COMPUTER NETWORK

BCSC 0008

SEM- IV

DR. VARUN MISHRA
DEPT. OF CSE
GLA UNIVERSITY
MATHURA

COMPUTER NETWORK : DEFINITION

- A computer network is a collection of computers or devices connected to share resources. Any device which can share or receive the data is called a Node.

- Through which the information or data propagate is known as channels, It can be guided or unguided.

COMPUTER NETWORKING : DEFINITION

- Computer Networking is the practice of connecting computers together to enable communication and data exchange between them.

- In general, Computer Network is a collection of two or more computers. It helps users to communicate more easily.

- The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate. Each device has an IP Address, that helps in identifying a device.

GOALS OF NETWORK

- **Resource Sharing** – Many organization has a substantial number of computers in operations, which are located apart. Ex. A group of office workers can share a common printer, fax, modem, scanner, etc.

- **High Reliability** – If there are alternate sources of supply, all files could be replicated on two or more machines. If one of them is not available, due to hardware failure, the other copies could be used.

- **Inter-process Communication** – Network users, located geographically apart, may converse in an interactive session through the network. In order to permit this, the network must provide almost error-free communications.

GOALS OF NETWORK CONT'D….

- **Flexible access** – Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another.
- **Security**– Computer networks must be secure to protect against unauthorized access, data breaches, and other security threats. This includes implementing measures such as firewalls, antivirus software, and encryption to ensure the confidentiality, integrity, and availability of data.
- **Performance**– Computer networks must provide high performance and low latency to ensure that applications and services are responsive and available when needed. This requires optimizing network infrastructure, bandwidth utilization, and traffic management.
- **Scalability-** Computer networks must be designed to scale up or down as needed to accommodate changes in the number of users, devices, and data traffic. This requires careful planning and management to ensure the network can meet current and future needs.

ADVANTAGES

- **Resource sharing:** Networks enable the sharing of resources such as printers, scanners, storage devices, and software applications, which can reduce costs and increase efficiency.
- **Communication and collaboration:** Networks provide a platform for communication and collaboration among users, allowing for easy sharing of information and ideas.
- **Centralized management:** Networks allow for centralized management of devices, users, and resources, making it easier to control and monitor the network.
- **Scalability:** Networks can be scaled up or down to accommodate changes in the number of users, devices, or data volume.
- **Accessibility:** Networks can provide remote access to resources, enabling users to work from anywhere and improving accessibility to information and resources.

DISADVANTAGES

- **Security vulnerabilities:** Networks can be vulnerable to security threats such as hacking, viruses, and malware, which can compromise sensitive **data and disrupt network operations.**
- **Complexity:** Networks can be complex to set up, configure, and maintain, requiring specialized knowledge and expertise.
- **Dependence on infrastructure:** Networks depend on the underlying infrastructure such as cables, routers, switches, and servers, which can be prone to failures or downtime, disrupting network operations.
- **Cost:** Networks can be expensive to set up and maintain, requiring investments in hardware, software, and personnel.
- **Performance limitations:** Networks have performance limitations such as bandwidth constraints, latency, and congestion, which can affect the speed and reliability of network operations.

TERMINOLOGIES

- **Network:** A network is a collection of computers and devices that are connected together to enable communication and data exchange.
- **Nodes:** Nodes are devices that are connected to a network. These can include computers, Servers, Printers, Routers, Switches, and other devices.
- **Protocol:** A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include TCP/IP, HTTP, and FTP.
- **Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh, and tree.

TERMINOLOGIES

- **Service Provider Networks:** These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.
- **IP Address**: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.
- **DNS:** The Domain Name System (DNS) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.
- **Firewall:** A firewall is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

COMPONENTS OF COMPUTER NETWORK

- A computer network consists of several physical components. In other words, two or more devices are connected via a computer network to exchange an almost infinite amount of data and services. Here Below are some physical components of computer Networks:
  - NIC(Network Interface Card)
  - HUB
  - Router
  - Modem
  - Switch
  - Nodes
  - Media
  - Repeater
  - Server

NETWORK INTERFACE CARD (NIC)

- NIC or network interface card is a network adapter used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique ID that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device, which means it works on the network model's physical and data link layers.

- **Types of NIC**
  - **Wired NIC:** Cables and Connectors use Wired NIC to transfer data.
  - **Wireless NIC:** These connect to a wireless network such as Wifi, Bluetooth, etc.

HUB

- A HUB is a multi-port repeater. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one.
- **Types of HUB**
  - **Repeater** suggests **HUB:** This is also known as Active HUB, it regenerates and amplifies the electric signal before sending them to all connected device. This hub is suitable to transmit data for long distance connections over the network.
  - **Passive HUB:** As the name suggests it does not amplify or regenerate electric signal, it is the simplest types of Hub among all and it is not suitable for long-distnace connections.
  - **Switching HUB:** This is also known as intelligent HUB, they provide some additional functionality over active and passive hubs. They analyze data packets and make decisions based on MAC address and they are operated on DLL(Data Link Layer).

ROUTER

- A Router is a device like a switch that routes data packets based on their IP addresses.
- The router is mainly a Network Layer device.
- Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets.
- The router divides the broadcast domains of hosts connected through it.

MODEM

- A Modem is a short form of Modulator/Demodulator.
- The Modem is a hardware component/device that can connect computers and other devices such as routers and switches to the internet.
- Modems convert or modulate the analog signals coming from telephone wire into a digital form that is in the form of 0s and 1s.

SWITCH

- A Switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports implies less traffic) and performance.

- A switch is a data link layer device.

- The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.

NODE

- Node is a term used to refer to any computing devices such as computers that send and receive network packets across the network.
- **Types of nodes**

  - **End Nodes:** These types of nodes are going to be the starting point or the end point of communication. E.g., computers, security cameras, network printers, etc.

  - **Intermediary Nodes:** These nodes are going to be in between the starting point or end point of the end nodes. E.g., Switches, Bridges, Routers, cell towers, etc.

MEDIA

- It is also known as Link which is going to carry data from one side to another side. This link can be Wired Medium (Guided Medium) and Wireless Medium (Unguided Medium). It is of two types:
  - Wired Media
    - Ethernet: Ethernet is the most widely used LAN technology, which is defined under IEEE standards 802.3.
    - Fibre Optic Cable: In this data is transferred in the form of light waves.
    - Coaxial Cable: Mainly used for audio and video communications.
    - USB Cable: USB Stands for Universal Serial Bus. Mainly used to connect PCs and smartphones.
  - Wireless Media
    - Examples of Wireless media are as follows:
    - Infrared (E.g. short-range communication – TV remote control).
    - Radio (E.g. Bluetooth, Wi-Fi).
    - Microwaves (E.g. Cellular system).
    - Satellite (E.g. Long range communications – GPS).

REPEATER

- Repeater is an important component of computer networks as it is used to regenerate and amplify signal in the computer networks.

- Repeaters are used to improve the quality of the networks and they are operated on the Physical Layer of the OSI Model.

SERVER

- A server is a computer program that provides various functionality to another computer program.
- The server plays a vital role in facilitating communication, data storage, etc.
- Servers have more data storage as compared to normal computers. They are designed for the specific purpose of handling multiple requests from clients.

TYPES

- **LAN:** A Local Area Network (LAN) is a network that covers a small area, such as an office or a home. LANs are typically used to connect computers and other devices within a building or a campus.
- **WAN:** A Wide Area Network (WAN) is a network that covers a large geographic area, such as a city, country, or even the entire world. WANs are used to connect LANs together and are typically used for long-distance communication.
- **Cloud Networks:** Cloud Networks can be visualized with a Wide Area Network (WAN) as they can be hosted on public or private cloud service providers and cloud networks are available if there is a demand. Cloud Networks consist of Virtual Routers, Firewalls, etc.

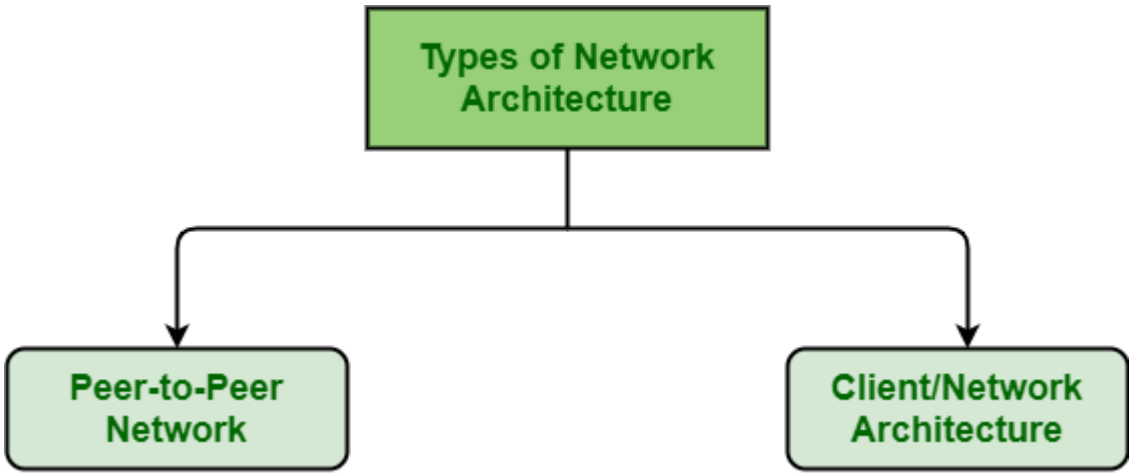
NETWORK ARCHITECTURE

- **Computer networks** are usually developed to fulfil needs of their clients and users. Network architecture generally refers to design of computer network or communications network.
- It simply describes allocation task between all of computers in network.
- It is simply way in which all network devices and services are organized and managed to connect clients like laptops, tablets, servers, etc. and also how tasks are allocated to computer.
- It also facilitates system-level functionality even robustness, extensibility, and evolvability.
- It is basically defined and described as physical and logical design of software, hardware, protocols, and media of data transmission.

NETWORK ARCHITECTURE

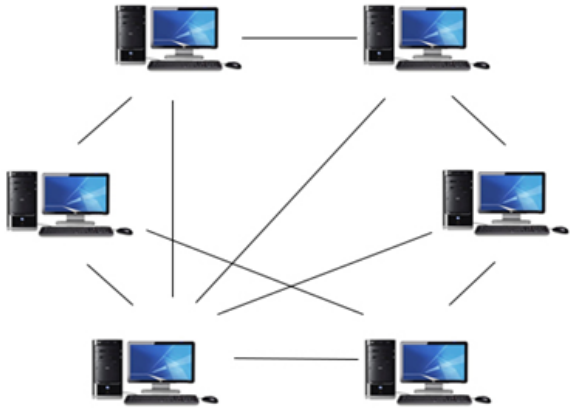
- **Client-Server Architecture:** Client-Server Architecture is a type of Computer Network Architecture in which Nodes can be Servers or Clients. Here, the server node can manage the Client Node Behavior.

- **Peer-to-Peer Architecture:** In P2P (Peer-to-Peer) Architecture, there is not any concept of a Central Server. Each device is free for working as either client or server.



PEER-TO-PEER

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- 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.



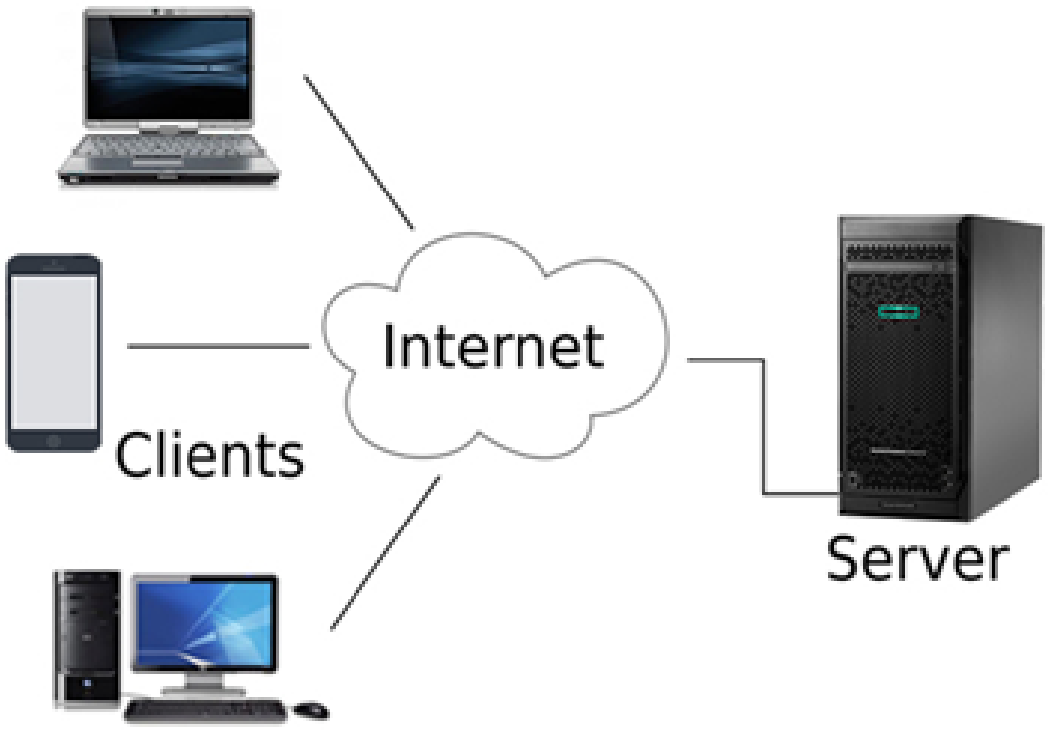
PEER-TO-PEER CONT'D…

- 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.

CLIENT-AND-SERVER

- 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.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.

CLIENT-AND-SERVER



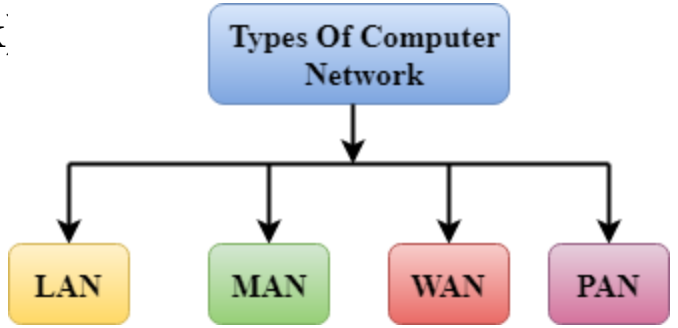
CLIENT-AND-SERVER CONT'D….

- Advantages Of Client/Server network:
  - A Client/Server network contains the centralized system. Therefore we can back up 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.

TYPES OF COMPUTER NETWORK

- A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.
- A computer network can be categorized by their size. A **computer network** is mainly of **four types**:

  - LAN(Local Area Network)
  - PAN(Personal Area Network)
  - MAN(Metropolitan Area Network
  - WAN(Wide Area Network)



LAN(LOCAL AREA NETWORK)

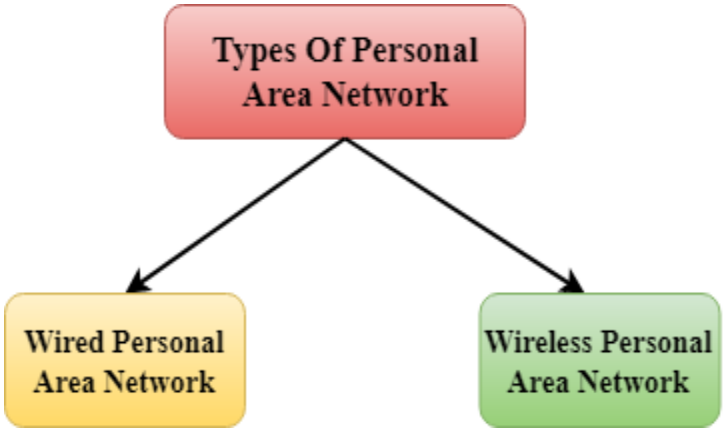
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware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

LAN(LOCAL AREA NETWORK)

PAN(PERSONAL AREA NETWORK)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

PAN(PERSONAL AREA NETWORK)

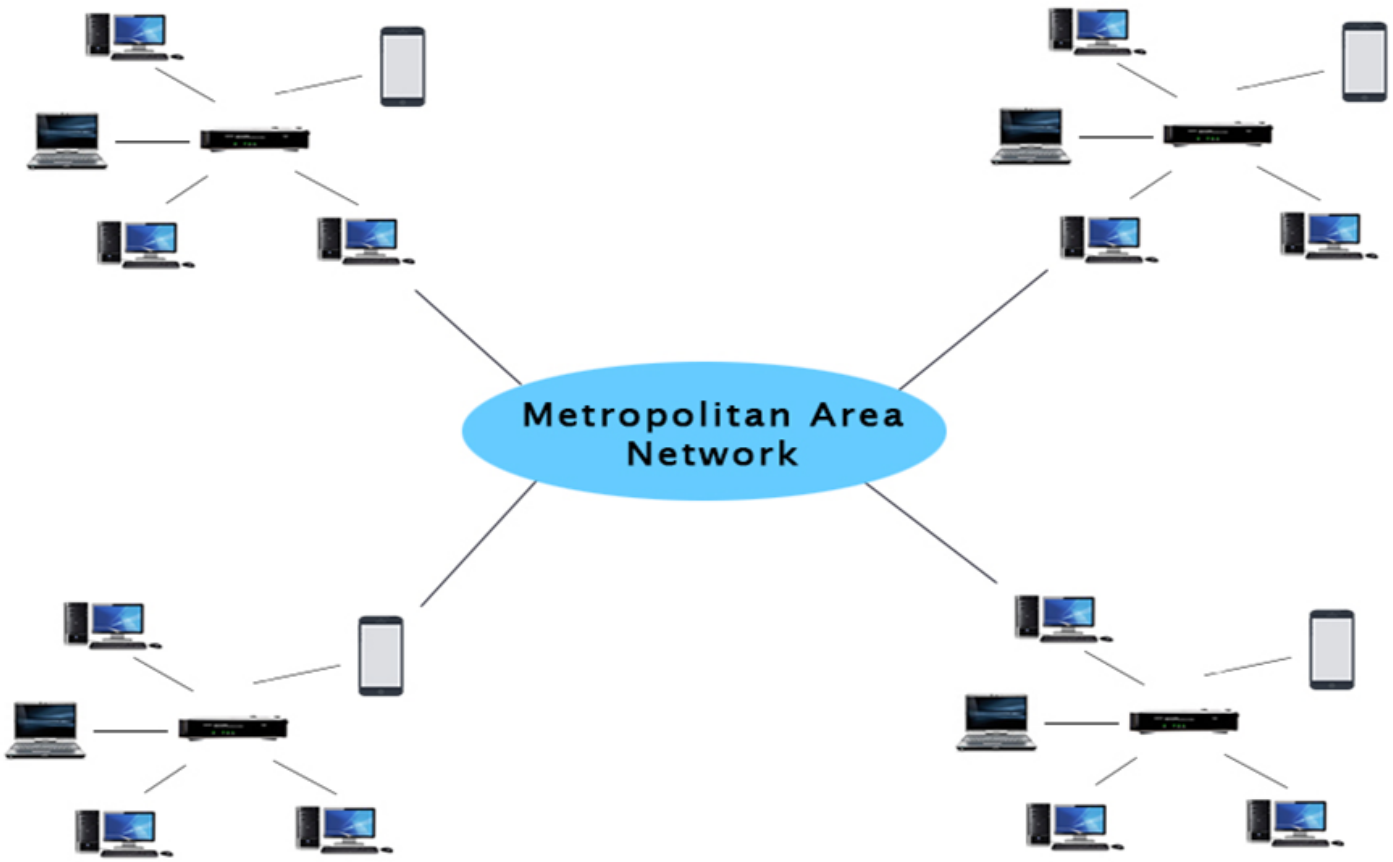


- **Wireless Personal Area Network** is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.
- **Wired Personal Area Network:** Wired Personal Area Network is created by using the USB.

