Unit 1

Computer Communication and Networks

Introduction

Computer Networks and its applications

Definition:

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.

Some of the applications are

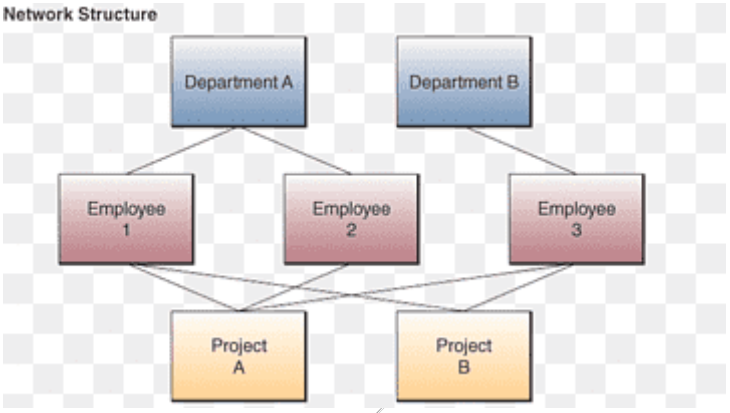
- **Electronic Messaging:**– Electronic mail (e-mail) is the most widely used network application.
- **Electronic Data Interchange (EDI):**– EDI permits business information to be transferred without using paper.
- **Financial Services: –** In Present, Financial services are completely dependent on computer networks. Main applications are credit history searches, foreign exchange and investment services, and Electronic Funds Transfer (EFT) that permits a user to transfer money without going into bank.
- **Teleconferencing:** – With The help of teleconferencing conferences are possible to occur without the participants being in the same place. Applications include simple text conferencing, voice conferencing, and video conferencing.
- Accessing Remote programs
- Value added communication facility
- Marketing and sales
- Manufacturing
- Electronic message
- Directory services

Network structure

Network structure is **a term used to describe the method of how data on a network is organized and viewed**.

It's important to have a systematic way of communicating with your customers, and this will largely depend on your network structure. Like a human backbone, without it, every part of the body will fall apart and suffer

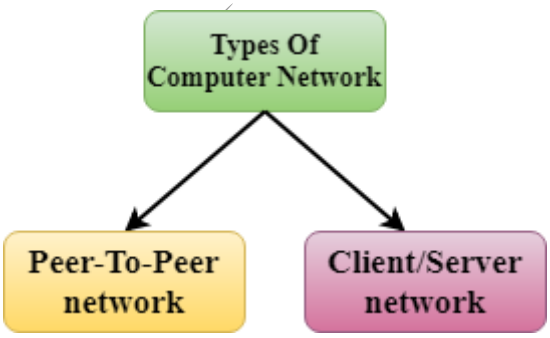
Example:



Network Architecture

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

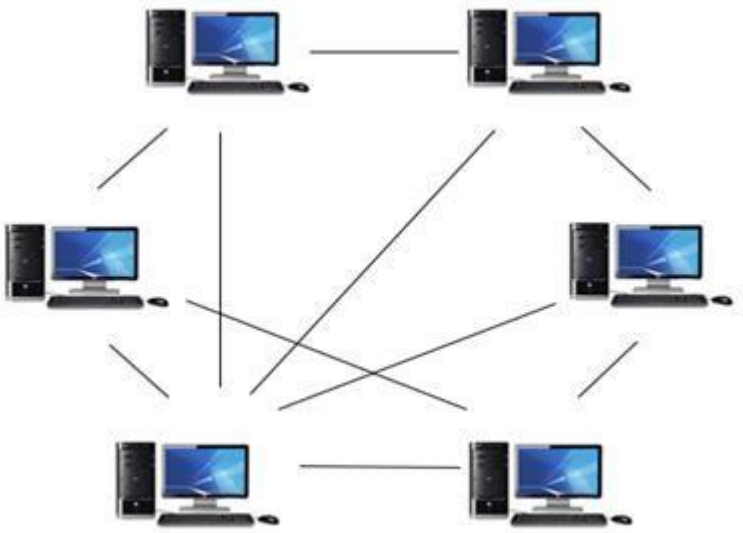
The two types of network architectures are used:



- Peer-To-Peer network
- Client/Server network

Peer-To-Peer network

- 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.



Advantages Of Peer-To-Peer Network:

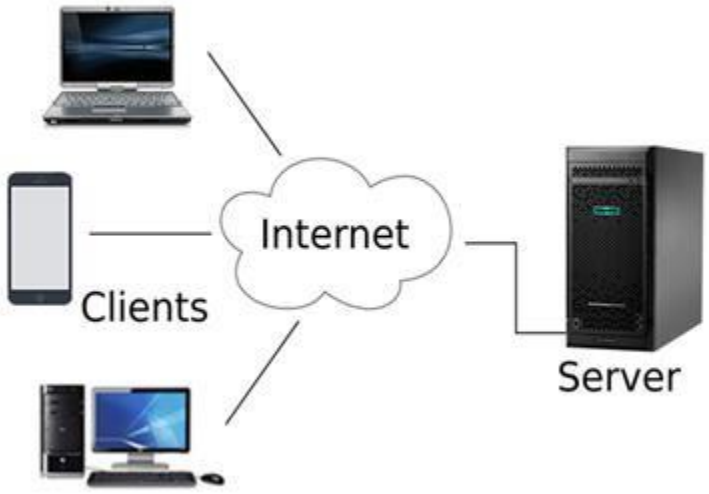
- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

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/Server Network

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



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.

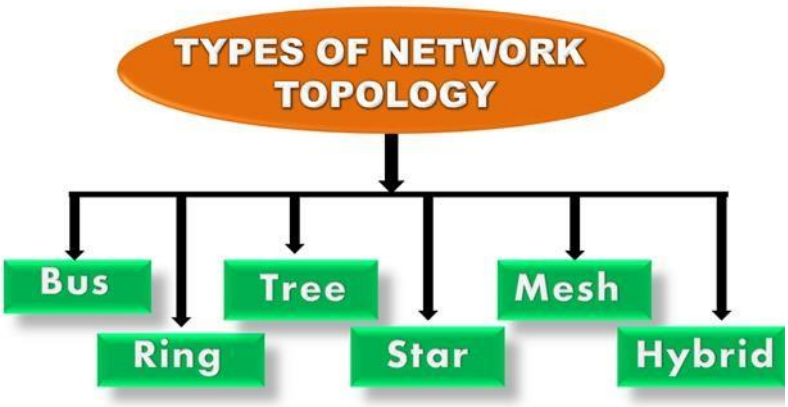
Topologies

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

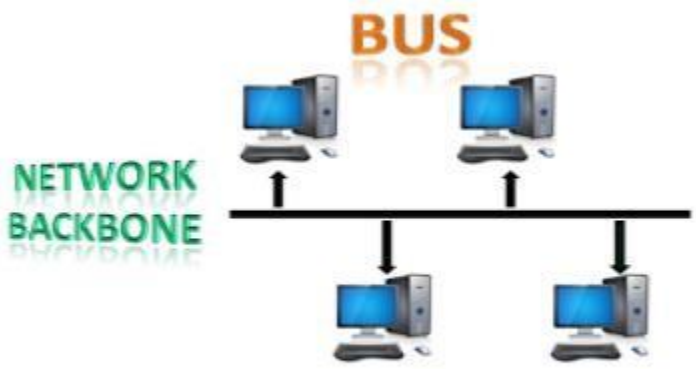
There are two types of topology:

- physical
- logical topology.

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



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 configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

Advantages of Bus topology:

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.

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.

Advantages of Ring topology:

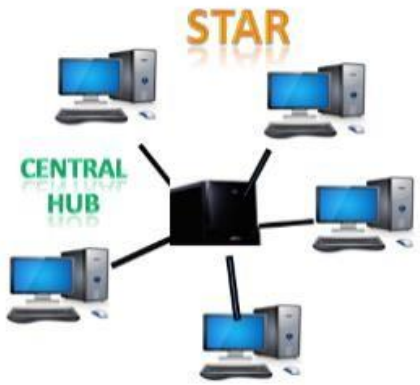
- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of

nodes. Adding new devices increases the communication delay.

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.

Advantages of Star topology

- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.

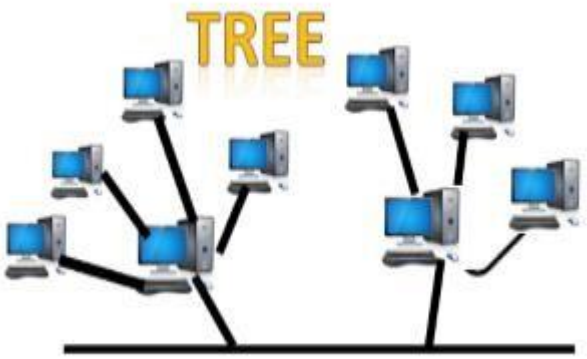
Disadvantages

- **A Central point of failure:** If the central hub or switch goes down, then

all the connected nodes will not be able to communicate with each other.

- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

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.

Advantages of Tree topology

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without more effort.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.

- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

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.

Advantages of Mesh topology:

Reliable: The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

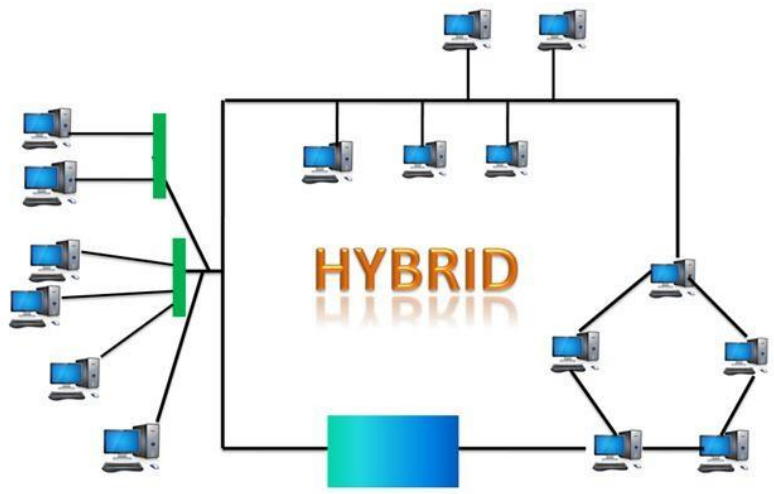
Fast Communication: Communication is very fast between the nodes.

Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of 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.

Advantages of Hybrid Topology

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology

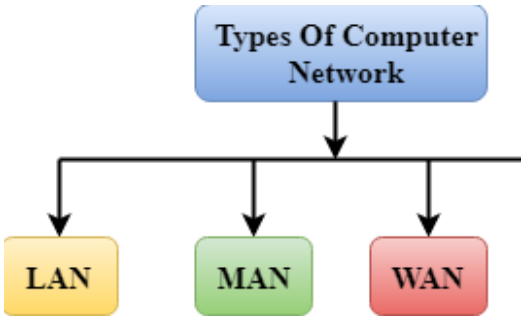
- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

Computer Network Types

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 **three types**:



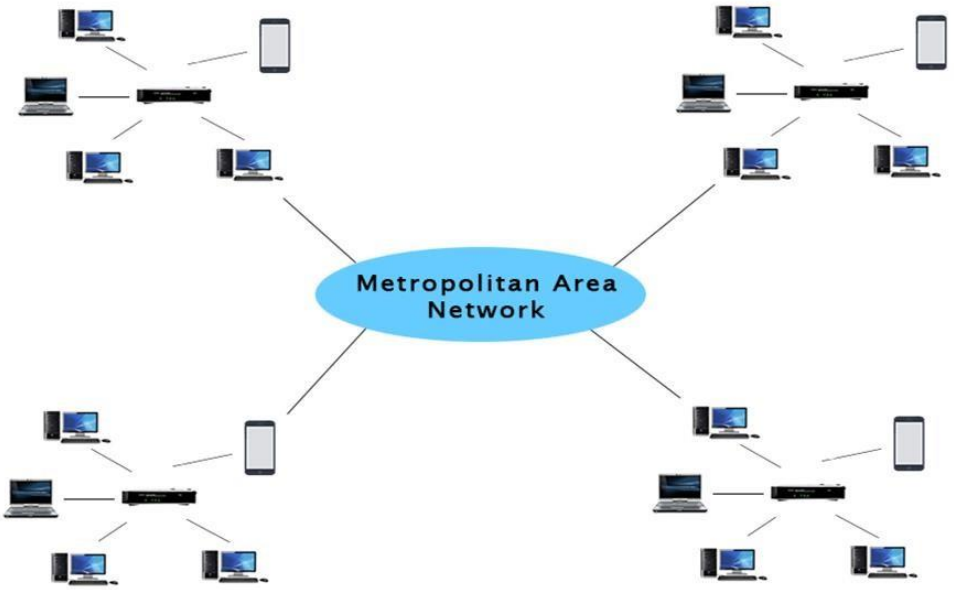
- LAN(Local Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

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.

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).

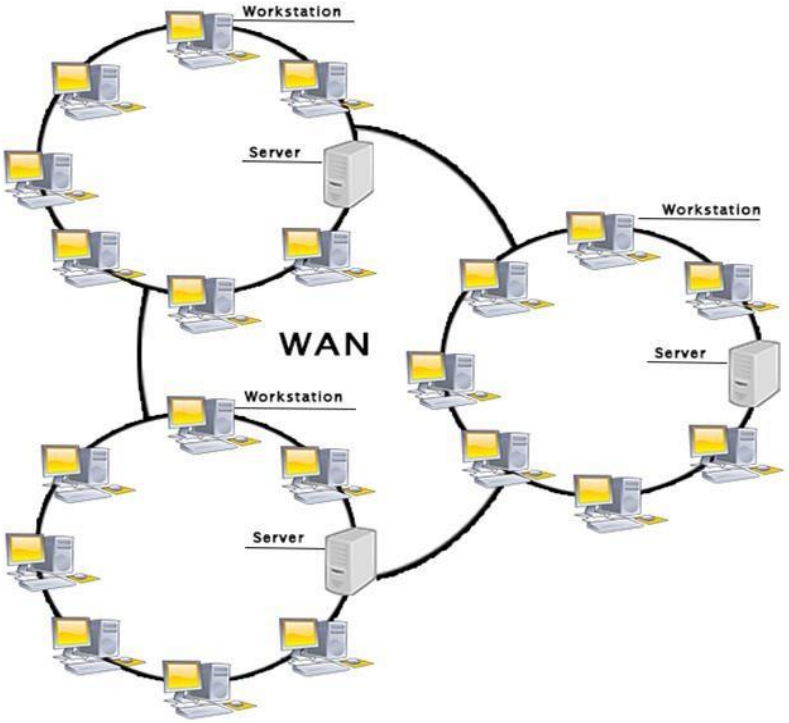


Uses Of Metropolitan Area Network:

- 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.



Advantages of Wide Area Network:

- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.

- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

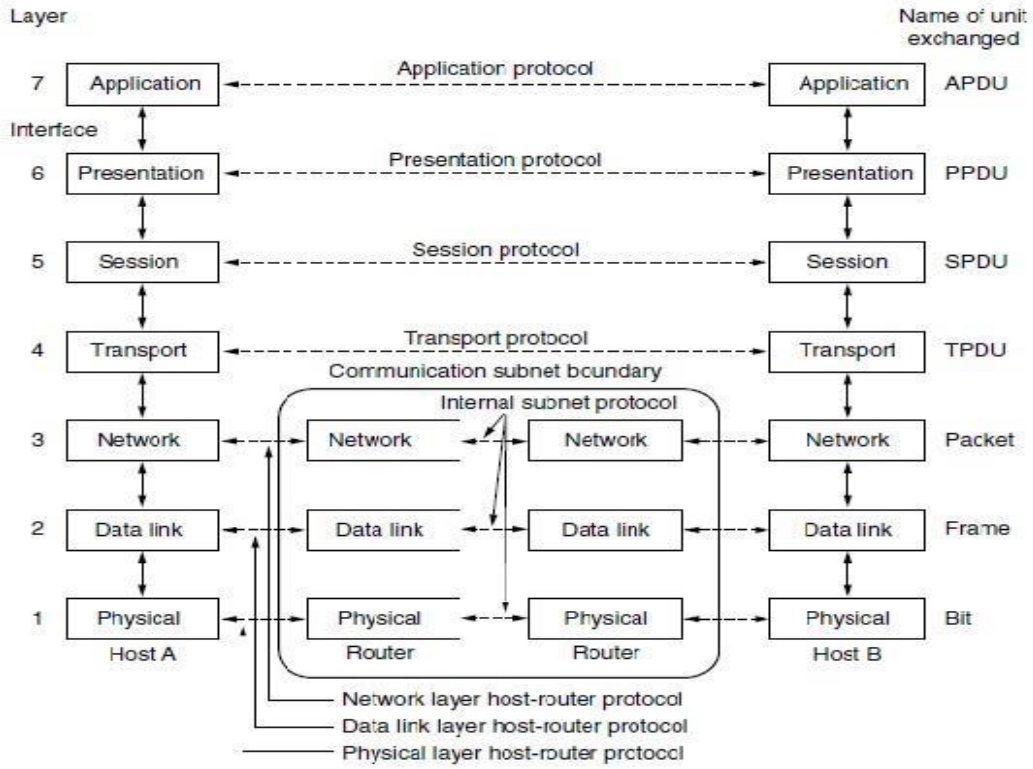
Disadvantages of Wide Area Network:

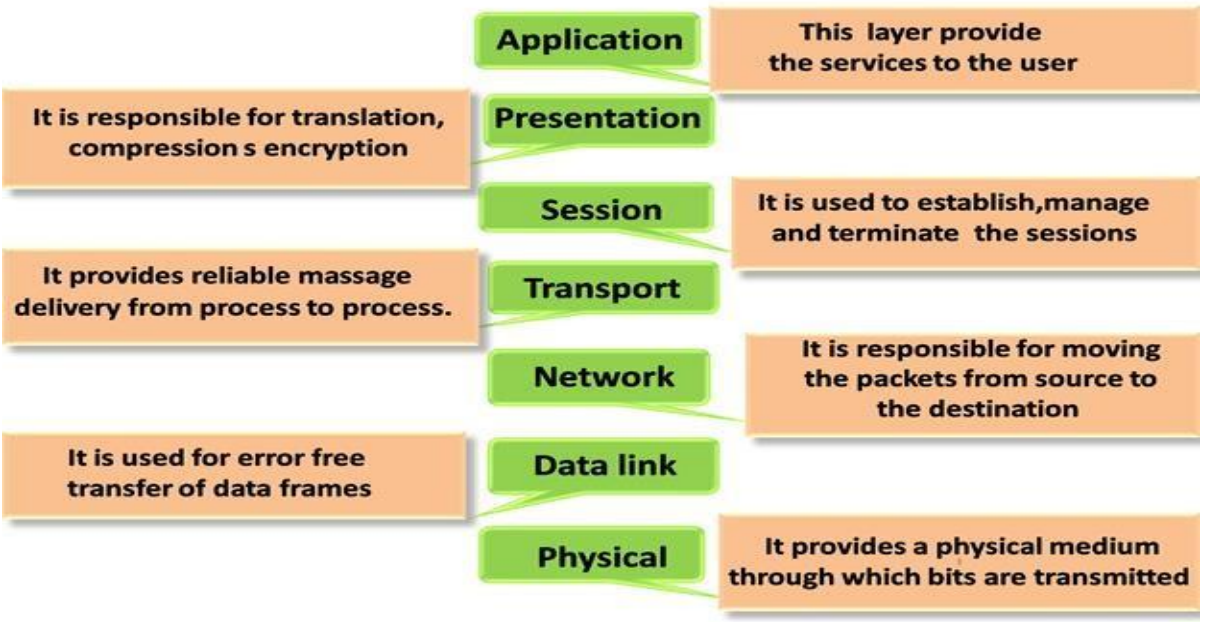
The following are the disadvantages of the Wide Area Network:

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

The OSI reference model

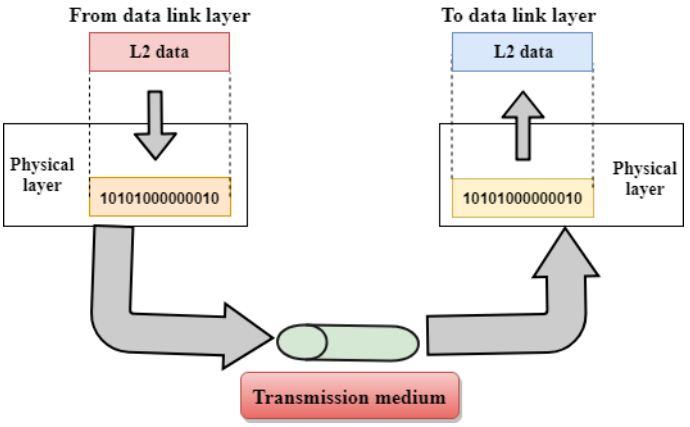
- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of **seven layers**, and each layer performs a particular network 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.





