
- The station resets the retransmission counters and completes frame transmission.



## Fiber Distributed Data Interface (FDDI)

The Fiber Distributed Data Interface (FDDI) is a standard developed by the American National Standards Institute (ANSI) for transmitting data on optical fiber cables. FDDI supports transmission rates of 100 megabits per second on token-passing networks.

FDDI provides high-speed network backbones that can be used to connect and extend LANs.

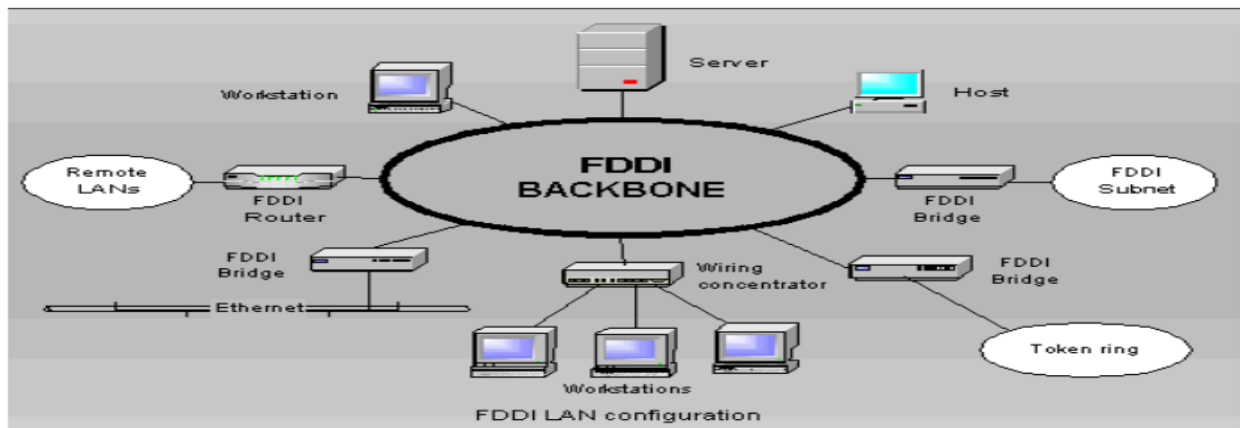


Figure 2. 3: Fiber Distributed Data Interface LAN configuration

Source: <http://aquaticws.com/fddi-network-47/>

## Features

- FDDI uses optical fiber as its physical medium.
- It operates in the physical and medium access control (MAC layer) of the Open Systems Interconnection (OSI) network model.
- It provides high data rate of 100 Mbps and can support thousands of users.
- It is used in LANs up to 200 kilometers for long distance voice and multimedia communication.
- FDDI technology can also be used as a backbone for a wide area network (WAN).

## Advantages of FDDI

The Fiber Distributed Data Interface allows the transmission of very large volumes of data over large distances. It provides high bandwidth.

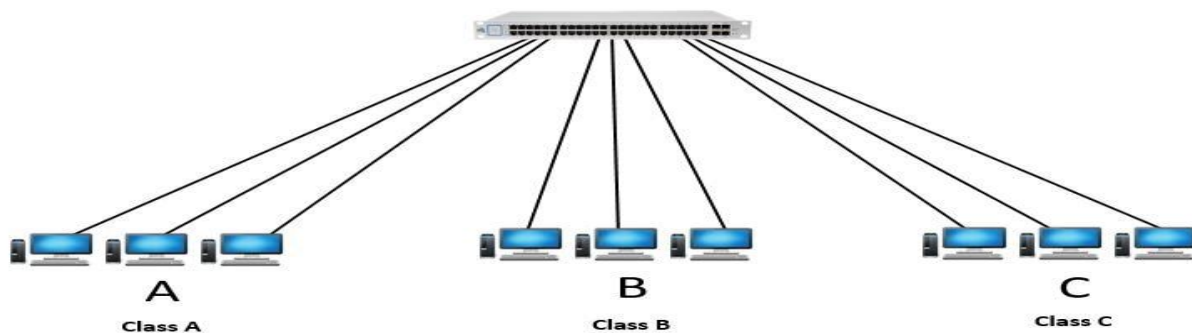
## Disadvantages



The Fiber Distributed Data Interface (FDDI) is an expensive technology to set up because the network devices require a special network card and also the required fiber optic cabling is expensive than twisted-pair cable. more cabling is required

## VLAN

VLAN stands for virtual local area network and refers to the logical connection of computers, servers, and other network devices into a [local area network](#) (LAN) despite their physical location. A VLAN groups these devices together into separate virtual networks, even if they're scattered in different places. Establishing VLANs helps businesses and organizations manage network resources, ensuring privacy, smooth traffic, and simplifying network communication.



## Types of VLAN

### **Port-based VLAN:**

In a port-based VLAN setup, individual switch ports are assigned to a specific VLAN. So, when a device connects to a port,

### **Protocol-based VLAN:**

Another type is a protocol-based VLAN. It assigns VLANs based on the protocol type of incoming frames, such as IP address



## MAC-based VLAN

MAC-based VLANs distribute network devices into different broadcast domains based on their [MAC addresses](#)

## Advantages of a VLAN

- Improved network performance and traffic management
- Enhanced security
- Better resource management
- Cost reduction
- **Flexibility**

## Disadvantages of a VLAN

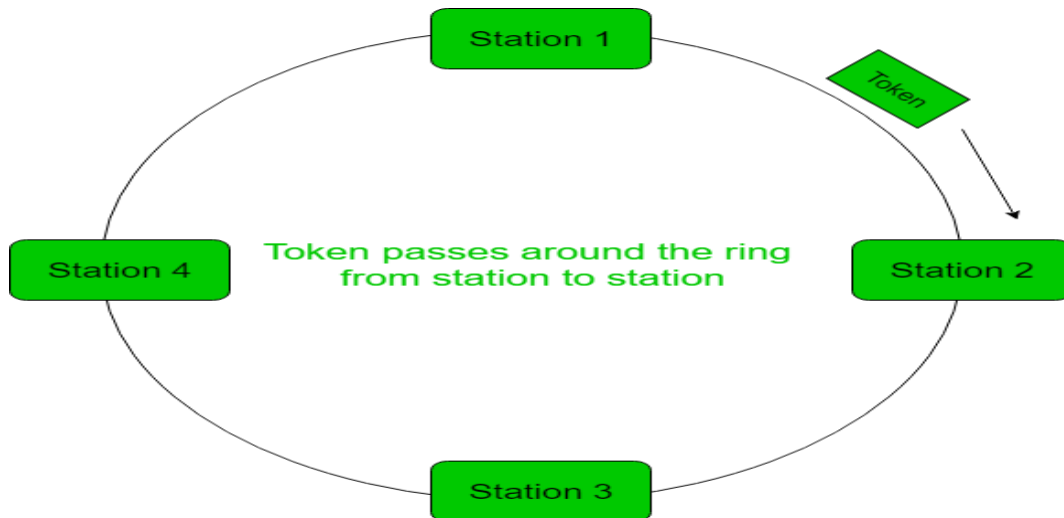
- Complex configuration
- Risk of misconfiguration