MAN(METROPOLITAN AREA NETWORK)

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

MAN(METROPOLITAN AREA NETWORK)



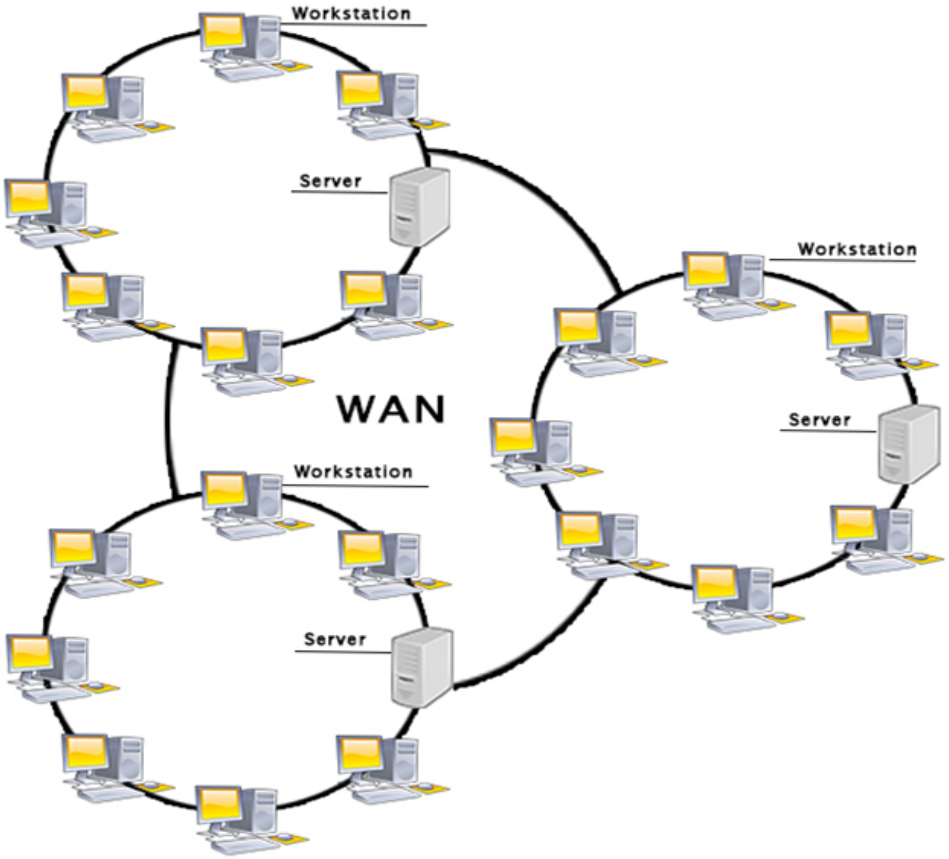
MAN

- Uses Of Metropolitan Area Network:
  - MAN is used in communication between the banks in a city.
  - It can be used in an Airline Reservation.
  - It can be used in a college within a city.
  - It can also be used for communication in the military.

WAN (WIDE AREA NETWORK)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.
-

WAN


Workstation
Server
Workstation
WAN
Server
Workstation
Server

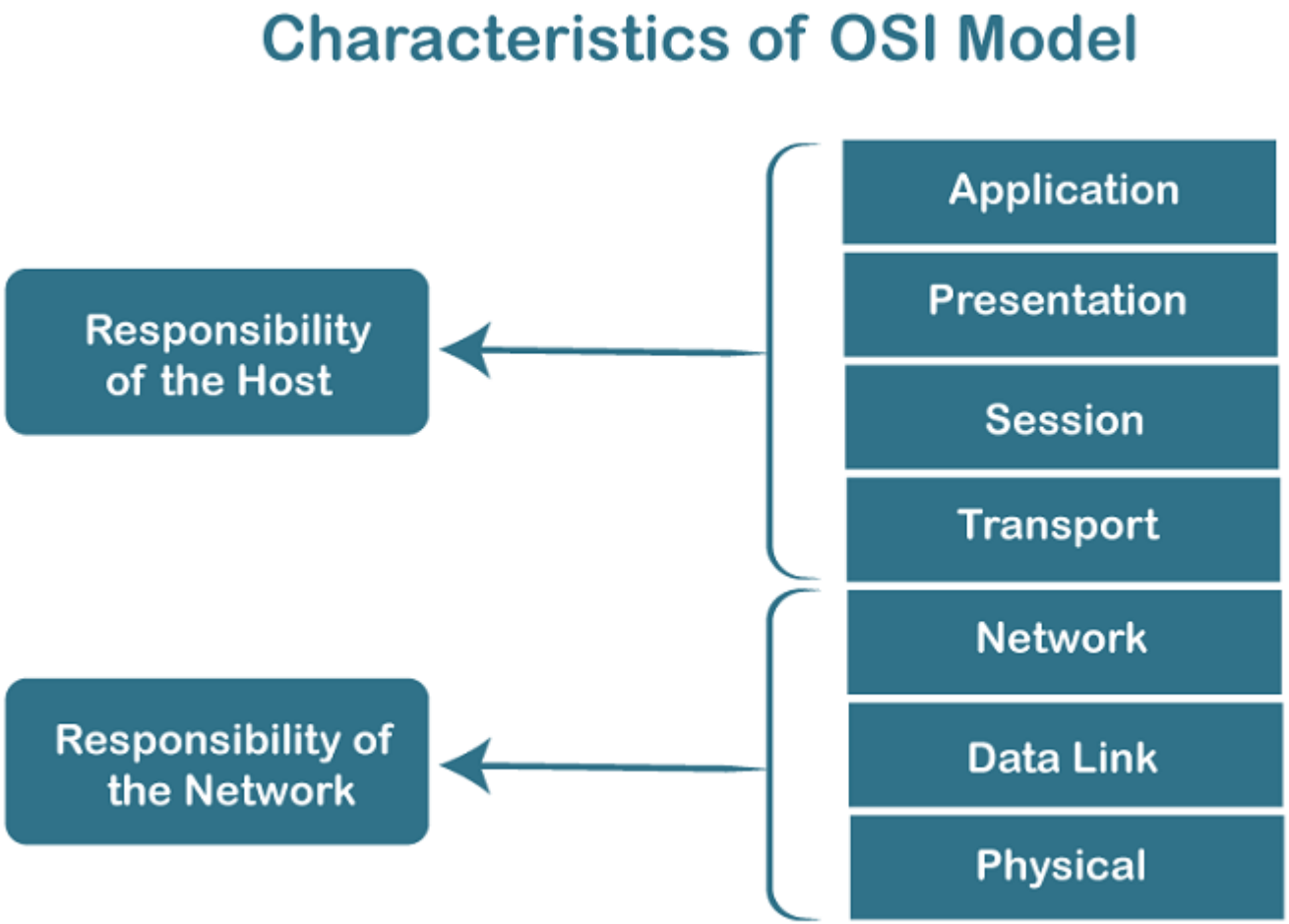
WAN

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

OSI REFERENCE MODEL

- OSI stands for **Open System Interconnection** 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 the 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 task assigned to each layer can be performed independently.

OSI REFERENCE MODEL



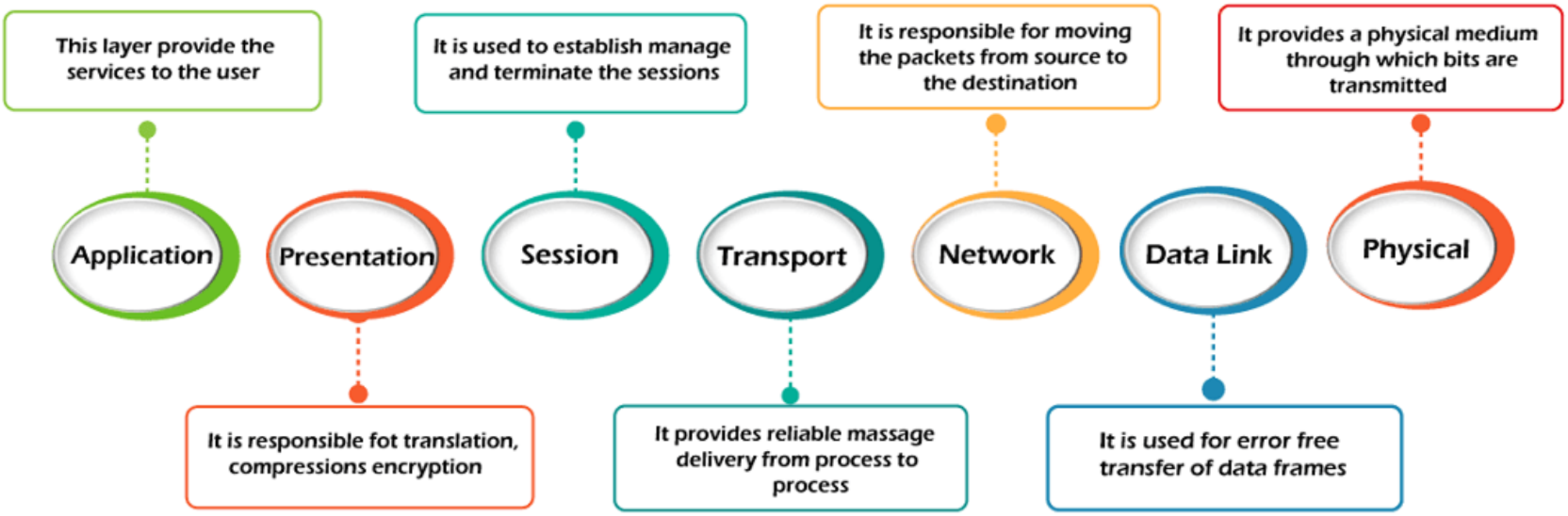
OSI REFERENCE MODEL

- The OSI model is divided into two layers: upper layers and lower layers.

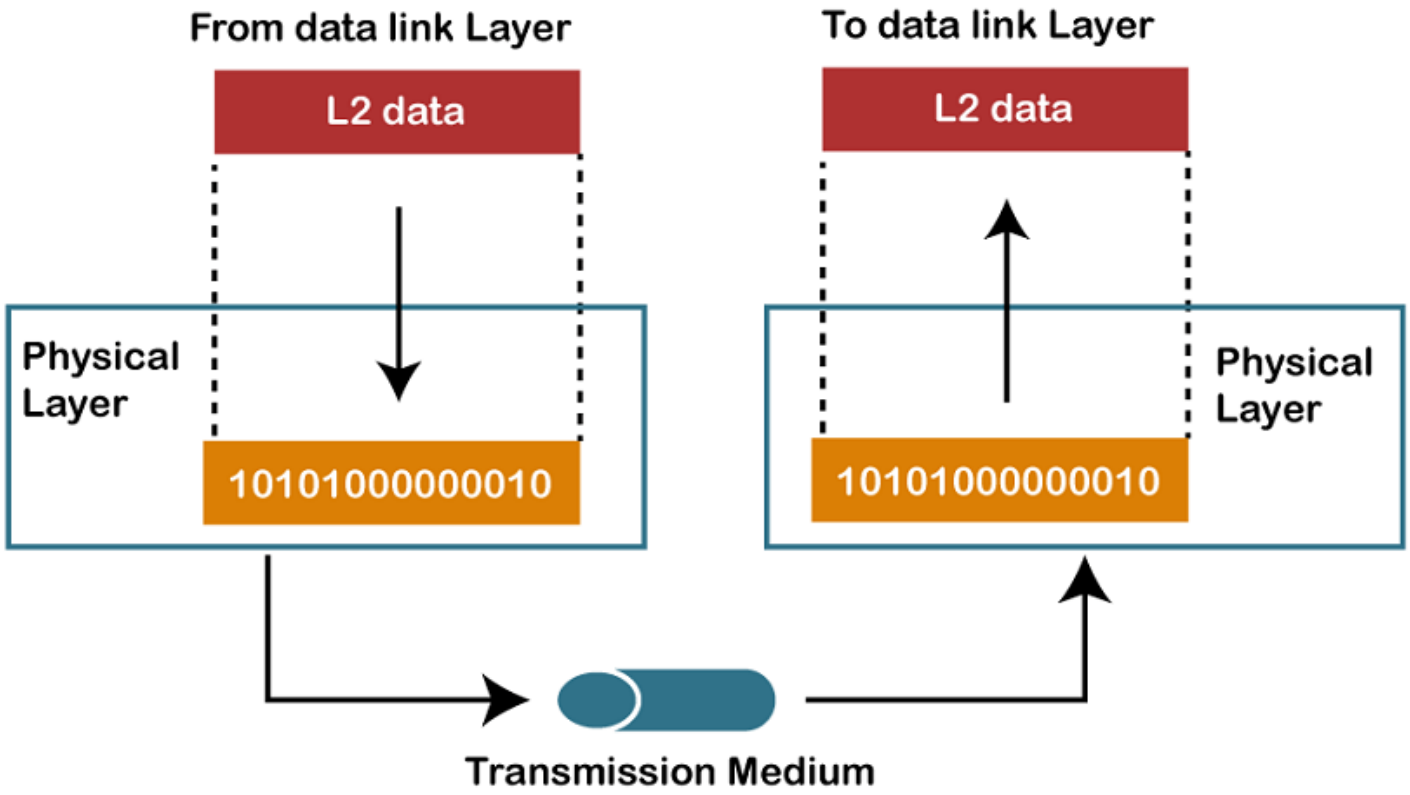
  - The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.

  - The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

OSI LAYERS


This layer provide the services to the user
Application
Presentation
It is responsible fot translation, compressions encryption
It is used to establish manage and terminate the sessions
Session
Transport
It provides reliable massage delivery from process to process
It is responsible for moving the packets from source to the destination
Network
Data Link
It is used for error free transfer of data frames
It provides a physical medium through which bits are transmitted
Physical

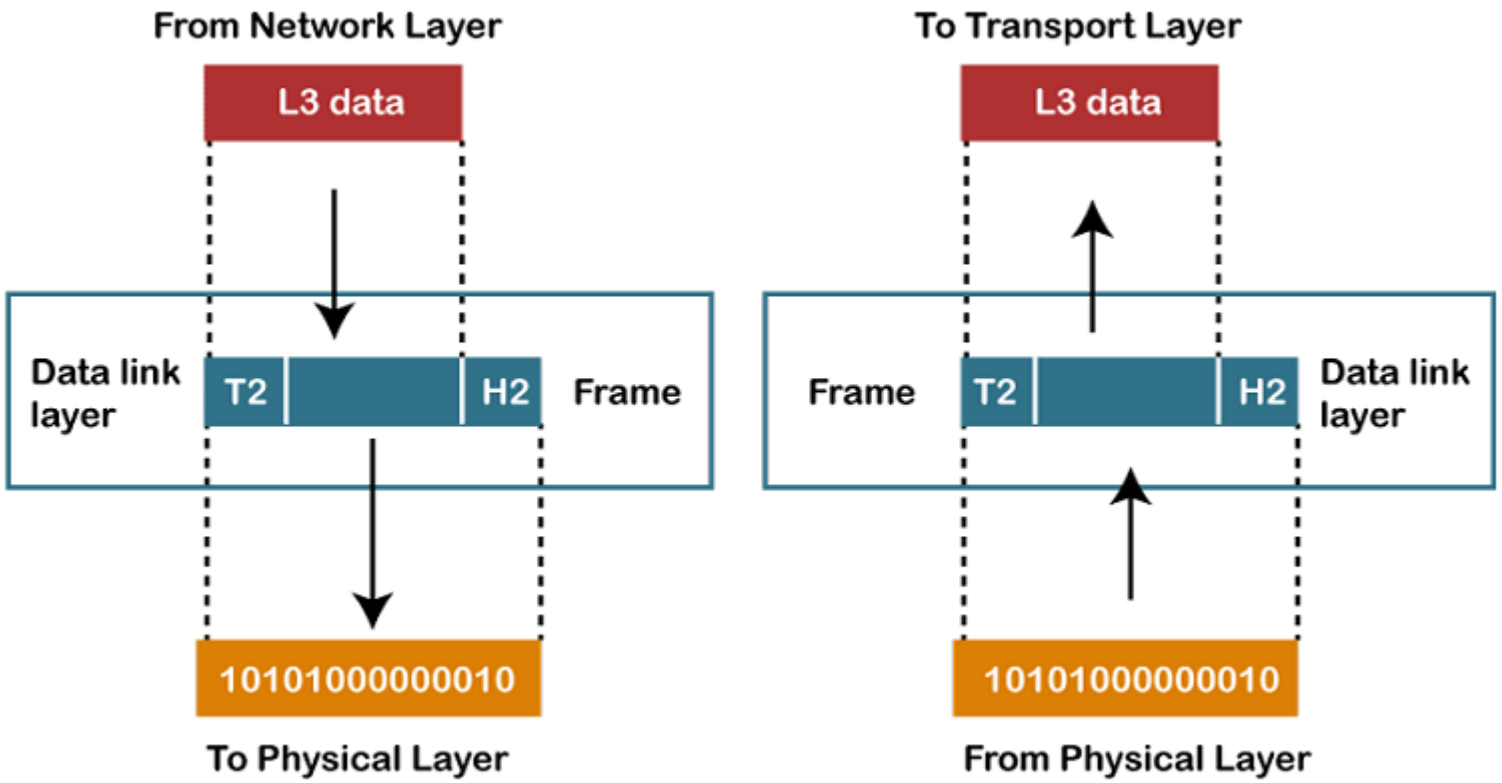
PHYSICAL LAYER



FUNCTIONS : 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 a Physical layer:
  - **Line Configuration:** It defines the way how two or more devices can be connected physically.
  - **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
  - **Topology:** It defines the way how network devices are arranged.
  - **Signals:** It determines the type of the signal used for transmitting the information.