In short

1.. Physical layer



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

2. Data Link Layer

- The data link layer establishes and terminates a connection between two physically-connected nodes on a network.
- It breaks up **packets** into **frames** and sends them from source to destination.
- This layer is composed of two parts—**Logical Link Control** (LLC), which identifies network protocols, performs error checking and synchronizes frames, and **Media Access Control** (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

3..Network Layer

The network layer has two main functions. One is breaking up **segments** into **network packets**, and reassembling the packets on the receiving end. The other is routing packets by **discovering the best path** across a physical network. The network layer uses **network addresses** (typically Internet Protocol addresses) to route packets to a destination node.

4.. Transport Layer

The transport layer takes data transferred in the session layer and breaks it into **"segments"** on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out **flow control,** sending data at a rate that matches the **connection speed of the receiving device**, and error control, checking if data was received incorrectly and if not, requesting it again.

5..Session layer

The session layer creates **communication channels, called sessions**, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set **checkpoints** during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

6..Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should **encode, encrypt, and compress data** so it is received correctly on the other end. The presentation layer takes any data transmitted by the

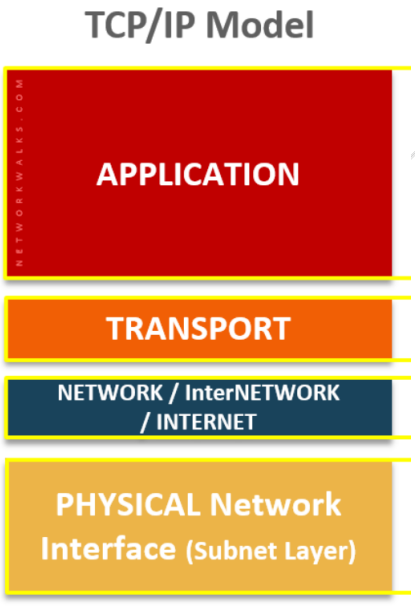
application layer and prepares it for transmission over the session layer.

7..Application layer

The application layer is used by end-user software such as **web browsers and email clients**. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

- **HTTP:** Hypertext transfer protocol allows the users to interact with the World Wide Web through browser applications.
- **SMTP:** Simple mail transfer protocol is used to send mails.
- **FTP:** File transfer protocol is used for transmitting files from one system to another.
- **DNS:** Domain name system is the phonebook of the internet.
- **TELNET:** Teletype network acts as a client-server protocol. It is used to provide bidirectional connection.

TCP/IP reference model



The TCP/IP model has four layers:

- Application Layer
- Transport Layer
- Network Layer
- Physical Layer

Application Layer

The application layer is a combination of the **application, presentation, and session layers**. This layer is responsible for interaction between the user and the application. Here, data is **formatted, converted, encrypted, decrypted, and set** to the user.

Protocols used by the application layer are:

- **HTTP:** Hypertext transfer protocol allows the users to interact with the World Wide Web through browser applications.
- **SMTP:** Simple mail transfer protocol is used to send mails.
- **FTP:** File transfer protocol is used for transmitting files from one system to another.
- **DNS:** Domain name system is the phonebook of the internet.
- **TELNET:** Teletype network acts as a client-server protocol. It is used to provide bidirectional connection.

Transport Layer

The transport layer is responsible for **end-to-end communication** and provides **error-free delivery** of data. This layer can transport the data through a **connection-oriented or connectionless layer**.

The two protocols used in the transport layer are user datagram protocol (UDP) and TCP.

- **UDP: User Datagran Protocol :** This protocol provides connectionless service and end-to-end delivery of transmission. It is considered an unstable protocol because it discovers the errors but does not specify them.
- **TCP: Transmission control protocol:** It provides all transport services to the application layer. TCP is a dependable protocol for error detection and retransmission. It assures that all segments must be received and recognized before completing the transmission and discarding the virtual circuit.

Network Layer

The network layer provides **host addressing** and **chooses the best path** to the destination network. This layer maintains the **quality of service** and offers **connectionless end-to-end networking**.

The protocols in the network layer are:

- **IPV4:** Internet protocol version 4 is employed for **packetizing, forwarding, and delivery** of packets. IP is an unreliable datagram protocol.
- **ICMPV4:** Interrupt control message protocol controls **all errors**. These mistakes are handled by ICMP protocol during the delivery of the message to target problems.
- **IGMP:** Internet group management protocol helps in **multicasting.**

Physical Layer

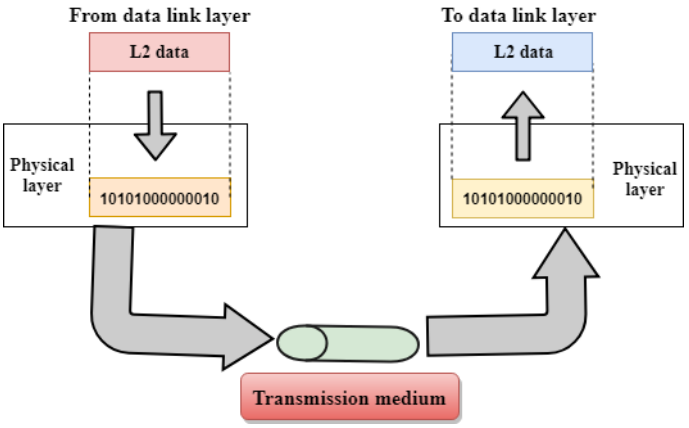
The physical layer interacts with the top level of the TCP/IP model application. This layer is the nearest end-user TCP/IP layer. It means that the consumers can connect with other software apps.

The physical layer interacts with software applications to develop media platforms. Data is constantly beyond the boundaries of the TCP/IP model to be interpreted in the application. **An application such as a data transfer, mail, remote login, etc., is an example of this layer**.

.

Unit 2

Physical Layer

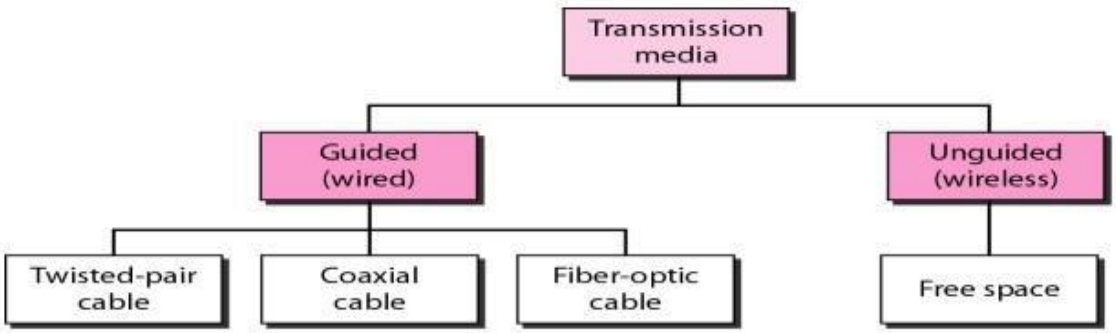


Transmission Media

Transmission media is a pathway that carries the **information** from sender to receiver. We use different types of **cables or waves** to transmit data. Data is transmitted normally through **electrical or electromagnetic signals**.

An electrical signal is in the form of **current.** An electromagnetic signal is series of electromagnetic energy pulses at various **frequencies**. These signals can be transmitted through copper wires, optical fibers, atmosphere, water and vacuum. Different Medias have different properties like bandwidth, delay, cost and ease of installation and maintenance. Transmission media is also called **Communication channel.**

Classes of transmission media



.

There are 2 types of transmission media:

- Guided
- Unguided

1. Guided Transmission Media:

Bounded media and wired media are other names for guided transmission media. They consist of cables or wires that transfer data. They go by the name "guided" because they act as a physical link between the transmitter and recipient devices. They are:

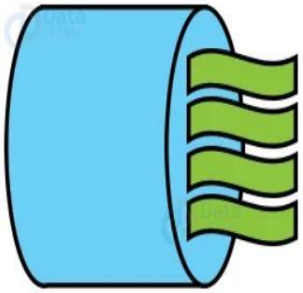
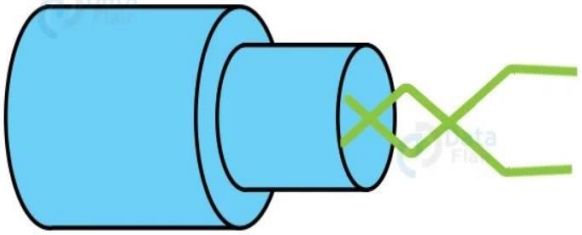
- Secure high-speed links.
- Generally used for shorter distances.

Some of these most popular guided transmission media are:

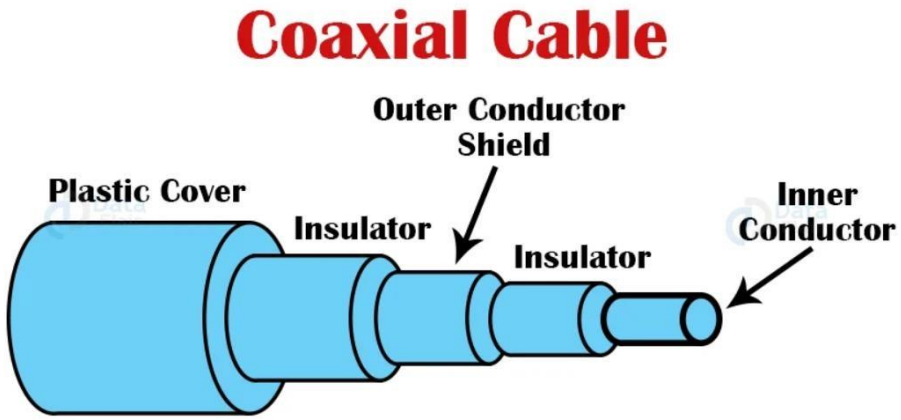
.

1. Twisted Pair Cable

It consists of 2 separately insulated conductor wires wound about each other.
Twisted Pair is of two types:

Unshielded Twisted Pair	Shielded Twisted Pair
	
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.	This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and data channels of telephone lines.
Advantages: ⇢ Least expensive ⇢ Easy to install ⇢ High-speed capacity	**Advantages:** ⇢ Better performance at a higher data rate in comparison to UTP ⇢ Eliminates crosstalk ⇢ Comparatively faster
Disadvantages: ⇢ not suitable to avoid external interference ⇢ Lower capacity and performance in comparison to STP (Shielded Twisted Pair) ⇢ Short distance transmission due to attenuation	**Disadvantages:** ⇢ Comparatively difficult to install and manufacture ⇢ More expensive ⇢ Bulky
Applications: Used in telephone connections and LAN networks	**Applications:** Shielding the interior components.

a. Coaxial Cable:



It features an exterior plastic covering and two parallel conductors, each with its own insulated protective cover. It operates in 2 ways: baseband and broadband.

.

Applications: Coaxial cables are commonly used in **cable TV and Radio frequency signals** are sent over coaxial wire.

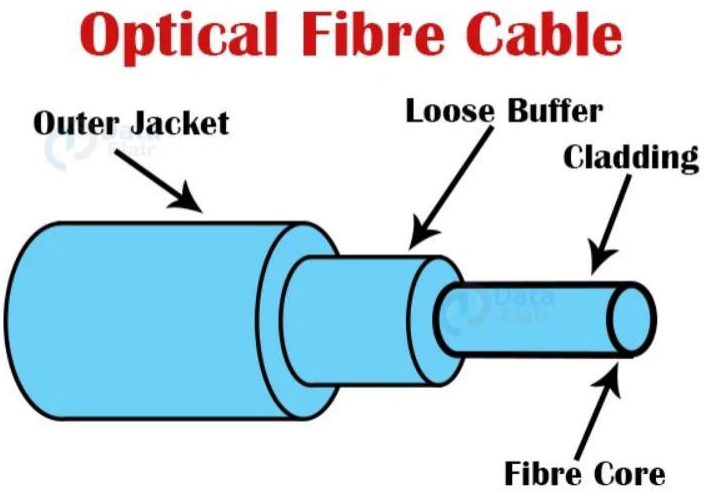
i. Advantages:

- High bandwidth.
- Better noise Immunity.
- Very cheap to install.
- Easy to install and upgrade.

ii. Disadvantages

- If there is a failure of the cable, the whole network may fail.

C. Optical fibre



It works on the principle of light reflection through a core composed of glass or plastic. The cladding surrounds the core, and the cladding is a less thick glass or plastic covering. It finds use in **large-volume data transfer.**

It is possible for the cable to be **unidirectional or bidirectional.**

Elements of optical fibre cable:

- **Core**: The core of an optical fibre is a small strand of glass or plastic. A core is the part of the fibre that transmits light. The amount of light transferred into the fibre depends upon the area of the core.
- **Cladding**: Cladding refers to the concentric layer of glass. The primary function of the cladding is to produce a lower refractive

.

index at the core interface, causing reflection within the core and allowing light waves to pass through the fibre.

- **Jacket**: A jacket is a type of protective layer made of plastic. The primary function of a jacket is to retain fibre strength, absorb stress, and provide further fibre protection.

Advantages and Disadvantages of optical fibre cable:

ii.Advantages

- Does not rust or corrode since there is no metal.
- Can transmit data at very high speed.
- Supports high bandwidth.
- There is less signal attenuation.
- Resistance to electromagnetic interference.

iii.Disadvantages:

- Installing and maintaining it is difficult.
- Fragile and expensive.

Applications of Fibre Optic cables:

- Medical Industry.
- Communication.
- Defence.
- Industries.
- Broadcasting.
- Lighting and Decorations.

2. Unguided Transmission Media:

Electromagnetic signals can also be transmitted without the use of a physical medium. These are also known as wireless or unbounded transmission media.

Some properties of unguided media are:

- Less secure than guided media.
- Used for longer distances.

.

Types of Unguided Transmission Media:

a)Infrared

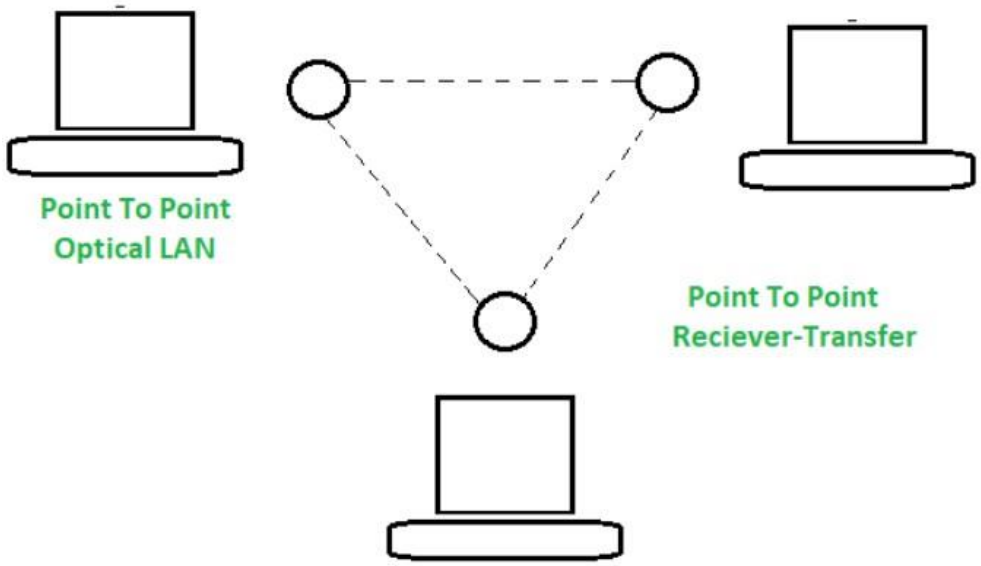
b)Radio waves

c)Microwave

a. Infrared:

When there is a need for very **short-range communication**, infrared waves are used. However, they fail to penetrate any walls/obstacles in the way of the signal.

The frequency ranges from **300 GHz to 400 GHz**.



Point -To-Point infrared media in a network

Characteristics of infrared transmission:

- It has a **large bandwidth**, thus the data rate will be **quite high**.
- Infrared waves are unable to penetrate the walls. As a result, infrared communication in one room cannot be disrupted by surrounding rooms.
- Infrared communication is more secure and also causes less interference.
- **Outside the building**, infrared communication is **unreliable** because the sun's rays interfere with the infrared radiation.

Advantages :

- Cost-effective and cheap.
- Large bandwidth.
- Easy to install.

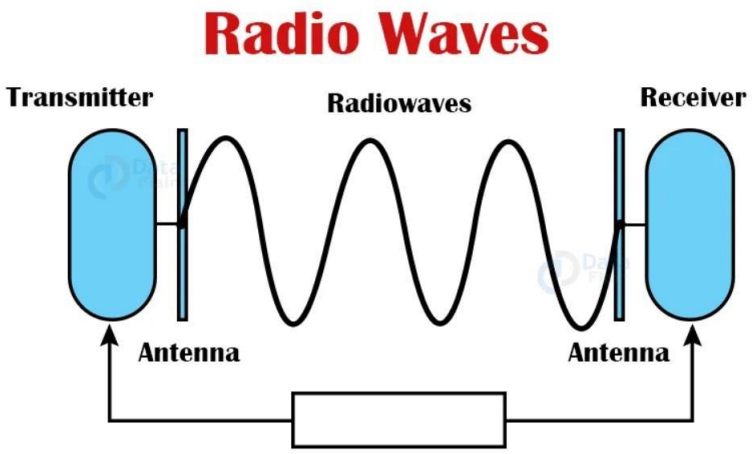
.

- Can be operated without any license.

Disadvantages:

- Cannot cross barriers.
- Long-range communication is not possible.

b. Radio waves:



Very commonly used and very simple to generate. These types of waves can pass through obstacles easily. Two antennas are used, one for the transmitting station and one for the receiving station (these antennas need not be aligned).

The frequency ranges from 3 kHz to 1GHz.

Advantages of Radio Transmission:

- Radio transmission is mostly utilized for wide area networks and mobile phones.
- Radio waves may penetrate barriers and cover a broad area.
- Faster transmission speed.

Disadvantages:

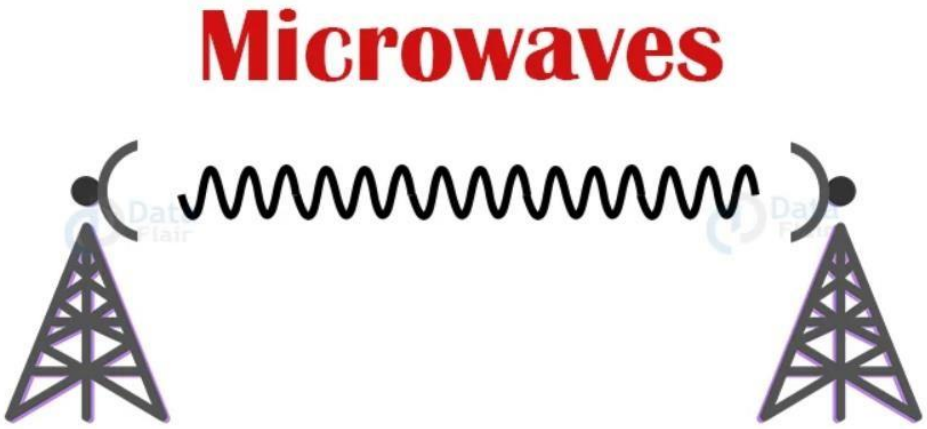
- Regulation of radio spectrum, thus it is expensive to buy.
- Cannot travel above the horizon because of the curvature of the earth.

.

Applications:

- AM and FM Radio
- Cordless phone

c. Microwaves:



It is a line-of-sight transmission, which means that the transmitting and receiving antennas must be correctly aligned. The distance reached by the signal is proportional to the antenna's height. These are mostly utilized for mobile phone communication and television broadcasting.
The frequency ranges from **1 GHz to 300GHz**.