## Token Ring

Token ring (IEEE 802.5) is a communication protocol in a local area network (LAN)

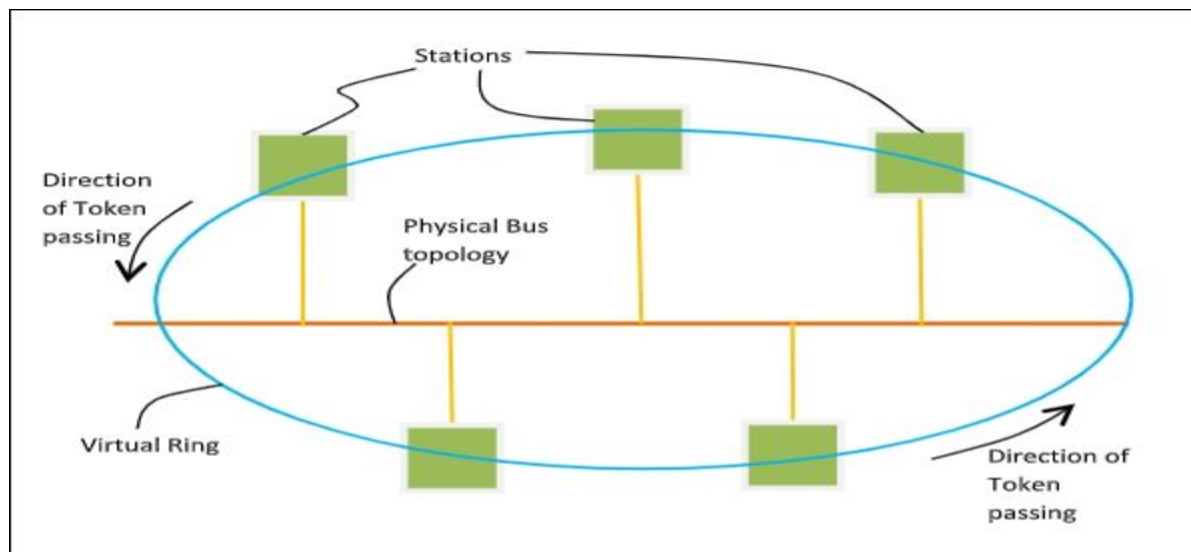
**Token Ring** protocol is a communication protocol used in Local Area Network (LAN). In a token ring protocol, the topology of the network is used to define the order in which stations send. The stations are connected to one another in a single ring. It uses a special three-byte frame called a "**token**" that travels around a ring. It makes use of [Token Passing](#) controlled access mechanism. Frames are also transmitted in the direction of the token. This way they will circulate around the ring and reach the station which is the destination.





## Token Bus

Token Bus (IEEE 802.4) is a standard for implementing token ring over virtual ring in LANs. The physical media has a bus or a tree topology and uses coaxial cables. A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring. Each node knows the address of its preceding station and its succeeding station. A station can only transmit data when it has the token. The working principle of token bus is similar to Token Ring.

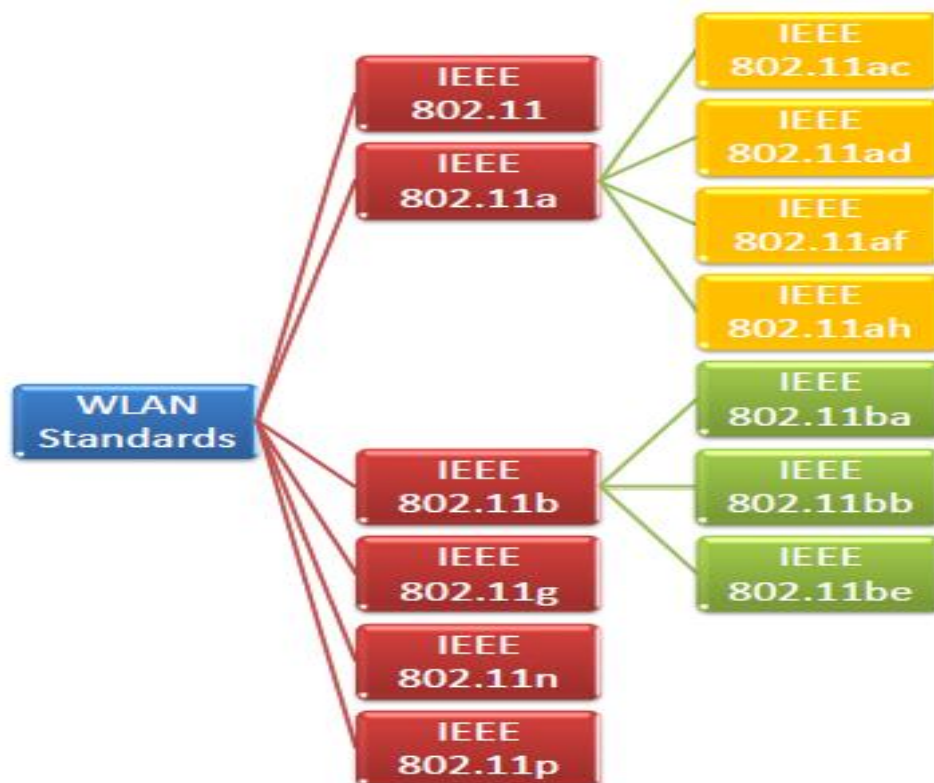




## **802.11(wireless LAN)**

IEEE 802.11 standard, popularly known as **WiFi**, lays down the architecture and specifications of wireless **LANs** (**WLANs**). WiFi or WLAN uses high frequency radio waves for connecting the nodes.

There are several standards of IEEE 802.11 WLANs. The prominent among them are 802.11, 802.11a, 802.11b, 802.11g, 802.11n and 802.11p. All the standards use carrier-sense multiple access with collision avoidance (CSMA/CA). Also, they have support for both centralised base station based as well as ad hoc networks



### **IEEE 802.11**

IEEE 802.11 was the original version released in 1997. It provided 1 Mbps or 2 Mbps data rate in the 2.4 GHz band and used either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS). It is obsolete now.