DATA LINK LAYER



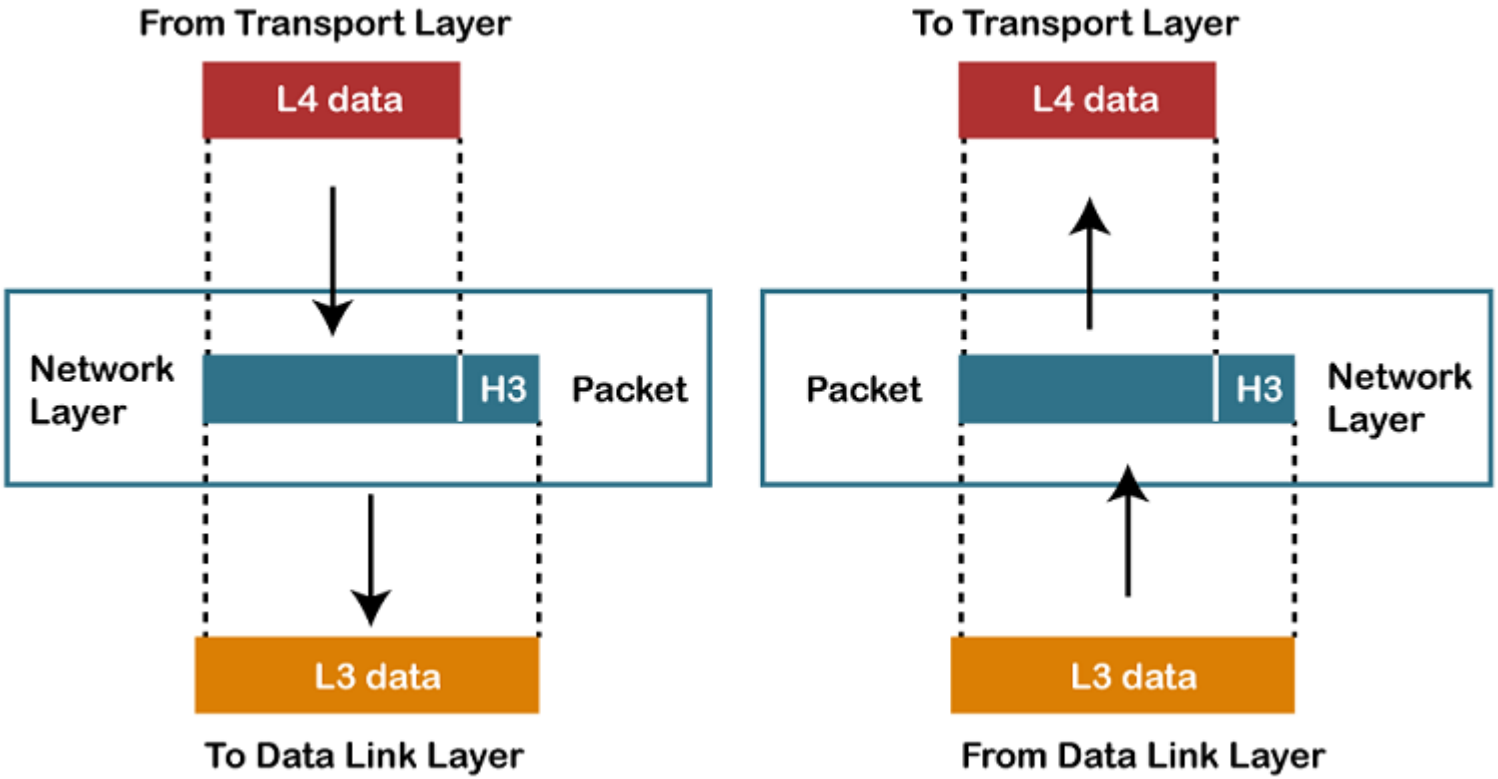
DLL

- 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:
  - **Logical Link Control Layer**
    - 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 also provides flow control.
  - **Media Access Control Layer**
    - 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: DLL

- **Framing:** 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.
- **Physical Addressing:** 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.
- **Flow Control:** 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 get 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.
- **Error Control:** 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. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** 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.

NETWORK LAYER



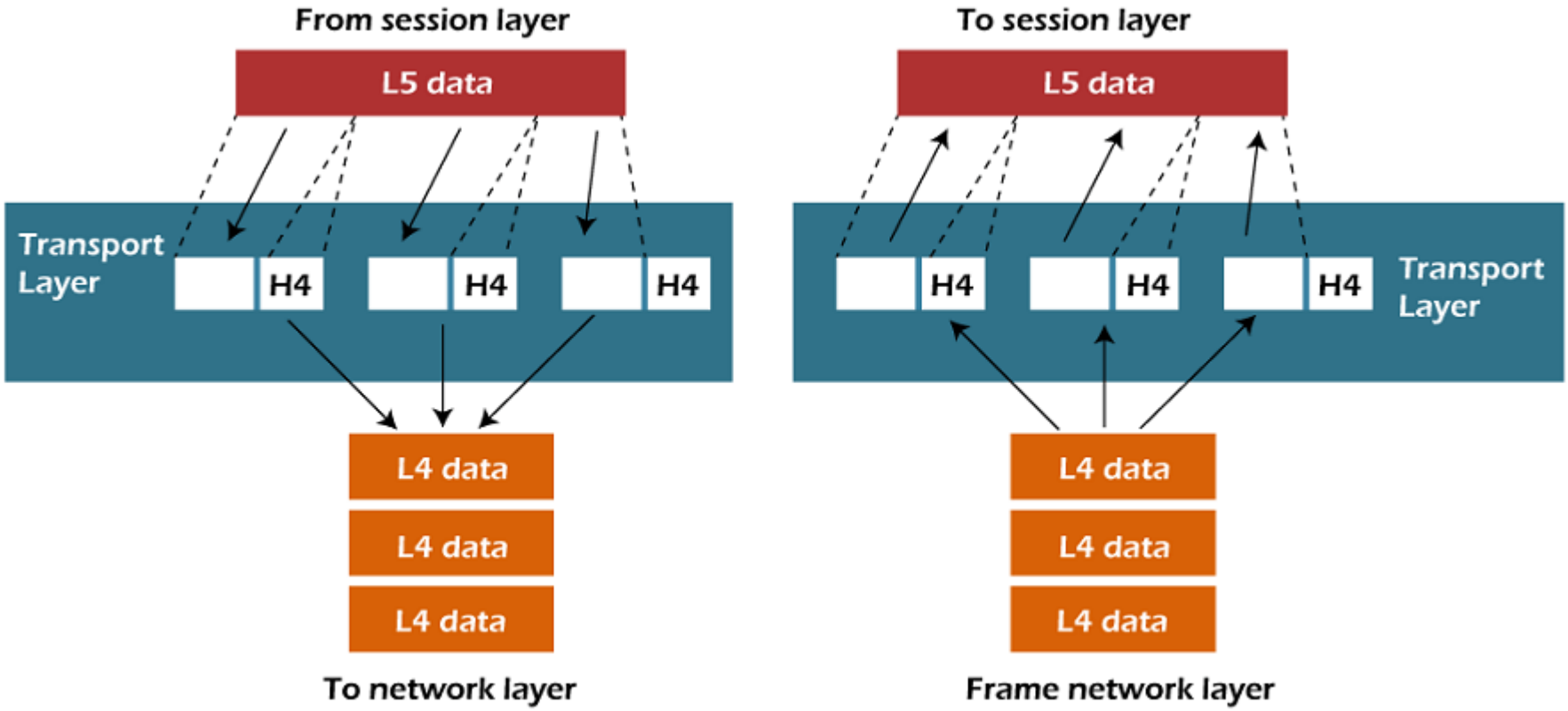
NETWORK LAYER

- 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.
- The 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. Examples of protocols are IP and Ipv6.

NETWORK LAYER : FUNCTIONS

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** 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.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** 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).

TRANSPORT LAYER



TRANSPORT LAYER

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent 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.

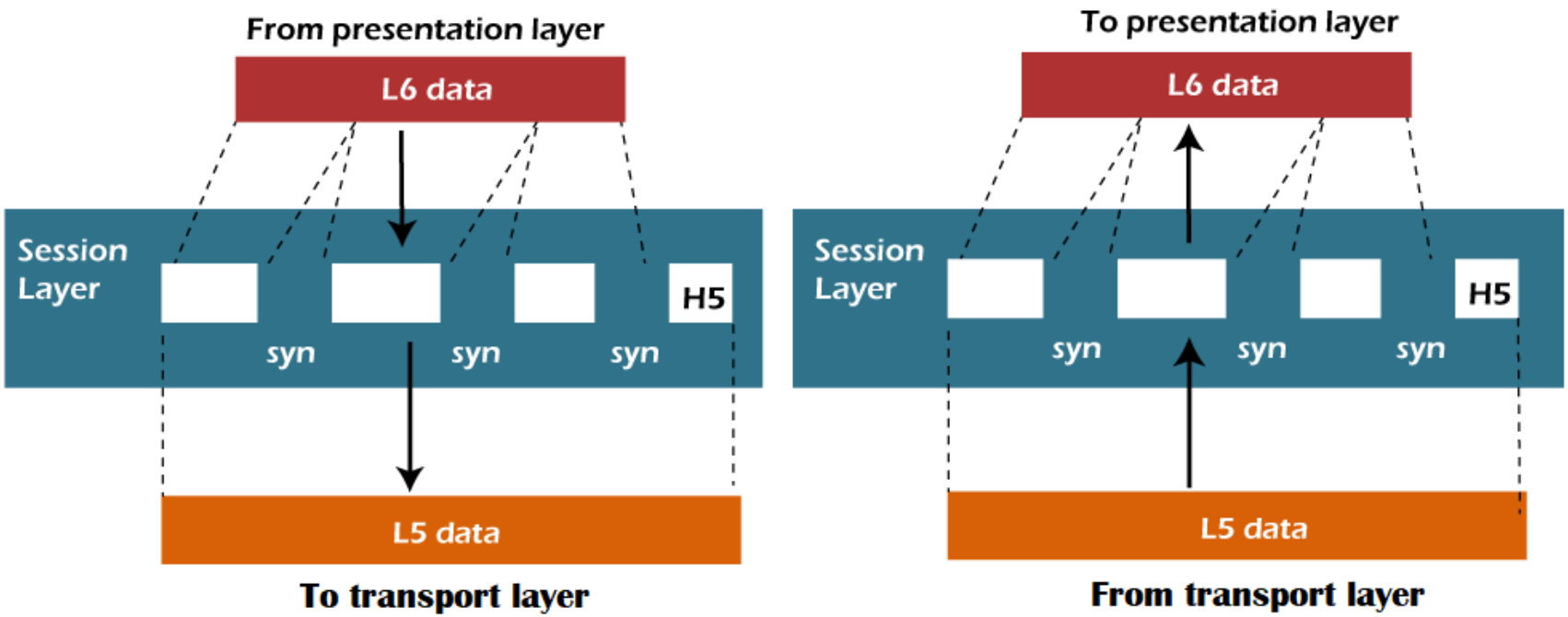
TRANSPORT LAYER CONT'D…

- **Transmission Control Protocol**
  - 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 transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

TRANSPORT LAYER: FUNCTIONS

- **Service-point addressing:** Computers 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.
- **Segmentation and reassembly:** 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 segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** 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 ensures that message reach at the destination without any error.

SESSION LAYER



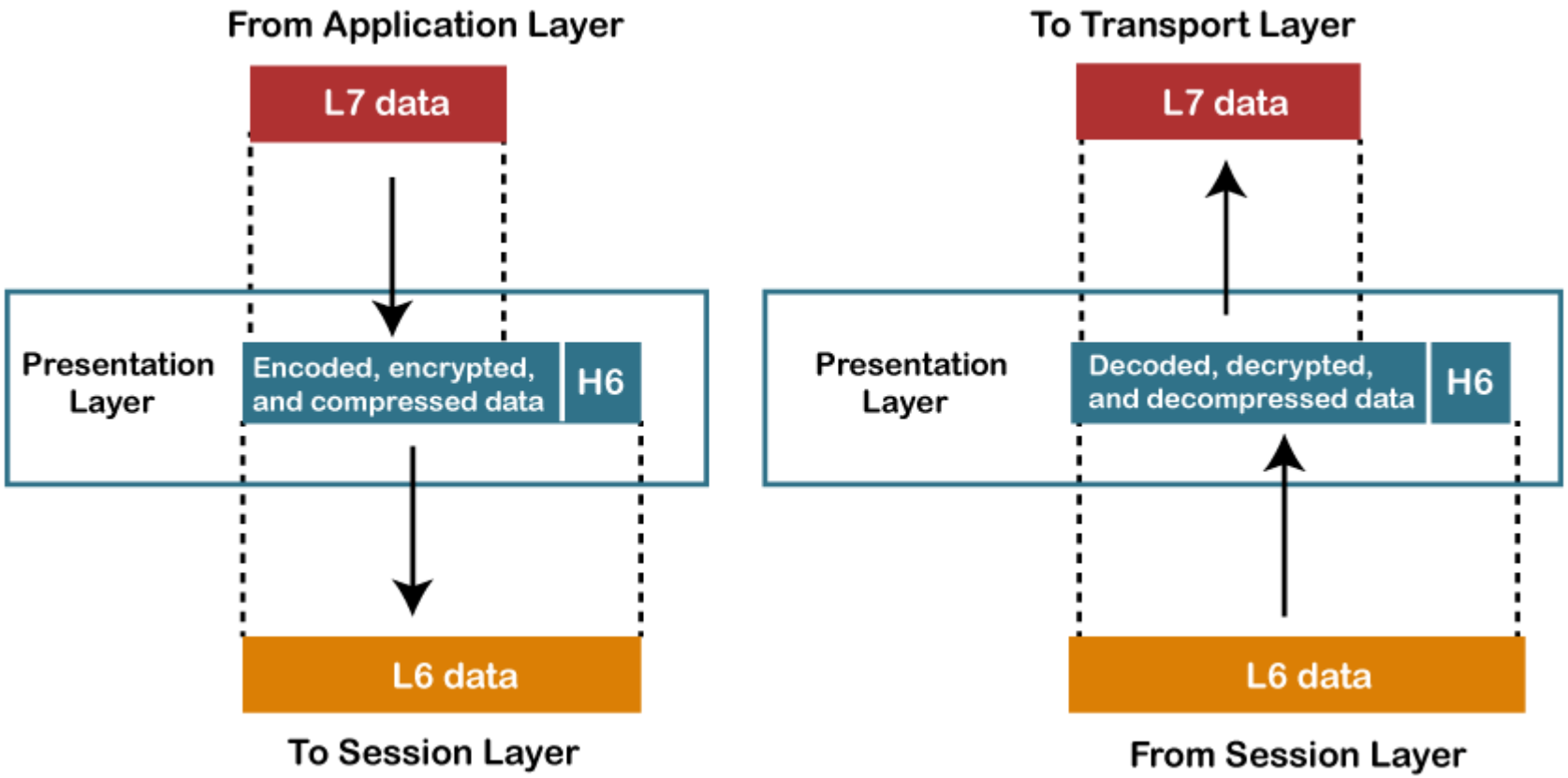
SESSION LAYER

- It is a layer 5 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.
- Functions of Session layer:

  - **Dialog control:** 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.

  - **Synchronization:** 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.