Characteristics of microwave:

- Frequency range: **4 to 23 GHz.**
- Bandwidth: It provides bandwidths ranging from **1 to 10 Mbps**.
- Short distance: inexpensive for short distance communication.
- Long distance: It is costly since a larger tower is required for a longer distance.
- Attenuation: loss of signal. Affected by environmental conditions and antenna size.

.

Advantage of microwave transmission:

- Microwave transmission is cheaper than cable transmission.
- It does not need any land for installation.
- Microwaves are more convenient in places where installing cables is difficult.
- Microwave transmission can be used to communicate across seas.

Disadvantages of microwave transmission:

- Eavesdropping: Eavesdropping makes communication unsafe. Any user with its own antenna can capture the signal in the air.
- Out of phase signal: Signal may shift out of phase.
- Weather condition: Any environmental disturbance may cause the signal distortion.
- Bandwidth allocation: Less bandwidth is available.

Applications

- Satellite Networks
- Cell phones

<u>Factors to consider when choosing transmission media:</u>

1. Bandwidth: Assuming all other variables stay constant, the bigger the bandwidth of a media, the faster the data transmission rate of a signal.

2. Transmission impairment: When the received signal differs from the sent signal owing to transmission impairment. Signal quality will be reduced as a result of transmission flaws.

3. Interference: Interference is described as the process of interrupting a signal as it travels through a communication channel as a result of the addition of some unwanted signal.

4. Radiation: We need to choose a medium that minimises signal leakage.

5. Attenuation: A transmission medium must also be chosen so as to minimise the signal loss over long distances.

6. Noise Absorption: External noise may impact the medium if it is not properly insulated against such interference.

.

Causes of Transmission Impairment:

1. Attenuation: Attenuation refers to the loss of energy, which occurs as the intensity of the signal diminishes as the distance increases, resulting in the loss of energy.

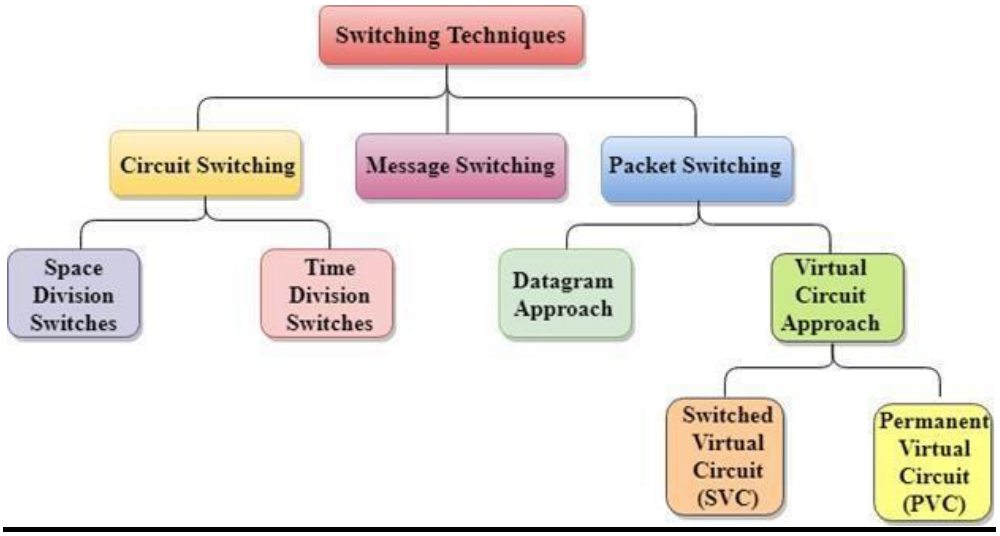
2. Distortion: Distortion happens when the form of the signal changes. This form of distortion is investigated using various signals with varying frequency. Because each frequency component has its own propagation speed, they arrive at various times, resulting in delay distortion.

3. Noise: When data is sent through a transmission media, an undesired signal is added to it, resulting in noise.

.

Switching

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission. Switching technique is used to connect the systems for making one-to-one communication.

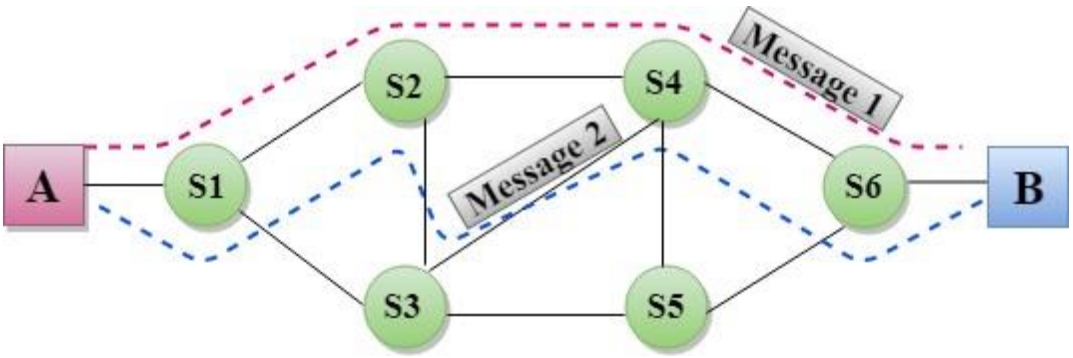


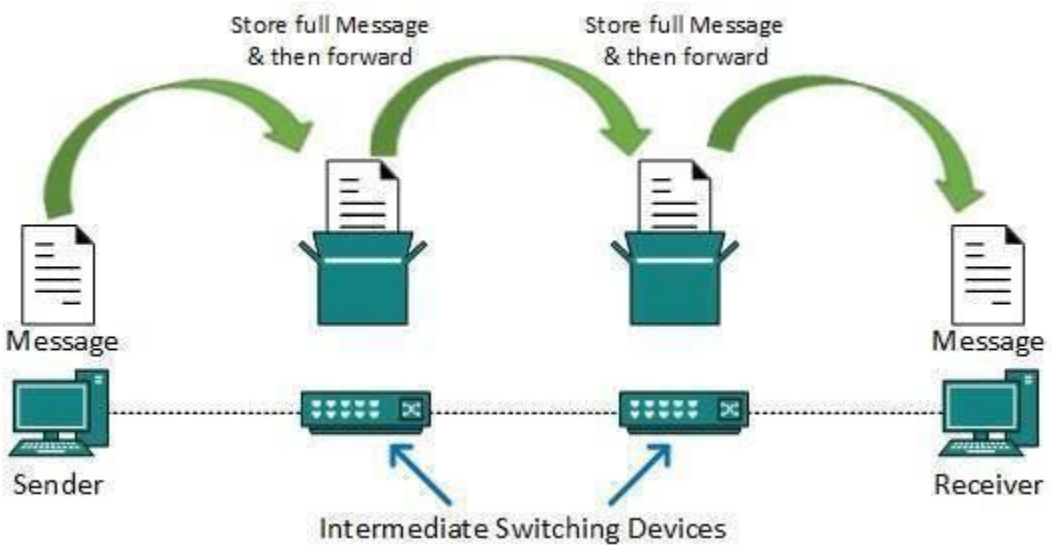
Message Switching

- There exists no dedicated path to transfer data.
- The entire message is treated as a single data unit.
- The message is then forwarded from hop to hop.
- **Store and Forward** is an important characteristic of message switching.
- The message carries a header that contains the full information about the destination.
- When any intermediate switch receives the message, it stores the entire message.
- The message is stored until sufficient resources become available to transfer it to the next switch.

.

- When resources become available, the switch forwards the message to the next switch.





Advantages

- Sharing of communication channels ensures better bandwidth usage.
- It reduces network congestion due to store and forward method. Any switching node can store the messages till the network is available.
- Broadcasting messages requires much less bandwidth than circuit

.

switching.

- Messages of unlimited sizes can be sent.
- It does not have to deal with out of order packets or lost packets as in packet switching.

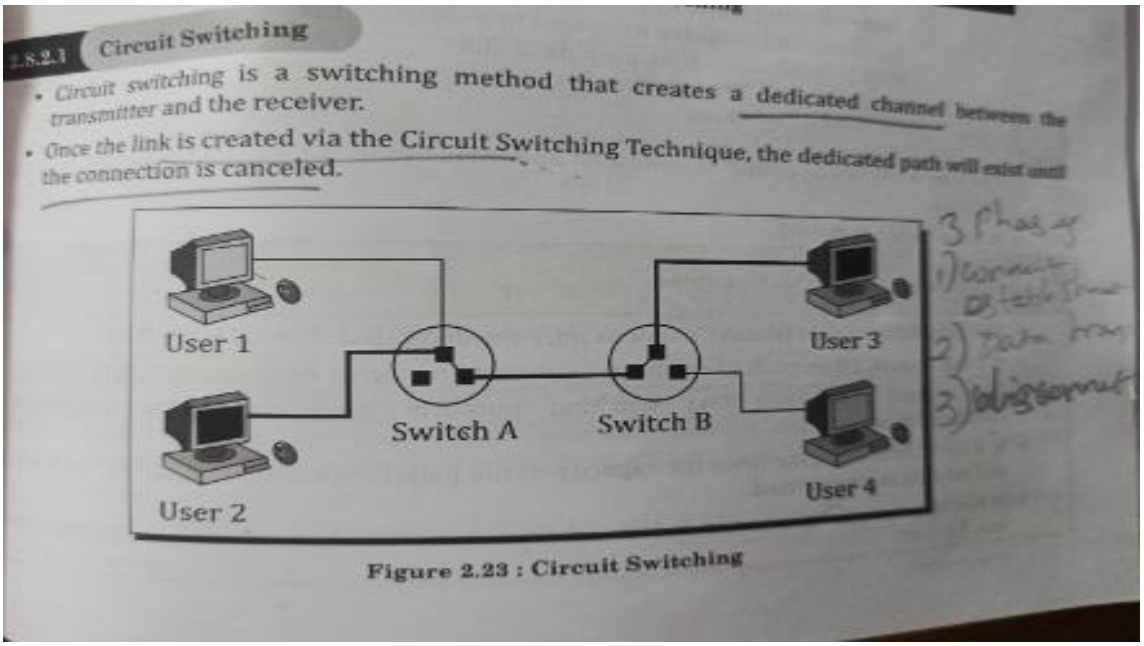
Disadvantages

- In order to store many messages of unlimited sizes, each intermediate switching node requires large storage capacity.
- Store and forward method introduces delay at each switching node. This renders it unsuitable for real time applications.

Packet Switching

- The entire message is broken down into smaller chunks called packets.
- The switching information is added in the header of each packet and transmitted independently.
- Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier.
- The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities.
- Packets are stored and forwarded according to their priority to provide quality of service.

Circuit Switching



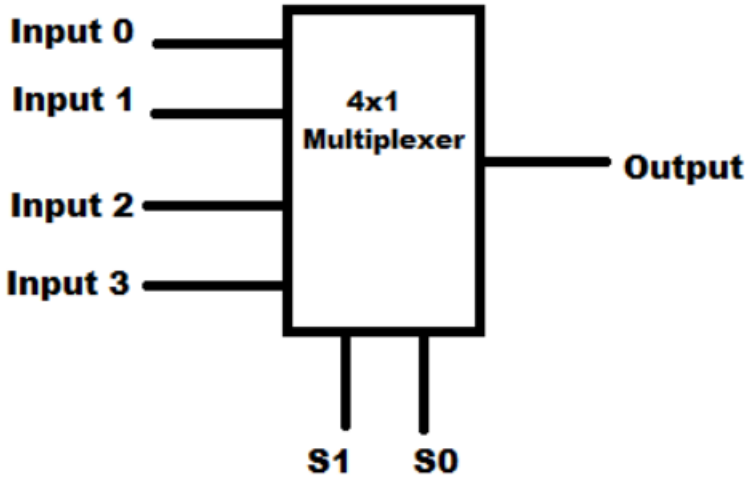
.

Multiplexing

Multiplexing is a technique used to combine multiple signals and transmit the combined signal over a transmission medium**.**

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

Multiplexer (MUX): Multiplexer is a combinational circuit that has **2^n input signal lines** and a **single output** line.



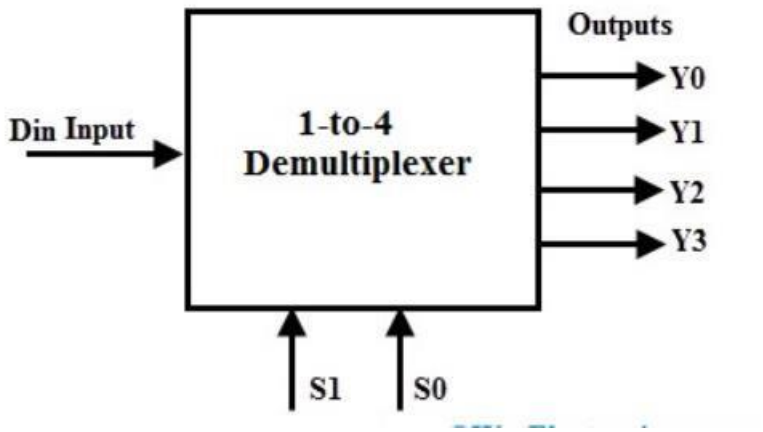
For example 4 X 1 multiplexer has 4 input data lines and 1 output line and **8 X 1 multiplexer** has 8 input data lines and 1 output line.

Multiplexer is used for multiplexing technique as it is combining multiple signals and producing single output signal.

Demultiplexer (DEMUX): Demultiplexer does exactly opposite of Multiplexing, it receives a **single input** signal and generates **2^n output** signals. Multiplexer is used at the source to combine the multiple input signals while Demultiplexer is used at the receiving side to generate the multiple signals from the received signal.

.

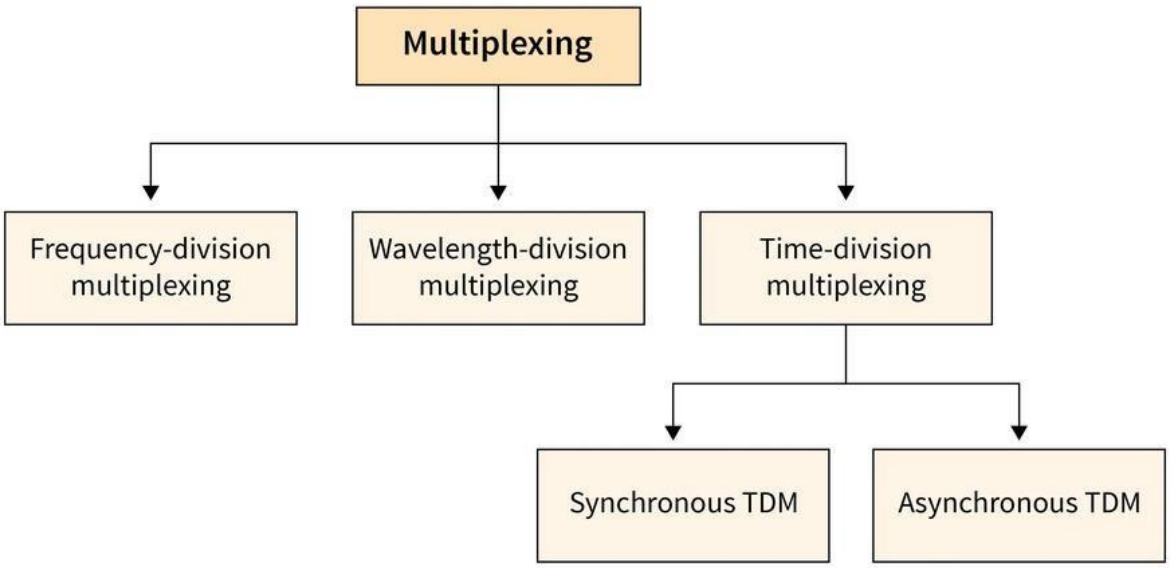
Demultiplexing is achieved by using a device called Demultiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.



For example 1 X 4 Demultiplexer is used to generate 4 output signals from a single signal.

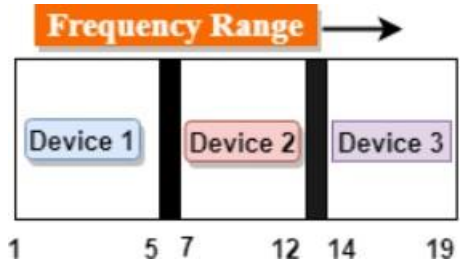
Types of Multiplexing Techniques

There are three types of Multiplexing



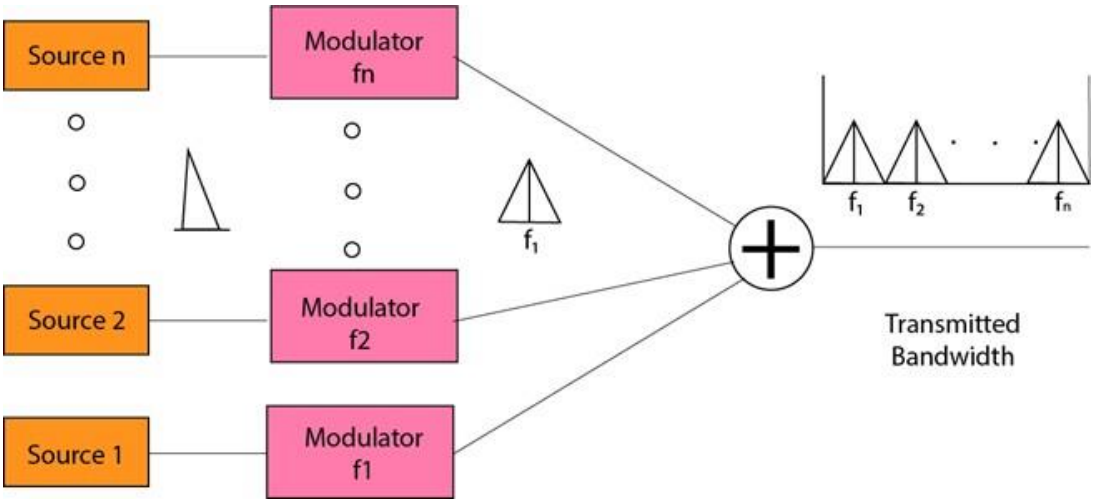
.

Frequency division multiplexing (FDM)

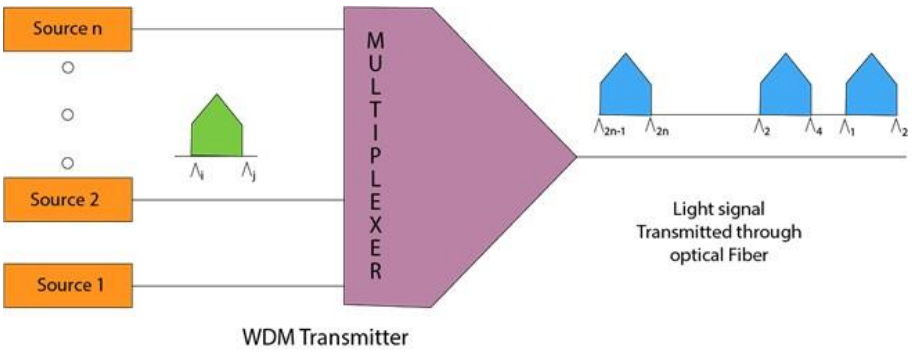


- It is an analog technique.
- **Frequency Division Multiplexing** is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.
- In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.
- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.
- **FDM** is mainly used in radio broadcasts and TV networks.

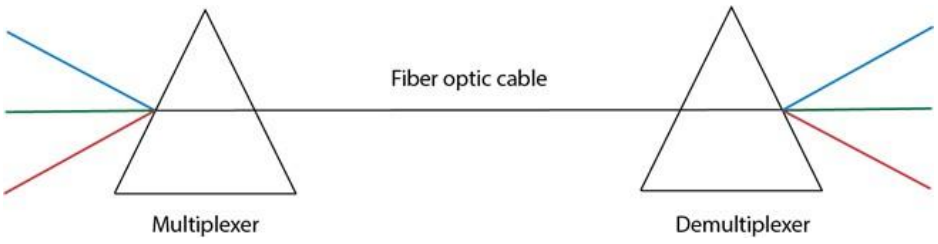
.