### **IEEE 802.11a**

802.11a was published in 1999 as a modification to 802.11



- **IEEE 802.11ac, or Wi-Fi 5**, was introduced in 2013 to support data rates at up to 3.5 Gbit/s, with still-greater bandwidth, additional channels, better modulation, and other features. It was the first Wi-Fi standard to enable the use of multiple input/multiple output (MIMO) technology so that multiple antennas could be used on both sending and receiving devices to reduce errors and boost speed.



# Network Layer

The network layer is the third layer of the OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model. Its primary function is to facilitate communication between different networks by providing routing, addressing, and forwarding of data packets

Here are some of the key functions of the network layer:

**Host-to-host Delivery of Data:** The network layer ensures that the packet is being delivered successfully from the sender to the receiver. This layer makes sure that the packet reaches the intended recipient only.

**Logical Addressing:** Every device connected to a network is assigned a unique logical address (like IP addresses in TCP/IP networks). The network layer ensures that packets are correctly routed based on these addresses.

**Routing:** The network layer determines the best path for data packets to travel from the source to the destination across multiple networks. It uses routing algorithms to make these decisions, considering factors like network congestion, shortest path, and reliability

**Packet Forwarding:** Once the route is determined, the network layer is responsible for forwarding data packets from one network to another until they reach their destination

**Fragmentation and Reassembly:** The network layer may fragment large packets into smaller

**Error Handling:** The network layer may also handle error detection and correction mechanisms to ensure the reliability of data transmission across networks.

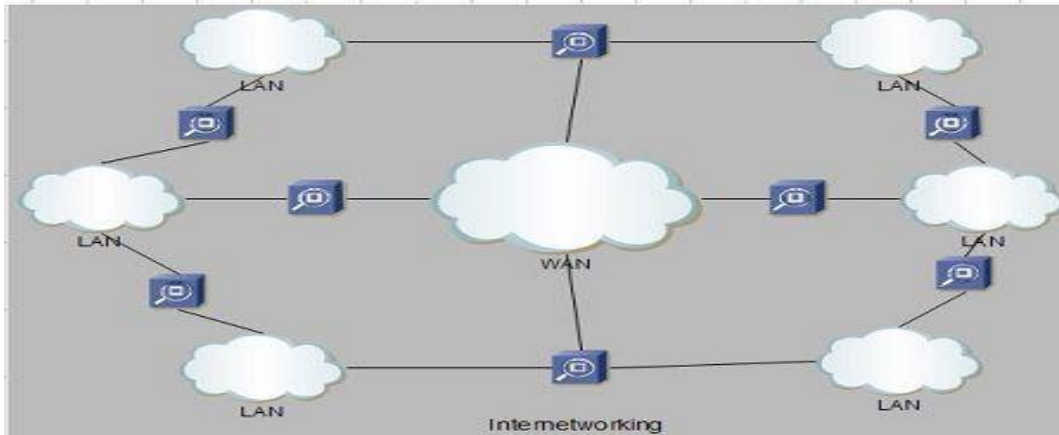
## Internetworking

Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices

Internetworking ensures data communication among networks owned and operated by different entities using a common data communication and the Internet Routing Protocol. The Internet is the largest pool of networks geographically located throughout the world but these networks are interconnected using the same protocol stack, TCP/IP. Internetworking is only possible when the all the connected networks use the same protocol stack or communication methodologies.

Internetworking provides worldwide connectivity, allowing users and devices to communicate and exchange resources from all over the world.





## **Circuit switching and packet switching**

### **Circuit Switching:**

**Circuit Switching** is a connection-oriented service. It provides a dedicated path from the sender to the receiver. In-circuit switching, a connection setup is required to send and receive data. It has very little chance of data loss and error due to the dedicated circuit, but a lot of bandwidth is wasted because the same path cannot be used by other senders during a congestion. Circuit switching is completely transparent

### **Advantages of Circuit Switching**

- It uses a fixed bandwidth.
- A dedicated communication channel increases the quality of communication.
- Data is transmitted with a fixed data rate.
- No waiting time at switches.
- Suitable for long continuous communication

### **Disadvantages of circuit switching**

- A dedicated connection makes it impossible to transmit other data even if the channel is free.
- Resources are not utilized fully.
- The time required to establish the physical link between the two stations is too long.
- A dedicated path has to be established for each connection.
- Circuit switching is more expensive

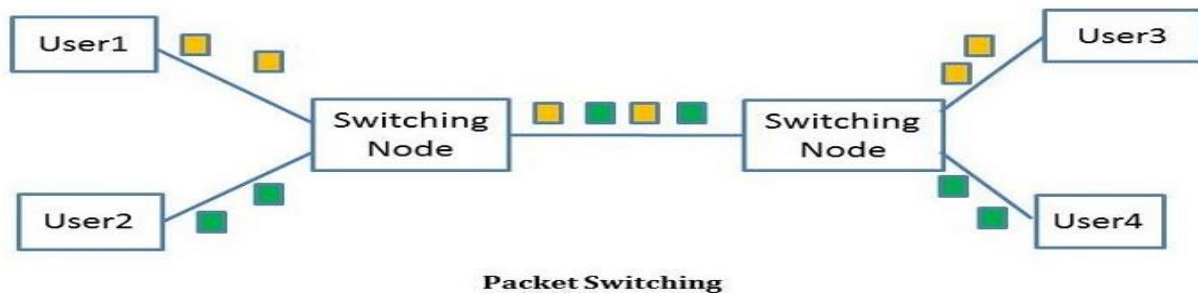
### **Packet Switching:**

**Packet Switching** in computer networks is a method of transferring data to a network in the form of packets. In order to transfer the file fast and efficiently manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet**



Packet switching is a connectionless network switching technique. Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination. There is no need to establish a dedicated circuit for communication.

It has more chance of data loss and error; the packets may arrive in the wrong order.



## **Advantages of Packet switching**

- It reduces access delay.
- Costs are minimized to great extent. Hence packet switching is a very cost-effective technique.
- Packets are rerouted in case of any problems. This ensures reliable communication.
- It is more efficient for data transmission because no need to establish the path.
- Several users can share the same channel simultaneously. Therefore packet switching makes use of available bandwidth efficiently

## **Disadvantages of Packet switching**

- Protocols used in the packet switching are complex.
- If the network becomes overloaded, packets are delayed or discarded, or dropped. This leads to the retransmission of lost packets by the sender.
- It is not secured if security protocols are not used during packet transmission

## **Difference between circuit switching and packet switching**



### **Circuit Switching**

Circuit switching requires a dedicated path before sending data from source to destination.