PRESENTATION LAYER



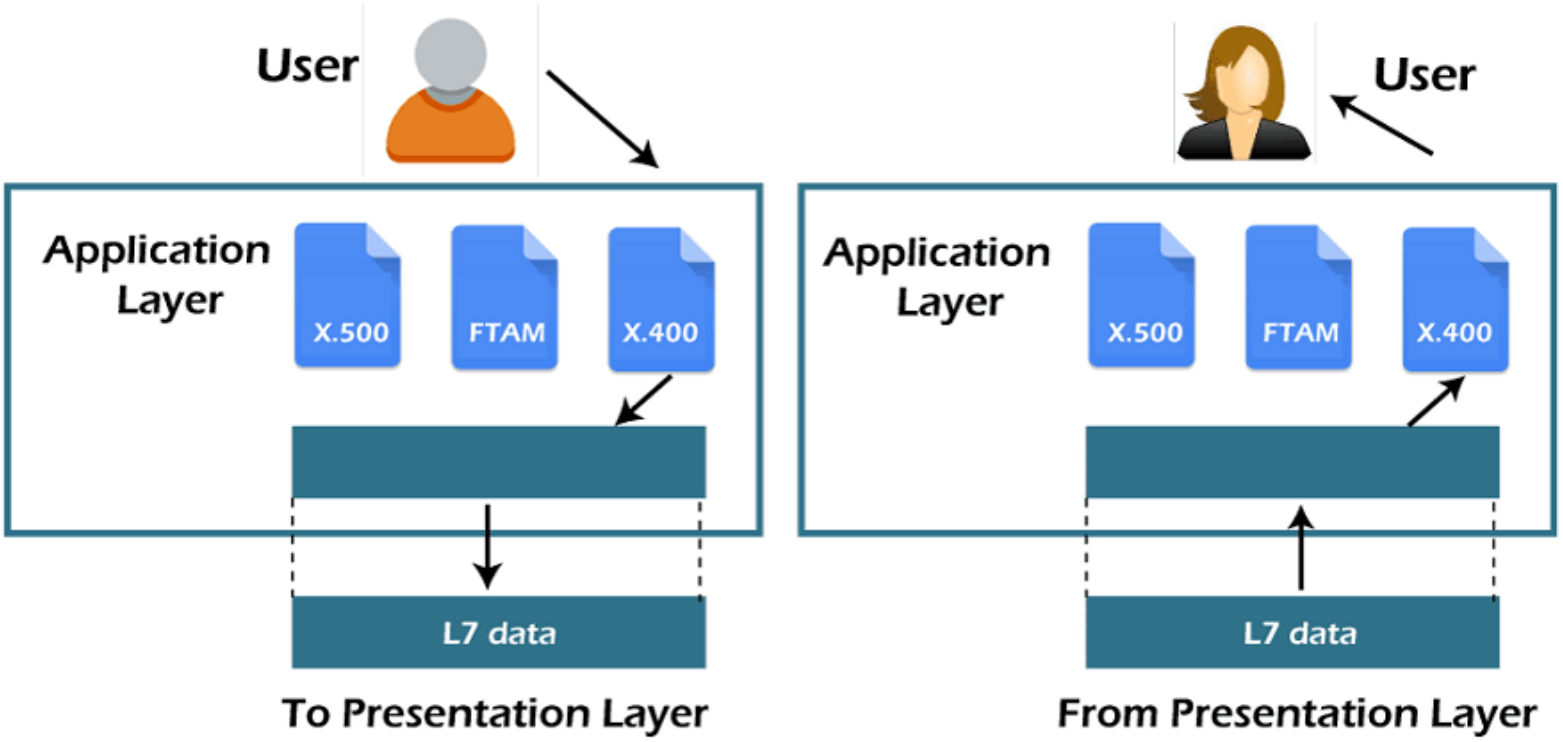
PRESENTATION LAYER

- 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.

PRESENTATION LAYER: FUNCTIONS

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. 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.
- **Encryption:** 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.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

APPLICATION LAYER



APPLICATION LAYER

- An application layer serves as a window for users and application processes 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 functions.
- This layer provides the network services to the end-users.
- **Functions of Application layer:**
  - **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
  - **Mail services:** An application layer provides the facility for email forwarding and storage.
  - **Directory services**: An application provides the distributed database sources and is used to provide that global information about various objects.

NETWORK TOPOLOGY

- Topology defines the structure of the network of how all the components are interconnected to each other.

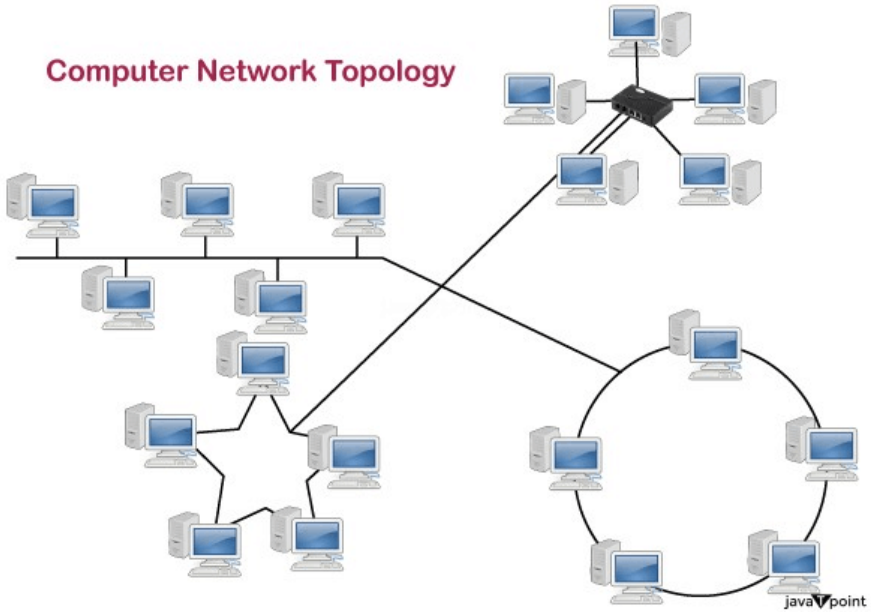
- There are two types of topology:

  - physical
  - logical topology.

NETWORK TOPOLOGY

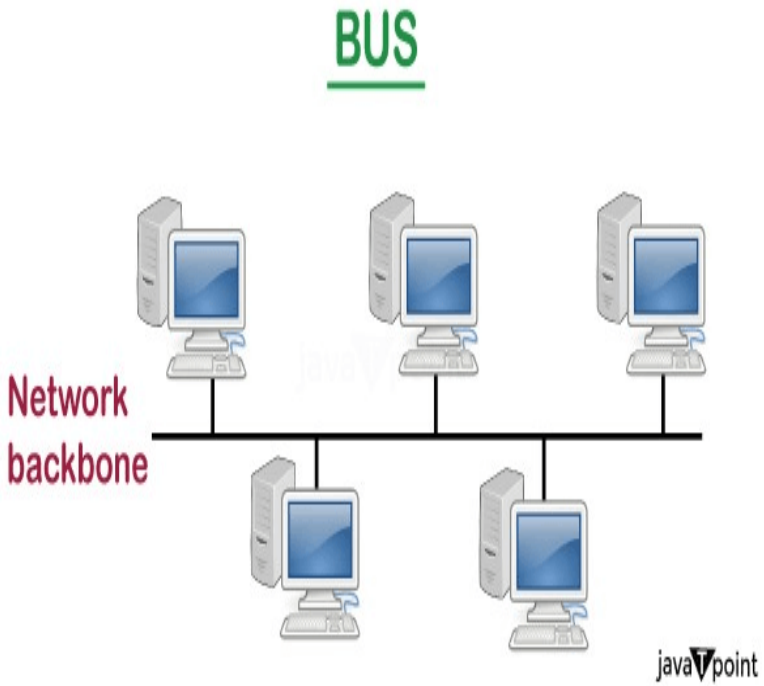
- Physical topology is the geometric representation of all the nodes in a network.

- There are six types of network topology which are Bus Topology, Ring Topology, Tree Topology, Star Topology, Mesh Topology, and Hybrid Topology.



BUS TOPOLOGY

- 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.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.

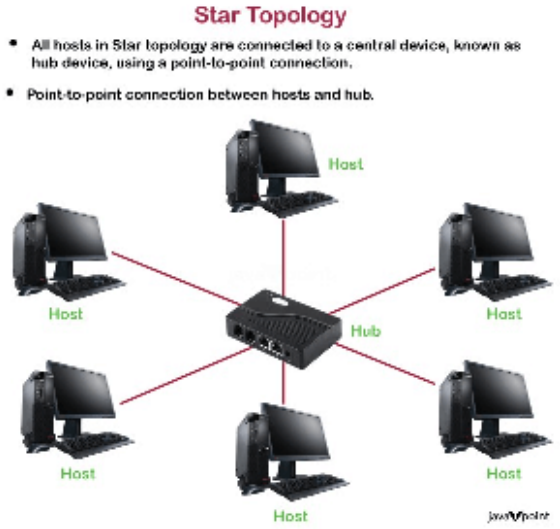


RING TOPOLOGY

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.
  - **Token passing:** It is a network access method in which token is passed from one node to another node.
  - **Token:** It is a frame that circulates around the network.

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.

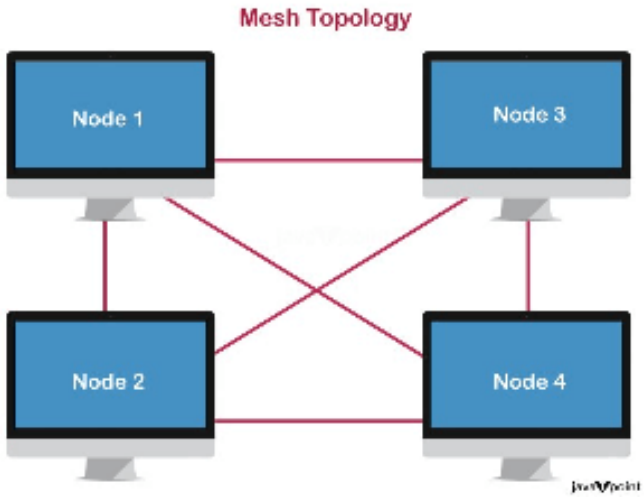


TREE TOPOLOGY

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

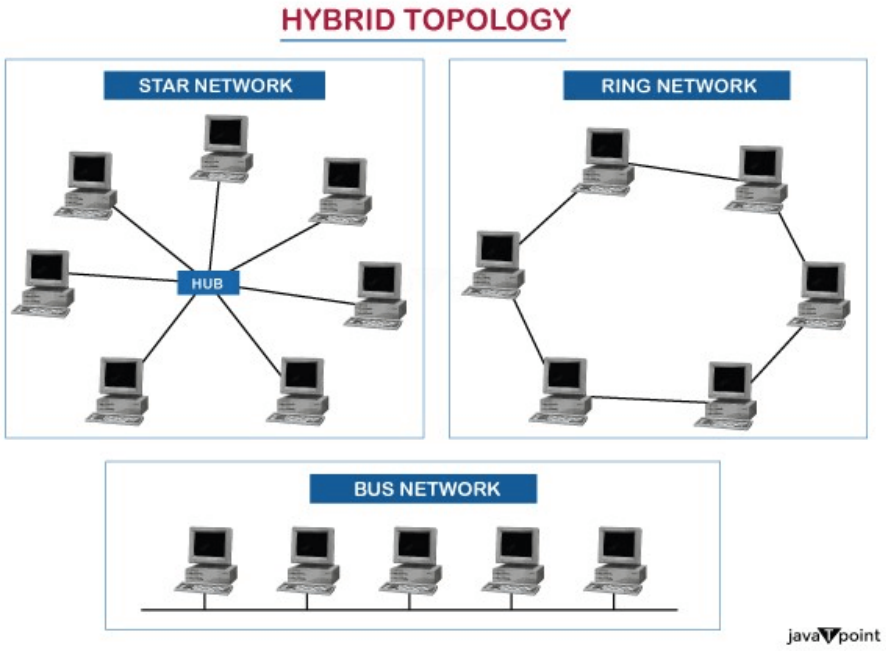
MESH TOPOLOGY

- Mesh technology 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.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula: **Number of cables = (n*(n-1))/2;**
- Where n is the number of nodes that represents the network.



HYBRID TOPOLOGY

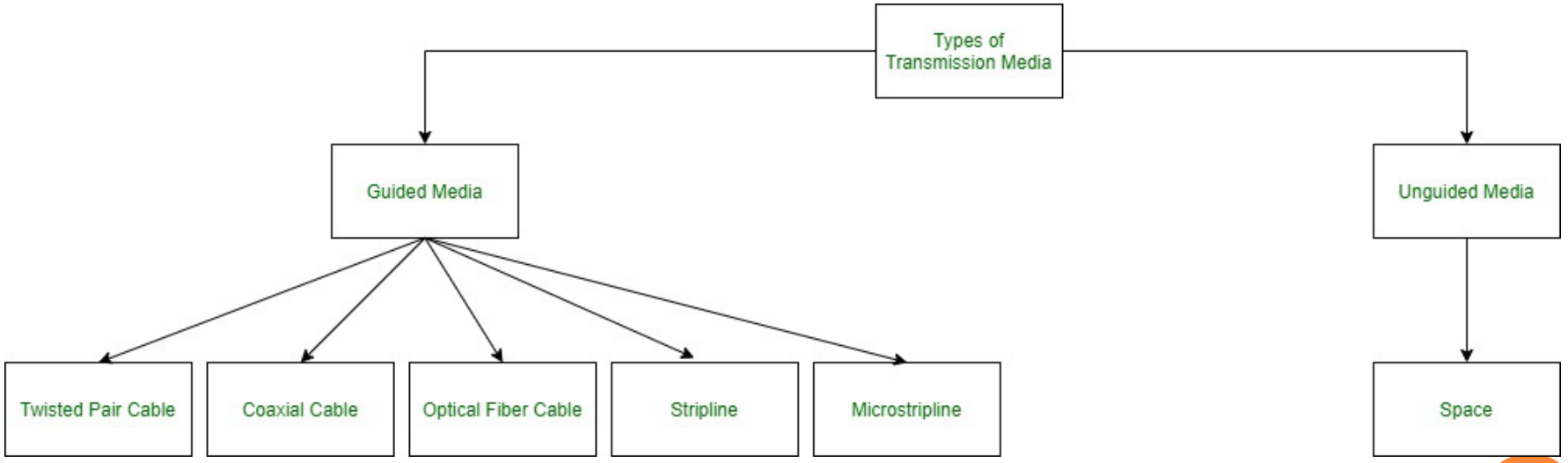
- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.



TRANSMISSION MEDIA

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another.

Transmission Media is broadly classified into the following types:



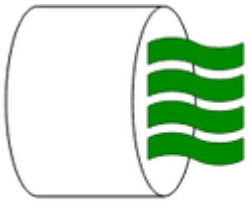
GUIDED MEDIA

- It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

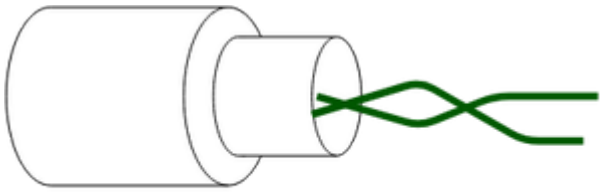
- Features:
  - High Speed
  - Secure
  - Used for comparatively shorter distances

GUIDED MEDIA TYPES

- **Twisted Pair Cable** – It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:
- **Unshielded Twisted Pair (UTP):** 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 applications.
- **Shielded Twisted Pair (STP):** This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



Unshielded Twisted Pair



Shielded Twisted Pair

GUIDED MEDIA TYPES

- **Coaxial Cable**: It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

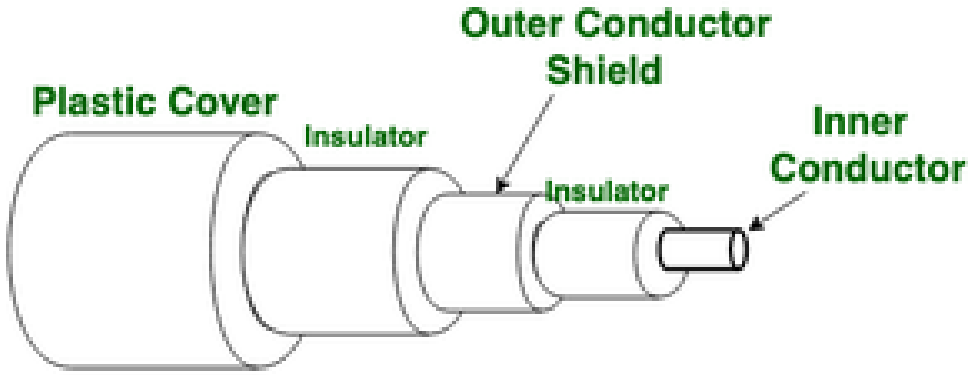


Figure of Coaxial Cable

GUIDED MEDIA TYPES

- **Optical Fiber Cable**: It uses the concept of refraction of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.
- The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

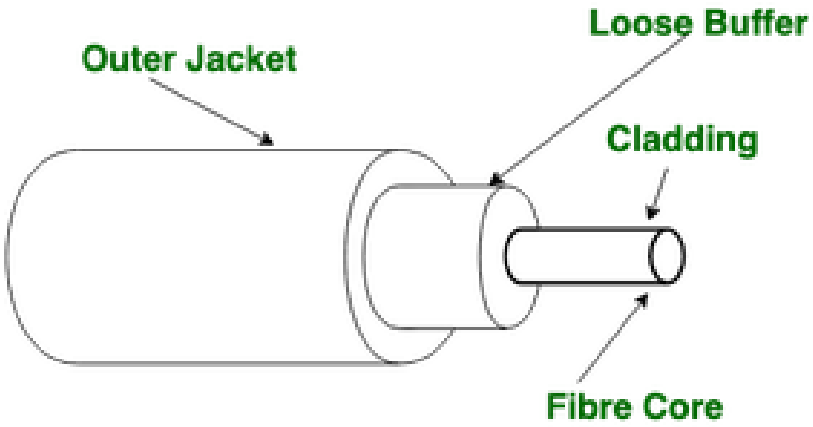


Figure of Optical Fibre Cable

GUIDED MEDIA TYPES

- **Stripline**: Stripline is a transverse electromagnetic (TEM) transmission line medium invented by Robert M. Barrett of the Air Force Cambridge Research Centre in the 1950s. Stripline is the earliest form of the planar transmission line. It uses a conducting material to transmit high-frequency waves it is also called a waveguide. This conducting material is sandwiched between two layers of the ground plane which are usually shorted to provide EMI immunity.

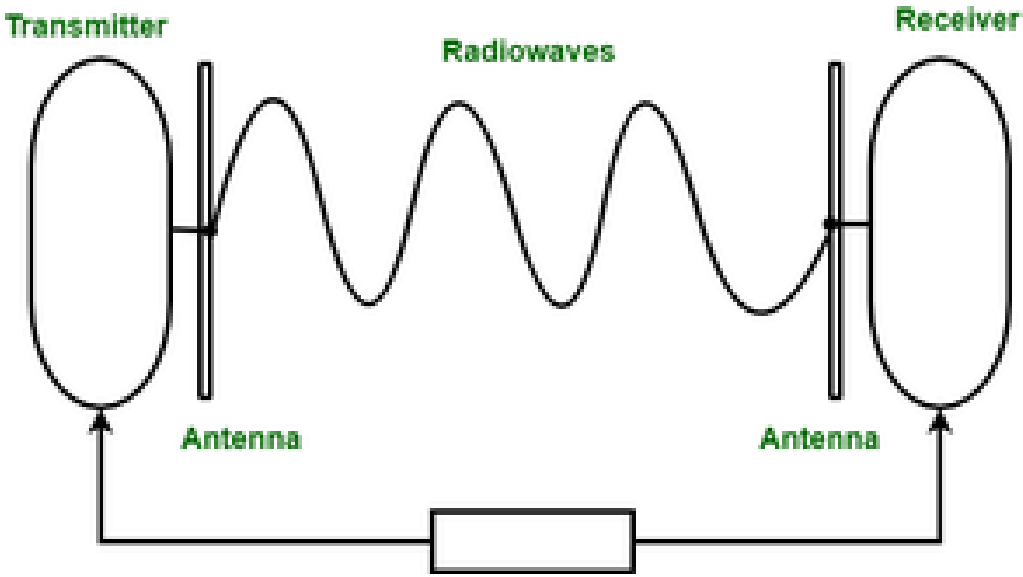
- Microstripline: In this, the conducting material is separated from the ground plane by a layer of dielectric.