Wavelength Division Multiplexing (WDM)



- Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.
- WDM is used on fibre optics to increase the capacity of a single fibre.
- It is used to utilize the high data rate capability of fibre optic cable.
- It is an analog multiplexing technique.
- Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.



.

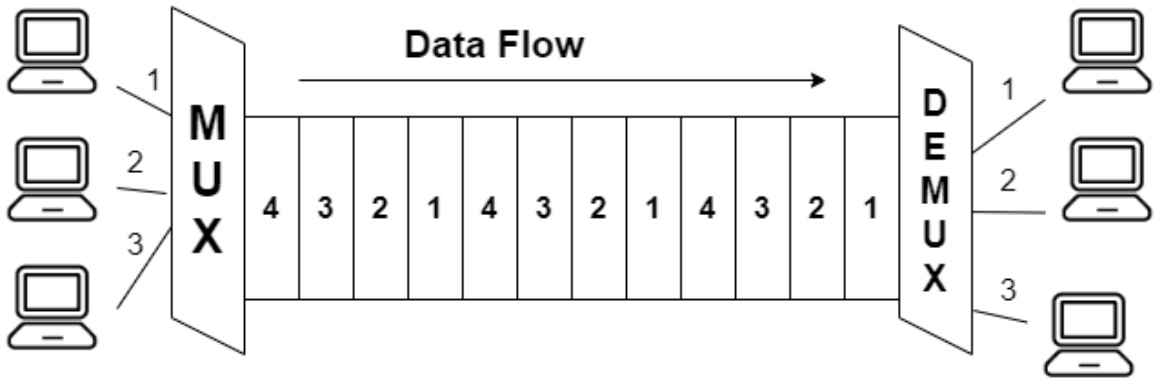
Time Division Multiplexing (TDM)

Time-Divison multiplexing is a digital technique for multiplexing.

- In this technique, the channel/link is divided on the basis of time instead of frequency.
- The total available time on the channel is divided between the different users on the channel.
- A particular time interval is allotted to each user on the channel and it is known as time slot/slice.
- In the time-division multiplexing, the data rate capacity should be much greater than the data rate that is required by the sending and receiving device.

TDM is further categorized into two:

- Synchronous Time-Divison Multiplexing
- Asynchronous Time-Divison Multiplexing



1. Synchronous Time-Divison Multiplexing

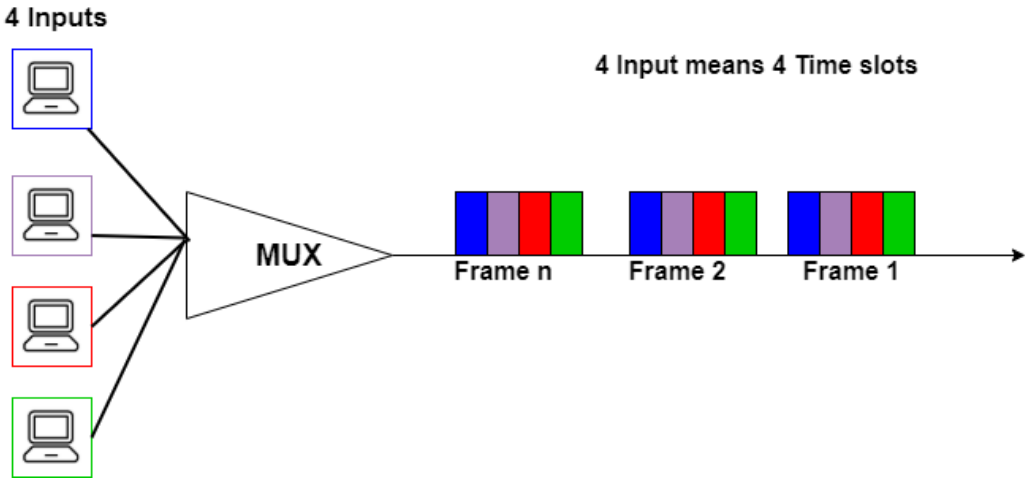
In Synchronous TDM, each of the Input connection has an allotment in the output even if it is not sending the data.

- In this multiplexing, each device is given the same time slot in order to transmit data over the link whether it has to send data to the receiver or not.
- Each device places data on the link whenever its time slot arrives Thus control is given to each device turn by turn.
- In case if any devices do not have any data to send then in that case the time slot for that device remains empty.
- In this multiplexing, if there are 'n' sending devices then

.

simultaneously there will be 'n' time slots which means one time slot for each device.

- Also, time slots are organized in the form of frames, where each frame consists of one or more time slots.



Advantages

- This technique is easy to implement.
- The performance is guaranteed in using this technique.

Disadvantages

- If a user has no data to transmit in that case time slots will get wasted.

2. Asynchronous Time-Division Multiplexing

Another name of Asynchronous TDM is Statical Time Divison Multiplexing. In this time slots are not fixed, rather time slots are allocated dynamically in order to improve the efficiency of bandwidth.

- The total speed of all the Input lines can be greater than the capacity of the path.

.

- In this Multiplexing, there are n input lines and m slots; thus always (m<n).
- There is no concept of predefined slots rather than slots are allocated dynamically on demand.
- In this multiplexing, the multiplexor mainly accepts the incoming input data and then it creates a frame that contains only data without any empty slots.
- Each slot mainly contains the address part that is used to identify the source of the input data.
- The number of frames in this multiplexing depends upon the statical analysis of the number of input lines.

Thus in the above diagram, out of 6 only 4 devices are sending data that are 1,2,4,6. In the above diagram, you can see that the data part contains the address in order to determine the source of the data. Like **A1**(data along with its source).

Advantages

- In this multiplexing, there is an efficient use of the capacity of transmission.

Disadvantages

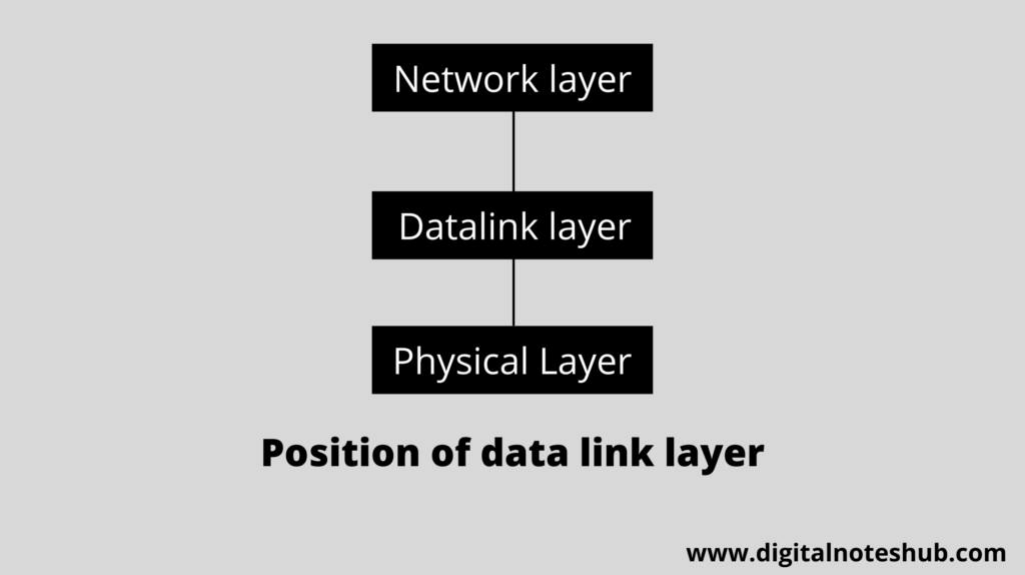
- In this Multiplexing, frames are of different sizes.
- There is a need for the buffer address information is also needed because there are no separate slots assigned for each user.
- This technique does not provide a fixed waiting time guarantee.

Unit 3

The Data Link Layer

Data link layer

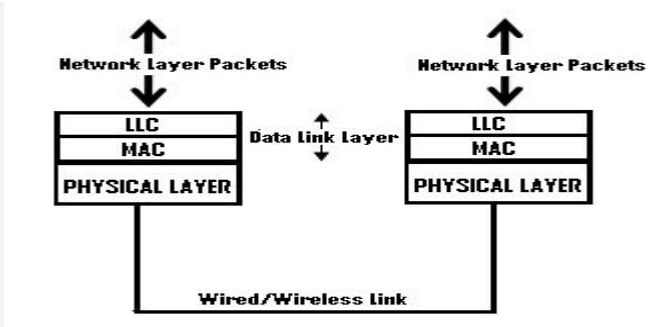
- ☐ The data link layer is the 2nd layer, and information at this layer is in the form of frames.
- ☐ The data link layer is mainly used to define the format of the data.
- ☐ The position of the data link layer is second in the internet model and stays between the network and physical layer as you can see in the following diagram.



It takes services from the physical layer and provides services to the network layer.

The primary function of this layer is **data synchronization**. The data link layer is further divided into two sub-layers as follows.

- ☐ Logical link control sub-layer
- ☐ Media access control sub-layer.



Logical link control (LLC) sub layer

The main functionality of the LLC layer is that it multiplexes the protocols over the MAC layer while sending and de-multiplex the protocols while receiving. This layer controls the flow control.

The error-checking of the data link layer is performed by LLC. It can also track the acknowledgments.

While transmitting data, if LLC detects any frame loss, immediately it sends back to the source to transmit over again. The LLC layer comes above the MAC layer and acts as an interface between the upper layers and the MAC layer.

Medium access control (MAC) sub layer

MAC address is defined and the Media Access Control address. It is a unique address that is allocated to the NIC(Network Interface Card) of the device. It is used as an address to transmit data within Ethernet or Wi-Fi.

This layer acts as an interface between the physical layer and the LLC layer in the OSI model. The main responsibility of the MAC layer is that it encapsulates the frames during transmission.

The MAC layer identifies and verifies the address of source stations and destinations. MAC layer performs multiple access resolution when there are more data frames.

MAC layer coordinates with the physical layer to seize a shared channel by using multiple MAC entities to avoid collisions.

Ethernet is an example of a medium that is defined through the MAC sub layer.

Data Link Layer design issues

The data link layer has to carry out several specific functions and the following are the main design issues of data link layer:

- Service Provided to Network Layer
- Frame synchronization
- Flow control
- Error control
- Addressing

☐ Service Provided to Network Layer

The data link layer provides services to the network layer. One of the main services is to transfer data from the source machine's network layer to the destination machine's network layer.

The network layer at the source machine transfers some data bits to the data link layer. Now the data link layer transmits these bits to the data link layer at the destination machine. The destination machine's data link layer hands over the bits to the network layer at the destination machine.

The types of services provided can be of three types –

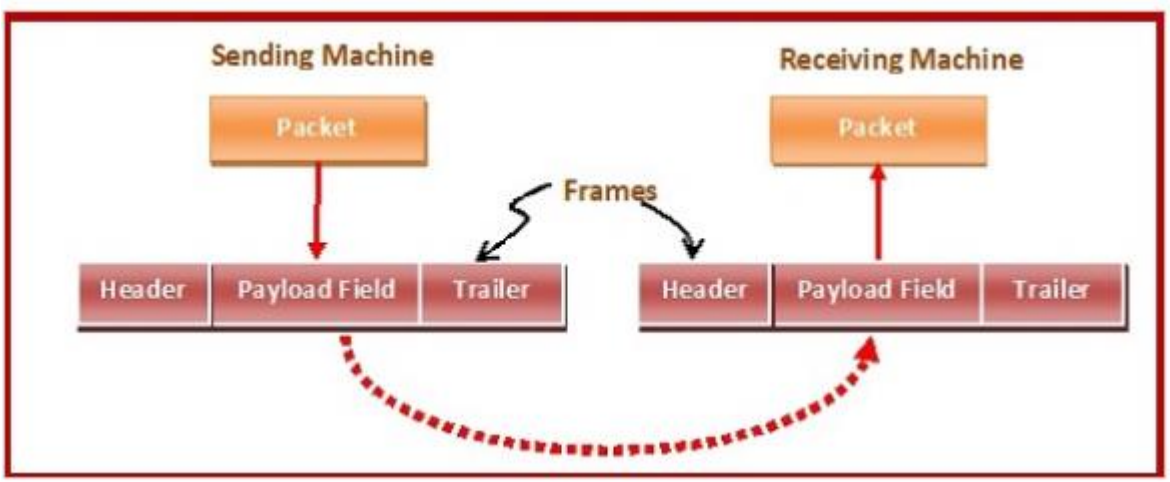
- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection - oriented service

☐ Frame Synchronization

Frame synchronization is one form the design issues of data link layer. The source machine sends data in a block called frame to the destination machine. The starting and ending of each frame must be recognized by the destination machine.

For frame recognition, every frame comprises three parts, A frame has three parts, namely

- Frame Header
- Payload field that contains the data packet from network layer
- Trailer



☐ Flow Control

The source machine should not send a data frame at a fast data rate as compared to the destination machine receiving data rate. When the sender sends the data at a high speed, the slow receiver cannot able to handle it and the frame can lose in such cases.

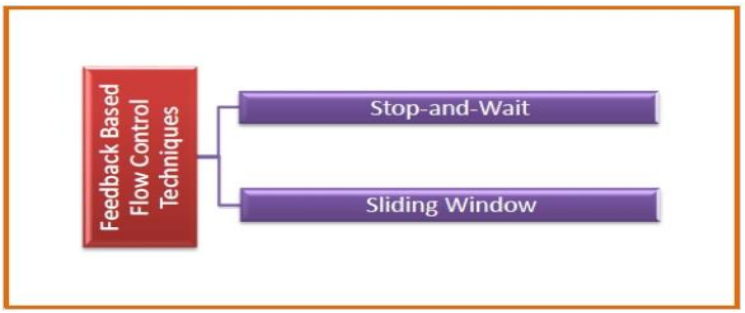
There are two types of techniques that are used for flow control as follows.

- Rate based flow control
- Feedback based flow control.

In data link layer, the sender continues to send frames only after it has received acknowledgments from the user for the previous frames. This is called feedback based flow control. Here, a restriction is imposed on the number of frames the sender can send before it waits for an acknowledgment from the receiver.

Feedback based Flow Control Techniques

Data link layer uses feedback based flow control mechanisms. There are two main techniques –



Stop and Wait

This protocol involves the following transitions –

- The sender sends a frame and waits for acknowledgment.
- Once the receiver receives the frame, it sends an acknowledgment frame back to the sender.

- On receiving the acknowledgment frame, the sender understands that the receiver is ready to accept the next frame. So it sender the next frame in queue.

Sliding Window

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

☐ **Error Control**

The errors made in bits during transmission from source to destination machines must be detected and corrected. The data link layer ensures error-free data transmission. For this, two types of error control techniques are used in the data link layer are as follows.

- Error detection techniques
- Error correction techniques

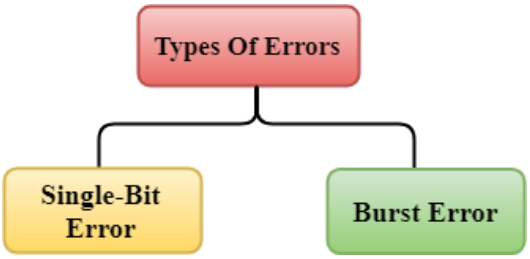
☐ **Addressing**

Addressing is also one of the design issues of data link layer. On a multipoint line, the identity of the individual machines must be specified while transmitting the data frames. Each frame comprises a header in which the source and destination addresses are placed.

Error Detection

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

Types Of Errors

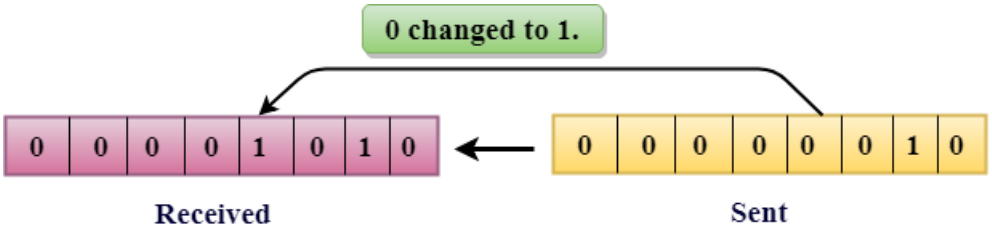


Errors can be classified into two categories:

- ☐ Single-Bit Error
- ☐ Burst Error

Single-Bit Error:

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1



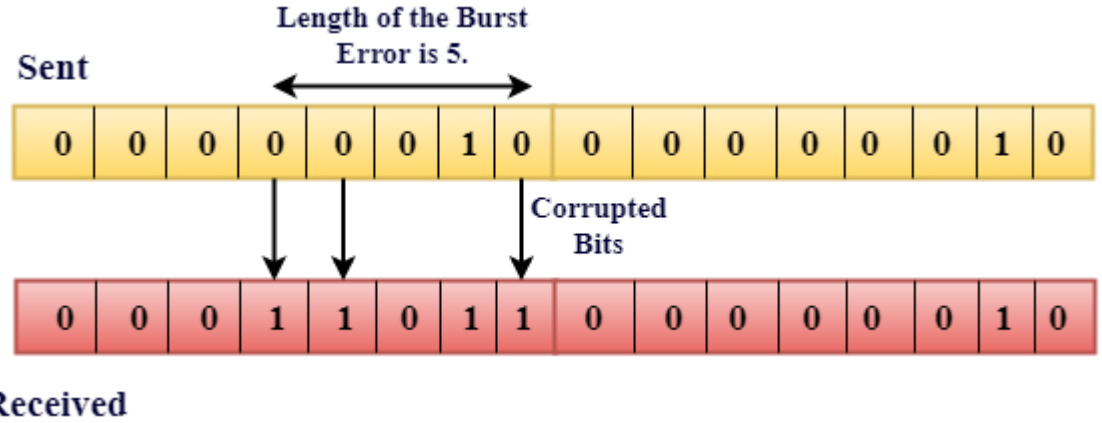
In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1.

Single-Bit Error does not appear more likely in Serial Data Transmission.
Single-Bit Error mainly occurs in Parallel Data Transmission.

For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

Burst Error:

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as **Burst Error**.
The Burst Error is determined from the first corrupted bit to the last corrupted bit.



The duration of noise in Burst Error is more than the duration of noise in Single-Bit.
Burst Errors are most likely to occur in Serial Data Transmission.
The number of affected bits depends on the duration of the noise and data rate.

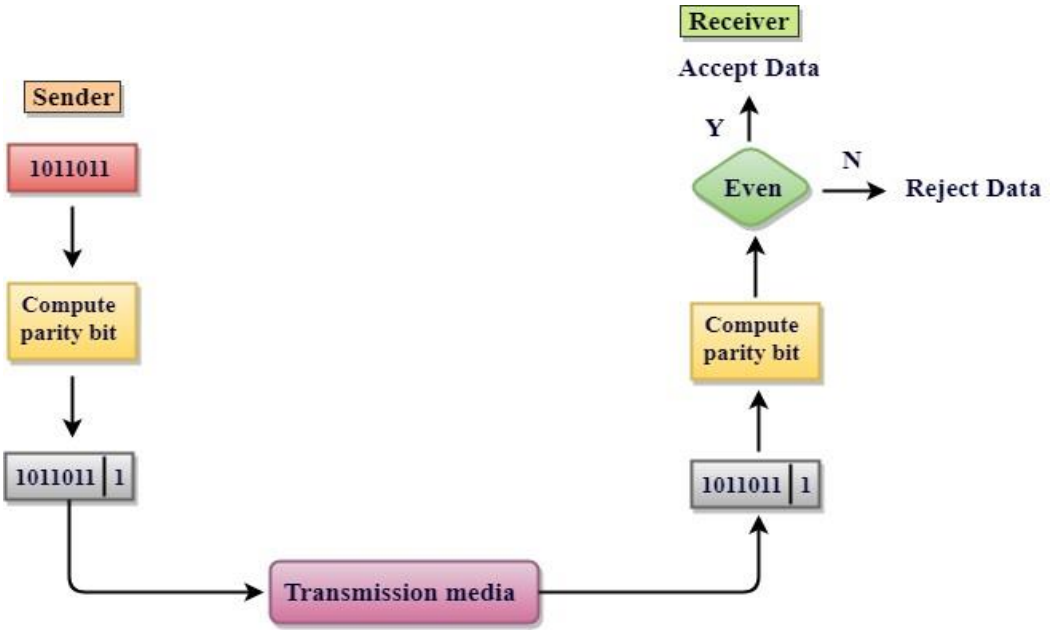
Error Detecting Techniques:

The most popular Error Detecting Techniques are:

- ☐ Single parity check
- ☐ Checksum
- ☐ Cyclic redundancy check

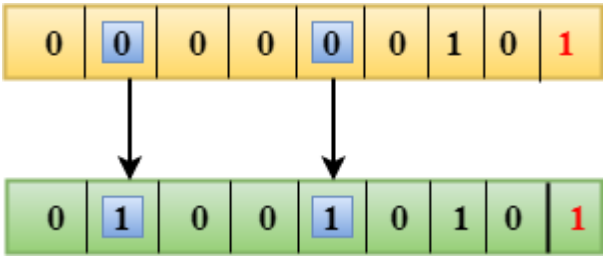
Single Parity Check

- ☐ Single Parity checking is the simple mechanism and inexpensive to detect the errors.
- ☐ In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.
- ☐ If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.
- ☐ At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- ☐ This technique generates the total number of 1s even, so it is known as even-parity checking.