It reserves the entire bandwidth in advance.

No store and forward transmission

Each packet follows the same route

Bandwidth wastage

The circuit switching network is implemented at the physical layer.

### **Packet Switching**

Packet switching does not require any dedicated path to send data from source to destination.

It does not reserve bandwidth in advance

It supports store and forward transmission

A packet can follow any route

No bandwidth wastage

Packet switching is implemented at the datalink layer and network layer

### **Addressing issues at network layer**

Addressing at the network layer involves assigning unique identifiers to devices within a network so that data packets can be properly routed to their destinations. Here are some common addressing issues at the network layer:

**IP Address Exhaustion:** The most significant addressing issue at the network layer is IPv4 address exhaustion

**Address Conflicts:** Address conflicts occur when two or more devices within the same network are assigned the same IP address. Address conflicts can disrupt network communication and lead to connectivity issues

**Dynamic Host Configuration Protocol (DHCP) Issues:** DHCP is a network protocol used to dynamically assign IP addresses to devices on a network. DHCP issues can arise if the DHCP server is misconfigured, unavailable



## IP address, Different classes, Private and Public address

### IP ADDRESS:

An [IP address](#), or Internet Protocol address, is a unique number assigned to every device (PC, mobile phone, router, etc.) on a computer network and used to communicate with each other and the internet.

IP Addresss stands for internet protocol address .An IP address is a unique number provide to each an every device

It is in the form of integric number which is separated by dot(.)

Example:192.168.10.50

### There are two main versions of the Internet Protocol:

**IPv4 (Internet Protocol version 4):** This is the older version of the protocol and is still widely used today. IPv4 addresses are 32 bits long, typically represented in decimal format, such as 192.168.1.1. However, due to the increasing number of devices connecting to the Internet, IPv4 addresses are becoming scarce

**IPv6 (Internet Protocol version 6):** IPv6 was developed to address the exhaustion of IPv4 addresses by using a larger address space. IPv6 addresses are 128 bits long, allowing for a significantly larger number of unique addresses. IPv6 addresses are typically represented in hexadecimal format, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334

IP Address :

#### IPV<sub>4</sub>

Length 32 bits

Octet 4

Range 0 to 255

4 billion ( $2^{32}$ )

192.168.10.50

#### IPV<sub>6</sub>

length 128 bits

octet 8

range 0 to FFFF(65535)

340trillion ( $2^{128}$ )

3FBB:1806:4545:2:100:L8FF:FE21:4748



## Different classes

IP addresses are divided into classes to allocate address space efficiently and to support networks of different sizes. The classes of IP addresses are based on the leading bits of the IP address and are categorized into five classes: A, B, C, D, and E. Here's a brief overview of each class:

1. **Class A:** The first bit of a Class A address is always set to 0. Class A addresses are designed for large networks with a vast number of hosts. The range of Class A addresses goes from 1.0.0.0 to 126.0.0.0. However, the address range 127.x.x.x is reserved for loopback and diagnostic functions.
2. **Class B:** The first two bits of a Class B address are always set to 10. Class B addresses are suitable for medium-sized networks. The range of Class B addresses goes from 128.0.0.0 to 191.255.0.0.
3. **Class C:** The first three bits of a Class C address are always set to 110. Class C addresses are intended for small networks. The range of Class C addresses goes from 192.0.0.0 to 223.255.255.0.
4. **Class D:** Class D addresses are used for multicast groups. The first four bits of a Class D address are always set to 1110. The range of Class D addresses goes from 224.0.0.0 to 239.255.255.255.
5. **Class E:** Class E addresses are reserved for experimental purposes and are not used in general practice. The first four bits of a Class E address are always set to 1111. The range of Class E addresses goes from 240.0.0.0 to 255.255.255.255.

## **Class of IP :**

Class A → 0 to 127 (125.255.22.15)

Local host used to:127.0.0.1

Class B → 128 to 191 (191.22.25.150)

Class C → 192 to 223 (192.205.10.20)

Class D → 224 to 239 (use for multicasting)

Class E → 240 to 255 (used for research)



## **Private and Public address**

**Private IP addresses** are used within a private network, such as a home or business network, and are not directly accessible from the Internet. They are reserved for internal use and can be reused in multiple private networks without conflict. Commonly used private IP address ranges include:

- Class A: 10.0.0.0 to 10.255.255.255
- Class B: 172.16.0.0 to 172.31.255.255
- Class C: 192.168.0.0 to 192.168.255.255

**Public IP addresses**, on the other hand, are assigned by ISPs (Internet Service Providers) or other Internet authorities and are routable on the Internet. They are globally unique and are used to identify devices on the Internet. Public IP addresses can be static (unchanging) or dynamic (changing periodically).

### **NOTE:**

**1. Public IP Address:** This address is available publicly and it is assigned by your network provider to your router, which further divides it to your devices. Public IP Addresses are of two types,

**Dynamic IP Address:** When you connect a smartphone or computer to the internet, your Internet Service Provider provides you an IP Address from the range of available IP Addresses. Now, your device has an IP Address and you can simply connect your device to the Internet and send and receive data to and from your device. The very next time when you try to connect to the internet with the same device, your provider provides you with different IP Addresses to the same device and also from the same available range. Since IP Address keeps on changing every time when you connect to the internet, it is called a Dynamic IP Address

- **Static IP Address:** Static address never changes. They serve as a permanent internet address. These are used by DNS servers. What are DNS servers? Actually, these are computers that help you to open a



- website on your computer. Static IP Address provides information such as device is located on which continent, which country, which city, and which
- Internet Service Provider provides internet connection to that particular device. Once, we know who is the ISP, we can trace the location of the device connected to the internet. Static IP Addresses provide less security than Dynamic IP Addresses because they are easier to track.

## **Subnet mask**

A subnet mask is a 32-bit number used in conjunction with an IP address to identify the network portion and the host portion of the address. It essentially tells devices on a network which part of an IP address is the network identifier and which part is the host identifier

Subnet masks consist of a series of contiguous 1 bits followed by a series of contiguous 0 bits. The 1 bits represent the network portion of the IP address, and the 0 bits represent the host portion.