UNGUIDED MEDIA TYPES

- It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.
- **Features:**
  - The signal is broadcasted through air
  - Less Secure
  - Used for larger distances
- There are 3 types of Signals transmitted through unguided media:

UNGUIDED MEDIA TYPES

- **Radio waves**: These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission. Further categorized as terrestrial and satellite.



UNGUIDED MEDIA TYPES

- **Microwaves**: It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

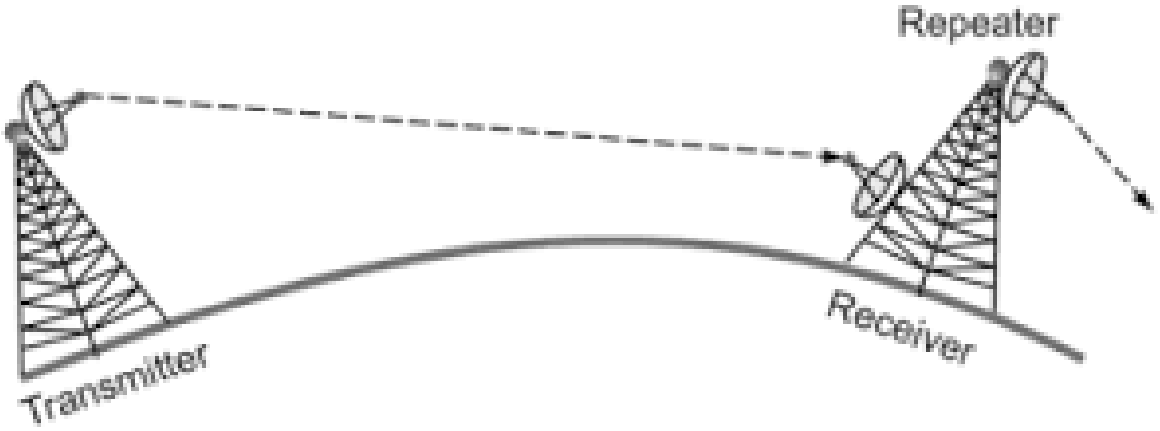
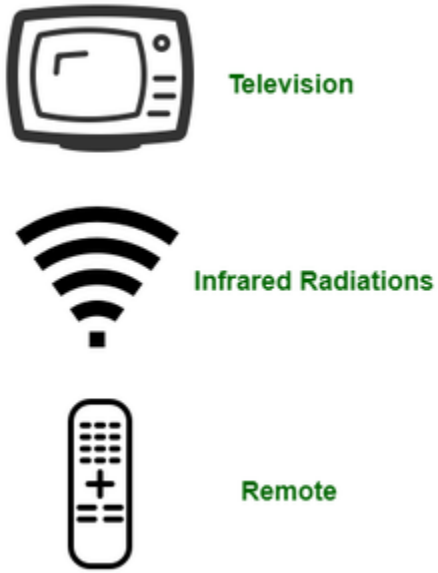


Fig: Microwave Transmission

UNGUIDED MEDIA TYPES

- **Infrared**: Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.



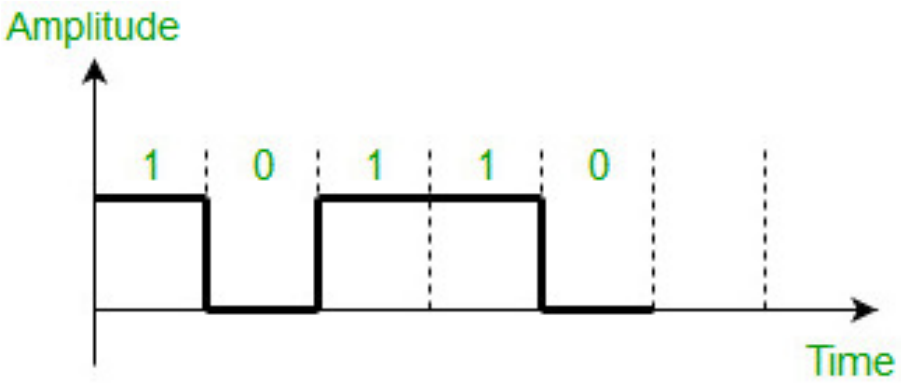
LINE CODING SCHEMES

- **Data** as well as **signals** that represents data can either be digital or analog. **Line coding** is the process of converting **digital data to digital signals**. By this technique we converts a sequence of bits to a digital signal. At the sender side digital data are encoded into a digital signal and at the receiver side the digital data are recreated by decoding the digital signal.
- We can roughly divide line coding schemes into five categories:
  - Unipolar (eg. NRZ scheme).
  - Polar (eg. NRZ-L, NRZ-I, RZ, and Biphase – Manchester and differential Manchester).
  - Bipolar (eg. AMI and Pseudoternary).
  - Multilevel
  - Multitransition

LINE CODING SCHEMES: UNI-POLAR

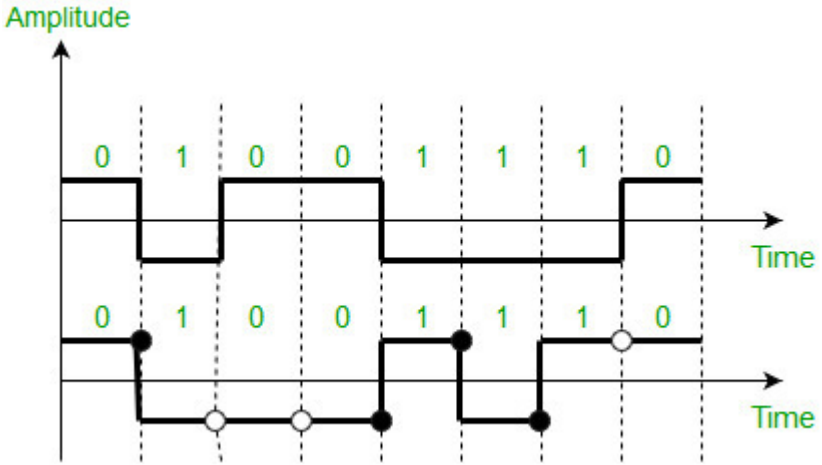
- In this scheme, all the signal levels are either above or below the axis.

- **Non return to zero (NRZ)** – It is unipolar line coding scheme in which positive voltage defines bit 1 and the zero voltage defines bit 0. Signal does not return to zero at the middle of the bit thus it is called NRZ.
- For example: Data =10110.



LINE CODING SCHEMES: POLAR

- In polar schemes, the voltages are on the both sides of the axis.
- **NRZ-L and NRZ-I** – These are somewhat similar to unipolar NRZ scheme but here we use two levels of amplitude (voltages). For **NRZ-L(NRZ-Level)**, the level of the voltage determines the value of the bit, typically binary 1 maps to logic-level high, and binary 0 maps to logic-level low, and for **NRZ-I(NRZ-Invert)**, two-level signal has a transition at a boundary if the next bit that we are going to transmit is a logical 1, and does not have a transition if the next bit that we are going to transmit is a logical 0. **Note** – For NRZ-I we are assuming in the example that previous signal before starting of data set "01001110" was positive. Therefore, there is no transition at the beginning and first bit "0" in current data set "01001110" is starting from +V. Example: Data = 01001110.



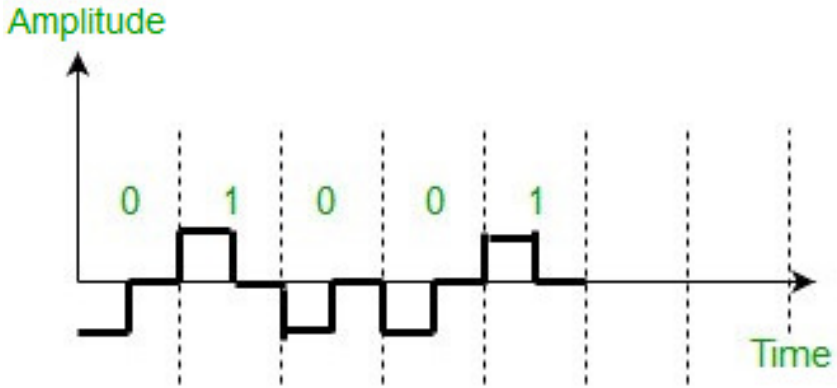
LINE CODING SCHEMES: POLAR

- Comparison between NRZ-L and NRZ-I: Baseline wandering is a problem for both of them, but for NRZ-L it is twice as bad as compared to NRZ-I.
- This is because of transition at the boundary for NRZ-I (if the next bit that we are going to transmit is a logical 1).
- Similarly self-synchronization problem is similar in both for long sequence of 0's, but for long sequence of 1's it is more severe in NRZ-L.

LINE CODING SCHEMES: POLAR

- **Return to zero (RZ)** – One solution to NRZ problem is the RZ scheme, which uses three values positive, negative, and zero. In this scheme signal goes to 0 in the middle of each bit. **Note** – The logic we are using here to represent data is that for bit 1 half of the signal is represented by +V and half by zero voltage and for bit 0 half of the signal is represented by -V and half by zero voltage. Example: Data = 01001.

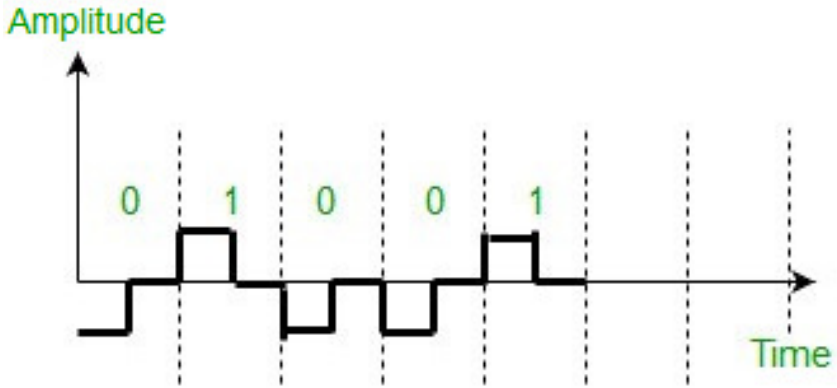
- Main disadvantage of RZ encoding is that it requires greater bandwidth. Another problem is the complexity as it uses three levels of voltage. As a result of all these deficiencies, this scheme is not used today. Instead, it has been replaced by the better-performing Manchester and differential Manchester schemes.



LINE CODING SCHEMES: POLAR

- **Return to zero (RZ)** – One solution to NRZ problem is the RZ scheme, which uses three values positive, negative, and zero. In this scheme signal goes to 0 in the middle of each bit. **Note** – The logic we are using here to represent data is that for bit 1 half of the signal is represented by +V and half by zero voltage and for bit 0 half of the signal is represented by -V and half by zero voltage. Example: Data = 01001.

- Main disadvantage of RZ encoding is that it requires greater bandwidth. Another problem is the complexity as it uses three levels of voltage. As a result of all these deficiencies, this scheme is not used today. Instead, it has been replaced by the better-performing Manchester and differential Manchester schemes.



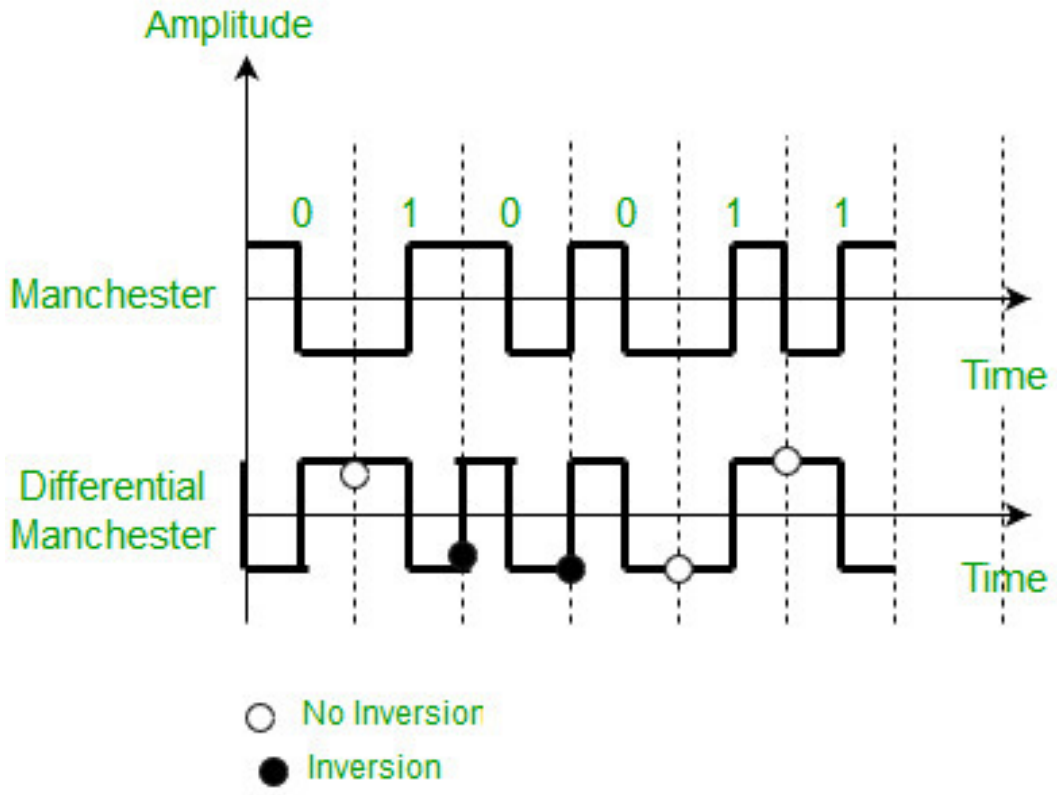
LINE CODING SCHEMES: POLAR

- **Biphase (Manchester and Differential Manchester)** – Manchester encoding is somewhat combination of the RZ (transition at the middle of the bit) and NRZ-L schemes. The duration of the bit is divided into two halves. The voltage remains at one level during the first half and moves to the other level in the second half. The transition at the middle of the bit provides synchronization. Differential Manchester is somewhat combination of the RZ and NRZ-I schemes. There is always a transition at the middle of the bit but the bit values are determined at the beginning of the bit. If the next bit is 0, there is a transition, if the next bit is 1, there is no transition.

- **Note – 1.** The logic we are using here to represent data using Manchester is that for bit 1 there is transition form -V to +V volts in the middle of the bit and for bit 0 there is transition from +V to -V volts in the middle of the bit. **2.** For differential Manchester we are assuming in the example that previous signal before starting of data set "010011" was positive. Therefore there is transition at the beginning and first bit "0" in current data set "010011" is starting from -V. Example: Data = 010011.

- The Manchester scheme overcomes several problems associated with NRZ-L, and differential Manchester overcomes several problems associated with NRZ-I as there is no baseline wandering and no DC component because each bit has a positive and negative voltage contribution. Only limitation is that the minimum bandwidth of Manchester and differential Manchester is twice that of NRZ.

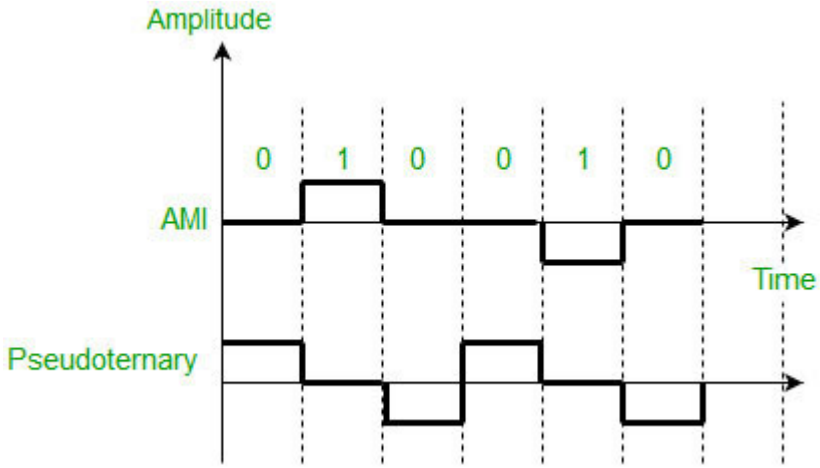
LINE CODING SCHEMES: POLAR



LINE CODING SCHEMES: BIPOLAR

- In this scheme there are three voltage levels positive, negative, and zero. The voltage level for one data element is at zero, while the voltage level for the other element alternates between positive and negative.
- **Alternate Mark Inversion (AMI)** – A neutral zero voltage represents binary 0. Binary 1's are represented by alternating positive and negative voltages.
- **Pseudoternary** – Bit 1 is encoded as a zero voltage and the bit 0 is encoded as alternating positive and negative voltages i.e., opposite of AMI scheme. Example: Data = 010010.

- The bipolar scheme is an alternative to NRZ. This scheme has the same signal rate as NRZ but there is no DC component as one bit is represented by voltage zero and other alternates every time.



CIRCUIT SWITCHING

- Circuit switching is a communication method where a dedicated communication path, or circuit, is established between two devices before data transmission begins.
- The circuit remains dedicated to the communication for the duration of the session, and no other devices can use it while the session is in progress.
- Circuit switching is commonly used in voice communication and some types of data communication.

PACKET SWITCHING

- Packet switching is a communication method where data is divided into smaller units called packets and transmitted over the network.
- Each packet contains the source and destination addresses, as well as other information needed for routing.
- The packets may take different paths to reach their destination, and they may be transmitted out of order or delayed due to network congestion.