Drawbacks Of Single Parity Checking

- ☐ It can only detect single-bit errors which are very rare.
- ☐ If two bits are interchanged, then it cannot detect the errors.



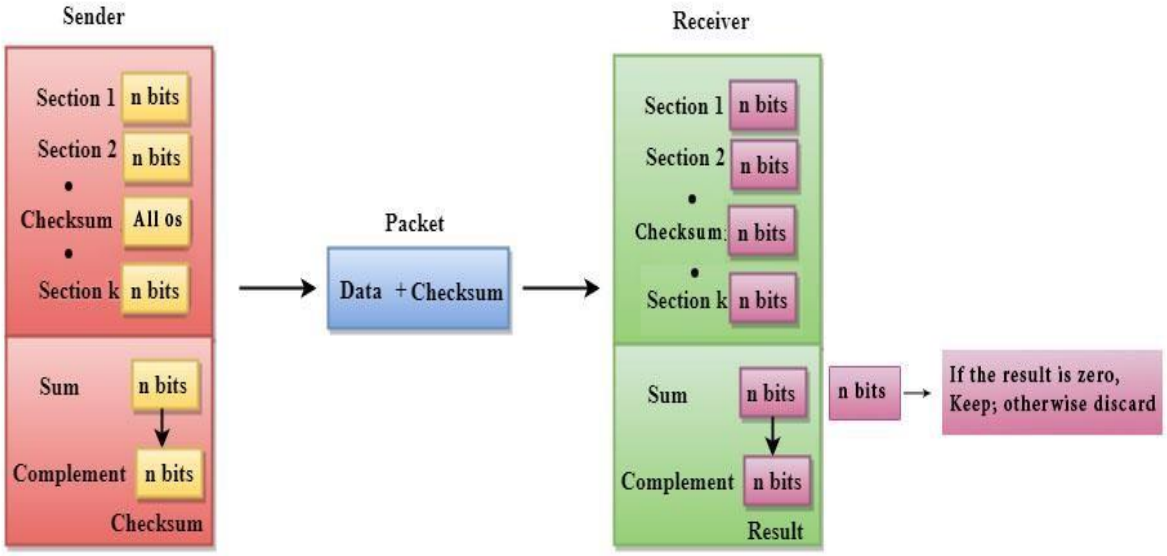
Checksum

A Checksum is an error detection technique based on the concept of redundancy.

It is divided into two parts:

1. **Checksum Generator**

A Checksum is generated at the sending side. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network.



1. The Sender follows the given steps:
2. The block unit is divided into k sections, and each of n bits.
3. All the k sections are added together by using one's complement t o get the sum.
4. The sum is complemented and it becomes the checksum field.
5. The original data and checksum field are sent across the network.

2. <u>Checksum Checker</u>

A Checksum is verified at the receiving side. The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented. If the complement of the sum is zero, then the data is accepted otherwise data is rejected.

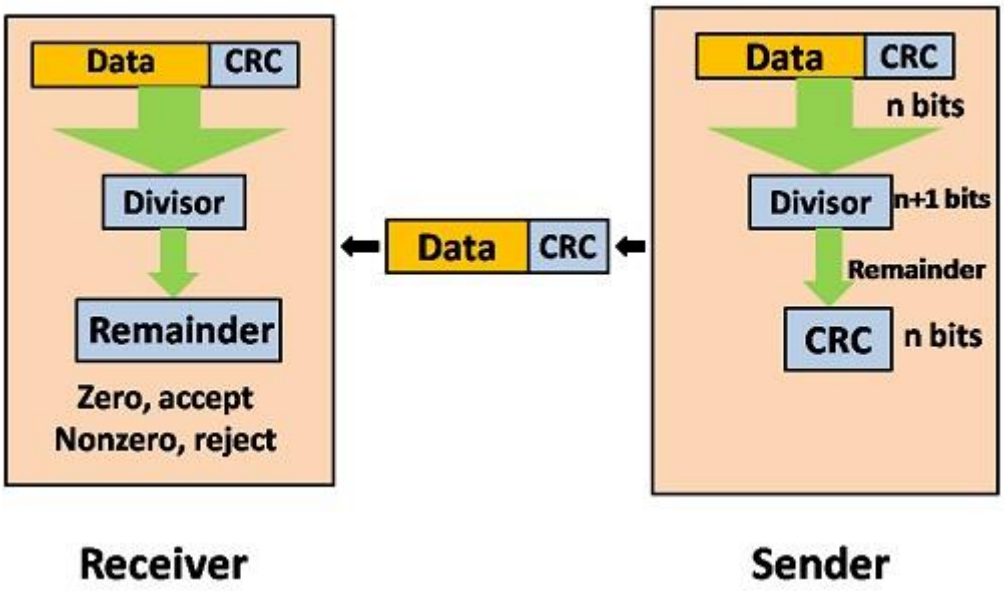
1. The Receiver follows the given steps:
2. The block unit is divided into k sections and each of n bits.
3. All the k sections are added together by using one's complement a lgorithm to get the sum.
4. The sum is complemented.
5. If the result of the sum is zero, then the data is accepted otherwis e the data is discarded.

<u>Cyclic Redundancy Check (CRC)</u>

CRC is a redundancy error technique used to determine the error.

Following are the steps used in CRC for error detection:

- In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.
- Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.
- Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.

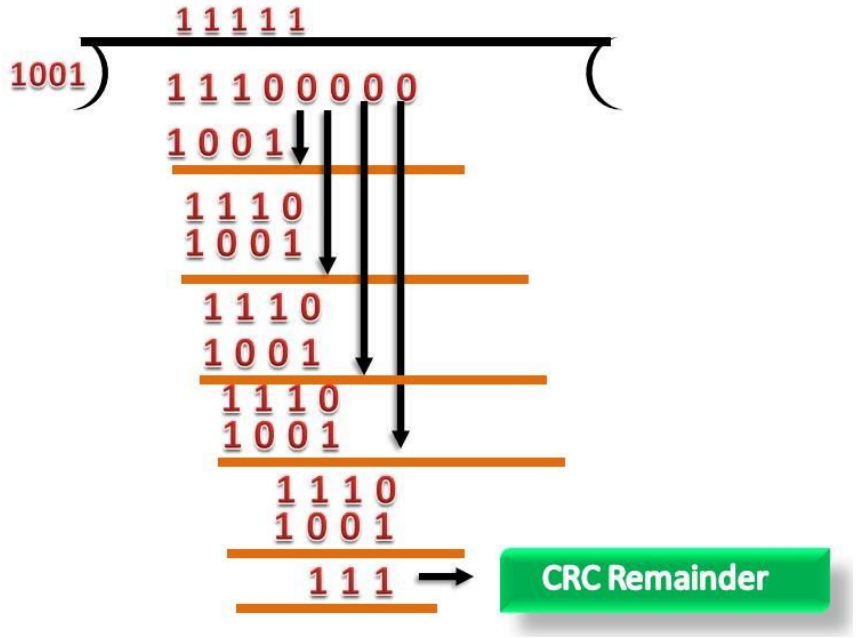


Let's understand this concept through an example:

Suppose the original data is 11100 and divisor is 1001.

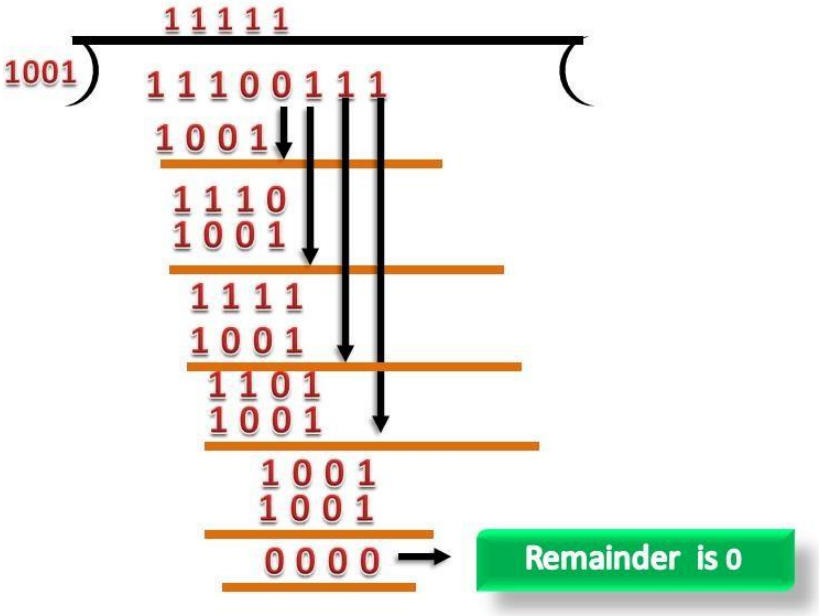
1) CRC Generator

- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.
- Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.



2) <u>CRC Checker</u>

- ☐ The functionality of the CRC checker is similar to the CRC generator.
- ☐ When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.
- ☐ A string is divided by the same divisor, i.e., 1001.
- ☐ In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted.



Polynomial Code

A polynomial code is a linear code having a set of valid code words that comprises of polynomials divisible by a shorter fixed polynomial is known as generator polynomial.

They are used for error detection and correction during the transmission of data as well as storage of data.

: 110001 represents:

$1 . x^5 + 1 . x^4 + 0 . x^3 + 0 . x^2 + 0 . x^1 + 1 . x^0$

$= x^5 + x^4 + x^0$

The **order** of a polynomial is the power of the highest non-zero coefficient. This is polynomial of order 5.

Types of Polynomial Codes

The types of polynomial codes are:

- ☐ Cyclic Redundancy Code
- ☐ Error Correction

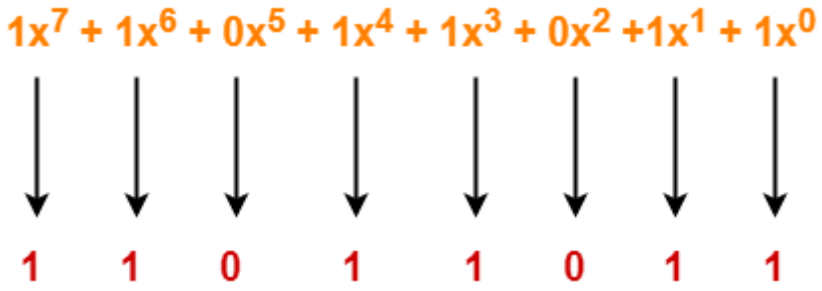
<u>Cyclic Redundancy Code</u>

- ☐ CRC generator is an algebraic polynomial represented as a bit pattern.
- ☐ Bit pattern is obtained from the CRC generator using the following rule-

The power of each term gives the position of the bit and the coefficient gives the value of the bit.

Example-

Consider the CRC generator is $x^7 + x^6 + x^4 + x^3 + x + 1$.
The corresponding binary pattern is obtained as-



Thus, for the given CRC generator, the corresponding binary pattern is 11011011.

Properties Of CRC Generator-

The algebraic polynomial chosen as a CRC generator should have at least the following properties-

Rule-01:

- ☐ It should not be divisible by x.
- ☐ This condition guarantees that all the burst errors of length equal to the length of polynomial are detected.

Rule-02:

- ☐ It should be divisible by x+1.
- ☐ This condition guarantees that all the burst errors affecting an odd number of bits are detected.

Important Notes-

If the CRC generator is chosen according to the above rules, then-

- ☐ CRC can detect all single-bit errors
- ☐ CRC can detect all double-bit errors provided the divisor contains at least three logic 1's.
- ☐ CRC can detect any odd number of errors provided the divisor is a factor of x+1.
- ☐ CRC can detect all burst error of length less than the degree of the polynomial.
- ☐ CRC can detect most of the larger burst errors with a high probability.

Steps Involved-

Error detection using CRC technique involves the following steps-

Step-01: Calculation Of CRC At Sender Side-

At sender side,

- ☐ A string of n 0's is appended to the data unit to be transmitted.
- ☐ Here, n is one less than the number of bits in CRC generator.
- ☐ Binary division is performed of the resultant string with the CRC generator.
- ☐ After division, the remainder so obtained is called as **CRC**.
- ☐ It may be noted that CRC also consists of n bits.

Step-02: Appending CRC To Data Unit-

At sender side,

- ☐ The CRC is obtained after the binary division.
- ☐ The string of n 0's appended to the data unit earlier is replaced by the CRC remainder.

Step-03: Transmission To Receiver-

- The newly formed code word (Original data + CRC) is transmitted to the receiver.

Step-04: Checking at Receiver Side-

At receiver side,

- The transmitted code word is received.
- The received code word is divided with the same CRC generator.
- On division, the remainder so obtained is checked.

The following two cases are possible-

Case-01: Remainder = 0

If the remainder is zero,

- Receiver assumes that no error occurred in the data during the transmission.
- Receiver accepts the data.

Case-02: Remainder ≠ 0

If the remainder is non-zero,

- Receiver assumes that some error occurred in the data during the transmission.
- Receiver rejects the data and asks the sender for retransmission.

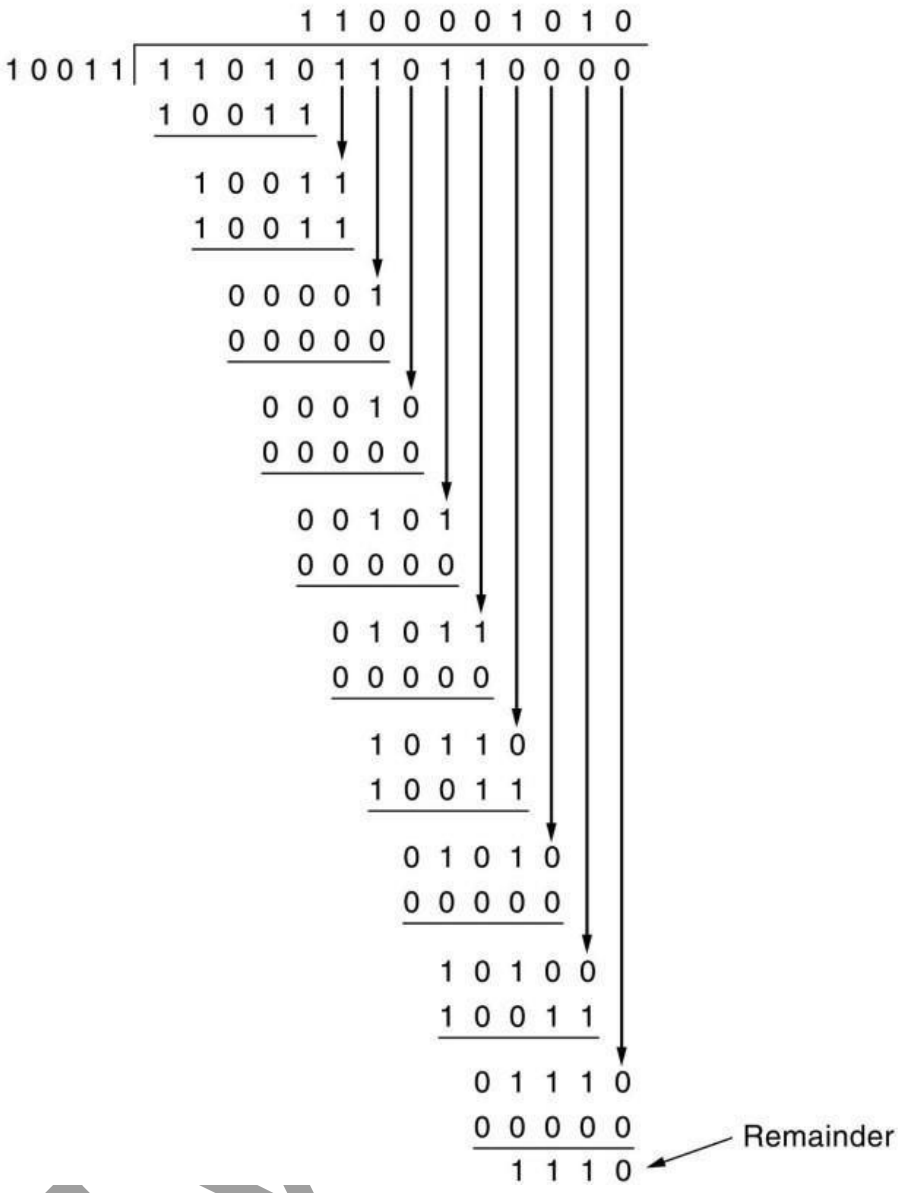
CYCLIC REDUNDANCY CHECK (CRC)-

A bit stream 1101011011 is transmitted using the standard CRC method. The generator polynomial is x^4+x+1. What is the actual bit string transmitted?

Solution-

- The generator polynomial $G(x) = x^4 + x + 1$ is encoded as 10011.
- Clearly, the generator polynomial consists of 5 bits.
- So, a string of 4 zeroes is appended to the bit stream to be transmitted.
- The resulting bit stream is 11010110110**0000**.

Now, the binary division is performed as-



From here, CRC = 1110.

Now,

- The code word to be transmitted is obtained by replacing the last 4 zeroes of 1101011011**0000** with the CRC.
- Thus, the code word transmitted to the receiver = 1101011011**1110**.

Hamming code

Hamming code is a special code in a Computer network, which is a set of **error-correction** codes. In Computer Graphics, it is mainly used for detecting and correcting errors that occur at the time of data transmission from sender to receiver.

Hamming Code

Parity Bits

A parity bit is added to the actual data block to make the number of 1's even or odd.

Basically, there are two types of parity bits:

Even parity: To check for even parity, if the total number of 1s is even, then the value of the parity bit is 0. If the total number of 1s occurrences is odd, then the value of the parity bit is 1.

Odd Parity: To check for odd parity, if the total number of 1s is even, then the value of parity bit is 1. If the total number of 1s is odd, then the value of parity bit is 0.

Algorithm of Hamming code:

The algorithm of the hamming code in computer networks comprises two major steps which are encoding and decoding a message. The data is encoded at the sender's side and decoded at the receiver's side.

Encode a message: We encode the message at the sender's side and then it is transmitted over the network. The following steps are involved in encoding a message.

- ☐ Write the bit position in the binary format.
- ☐ Calculate the number of redundant bits for a message.
- ☐ Do the positioning of redundant bits.
- ☐ Then do the calculations and calculate the value of each redundant bit.
- ☐ Append the redundant bits with actual data and transmit.

Decode the message: At the destination end, the receiver receives the encoded message and performs the recalculations to calculate the errors. If the message has an error, then these errors are corrected. To perform recalculations following steps are performed.

- ☐ Calculate the number of redundant bits using the same formula.
- ☐ Do the positioning of redundant bits.
- ☐ The parity checking technique is used to check parity bits.
- ☐ Perform error detection and correction.

Hamming Code Example

Let's take a hamming code example of a bit word 1011 is to be transmitted from the sender to the destination machine.

Construct the even parity seven-bit hamming code for this data.

The binary format of bits.

	R4	R3	R2	R1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0
11	1	0	1	1

R1-->1,3,5,7,9,11
R2-->2,3,6,7,10,1
R3 -->4,5,6,7
R4-->8,9,10,11

Positioning of redundant bits.

The positions which correspond to the power of 2 are filled with redundant bits. It means at positions 1,2, and 4 redundant bits are placed.

As in the above example, Number of data bits = 4

So the number of redundant of bits = 3

total number of bits to be transmitted = 4+3 = 7

D7	D6	D5	R4	D3	R2	R1

So put the bits into the above code word.