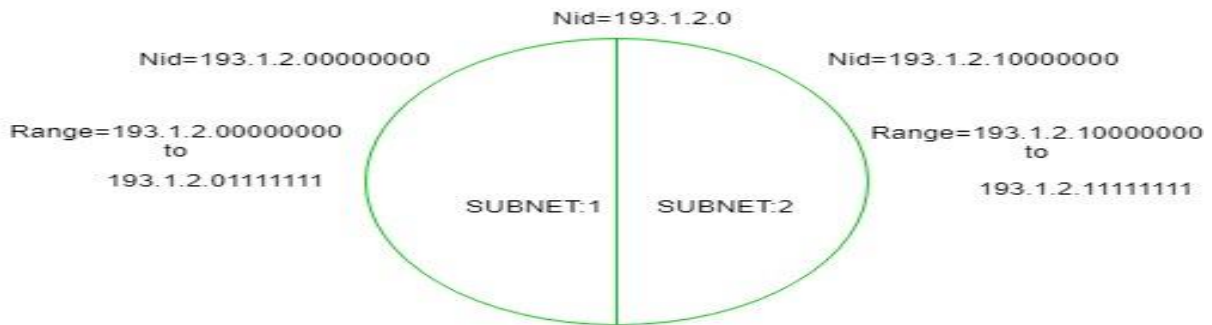
For example, a subnet mask of 255.255.255.0, often expressed in binary as 11111111.11111111.11111111.00000000, means that the first 24 bits (or the first 3 octets) of the IP address represent the network, and the last 8 bits (or the last octet) represent the host

| IP Address Class | Default Subnet Mask |
|------------------|---------------------|
| Class A          | 255.0.0.0           |
| Class B          | 255.255.0.0         |
| Class C          | 255.255.255.0       |

## **Sub-Netting:**

Subnetting is the process of dividing a single large network into multiple smaller networks, called subnets. This is typically done to improve network performance, security, and organization. Subnetting allows network administrators to segment a large network into smaller, more manageable parts, each with its own unique network address.





## **Classless addressing**

Classless addressing, also known as Classless Inter-Domain Routing (CIDR), is a method of IP address allocation that allows for more flexible allocation of IP addresses than the traditional class-based addressing system (Class A, B, and C).

In classful addressing, IP addresses were divided into predefined classes, each with a fixed number of network bits and host bits. For example:

- Class A: 8 network bits, 24 host bits
- Class B: 16 network bits, 16 host bits
- Class C: 24 network bits, 8 host bits

However, classful addressing led to inefficient use of IP address space, especially with the rapid growth of the internet. Classless addressing, introduced with CIDR, allows for the allocation of IP addresses without strict to class boundaries.

Ex. 192.168.1.0/24

Means that the first 24 bits represent the network portion of the address, and the remaining bits represent the host portion

10.0.0.0/8 means that the first 8 bits represent the network portion

Overall, classless addressing provides greater flexibility and efficiency in IP address allocation compared to the older Classful addressing scheme

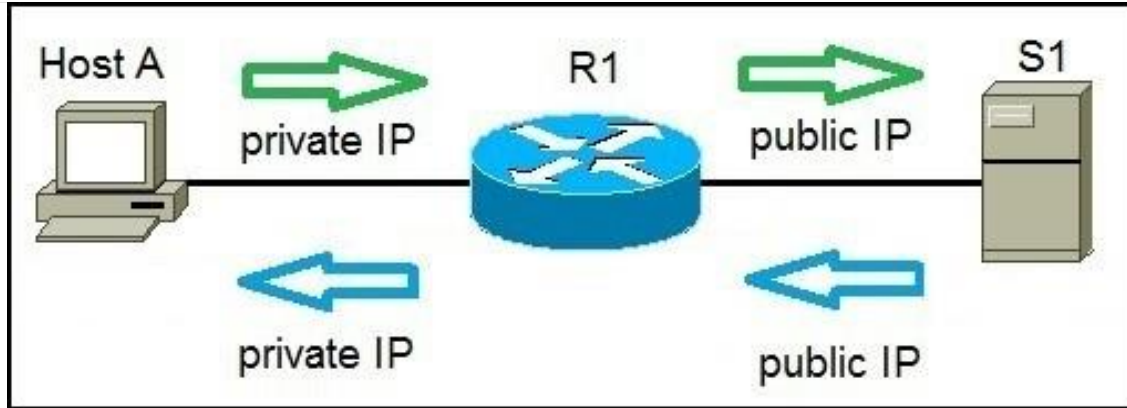
## **Network Address Translation(NAT)**

Network Address Translation (NAT) is a technique used in networking to modify network address information in packet headers while they are in transit across a traffic routing device. NAT allows devices within a private network to communicate with devices on external networks, such as the internet, by translating their private IP addresses into public IP addresses and vice versa.



**Private IP Addresses:** Devices within a private network are assigned private IP addresses . These IP addresses are not globally unique and cannot be routed over the internet.

**Public IP Address:** The NAT device, typically a router or firewall, is assigned a public IP address that is routable over the internet.



There are several types of NAT:

- **Static NAT:** Maps a single private IP address to a single public IP address.
- **Dynamic NAT:** Maps multiple private IP addresses to a pool of public IP addresses on a first-come, first-served basis.
- **PAT (Port Address Translation):** Maps multiple private IP addresses to a single public IP address using different ports. This is also known as NAT overload.
- **NAT64:** Facilitates communication between IPv6-only and IPv4-only hosts by translating IPv6 addresses to IPv4 addresses and vice versa.

## Routing:

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.



- The routing algorithm initializes and maintains the routing table for the process of path determination.

## **Static and Dynamic Routing**

### **Static Routing:**

Static Routing is also known as **non-adaptive** routing which doesn't change the routing table unless the network administrator changes or modifies them manually. Static routing does not use complex routing algorithms and It provides high or more security than dynamic routing

### **Dynamic Routing:**

Dynamic routing is also known as **adaptive** routing which changes the routing table according to the change in topology. [Dynamic routing](#) uses complex routing algorithms and it does not provide high security like [static routing](#). When the network change(topology) occurs, it sends the message to the router to ensure that changes then the routes are recalculated for sending updated routing information.