MULTIPLEXING

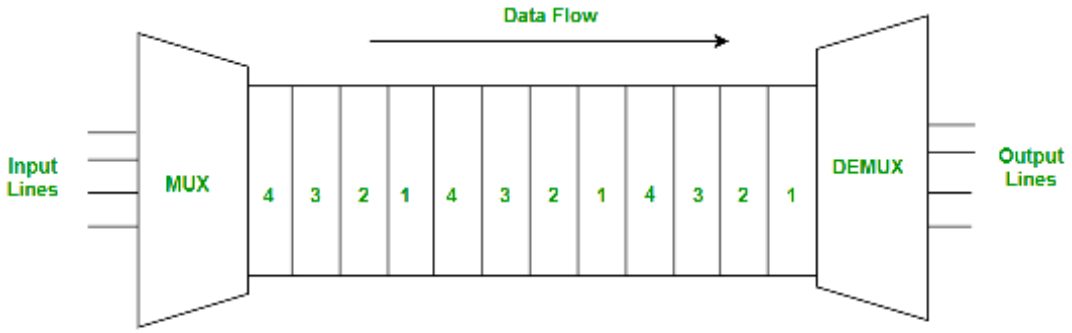
- **Multiplexing** is the sharing of a medium or bandwidth. It is the process in which multiple signals coming from multiple sources are combined and transmitted over a single communication/physical line.

MULTIPLEXING: TYPES

- Frequency Division Multiplexing (FDM)
- Time-Division Multiplexing (TDM)
- Wavelength Division Multiplexing (WDM)
- Code-division multiplexing (CDM)
- Space-division multiplexing (SDM)

TDM

- Time-division multiplexing is defined as a type of multiplexing wherein FDM, instead of sharing a portion of the bandwidth in the form of channels, in TDM, time is shared. Each connection occupies a portion of time in the link.
- In Time Division Multiplexing, all signals operate with the same frequency (bandwidth) at different times.
- There are two types of Time Division Multiplexing :
- Synchronous Time Division Multiplexing
- Statistical (or Asynchronous) Time Division Multiplexing

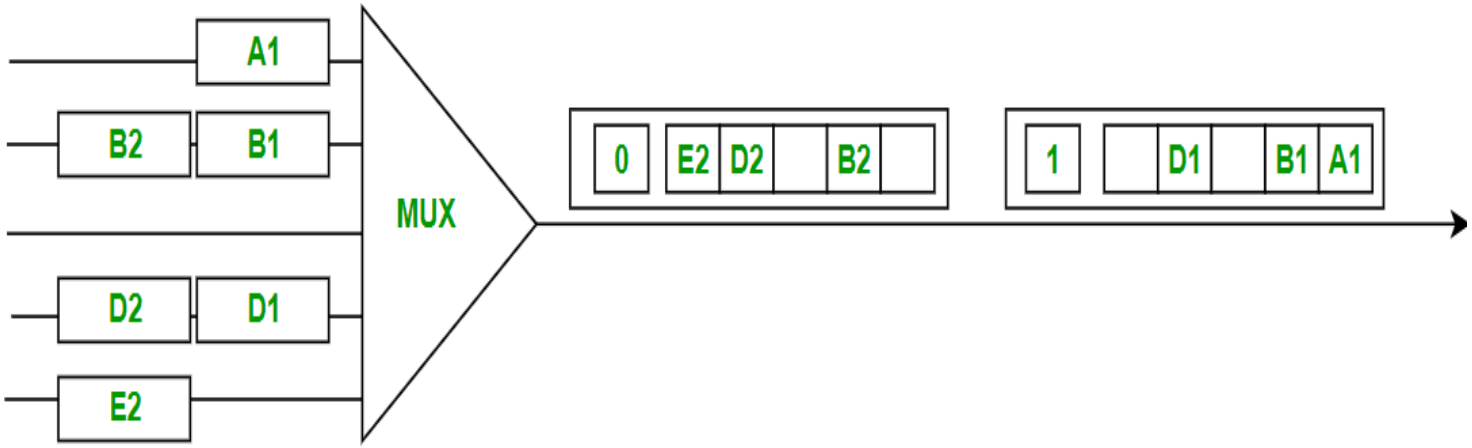


SYNCHRONOUS TDM

Synchronous TDM :

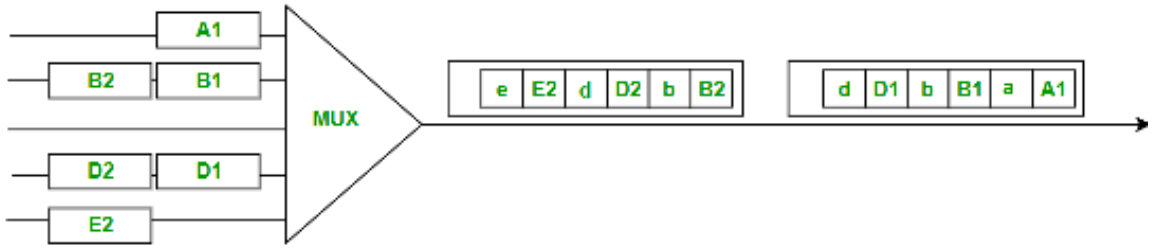
- Synchronous TDM is a type of Time Division Multiplexing where the input frame already has a slot in the output frame. Time slots are grouped into frames. One frame consists of one cycle of time slots.
- Synchronous TDM is not efficient because if the input frame has no data to send, a slot remains empty in the output frame.
- In synchronous TDM, we need to mention the synchronous bit at the beginning of each frame.

SYNCHRONOUS TDM



STATISTICAL (OR ASYNCHRONOUS) TDM

- Statistical TDM is a type of Time Division Multiplexing where the output frame collects data from the input frame till it is full, not leaving an empty slot like in Synchronous TDM.
- In statistical TDM, we need to include the address of each particular data in the slot that is being sent to the output frame.
- Statistical TDM is a more efficient type of time-division multiplexing as the channel capacity is fully utilized and improves the bandwidth efficiency.

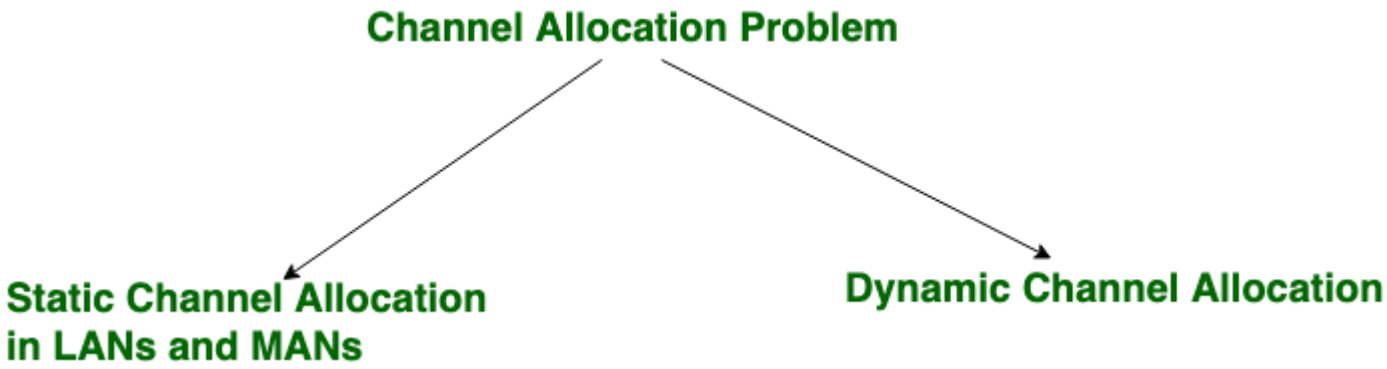


CHANNEL ALLOCATION

- **Channel allocation** is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place.
- If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion.
- If the number of users are small and don't vary at times, then Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

CHANNEL ALLOCATION CONT'D..

- Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.



STATIC CHANNEL ALLOCATION

- It is the classical or traditional approach of allocating a single channel among multiple competing users using Frequency Division Multiplexing (FDM). if there are N users, the frequency channel is divided into N equal sized portions (bandwidth), each user being assigned one portion. since each user has a private frequency band, there is no interference between users.
- However, it is not suitable in case of a large number of users with variable bandwidth requirements.
  It is not efficient to divide into fixed number of chunks.

T = 1/(U*C-L) T(FDM) = N*T(1/U(C/N)-L/N)
Where,

T = mean time delay,
C = capacity of channel,
L = arrival rate of frames,
1/U = bits/frame,
N = number of sub channels,
T(FDM) = Frequency Division Multiplexing Time

DYNAMIC CHANNEL ALLOCATION

- In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized.
- This allocation scheme optimizes bandwidth usage and results is faster transmissions.
- Dynamic channel allocation is further divided into: *Centralized Allocation and Distributed Allocation*

MULTIPLE ACCESS PROTOCOLS

- The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-
  - Data Link Control
  - Multiple Access Control

DATA LINK CONTROL

- The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control.

MULTIPLE ACCESS CONTROL

- If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously.

- Hence multiple access protocols are required to decrease collision and avoid crosstalk.

- For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created(data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.

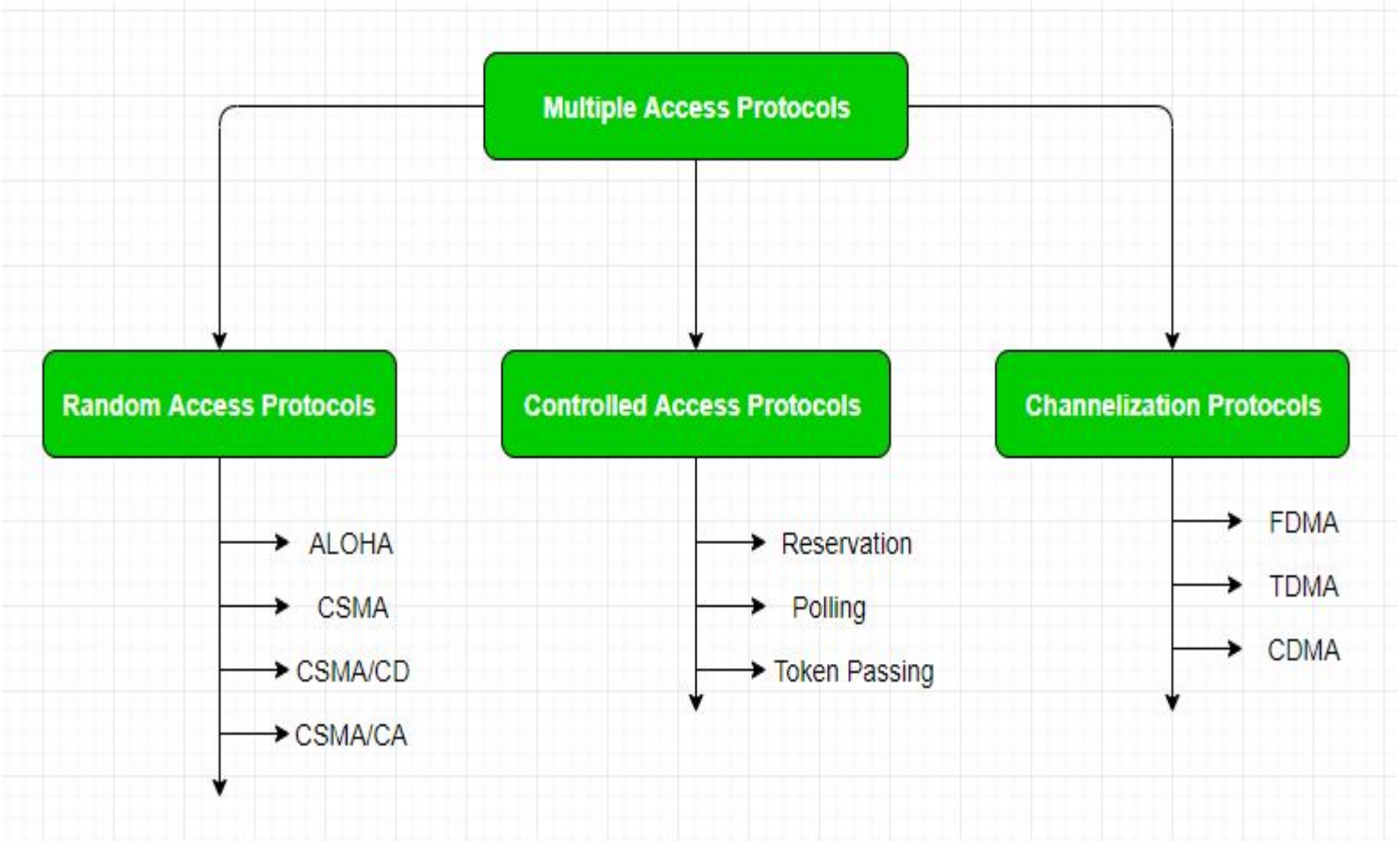
MULTIPLE ACCESS CONTROL

- If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously.

- Hence multiple access protocols are required to decrease collision and avoid crosstalk.

- For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created(data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.

MULTIPLE ACCESS PROTOCOLS



RANDOM ACCESS PROTOCOLS

- In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:

- There is no fixed time for sending data
- There is no fixed sequence of stations sending data

RANDOM ACCESS PROTOCOL: ALOHA

(a) **ALOHA –** It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

It is divided into two categories:

- Pure ALOHA
- Slotted ALOHA

RANDOM ACCESS PROTOCOL: PURE ALOHA

When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.

```
Vulnerable Time = 2* Frame transmission
time
Throughput = G exp{-2*G} Maximum throughput
= 0.184 for G=0.5
```

RANDOM ACCESS PROTOCOL: SLOTTED ALOHA

It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

```
Vulnerable Time = Frame transmission time
Throughput = G exp{-*G}
Maximum throughput = 0.368 for G=1
```

RANDOM ACCESS PROTOCOL: CSMA

(b) CSMA – Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay.

For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

RANDOM ACCESS PROTOCOL: CSMA ACCESS MODES

- **1-persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- **O-persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

RANDOM ACCESS PROTOCOL: CSMA/CD & CSMA/CA

- **(c) CSMA/CD** – Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected.
- **(d) CSMA/CA** – Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.

RANDOM ACCESS PROTOCOL: CSMA/CD & CSMA/CA

- CSMA/CA avoids collision by:
  - **Interframe space** – Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
  - **Contention Window** – It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
  - **Acknowledgement** – The sender re-transmits the data if acknowledgement is not received before time-out.

CONTROLLED ACCESS PROTOCOL

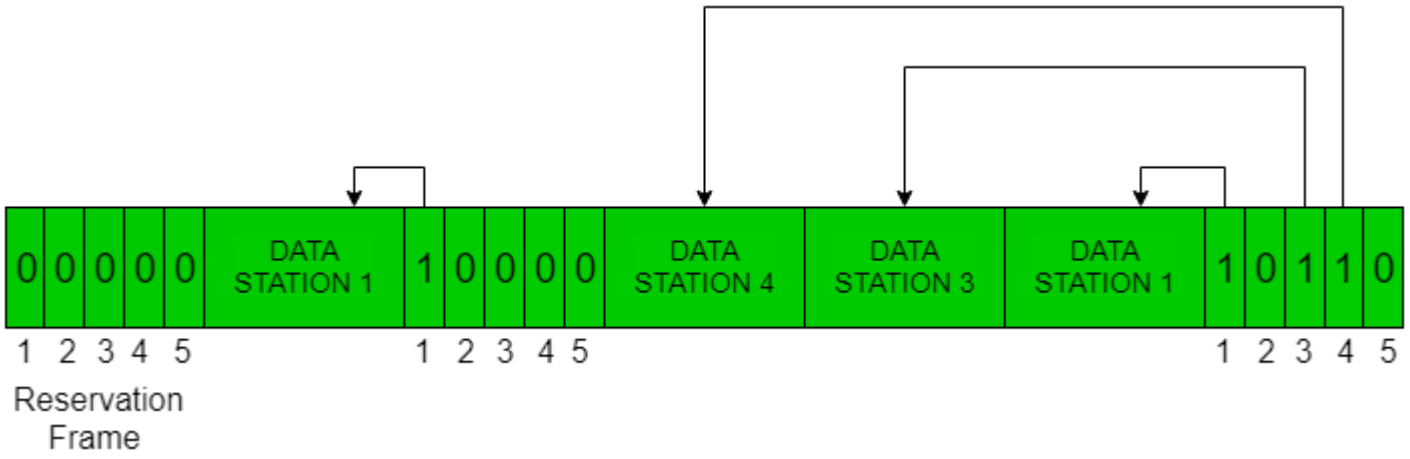
- In this, the data is sent by that station which is approved by all other stations.
- In controlled access, the stations seek information from one another to find which station has the right to send. It allows only one node to send at a time, to avoid the collision of messages on a shared medium. The three controlled-access methods are:
  - Reservation
  - Polling
  - Token Passing

CONTROLLED ACCESS PROTOCOL: RESERVATION

- In the reservation method, a station needs to make a reservation before sending data.
- The timeline has two kinds of periods:
  - Reservation interval of fixed time length
  - Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.
- In general, i th station may announce that it has a frame to send by inserting a 1 bit into i th slot. After all N slots have been checked, each station knows which stations wish to transmit.
- The stations which have reserved their slots transfer their frames in that order.
- After data transmission period, next reservation interval begins.
- Since everyone agrees on who goes next, there will never be any collisions.

CONTROLLED ACCESS PROTOCOL: RESERVATION

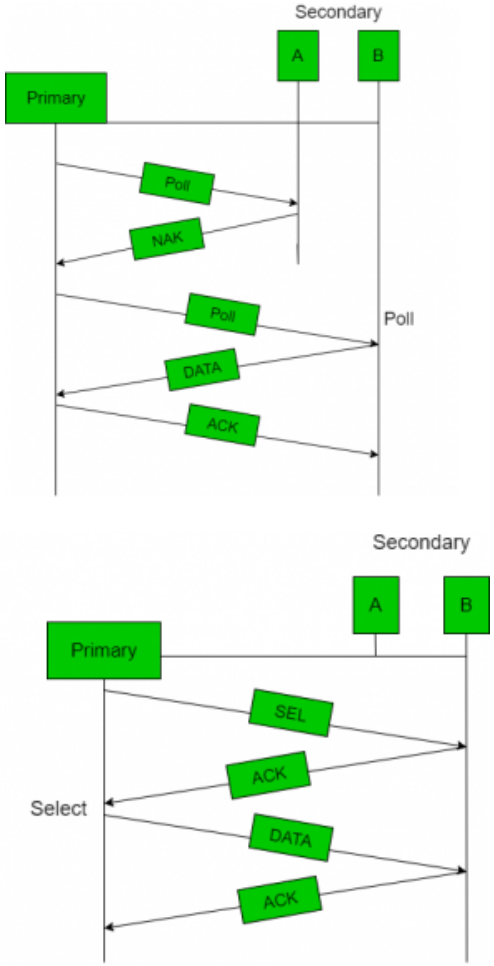
- The following figure shows a situation with five stations and a five-slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.