1	0	1	R4	1	R2	R1

Decide the Redundant bits

We calculate R1 bit using all bit positions whose binary representation includes 1 in the least significant position. It means bits 1,3,5,7 are used to calculate the value of the R1 bit.

We calculate the R2 bit using all the bit positions whose binary representation includes 1 in the second position from the least significant bits. It means bits 2,3,6,7 are used to calculate the value of the R2 bit.

We calculate the R4 bit using all the bit positions whose binary representation includes 1 in the third position from the least significant bits. It means bits 4,5,6,7 are used to calculate the value of the R4 bit.

We have to construct an even parity bit hamming code, as mentioned in the above example.

To calculate the redundant bit, use the even parity checking technique. It means the number 1's should be even as shown in the example below.

Decide R1 - R1,D3, D5, D7
as D3 D5 D7 =111 put R1 = 1 in order to have even parity

Decide R2 - R2,D3,D6,D7
as D3 D6 D7 = 101 hence Set R2= 0

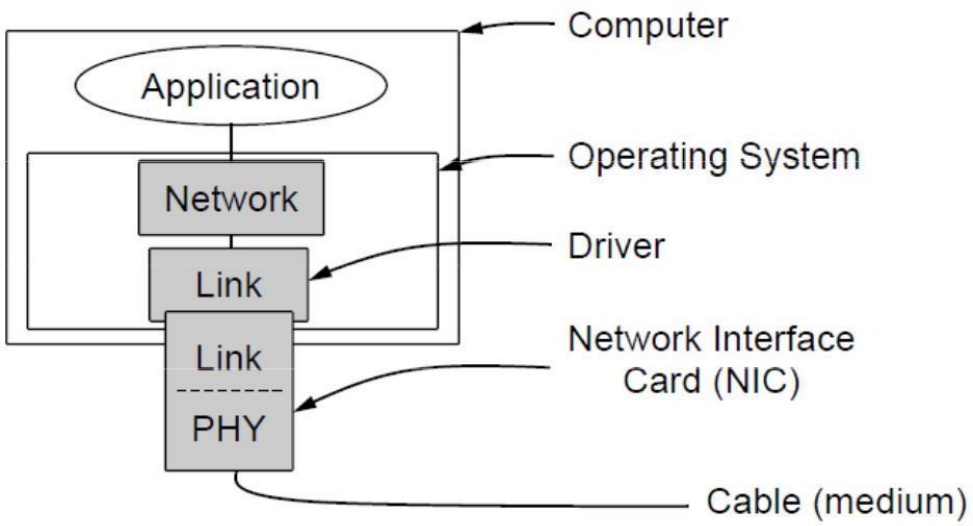
Decide R4 - R4,D5,D6,D7
as D5 D6 D7 = 101 so Set R4=0

Now we have calculated the valve of redundant bits to fill the value of redundant bits into the corresponding position. So following is the complete codeword to transmit.

1	0	1	0	1	0	1

Elementary data link protocols

- The physical layer, data link layer, and network layer are independent processes that communicate by passing messages back and forth.
- Machine A wants to send a long stream of data to machine B using a reliable connection to machine B using a reliable, connection-oriented service.
- Machines do not crash.



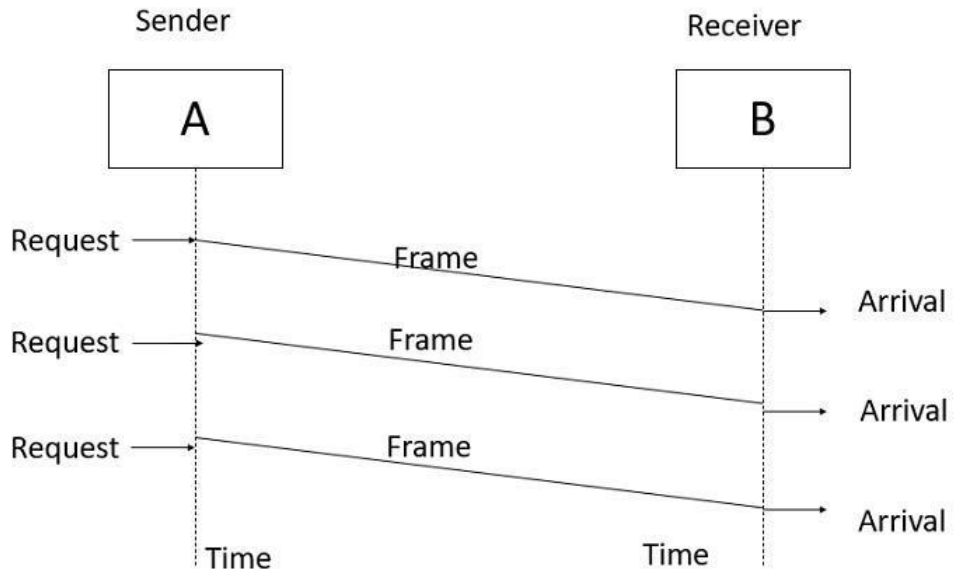
Elementary Data Link protocols are classified into three categories, as given below –

- Protocol 1 – Unrestricted simplex protocol
- Protocol 2 – Simplex stop and wait protocol
- Protocol 3 – Simplex protocol for noisy channels.

Unrestricted Simplex Protocol

- ☐ Data transmitting is carried out in one direction only.
- ☐ The transmission (Tx) and receiving (Rx) are always ready and the processing time can be ignored.
- ☐ In this protocol, infinite buffer space is available, and no errors are occurring that is no damage frames and no lost frames.

The Unrestricted Simplex Protocol is diagrammatically represented as follows –



Simplex Stop and Wait protocol

- ☐ In this protocol we assume that data is transmitted in one direction only. No error occurs; the receiver can only process the received information at finite rate.
- ☐ These assumptions imply that the transmitter cannot send frames at rate faster than the receiver can process them.

The main problem here is how to prevent the sender from flooding the receiver. The general solution for this problem is to have the receiver send some sort of feedback to sender, the process is as follows –

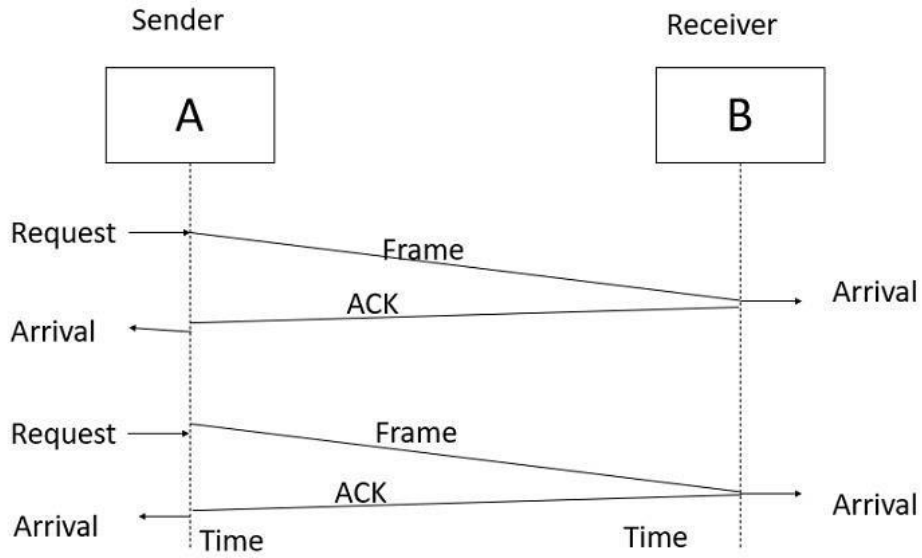
Step1 – The receiver send the acknowledgement frame back to the sender telling the sender that the last received frame has been processed and passed to the host.

Step 2 – Permission to send the next frame is granted.

Step 3 – The sender after sending the sent frame has to wait for an acknowledge frame from the receiver before sending another frame.

This protocol is called Simplex Stop and wait protocol, the sender sends one frame and waits for feedback from the receiver. When the ACK arrives, the sender sends the next frame.

The Simplex Stop and Wait Protocol is diagrammatically represented as follows –



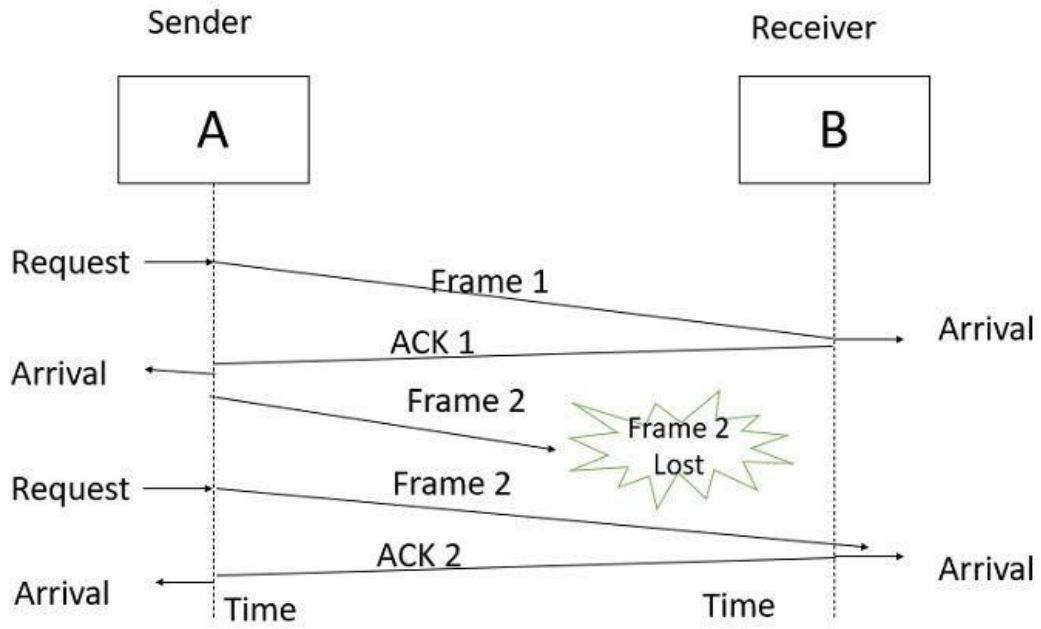
Simplex Protocol for Noisy Channel

Data transfer is only in one direction, consider separate sender and receiver, finite processing capacity and speed at the receiver, since it is a noisy channel, errors in data frames or acknowledgement frames are expected. Every frame has a unique sequence number.

After a frame has been transmitted, the timer is started for a finite time. Before the timer expires, if the acknowledgement is not received , the

frame gets retransmitted, when the acknowledgement gets corrupted or sent data frames gets damaged, how long the sender should wait to transmit the next frame is infinite.

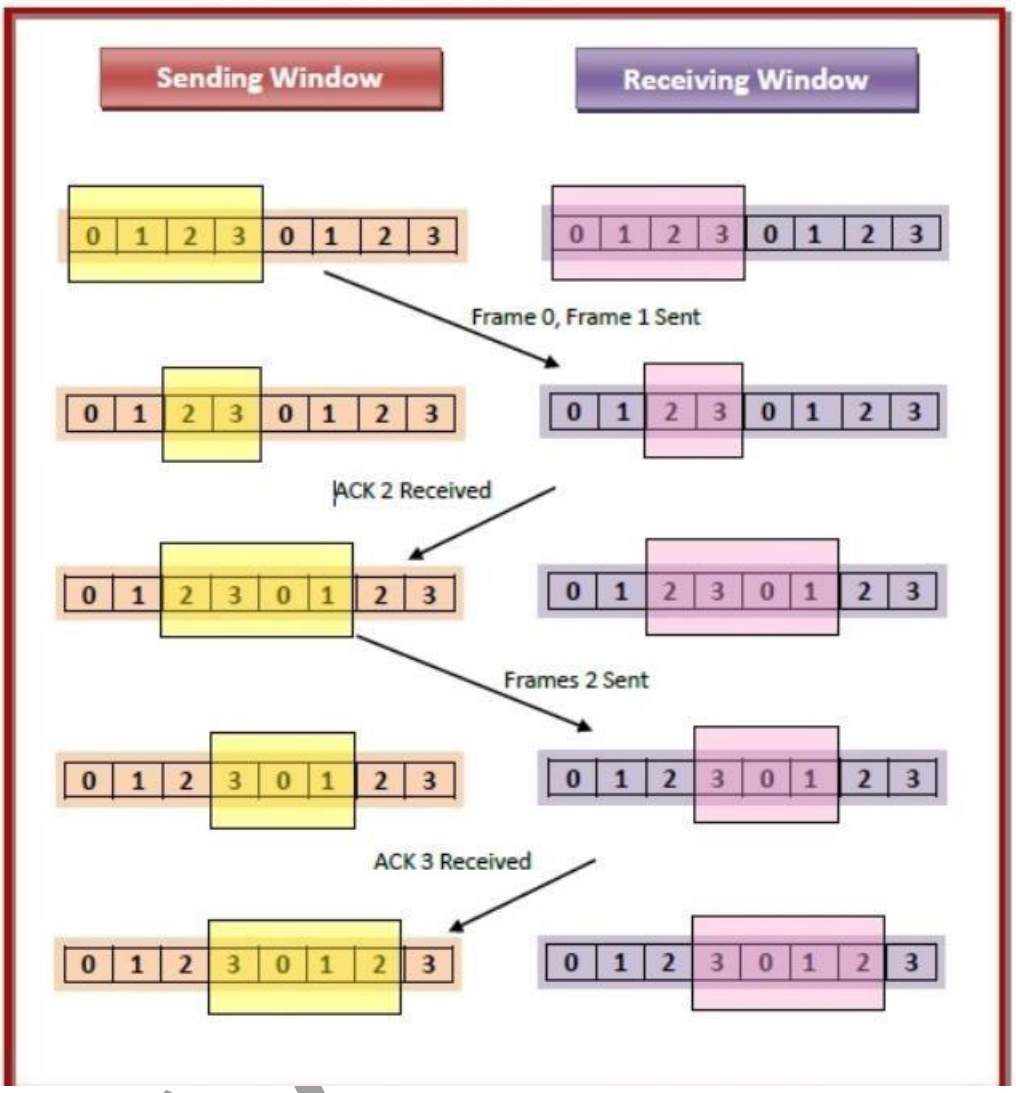
The Simplex Protocol for Noisy Channel is diagrammatically represented as follows –



Sliding Window Protocol

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

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



Sliding Window (Sender and Receiver side):

a. Sender Side:

The sequence number of the frame occupies a field in the frame. So, the sequence number should be kept to a minimum.

The sequence number ranges from 0 to 2k-1 if the frame header allows k bits.

The sender maintains a list of sequence numbers that are only allowed to be sent by the sender.

The sender window can only be 2k-1 in size.

For example, if the frame allows 4 bits, the window's size is 2 raised to the power 4 -1 16-1=15.

The sender has a buffer with the same size as the window.

b. Receiver Side:

On the receiver side, the size of the window is always 1.

The receiver acknowledges a frame by sending an ACK frame to the sender, along with the sequence number of the next expected frame.

The receiver declares explicitly that it is ready to receive N subsequent frames, starting with the specified number.

We use this scheme in order to acknowledge multiple frames.

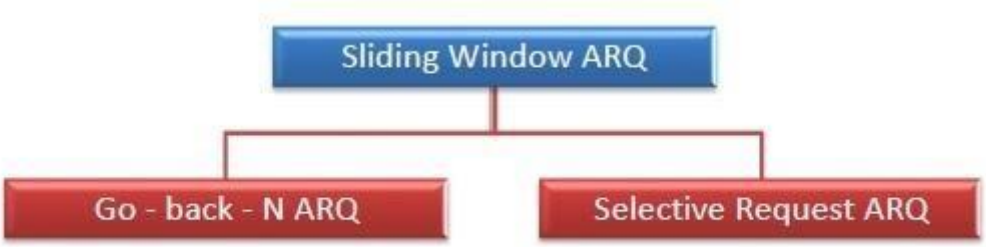
The receiver's window can hold 2,3,4 frames, but the ACK frame will be held until frame 4 arrives. It will send the

ACK along with sequence number 5 after the arrival, with which the acknowledgment of 2,3,4 will be done one at a time.

The receiver requires a buffer size of one.

Types of Sliding Window Protocols

The Sliding Window ARQ (Automatic Repeat reQuest) protocols are of two categories –



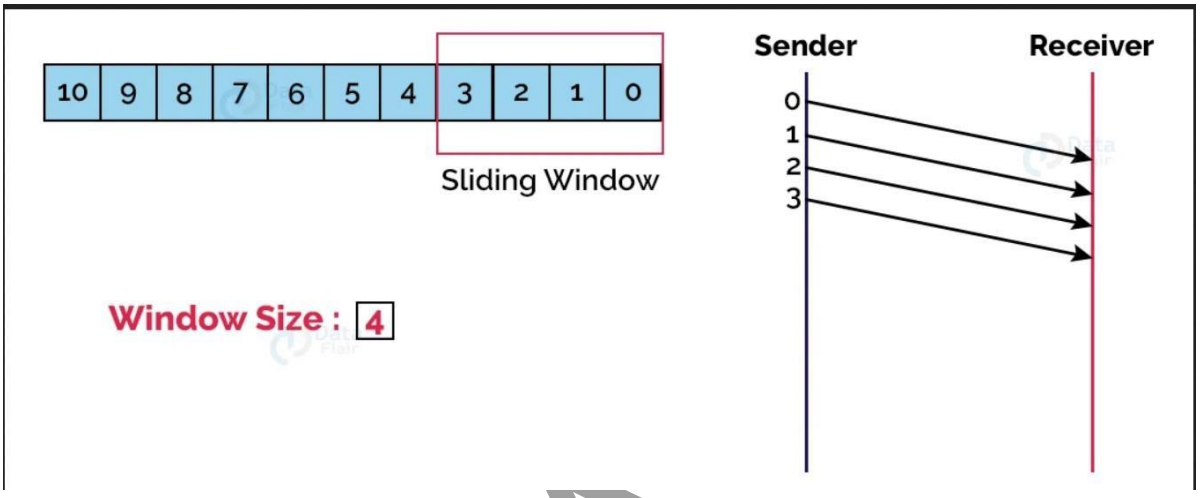
1. Go-Back-N ARQ:

The Go-Back-N Automatic Repeat Request protocol is also known as the Go-Back-N ARQ protocol. A sliding window method finds use in this data link layer protocol. In the event of corruption or loss of frames, all subsequent frames must be sent again.

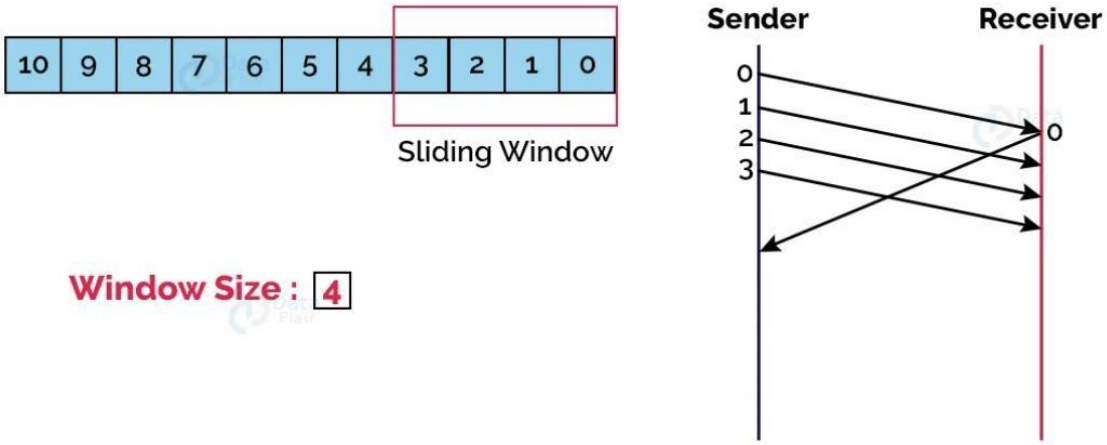
In this protocol, the sender window size is N. The size of the receiver window is always one.

In the event of transmission of a corrupted frame, the receiver cancels it. The receiver does not accept a corrupted frame. The sender sends the correct frame again when the timer expires.