### **Difference between Static and Dynamic Routing:**

| S.NO | Static Routing                                          | Dynamic Routing                                                   |
|------|---------------------------------------------------------|-------------------------------------------------------------------|
| 1.   | In static routing routes are user-defined.              | In dynamic routing, routes are updated according to the topology. |
| 2.   | Static routing does not use complex routing algorithms. | Dynamic routing uses complex routing algorithms.                  |
| 3.   | Static routing provides high or more security.          | Dynamic routing provides less security.                           |
| 4.   | Static routing is manual.                               | Dynamic routing is automated.                                     |



| S.NO | Static Routing                                                 | Dynamic Routing                                                           |
|------|----------------------------------------------------------------|---------------------------------------------------------------------------|
| 5.   | Static routing is implemented in small networks.               | Dynamic routing is implemented in large networks.                         |
| 6.   | In static routing, additional resources are not required.      | In dynamic routing, additional resources are required.                    |
| 7.   | In static routing, failure of the link disrupts the rerouting. | In dynamic routing, failure of the link does not interrupt the rerouting. |
| 8.   | Less Bandwidth is required in Static Routing.                  | More Bandwidth is required in Dynamic Routing.                            |
| 9.   | Static Routing is difficult to configure.                      | Dynamic Routing is easy to configure.                                     |
| 10.  | Another name for static routing is non-adaptive routing.       | Another name for dynamic routing is adaptive routing.                     |

### **Interior and Exterior Routing:**

Interior routing is the process of exchanging routing information within a single autonomous system (AS) or network. It involves the communication between routers within the same network to determine the best paths for forwarding data packets between devices.

Interior routing protocols (IGPs - Interior Gateway Protocols) are used for this purpose. These protocols enable routers within the same AS to share information about network topology

Common interior routing protocols include:

1. **Routing Information Protocol (RIP):** A simple distance-vector routing protocol that measures the number of hops to reach a destination.
2. **Open Shortest Path First (OSPF):** A link-state routing protocol that calculates the shortest path to each destination based on the cost of links.

### **Exterior Routing**

Exterior routing is the process of exchanging routing information between different autonomous systems or networks. It involves the communication between routers that connect separate



autonomous system such as those operated by different Internet Service Providers (ISPs), large organizations, or other entities.

The primary protocol used for exterior routing on the Internet is the Border Gateway Protocol (BGP)

### **Network layer protocols:**

A network protocol is a set of established rules that specify how to format, send and receive data so that computer network endpoints, including computers, servers, routers and virtual machine.

#### **Some of the key network layer protocols include:**

##### **1. Internet Protocol (IP):**

IP is the foundational protocol of the Internet and is responsible for addressing and routing packets between hosts on different networks.

##### **2. Internet Control Message Protocol (ICMP):**

ICMP is used for error reporting and diagnostic functions within IP networks. It helps in troubleshooting network connectivity issues and reporting errors to the source host.

##### **3. Address Resolution Protocol (ARP):**

ARP is used to map IP addresses to MAC addresses within a local network. It resolves IP addresses to MAC addresses to facilitate communication between devices on the same network.

##### **4. Reverse Address Resolution Protocol (RARP):**

RARP stands for Reverse Address Resolution Protocol. RARP works opposite of ARP. Reverse Address Resolution Protocol is used to convert MAC address ie. physical address into IP address ie. logical address

##### **5. Internet Group Management Protocol (IGMP):**

IGMP is used by IP hosts to report their multicast group memberships to multicast routers. It enables efficient delivery of multicast traffic to interested hosts within a network.



## Transport Layer

The transport Layer is the second layer in the [TCP/IP model](#) and the fourth layer in the [OSI model](#). It is an end-to-end layer used to deliver messages to a host. It is termed an end-to-end layer because it provides a point-to-point connection rather than hop-to-hop, between the source host and destination host to deliver the services reliably

### Working of Transport Layer

The transport layer takes services from the [Application layer](#) and provides services to the [Network layer](#).

**At the sender's side:** The transport layer receives data (message) from the Application layer and then performs Segmentation, divides the actual message into segments, adds the source and destination's port numbers into the header of the segment, and transfers the message to the Network layer.

**At the receiver's side:** The transport layer receives data from the Network layer, reassembles the segmented data, reads its header, identifies the port number, and forwards the message to the appropriate port in the Application layer.

### Responsibilities of a Transport Layer

- It provides a process to process delivery or end to end delivery of the entire message from the sender to the receiver.
- This layer checks for errors during transmission.
- It controls the flow control mechanism and prevents data loss due to the speed mismatch of the sender and receiver.
- This layer divides the stream of bytes received from the upper layer into segments at the sender side and reassembles at the receiver side.

The following are the design issues with transport layer:

- Efficient delivery of data with proper correction.
- Managing error control and flow control.
- Obtaining data from the Session layer, divide it into segments and transmit to the network layer



## Congestion control

**Congestion Control** refers to the methods used to prevent network congestion, where too much data is being sent too quickly, leading to packet loss, delays, and reduced overall network performance. Here's how congestion control is handled at the Transport Layer:

### 1. **TCP Congestion Control Algorithms:**

- **Slow Start:** Initially increases the transmission rate exponentially to quickly find the network's capacity.
- **Congestion Avoidance:** Once congestion is detected (e.g., through packet loss), the transmission rate is increased more slowly to avoid further congestion.
- **Fast Retransmit and Fast Recovery:** Quickly retransmits lost packets and adjusts the congestion window to recover from packet loss without starting from scratch.

## Flow control

The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model. TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques. It uses the method of sliding window protocol which is accomplished by the receiver by sending a window back to the sender informing the size of data it can receive.

## Quality of service

**Quality of Service (QoS)** in the Transport Layer involves managing and prioritizing network traffic to ensure that performance meets the needs of various applications, especially under heavy load or constrained network conditions.

### 1. **QoS Mechanisms:**

- **Prioritization:** Assigning different priority levels to different types of traffic (e.g., VoIP, video streaming, regular data).
- **Bandwidth Management:** Allocating sufficient bandwidth for high-priority or critical applications.



- **Traffic Shaping:** Controlling the flow of data into the network to ensure smooth transmission and avoid bursts that can cause congestion.

## Note

### Summary

The Transport Layer's role in handling congestion control, flow control, and quality of service is critical for maintaining the performance, reliability, and efficiency of data transmission across networks. Each of these areas addresses specific challenges:

## Transport layer addressing sockets, Port

In the Transport Layer, addressing mechanisms such as sockets and ports are fundamental for enabling communication between applications across a network. These mechanisms ensure that data is delivered to the correct application process on a given device

### Sockets

**Socket** is an endpoint for communication between two machines. It is defined by the combination of an IP address and a port number, enabling multiple applications to use the network simultaneously without interfering with each other.

- **Socket Components:**
- **IP Address:** Identifies the host machine on the network.
- **Port Number:** Identifies a specific application or process on the host machine

### Ports

**Port Numbers** are numerical identifiers in the range of 0 to 65535, used to distinguish different processes or services on a host. Ports are divided into several ranges:

- **Well-Known Ports (0-1023):**
- Reserved for common services and protocols (e.g., HTTP uses port 80, HTTPS uses port 443, FTP uses port 21).