CONTROLLED ACCESS PROTOCOL: POLLING

- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.
- Although all nodes receive the message the addressed one responds to it and sends data if any. If there is no data, usually a “poll reject”(NAK) message is sent back.
- Problems include high overhead of the polling messages and high dependence on the reliability of the controller.

CONTROLLED ACCESS PROTOCOL: POLLING



CONTROLLED ACCESS PROTOCOL: POLLING

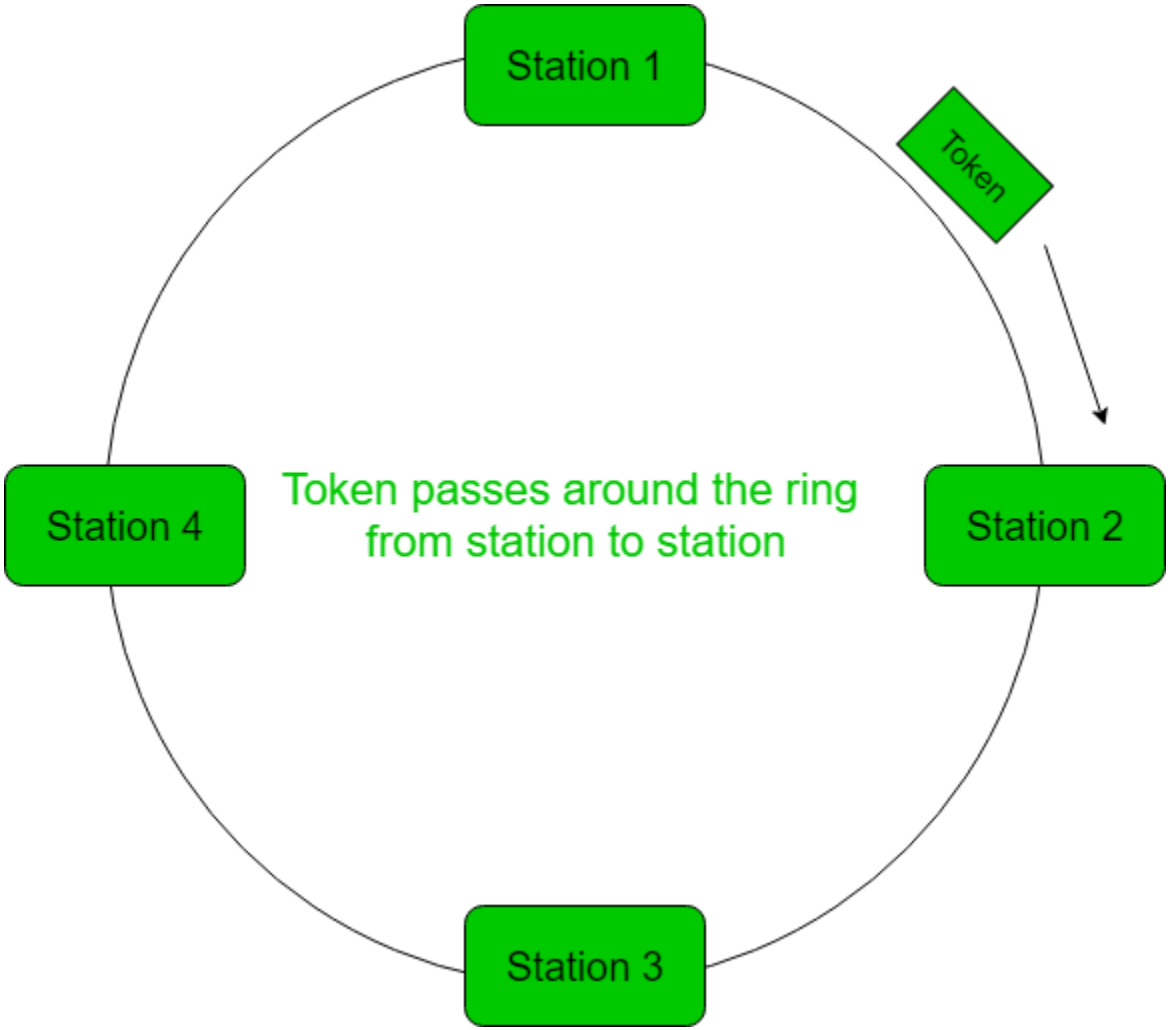
- **Efficiency** Let T_{poll} be the time for polling and T_t be the time required for transmission of data. Then,

- Efficiency = $T_t/(T_t + T_{poll})$

CONTROLLED ACCESS PROTOCOL: TOKEN PASSING

- In token passing scheme, the stations are connected logically to each other in form of ring and access to stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas incase of Token bus, each station uses the bus to send the token to the next station in some predefined order.
- In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.
- After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbors and the other N – 1 stations to send a frame, if they have one.
- There exists problems like duplication of token or token is lost or insertion of new station, removal of a station, which need be tackled for correct and reliable operation of this scheme.

CONTROLLED ACCESS PROTOCOL: TOKEN PASSING



CONTROLLED ACCESS PROTOCOL: TOKEN PASSING

- **Performance** of token ring can be concluded by 2 parameters:-
- **Delay**, is a measure of time between when a packet is ready and when it is delivered. So, the average time (delay) required to send a token to the next station = a/N.
- **Throughput**, which is a measure of successful traffic.

Throughput, **S = 1/(1 + a/N) for a<1**
and
S = 1/{a(1 + 1/N)} for a>1.
Where,

N = number of stations
a = T_p/T_t (T_p = propagation delay and T_t = transmission delay)

CHANNELIZATION

- In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.
- **Frequency Division Multiple Access (FDMA)** – The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.
- **Time Division Multiple Access (TDMA)** – In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.

CHANNELIZATION

- **Code Division Multiple Access (CDMA)** – One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly, data from different stations can be transmitted simultaneously in different code languages.
- **Orthogonal Frequency Division Multiple Access (OFDMA)** – In OFDMA the available bandwidth is divided into small subcarriers in order to increase the overall performance, Now the data is transmitted through these small subcarriers. it is widely used in the 5G technology.
- **Spatial Division Multiple Access (SDMA)** – SDMA uses multiple antennas at the transmitter and receiver to separate the signals of multiple users that are located in different spatial directions. This technique is commonly used in MIMO (Multiple-Input, Multiple-Output) wireless communication systems.

FEATURES OF MULTIPLE ACCESS PROTOCOLS:

- **Contention-based access:** Multiple access protocols are typically contention-based, meaning that multiple devices compete for access to the communication channel. This can lead to collisions if two or more devices transmit at the same time, which can result in data loss and decreased network performance.
- **Carrier Sense Multiple Access (CSMA):** CSMA is a widely used multiple access protocol in which devices listen for carrier signals on the communication channel before transmitting. If a carrier signal is detected, the device waits for a random amount of time before attempting to transmit to reduce the likelihood of collisions.
- **Collision Detection (CD):** CD is a feature of some multiple access protocols that allows devices to detect when a collision has occurred and take appropriate action, such as backing off and retrying the transmission.
- **Collision Avoidance (CA):** CA is a feature of some multiple access protocols that attempts to avoid collisions by assigning time slots to devices for transmission.
- **Token passing:** Token passing is a multiple access protocol in which devices pass a special token between each other to gain access to the communication channel. Devices can only transmit data when they hold the token, which ensures that only one device can transmit at a time.
- **Bandwidth utilization:** Multiple access protocols can affect the overall bandwidth utilization of a network. For example, contention-based protocols may result in lower bandwidth utilization due to collisions, while token passing protocols may result in higher bandwidth utilization due to the controlled access to the communication channel.

OVERVIEW OF IEEE STANDARDS

- The IEEE Standards in computer networks assure communication and transmission among various devices and gadgets.

- In addition to that, it also ensures that the Internet and its technologies adhere to their set of rules so that networking and communication take place efficiently and appropriately.

OVERVIEW OF IEEE STANDARDS

IEEE standards in CN	Description
IEEE 802	It is used for the overview and architecture of LAN/MAN.
IEEE 802.1	It is used for bridging and management of LAN/MAN.
IEEE 802.2	It is used in Logical Link Control (LLC).
IEEE 802.3	It is used in Ethernet (CSMA/CD access method).
IEEE 802.4	It is used for token passing bus access methods and the physical layer specifications.
IEEE 802.5	It is used for token ring access methods and the physical layer specifications.
IEEE 802.6	It is used in distributed Queue Dual Bus (DQDB) access method and for the physical layer specifications (MAN).
IEEE 802.7	It is used in broadband LAN.
IEEE 802.8	It is used in fiber optics.
IEEE 802.9	It is used in isochronous LANs.
IEEE 802.10	It is used in interoperable LAN/MAN security.
IEEE 802.11	It is used in wireless LAN, MAC, and Physical layer specifications.
IEEE 802.12	It is used in the demand-priority access method, in the physical layer, and in repeater specifications.

OVERVIEW OF IEEE STANDARDS CONT'D…

IEEE standards in CN	Description
IEEE 802.13	It is not used.
IEEE 802.14	It is used in cable modems (not used now).
IEEE 802.15	It is used in WPAN (Wireless Personal Area Network).
IEEE 802.16	It is used in Wireless MAN (Wireless Metropolitan Area Network).
IEEE 802.17	It is used in RPR access (Resilient Packet Ring).
IEEE 802.13	It is not used.

DATA LINK LAYER

- The data link layer is the second layer from the bottom in the OSI (Open System Interconnection) network architecture model.
- It is responsible for the node-to-node delivery of data.
- Its major role is to ensure error-free transmission of information.

DATA LINK SUB-LAYERS

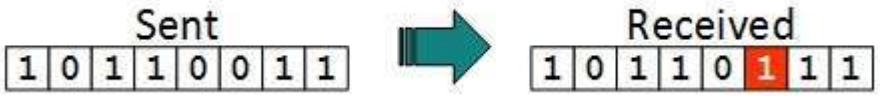
- **Logical Link Control (LLC)**
  - This sublayer of the data link layer deals with multiplexing, the flow of data among applications and other services, and LLC is responsible for providing error messages and acknowledgments as well.
- **Media Access Control (MAC)**
  - MAC sublayer manages the device's interaction, responsible for addressing frames, and also controls physical media access.

ERROR DETECTION

- **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.
- Data (Implemented either at the Data link layer or Transport Layer of the OSI Model) may get scrambled by noise or get corrupted whenever a message is transmitted. To prevent such errors, error-detection codes are added as extra data to digital messages. This helps in detecting any errors that may have occurred during message transmission.

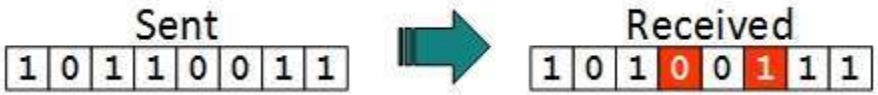
TYPES OF ERRORS

- **Single bit error**



In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



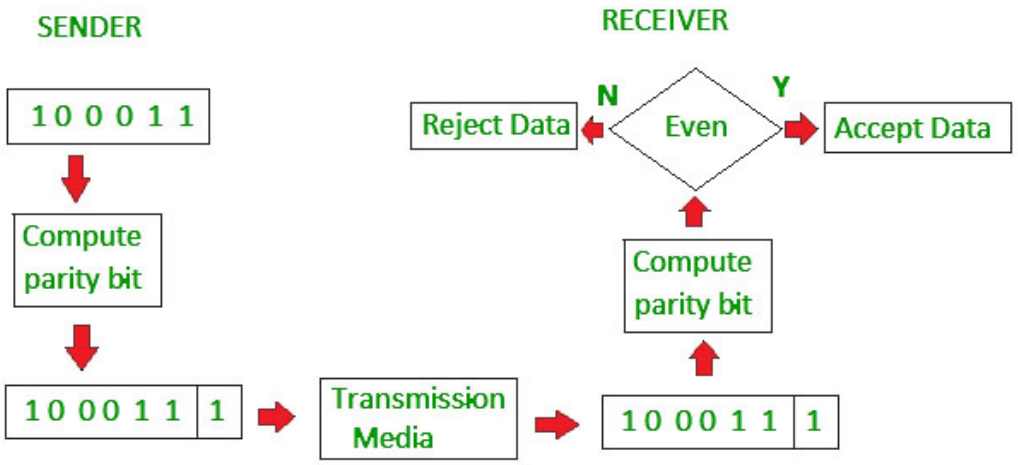
Frame is received with more than one bits in corrupted state

- **Burst error**

Frame contains more than1 consecutive bits corrupted.

ERROR DETECTION: SINGLE 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
- This scheme makes the total number of 1's even, that is why it is called even parity checking.



ERROR DETECTION: SINGLE PARITY CHECK

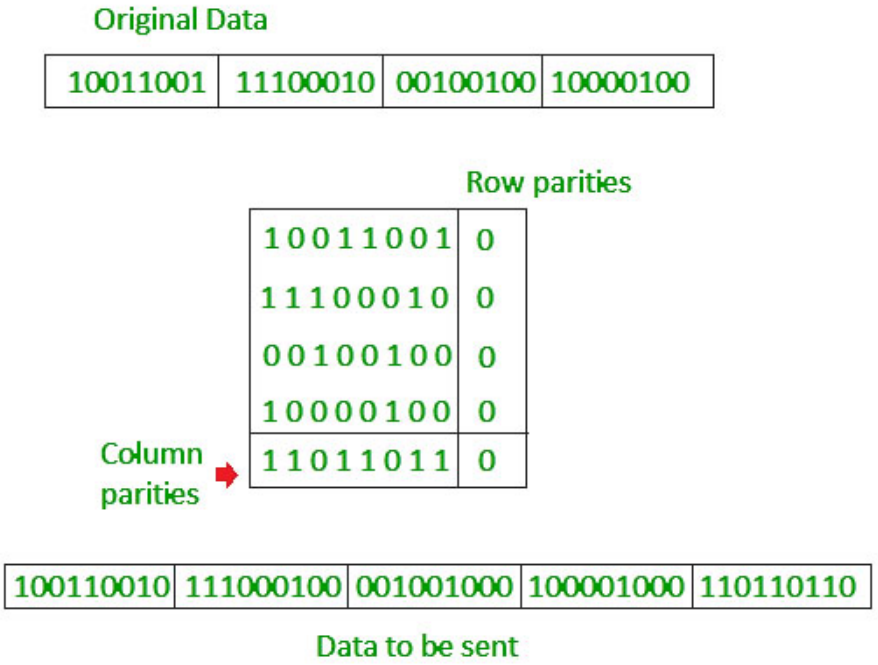
Disadvantages

- Single Parity check is not able to detect even no. of bit error.
- **For example,** the Data to be transmitted is **101010**. Codeword transmitted to the receiver is 1010101 (we have used even parity).

- Let's assume that during transmission, two of the bits of code word flipped to 1111101.
  On receiving the code word, the receiver finds the no. of ones to be even and hence **no error,** *which is a wrong assumption.*

ERROR DETECTION: TWO-DIMENSIONAL PARITY CHECK

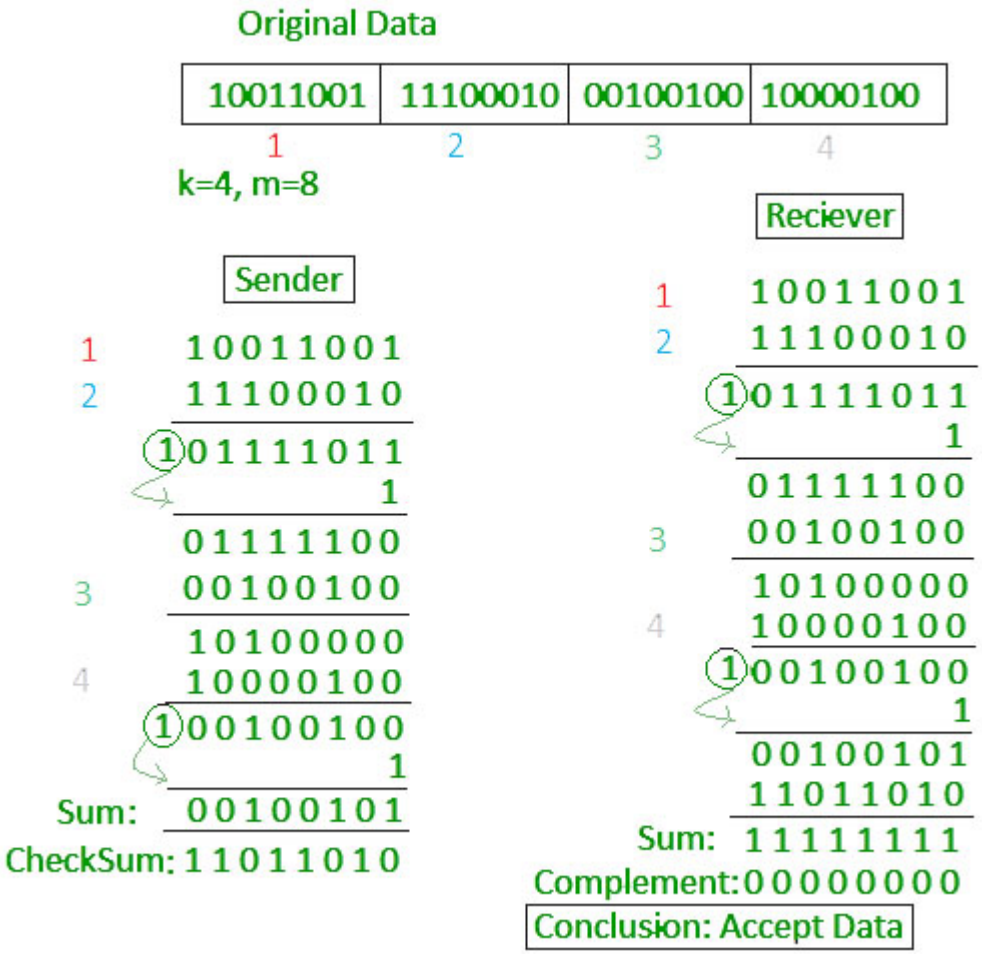
- **Two-dimensional Parity check** bits are calculated for each row, which is equivalent to a simple parity check bit.
- Parity check bits are also calculated for all columns, then both are sent along with the data.
- At the receiving end, these are compared with the parity bits calculated on the received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



ERROR DETECTION: CHECKSUM

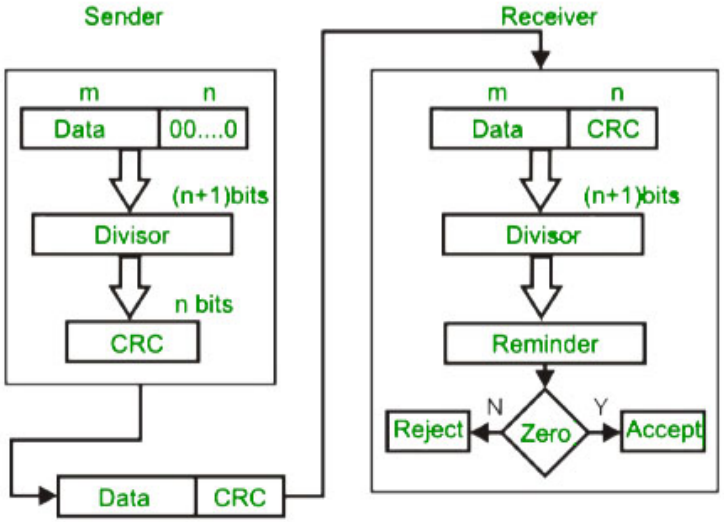
- Checksum error detection is a method used to identify errors in transmitted data. The process involves dividing the data into equally sized segments and using a 1's complement to calculate the sum of these segments. The calculated sum is then sent along with the data to the receiver. At the receiver's end, the same process is repeated and if all zeroes are obtained in the sum, it means that the data is correct.
- **Checksum – Operation at Sender's Side**
  - Firstly, the data is divided into k segments each of m bits.
  - On the sender's end, the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
  - The checksum segment is sent along with the data segments.
- **Checksum – Operation at Receiver's Side**
  - At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
  - If the result is zero, the received data is accepted; otherwise discarded
- **Disadvantages**
  - If one or more bits of a segment are damaged and the corresponding bit or bits of opposite value in a second segment are also damaged.