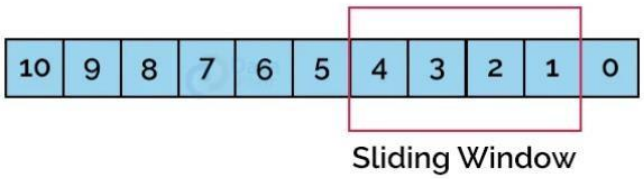
Example of Go-Back-N ARQ:



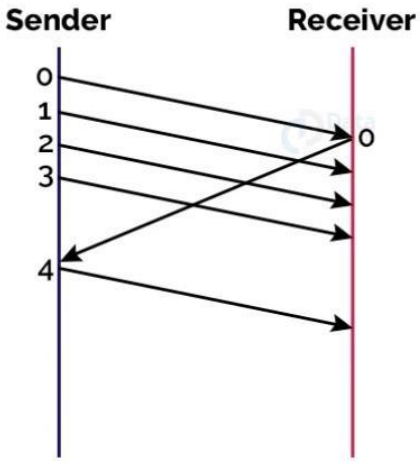
a. First, the sender sends the first four frames in the window (here the window size is 4).



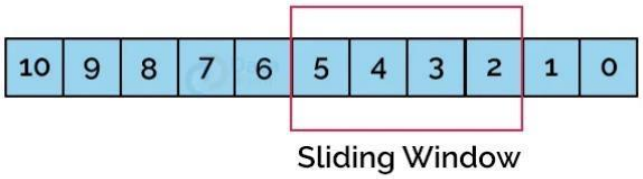
b. Then, the receiver sends the acknowledgment for the 0th frame.



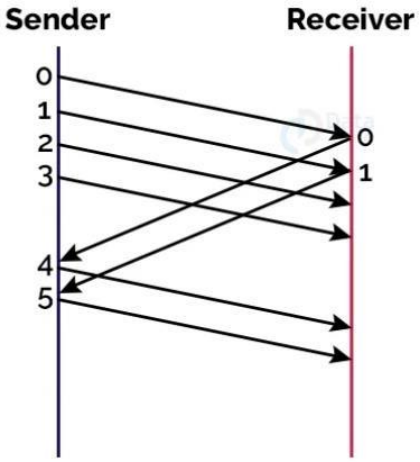
Window Size : 4



c. The receiver then slides the window over and sends the next frame in the queue.



Window Size : 4



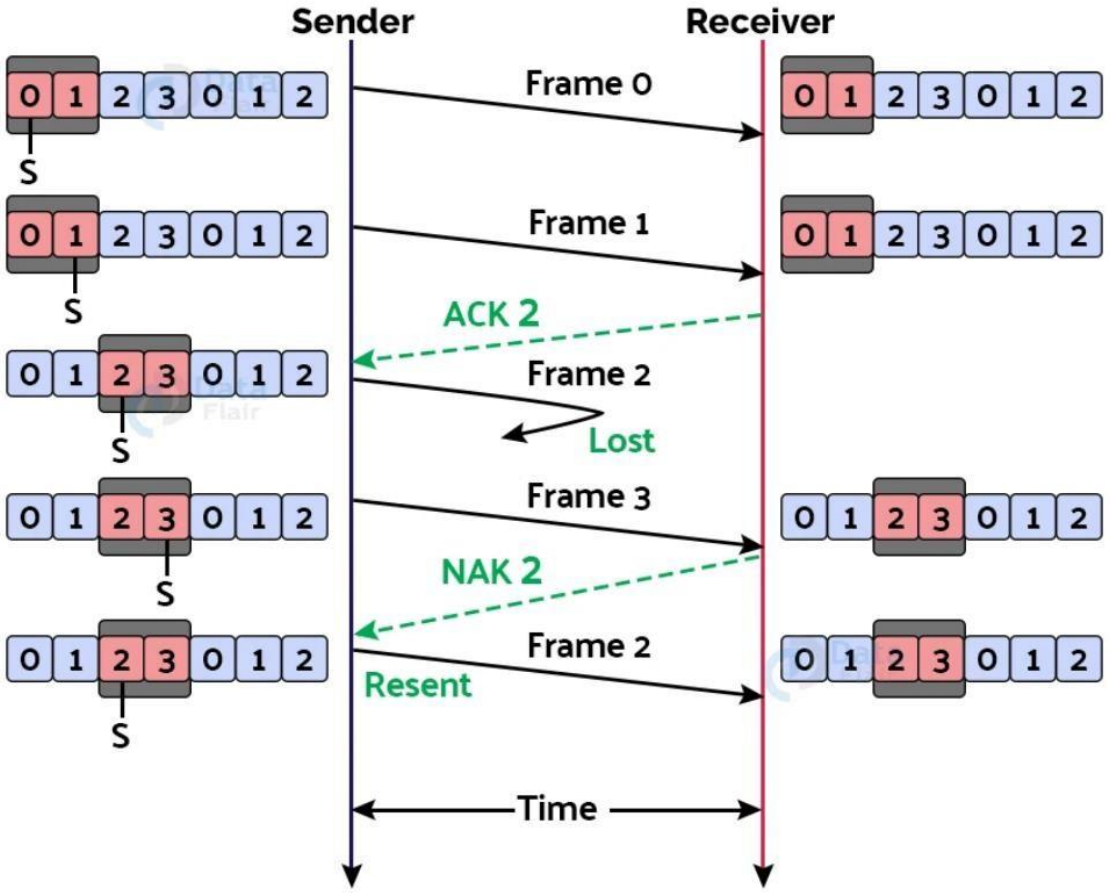
d. Accordingly, the receiver sends the acknowledgement for the 1st frame, and upon receiving that, the sender slides the window again and sends the next frame. This process keeps on happening until all the frames are sent successfully.

2. Selective Repeat ARQ:

Selective Repeat ARQ (Selective Repeat Automatic Repeat Request) is another name for Selective Repeat ARQ. A sliding window method is used in this data link layer protocol. If the frame has fewer errors, Go-Back-N ARQ works well. However, if the frame contains a lot of errors, sending

the frames again will result in a lot of bandwidth loss. As a result, we employ the Selective Repeat ARQ method. The size of the sender window is always equal to the size of the receiver window in this protocol. The sliding window's size is always greater than 1.

Example of Selective Repeat ARQ:



a. First, the sender sends the contents of the first window, which are frames 0 and 1 (because the window size is 2).

b. When the receiver receives the frames sent above, it sends an acknowledgment for frame 2 (because frame 2 is the frame it expects to receive next).

c. The sender then sends frames 2 and 3, however, frame 2 is lost on the way. The receiver thus sends back a "NAK" signal or a non-acknowledgment to let the sender know that frame 2 has been lost, and thus the sender retransmits frame 2.

Unit 5:Transport Layer

By:

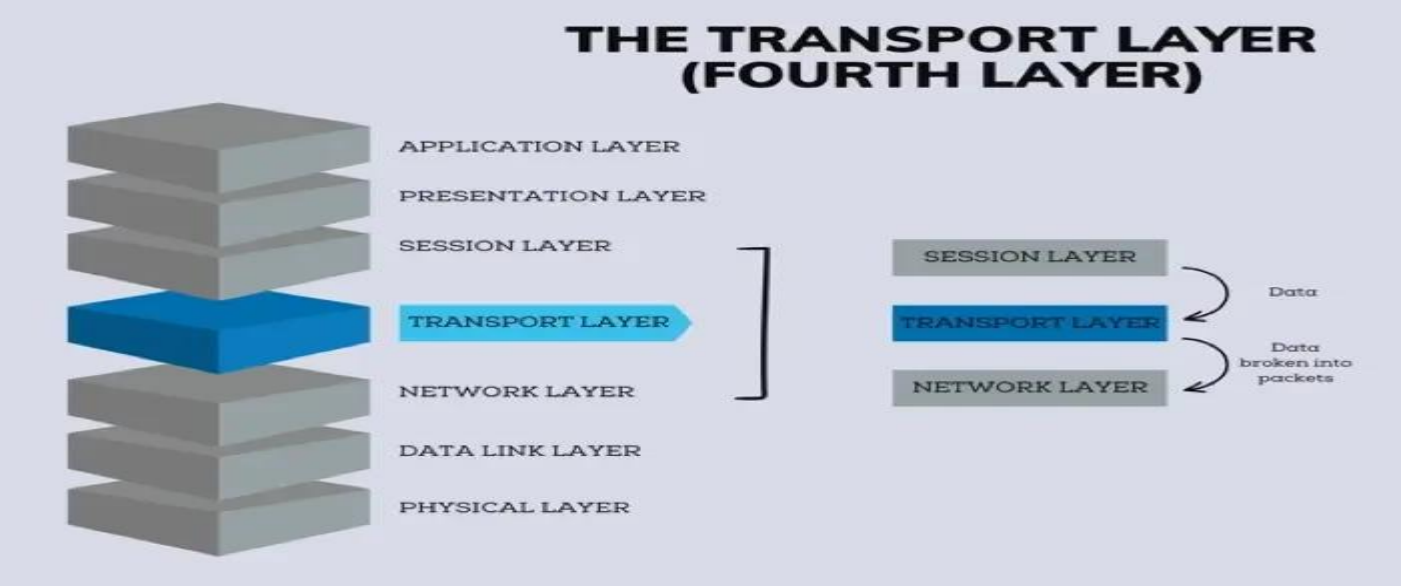
Prof.Anusha Priyadharshini.C

HOD of computer science

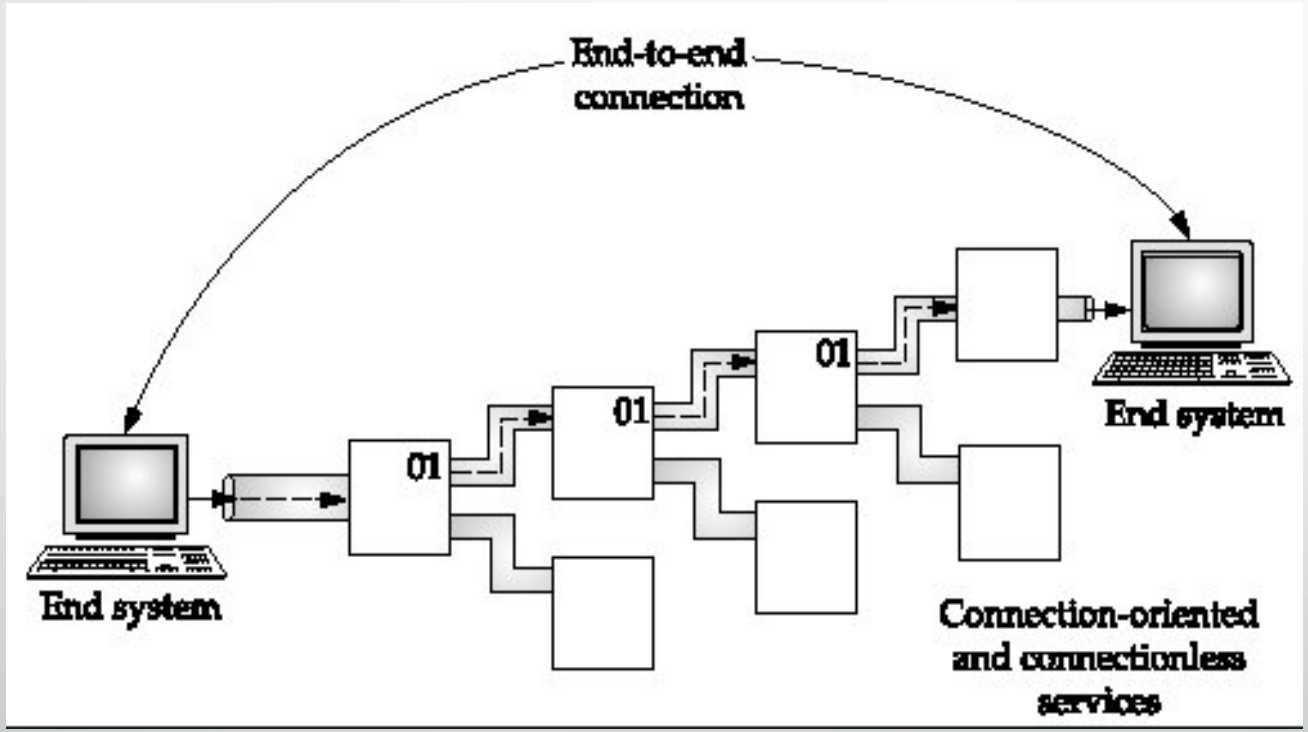
The National Degree college,Bagepalli

Define Network layer

- The transport Layer is the second layer in the TCP/IP model and the fourth layer in the OSI model. It is an end-to-end layer used to deliver messages to a host. It is termed an end-to-end layer because it provides a point-to-point connection rather than hop-to-hop, between the source host and destination host to deliver the services reliably. The unit of data encapsulation in the Transport Layer is a segment.



Example of end to end connection



Responsibilities of a Transport Layer

- The Process to Process Delivery
- End-to-End Connection between Hosts
- Multiplexing and Demultiplexing
- Congestion Control
- Data integrity and Error correction
- Flow control

QoS(Quality of service)

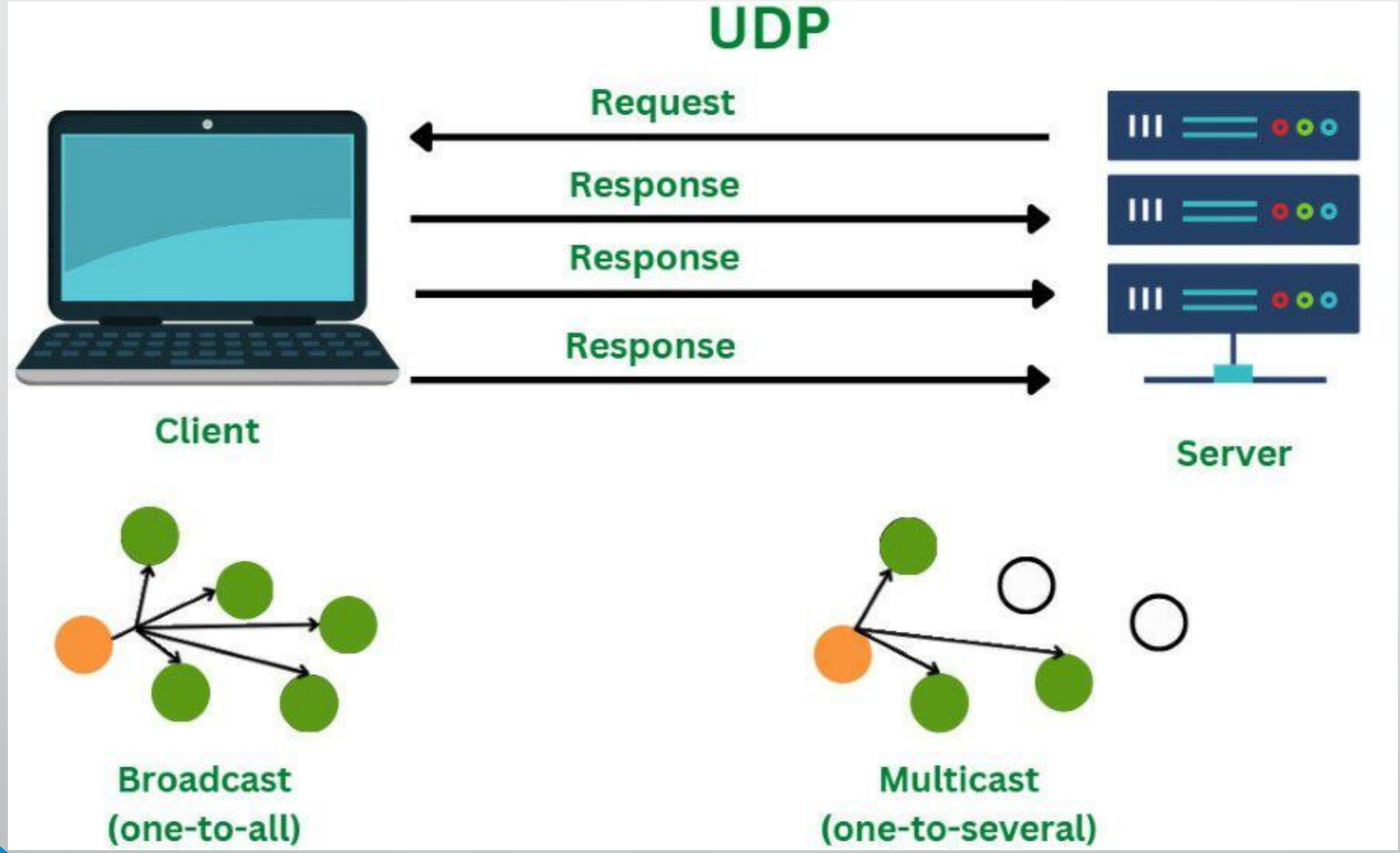
- QoS or Quality of service is a measurement of the overall performance of a service such as a computer network,telephony,or cloud computing.QoS in networking refers to the technology used to manage traffic passing through the network and ensure the performance like jitter,packet loss and latency in the network.

Transport Layer Protocols

- The transport layer is represented majorly by TCP and UDP protocols.
- Today almost all operating systems support multiprocessing multi-user environments. This transport layer protocol provides connections to the individual ports. These ports are known as protocol ports.
- Transport layer protocols work above the IP protocols and deliver the data packets from IP serves to destination port and from the originating port to destination IP services.

1. UDP

- UDP stands for User Datagram Protocol.
- User Datagram Protocol provides a nonsequential transmission of data.
- It is a connectionless transport protocol.
- UDP protocol is used in applications where the speed and size of data transmitted is considered as more important than the security and reliability.
- User Datagram is defined as a packet produced by User Datagram Protocol. UDP protocol adds checksum error control, transport level addresses.


UDP
Request
Response
Response
Response
Client
Server
Broadcast
(one-to-all)
Multicast
(one-to-several)

UDP Segment(packet format)

- While the TCP header can range from 20 to 60 bytes, the UDP header is a fixed, basic 8 bytes.
- All required header information is contained in the first 8 bytes, with data making up the remaining portion.
- Because UDP port number fields are 16 bits long, the range of possible port numbers is defined as 0 to 65535, with port 0 being reserved.