## **Segmentation and reassembly:**

**Segmentation** involves breaking down large data packets into smaller, manageable segments before they are sent over the network. This is necessary because most network protocols and technologies have limits on the size of the data packets they can handle

**Reassembly** is the process of putting the segmented pieces of data back together in the correct order to reconstruct the original message at the destination.

## **Connection oriented and connectionless service**

A **connection-oriented service** involves establishing a connection between two communicating devices before any data is transmitted. This connection remains active until the communication session ends.

### **Key Characteristics:**

1. **Connection Establishment:** A setup phase is required where a connection is established between the sender and receiver. This typically involves a handshake process.
2. **Reliable Data Transfer:** Guarantees that data is delivered accurately and in the correct order. Lost or corrupted packets are retransmitted.
3. **Flow Control:** Manages the rate of data transmission to prevent overwhelming the receiver.
4. **Congestion Control:** Adjusts the transmission rate based on network conditions to prevent congestion.
5. **Connection Termination:** A teardown phase occurs to close the connection once the communication is complete.

A **connectionless service** involves sending data without establishing a connection between the sender and receiver. Each data packet is treated independently, and there is no guarantee of delivery, order, or integrity.

### **Key Characteristics:**

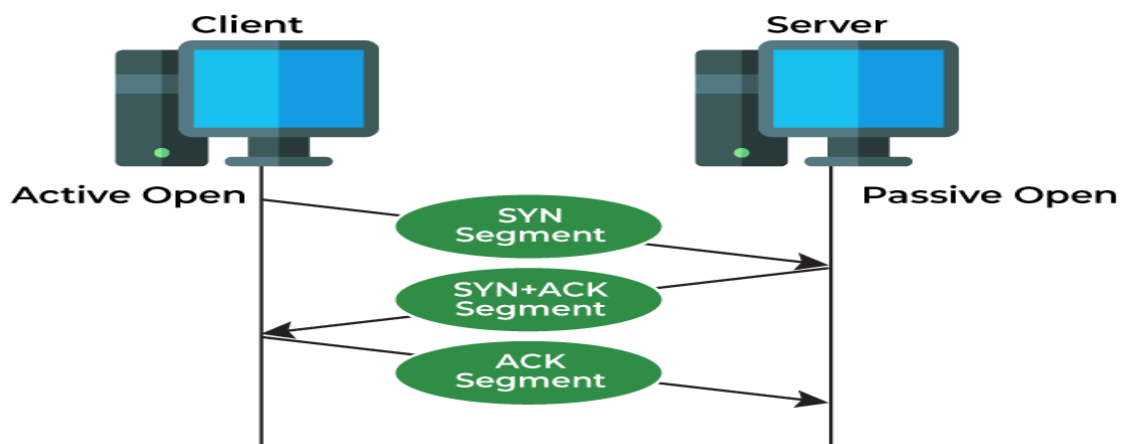
1. **No Connection Establishment:** Data packets are sent without any setup phase.
2. **Unreliable Data Transfer:** No guarantees are made regarding delivery, order, or error correction.



3. **No Flow Control:** The sender does not manage the rate of data transmission.
4. **No Congestion Control:** The network does not adjust the transmission rate based on congestion

## Transmission Control Protocol (TCP)

[TCP \(Transmission Control Protocol\)](#) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.



### Advantages of TCP

- It is reliable for maintaining a connection between Sender and Receiver.
- It is responsible for sending data in a particular sequence.
- Its operations are not dependent on OS.
- It allows and supports many routing protocols.
- It can reduce the speed of data based on the speed of the receiver.

### Disadvantages of TCP

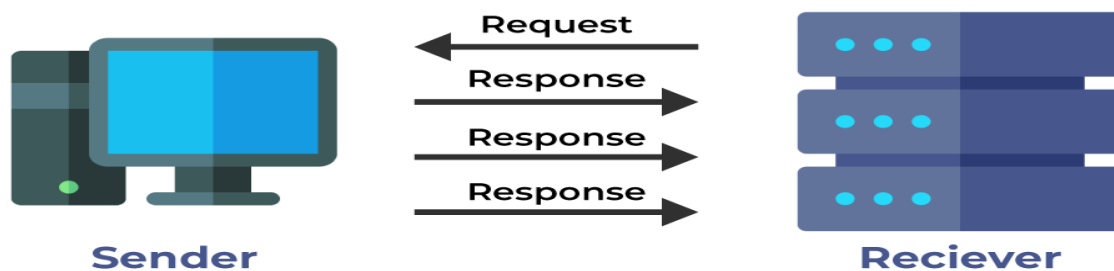
- It is slower than UDP and it takes more bandwidth.
- Slower upon starting of transfer of a file.



- Not suitable for LAN and PAN Networks.
- It does not have a multicast or broadcast category.
- It does not load the whole page if a single data of the page is missing.

## User Datagram Protocol (UDP)

[User Datagram Protocol \(UDP\)](#) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as the UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. So, there is no need to establish a connection before data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network. The UDP enables process-to-process communication.



### Advantages of UDP

- It does not require any connection for sending or receiving data.
- Broadcast and Multicast are available in UDP.
- UDP can operate on a large range of networks.
- UDP has live and real-time data.
- UDP can deliver data if all the components of the data are not complete

### Disadvantages of UDP

- We can not have any way to acknowledge the successful transfer of data.
- UDP cannot have the mechanism to track the sequence of data.
- UDP is connectionless, and due to this, it is unreliable to transfer data.
- In case of a Collision, UDP packets are dropped by Routers in comparison to TCP.
- UDP can drop packets in case of detection of errors.



*Where TCP is Used?*

- Sending Emails
- Transferring Files
- Web Browsing

*Where UDP is Used?*

- Gaming
- Video Streaming
- Online Video Chats

| Factor              | TCP                                                                   | UDP                                                                     |
|---------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------|
| Connection type     | Requires an established connection before transmitting data           | No connection is needed to start and end a data transfer                |
| Data sequence       | Can sequence data (send in a specific order)                          | Cannot sequence or arrange data                                         |
| Data retransmission | Can retransmit data if packets fail to arrive                         | No data retransmitting. Lost data can't be retrieved                    |
| Delivery            | Delivery is guaranteed                                                | Delivery is not guaranteed                                              |
| Check for errors    | Thorough error-checking guarantees data arrives in its intended state | Minimal error-checking covers the basics but may not prevent all errors |
| Broadcasting        | Not supported                                                         | Supported                                                               |
| Speed               | Slow, but complete data delivery                                      | Fast, but at risk of incomplete data delivery                           |







## **Application layer and its function**

The application layer is the topmost layer in the OSI (Open Systems Interconnection) model and the TCP/IP model of networking. It serves as the interface between the network services and the end-user applications. The primary function of the application layer is to facilitate communication and data exchange between software applications and network services.