CHECKSUM

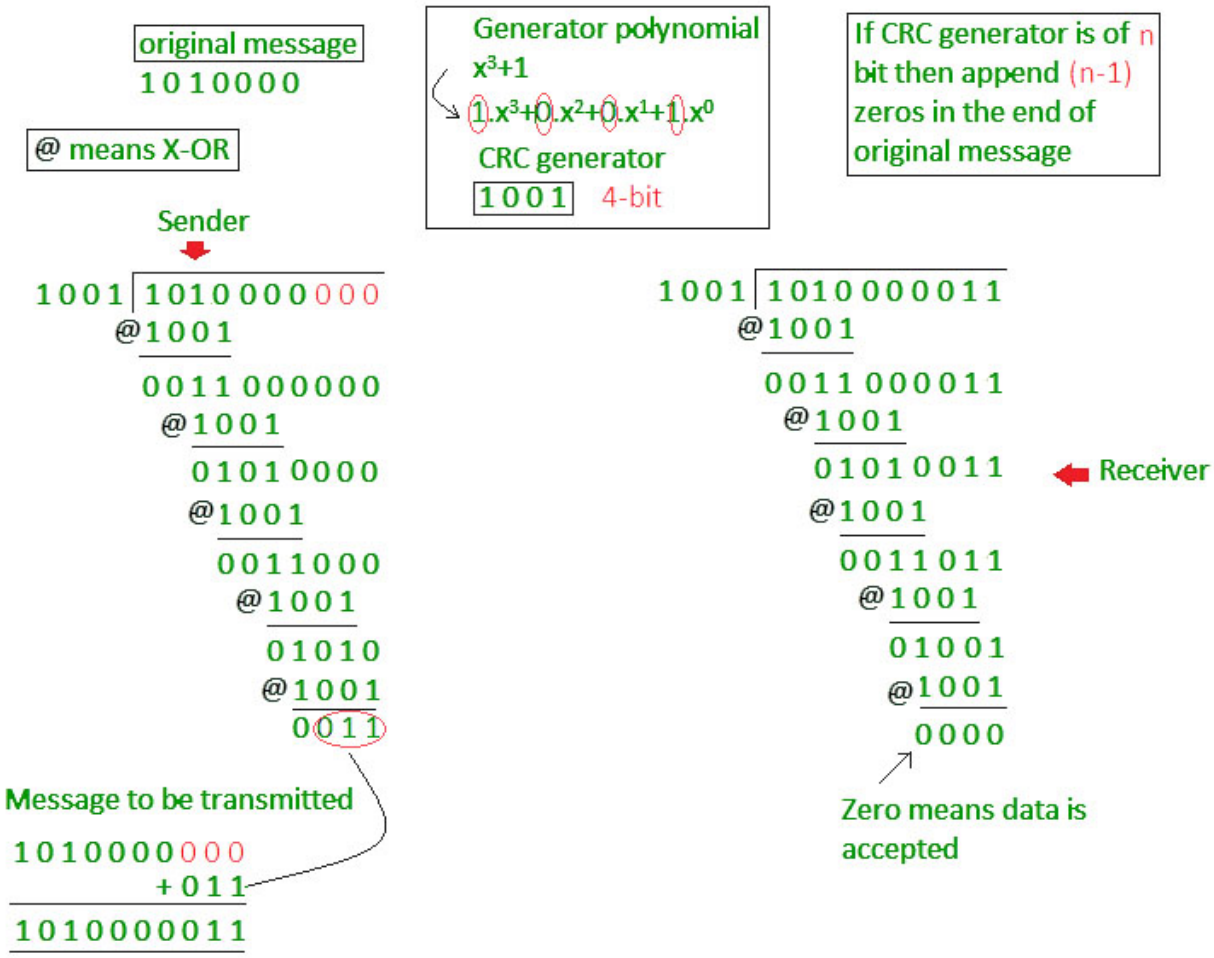

Original Data
10011001
11100010
00100100
10000100
1
2
3
4
k=4, m=8
Sender
1 10011001
2 11100010
1 01111011
1
01111100
3 00100100
10100000
4 10000100
1 00100100
1
Sum: 00100101
CheckSum: 11011010
Reciever
1 10011001
2 11100010
1 01111011
1
01111100
3 00100100
10100000
4 10000100
1 00100100
1
00100101
11011010
Sum: 11111111
Complement: 00000000
Conclusion: Accept Data

ERROR DETECTION: 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.



CYCLIC REDUNDANCY CHECK (CRC)



ERROR CORRECTION

- When the data is sent from the **sender side** to the receiver's side it needs to be detected and corrected. So an error correction method is used for this purpose.
- Following are the two ways through which error correction can be handled:
- **Backward Error Correction**
  - In this method, When any error is found in the data at the receiver's end. Then the request for resending the whole data unit is sent by the receiver.
- **Forward Error Correction**
  - In this method, an error-correcting code is used by the receiver that automatically corrects the errors.

HAMMING CODES

- **Parity bits:** The **parity bits** are the special type of bits that are added to the original data of binary bits to make the total 1s either even or odd.
- **Even parity:** For checking the even parity, the following concept is used: The value of the even parity bit will be **0** if the total occurrence of 1s is even and the value of the parity bit can be 1 if the total occurrence of 1s is odd.
- **Odd Parity:** For checking the even parity, the following concept is used: The value of the parity bit will be 1 if the total occurrence of 1s is even and the value of the parity bit can be 0 if the total occurrence of 1s is odd.

USING HAMMING DISTANCE :

For error correction, the minimum hamming distance required to correct t errors is:

$$d_{min} = 2t+1$$

- For example, if 20 errors are to be corrected then the minimum hamming distance has to be 2*20+1= 41 bits.

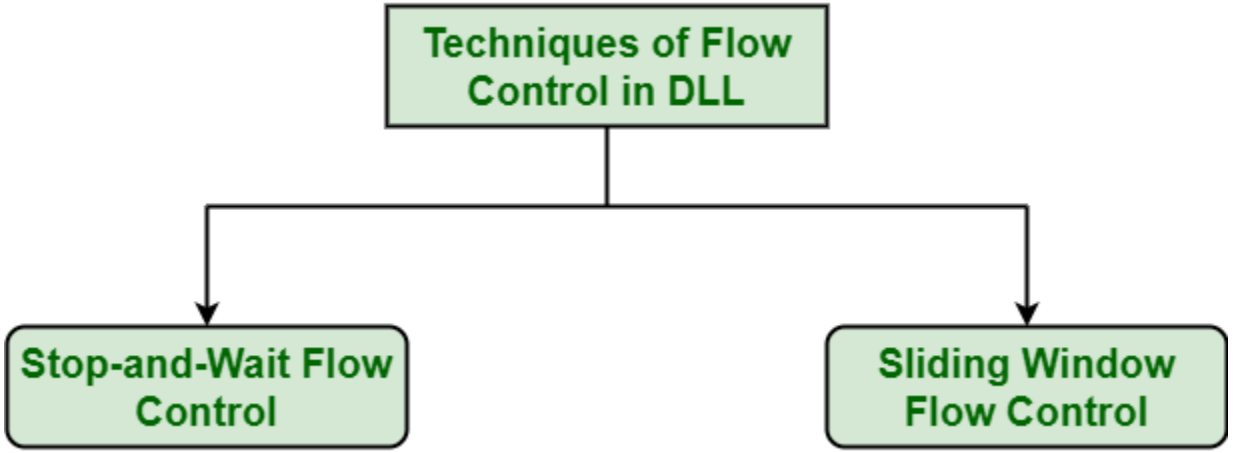
- This means, lots of redundant bits need to be sent with the data. This technique is very rarely used as we have large amount of data to be sent over the networks, and such a high redundancy cannot be afforded most of the time.

FLOW CONTROL

- 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 is actually set of procedures that explains sender about how much data or frames it can transfer or transmit before data overwhelms receiver.
- The receiving device also contains only limited amount of speed and memory to store data. This is why receiving device should be able to tell or inform the sender about stopping the transmission or transferring of data on temporary basis before it reaches limit. It also needs buffer, large block of memory for just storing data or frames until they are processed.

FLOW CONTROL TECHNIQUES

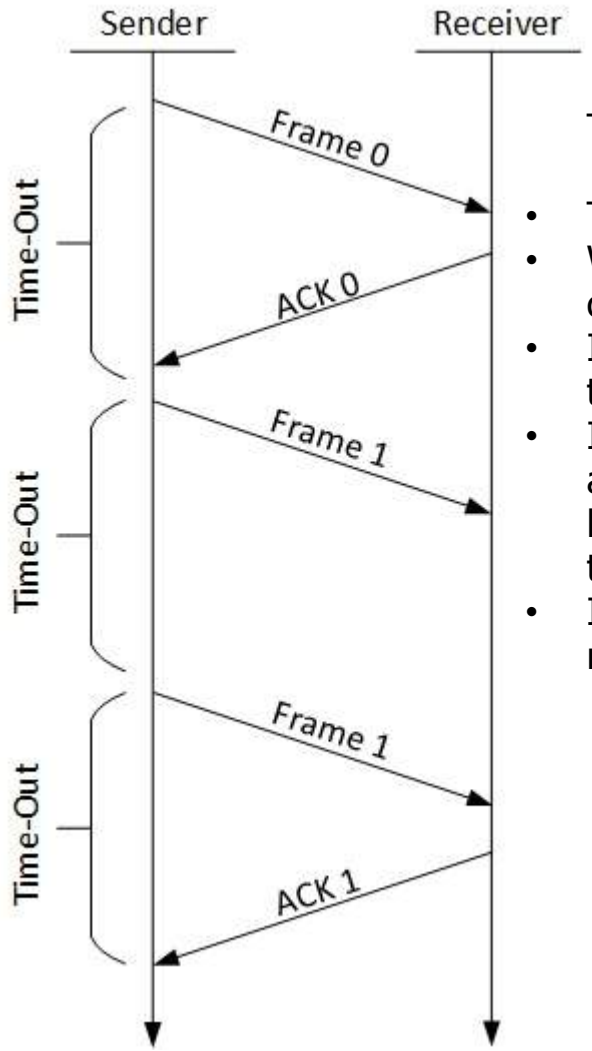
- There are basically two types of techniques being developed to control the flow of data.



STOP-AND-WAIT FLOW CONTROL

- **Stop-and-Wait Flow Control :** This method is the easiest and simplest form of flow control. In this method, basically message or data is broken down into various multiple frames, and then receiver indicates its readiness to receive frame of data. When acknowledgement 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. It leads to inefficiency i.e. less productivity if propagation delay is very much longer than the transmission delay and Ultimately In this method sender sent single frame and receiver take one frame at a time and sent acknowledgement(which is next frame number only) for new frame.
- **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 fairly 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.

STOP-AND-WAIT FLOW CONTROL



The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.

SLIDING WINDOW FLOW CONTROL

- **Sliding Window Flow Control :** This method is required where reliable in-order delivery of packets or frames is very much needed like in data link layer. It is point to point protocol that assumes that none of the other entity tries to communicate until current data or frame transfer gets completed.
- In this method, sender transmits or sends various frames or packets before receiving any acknowledgement. In this method, both the sender and receiver agree upon total number of data frames after which acknowledgement is needed to be transmitted. Data Link Layer requires and uses this method that simply allows sender to have more than one unacknowledged packet "in-flight" at a time. This increases and improves network throughput. and Ultimately In this method sender sent multiple frame but receiver take one by one and after completing one frame acknowledge(which is next frame number only) for new frame.
- **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.

SLIDING WINDOW FLOW CONTROL : TYPES

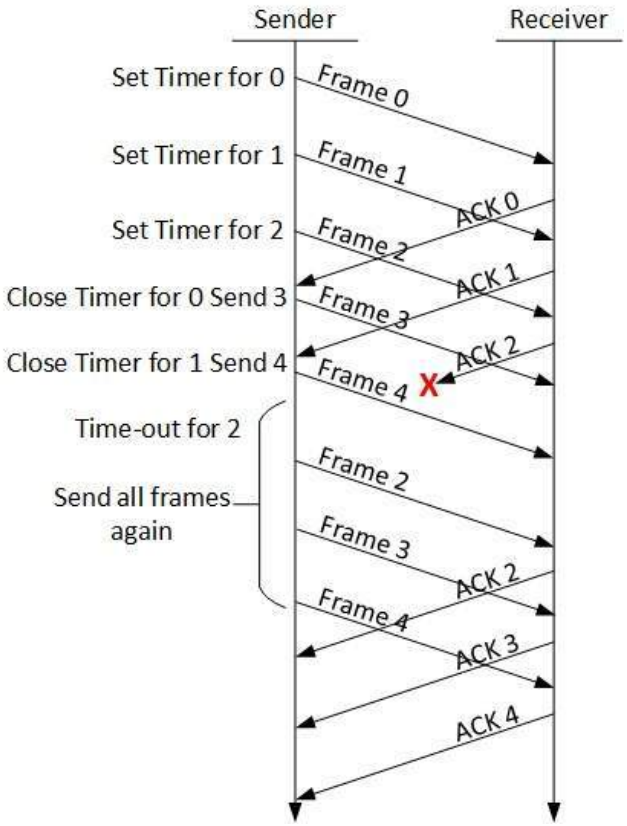
- There are two types of Sliding Window Protocol which include
  - Go-Back-N ARQ and
  - Selective Repeat ARQ

- Go-Back-N ARQ
  - Go-Back-N ARQ allows sending more than one frame before getting the first frame's acknowledgment. It is also known as sliding window protocol since it makes use of the sliding window notion. There is a limit to the amount of frames that can be sent, and they are numbered consecutively. All frames beginning with that frame are retransmitted if the acknowledgment is not received in a timely manner.
- Selective Repeat ARQ
  - Additionally, this protocol allows additional frames to be sent before the first frame's acknowledgment is received. But in this case, the excellent frames are received and buffered, and only the incorrect or lost frames are retransmitted.

GO-BACK-N ARQ

- Stop and wait ARQ mechanism does not utilize the resources at their best. When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.

The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.
When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received 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.

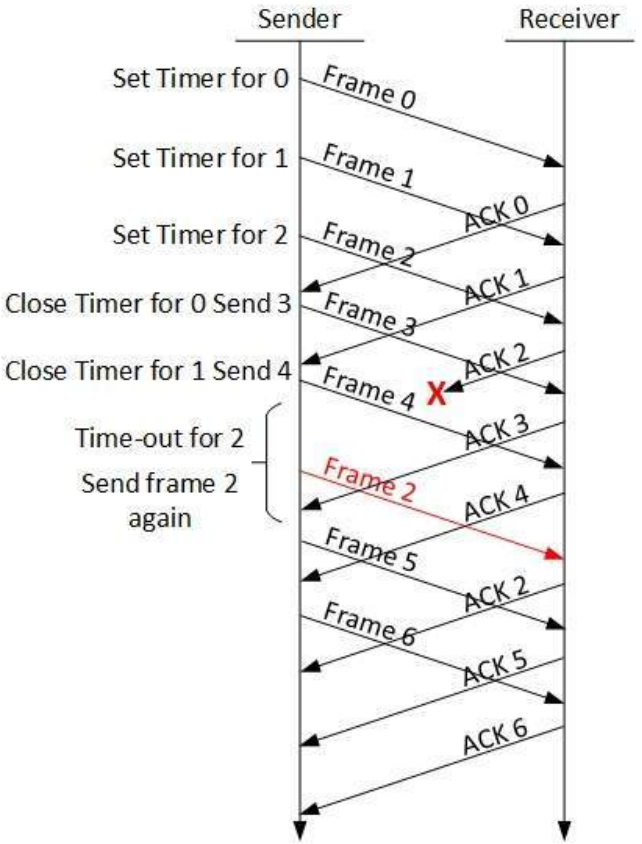


SELECTIVE REPEAT ARQ

- In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.

In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.

The sender in this case, sends only packet for which NACK is received.



THANK YOU !!