The Application Layer interface directly interacts with application and provides common web application services

### Key Functions of the Application Layer

#### 1. **User Interface:**

- Provides a platform for user interaction with the network.
- Examples include web browsers, email clients, and file transfer applications.

#### 2. **Application Services:**

- Supports various network applications and services such as email, file transfer, web browsing, and remote access.
- Examples include HTTP for web browsing, SMTP for email, and FTP for file transfers.

#### 3. **Data Presentation and Encoding:**

- Ensures that data is presented in a readable format for the receiving application.
- Manages data encoding, serialization, and formatting.
- Examples include converting text to ASCII or Unicode, image formats like JPEG or PNG, and video formats like MPEG.

#### 4. **Session Management:**

- Establishes, manages, and terminates sessions between applications.
- Ensures that sessions are maintained and data is synchronized.
- Examples include managing login sessions and maintaining state information in web applications.

#### 5. **Data Exchange and Protocols:**



- Implements protocols that enable communication between applications on different devices.
- Ensures data integrity, error recovery, and data synchronization.
- Examples include HTTP, FTP, SMTP, POP3, IMAP, and DNS.

#### 6. **Resource Sharing:**

- Facilitates the sharing of resources such as files, printers, and other network services.
- Examples include network file sharing protocols like SMB/CIFS and network printing protocols like IPP.

**Application Layer Protocols:** The application layer provides several protocols which allow any software to easily send and receive information and present meaningful data to its users.

- **SMTP:** SMTP stands for Simple Mail Transfer Protocol. It is used to transfer electronic mail from one user to another user. SMTP is used by end users to send emails with ease. SMTP uses port numbers 25.

#### • **POP3 (Post Office Protocol 3):**

- Used for retrieving emails from a mail server.
- Downloads emails to the local device and typically deletes them from the server.

#### • **IMAP (Internet Message Access Protocol):**

- Used for retrieving emails from a mail server.
- Allows multiple devices to access and manage emails without downloading them.

- **HTTP:** HTTP stands for Hyper Text Transfer Protocol. It is the foundation of the World Wide Web (WWW). HTTP works on the client server model. This protocol is used for transmitting hypermedia documents like HTML. This protocol was designed particularly for the communications between the web browsers and web servers, but this protocol can also be used for several other purposes. HTTP is a stateless protocol (network protocol in which a client sends requests to server and server responses back as per



the given state), which means the server is not responsible for maintaining the previous client's requests. HTTP uses port number 80.

- **HTTPS (HTTP Secure):**

- An extension of HTTP that provides secure communication over a computer network.
- Uses encryption protocols like SSL/TLS.

**FTP:** FTP stands for File Transfer Protocol. This protocol helps to transfer different files from one device to another. FTP promotes sharing of files via remote computer devices with reliable, efficient data transfer. FTP uses port number 20 for data access and port number 21 for data control.

- **TELNET:** Telnet stands for Telecommunications Network. This protocol is used for managing files over the Internet. It allows the Telnet clients to access the resources of Telnet server. Telnet uses port number 23.
- **DNS:** DNS stands for Domain Name System. The DNS service translates the domain name (selected by user) into the corresponding IP address. For example- If you choose the domain name as www.abcd.com, then DNS must translate it as 192.36.20.8 (random IP address written just for understanding purposes). DNS protocol uses the port number 53.
- **DHCP:** DHCP stands for Dynamic Host Configuration Protocol. It provides IP addresses to hosts. Whenever a host tries to register for an IP address with the DHCP server, DHCP server provides lots of information to the corresponding host. DHCP uses port numbers 67 and 68.

## WWW(**World Wide Web**)

World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc. The WWW, along with internet, enables the retrieval and display of text and media to your device.



## **PuTTY:**

PuTTY is a popular and free software tool used in computer networking for various remote access tasks. It is primarily a terminal emulator, serial console, and network file transfer application that supports several network protocols. PuTTY is widely used by network administrators, developers, and IT professionals to manage and configure remote systems.

### Key Features of PuTTY

#### 1. **Terminal Emulation:**

- Provides a graphical interface for accessing remote systems.
- Emulates various types of terminals such as xterm, VT102, and ECMA-48.

#### 2. **Supported Protocols:**

- **SSH (Secure Shell):** For secure remote login and command execution.
- **Telnet:** For unencrypted remote login and command execution.

#### 3. **Secure Communication:**

- Supports SSH-1 and SSH-2 protocols for encrypted communication.
- Includes features like public key authentication and port forwarding.

#### 4. **File Transfer:**

- **PSCP (PuTTY Secure Copy):** A command-line tool for secure file transfer over SSH.
- **PSFTP (PuTTY SFTP):** An interactive file transfer tool using the SFTP protocol

- .

### Common Use Cases for PuTTY

#### 1. **Remote Server Management:**

- Accessing and managing Linux/Unix servers from a Windows machine.
- Performing administrative tasks, running scripts, and monitoring server performance.



## 2. **Network Device Configuration:**

- Connecting to network devices like routers, switches, and firewalls via SSH or serial console for configuration and troubleshooting.

## 3. **Secure File Transfers:**

- Using PSCP or PSFTP to transfer files securely between local and remote systems.

## 4. **Development and Debugging:**

- Developers use PuTTY to access remote development environments, run applications, and debug issues on remote servers.

## **WinSCP:**

WinSCP is a free, open-source file transfer software for Windows. It provides a graphical user interface (GUI) to facilitate secure file transfers between a local computer and remote servers. WinSCP supports multiple file transfer protocols, including Secure File Transfer Protocol (SFTP) and Secure Copy Protocol (SCP), which run over SSH, as well as FTP and WebDAV.

## Common Use Cases for WinSCP

### 1. **Website Management:**

- Upload and update website files securely.
- Manage website content on remote web servers.

### 2. **Server Administration:**

- Transfer configuration files and scripts to and from servers.
- Backup server data to local machines or other servers.

### 3. **Development and Testing:**

- Synchronize code between local development environments and remote test servers.
- Collaborate with team members by sharing files on remote servers.

### 4. **File Backup and Synchronization:**



- Automate regular backups of important files to remote storage.
- Synchronize directories between local and remote locations.

WinSCP is a powerful and versatile tool for secure file transfer and management, providing a user-friendly interface and robust features for both novice and experienced users. Its support for multiple protocols, integration with PuTTY, and extensive scripting capabilities make it a valuable resource for web developers, server administrators, and IT professionals looking to efficiently manage and transfer files between local and remote systems.