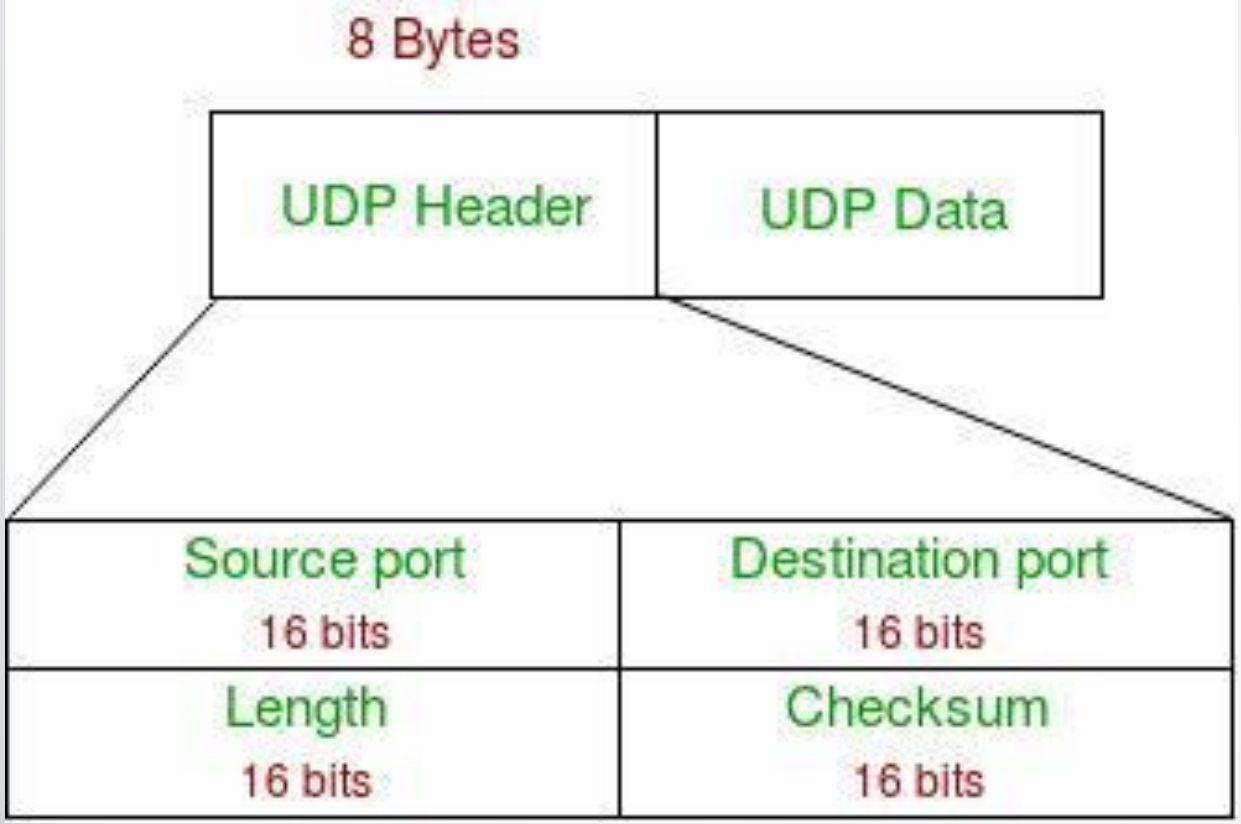


Fig:UDP PACKET/SEGMENT FORMAT

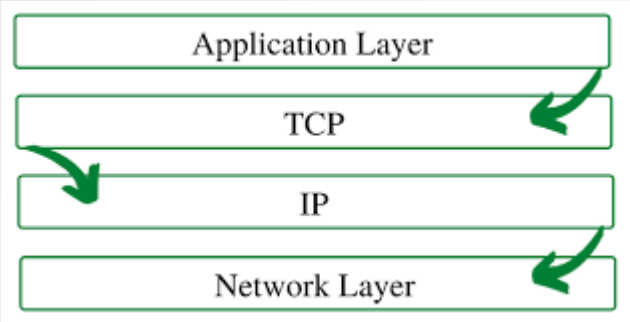
- **Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
- **Destination Port:** This 2-byte element is used to specify the packet's destination port.
- **Length:** The whole length of a UDP packet, including the data and header. The field has sixteen bits.
- **Cheksum:** The checksum field is two bytes long. The data is padded with zero octets at the end (if needed) to create a multiple of two octets. It is the 16-bit one's complement of the one's complement sum of the UDP header, the pseudo-header containing information from the IP header, and the data.

Features of UDP Protocol

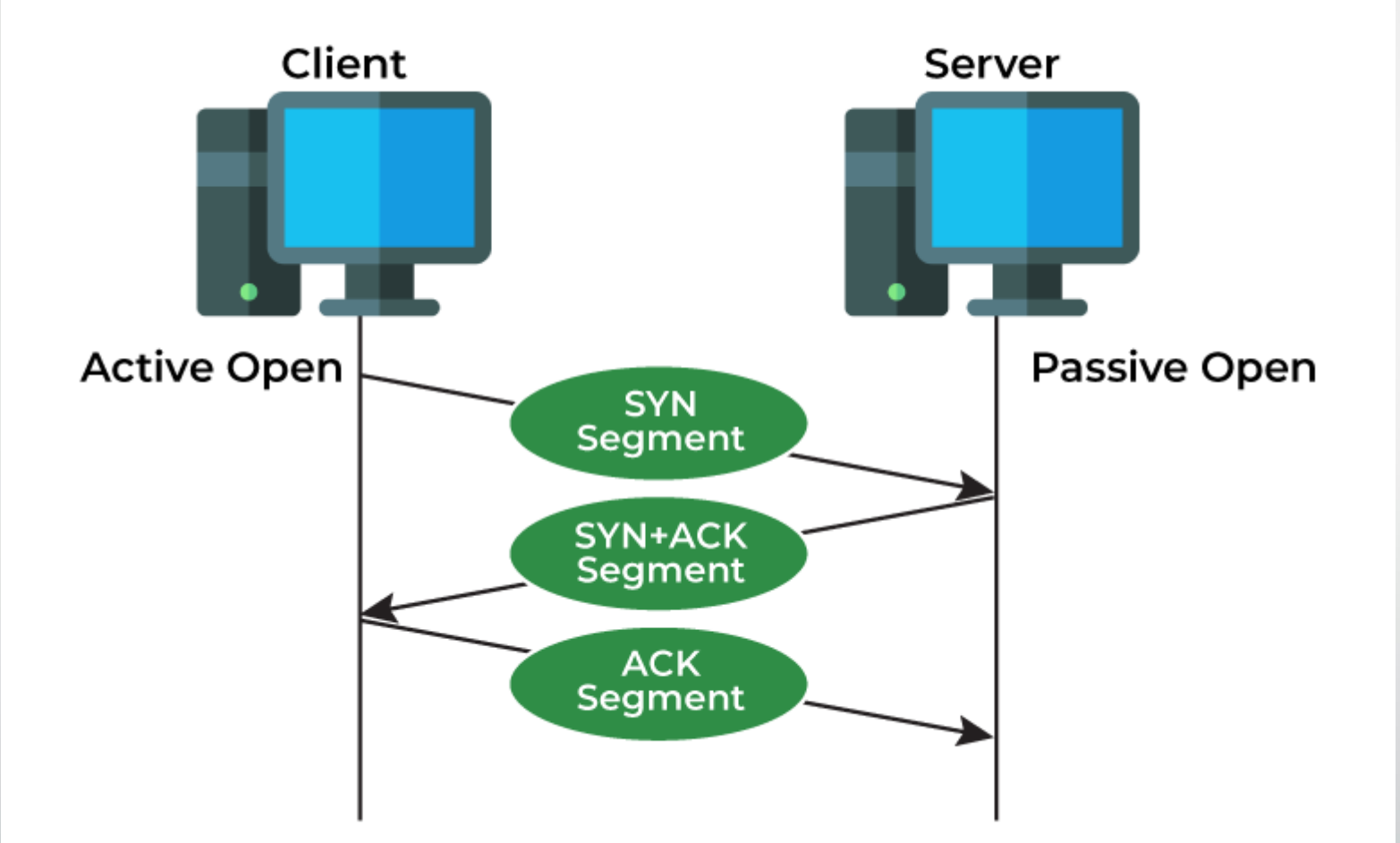
- 1.Transport layer Protocol
  - Used datagram protocol is a transport layer protocol.
- 2.connectionless
  - UDP protocol is connectionless protocol,so it does not establish any virtual path before transmitting the data.
  - Since it is connectionless,so packets are sent from different paths between sender and receiver.
- 3.Ordered delivery of data is not guaranteed.
  - Udp does not guarantee the order of the datagram.A datagram can be in any order
  - The UDP protocol uses different port number for transmitting data to the correct destination.
  - The port numbers are defined between 0-1023.
- 4.Faster Transmission.
  - Udp provides faster data transmission as there is no prior connection establishment before transmitting data.

- **Advantages of UDP**
- UDP also provides multicast and broadcast transmission of data.
- UDP protocol is preferred more for small transactions such as DNS lookup.
- It is a connectionless protocol, therefore there is no compulsion to have a connection-oriented network.
- UDP provides fast delivery of messages.
- **Disadvantages of UDP**
- In UDP protocol there is no guarantee that the packet is delivered.
- UDP protocol suffers from worse packet loss.
- UDP protocol has no congestion control mechanism.
- UDP protocol does not provide the sequential transmission of data.

Transmission control protocol(TCP)

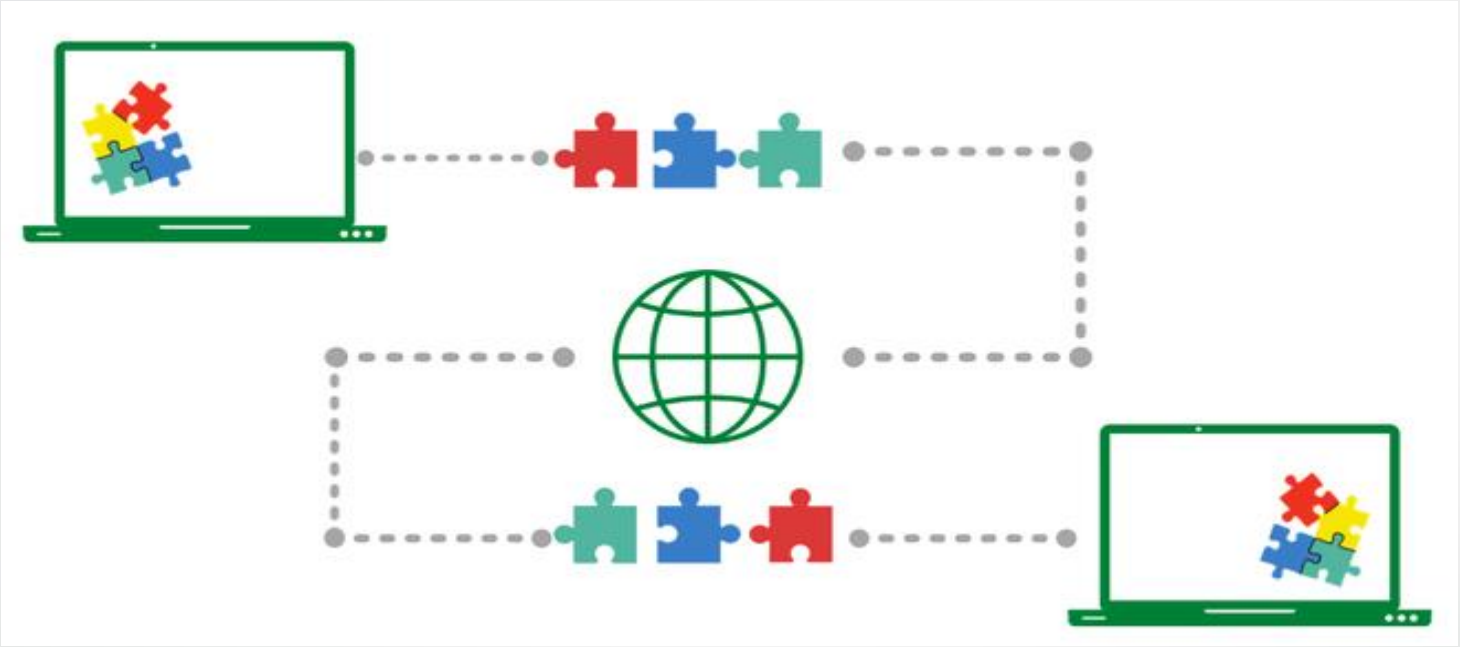


TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between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



Transmission Control Protocol

WORKING OF TCP



In the figure,We can see that the message is being broken down, then reassembled from a different order at the destination

For example, When a user requests a web page on the internet, somewhere in the world, the server processes that request and sends back an HTML Page to that user. The server makes use of a protocol called the HTTP Protocol. The HTTP then requests the TCP layer to set the required connection and send the HTML file.

Now, the TCP breaks the data into small packets and forwards it toward the Internet Protocol (IP) layer. The packets are then sent to the destination through different routes.

Features of TCP

- Some of the most prominent features of Transmission control protocol are

1. Segment Numbering System

- TCP keeps track of the segments being transmitted or received by assigning numbers to each and every single one of them.
- *Acknowledgment Numbers* are assigned to received segments.

2. Connection Oriented

- It means sender and receiver are connected to each other till the completion of the process.
- The order of the data is maintained i.e. order remains same before and after transmission.

Features of TCP(cont..)

3.Full Duplex

- In TCP data can be transmitted from receiver to the sender or vice – versa at the same time.
- It increases efficiency of data flow between sender and receiver.

4.Flow Control

- Flow control limits the rate at which a sender transfers data. This is done to ensure reliable delivery.
- The receiver continually hints to the sender on how much data can be received (using a sliding window.

5. Error Control

- TCP implements an error control mechanism for reliable data transfer.

6. Congestion Control

- TCP takes into account the level of congestion in the network
- Congestion level is determined by the amount of data sent by a sender

Most common TCP/IP protocols

- HTTP, HTTPS - for web browsing,
- FTP, TFTP, NFS - for file transfer,
- SMTP - for sending email messages,
- POP3 - for receiving email messages,
- IMAP - for managing email messages on the server,
- Telnet, rLogin - for accessing remote computers,
- SNMP - for network management,

Advantages

- It is a reliable protocol.
- It provides an error-checking mechanism as well as one for recovery.
- It gives flow control.
- It makes sure that the data reaches the proper destination in the exact order that it was sent.
- Open Protocol, not owned by any organization or individual.
- It assigns an IP address to each computer on the network and a domain name to each site thus making each device site to be distinguishable over the network.

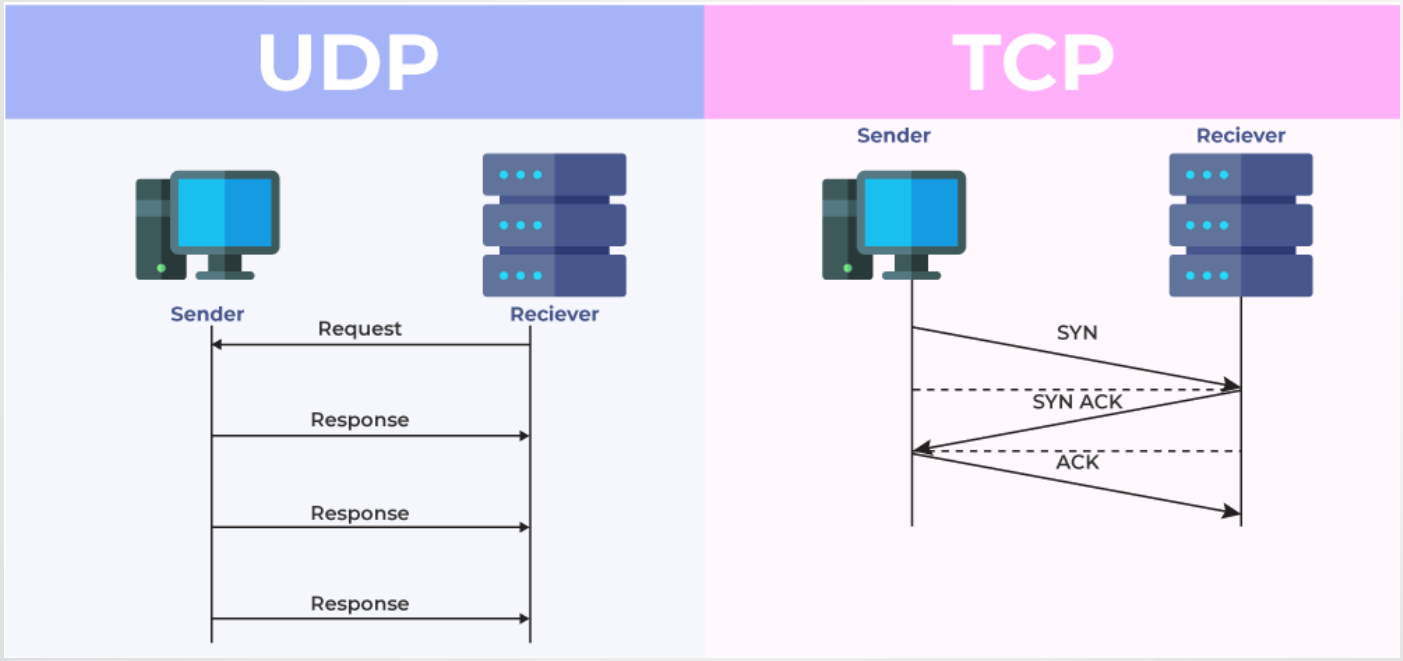
Disadvantages

- TCP is made for Wide Area Networks, thus its size can become an issue for small networks with low resources.
- TCP runs several layers so it can slow down the speed of the network.
- It is not generic in nature. Meaning, it cannot represent any protocol stack other than the TCP/IP suite. E.g., it cannot work with a Bluetooth connection.
- No modifications since their development around 30 years ago.

Which Protocol is Better: TCP or UDP?

- The answer to this question is difficult because it totally depends on what work we are doing and what type of data is being delivered. UDP is better in the case of online gaming as it allows us to work lag-free. TCP is better if we are transferring data like photos, videos, etc. because it ensures that data must be correct has to be sent.
- In general, both TCP and UDP are useful in the context of the work assigned by us. Both have advantages upon the works we are performing, that’s why it is difficult to say, which one is better.

Difference between UDP and TCP



Where TCP is Used?

- Sending Emails
- Transferring Files
- Web Browsing

Where UDP is Used?

- Gaming
- Video Streaming
- Online Video Chats

Differences between TCP and UDP

Basis	Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Type of Service	TCP is a connection-oriented protocol. Connection orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, or terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error-checking mechanism using checksums.
Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.

Sequence	Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Protocols	TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.
Applications	This protocol is primarily utilized in situations when a safe and trustworthy communication procedure is necessary, such as in email, on the web surfing, and in military services.	This protocol is used in situations where quick communication is necessary but where dependability is not a concern, such as VoIP, game streaming, video, and music streaming, etc.

Application layer

- The Application Layer is topmost layer in the Open System Interconnection (OSI) model. This layer provides several ways for manipulating the data (information) which actually enables any type of user to access network with ease. This layer also makes a request to its bottom layer, which is presentation layer for receiving various types of information from it. The Application Layer interface directly interacts with application and provides common web application services. This layer is basically highest level of open system, which provides services directly for application process.

Functions of Application Layer :

- Application Layer provides a facility by which users can forward several emails and it also provides a storage facility.
- This layer allows users to access, retrieve and manage files in a remote computer.
- It allows users to log on as a remote host.
- This layer provides access to global information about various services.
- This layer provides services which include: e-mail, transferring files, distributing results to the user, directory services, network resources and so on.
- It provides protocols that allow software to send and receive information and present meaningful data to users.
- It handles issues such as network transparency, resource allocation and so on.
- This layer serves as a window for users and application processes to access network services.

Network Application Architecture
client-server architecture

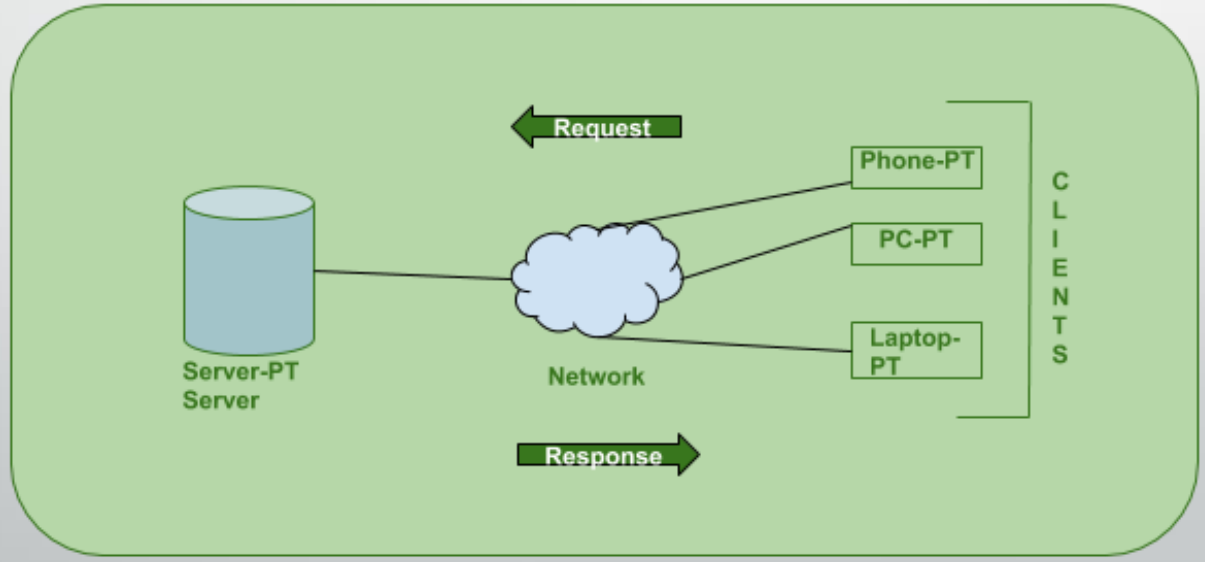
- The Client-server model is a distributed application structure that partitions task or workload between the providers of a resource or service, called servers, and service requesters called clients. In the client-server architecture, when the client computer sends a request for data to the server through the internet, the server accepts the requested process and deliver the data packets requested back to the client.

How the Client-Server Model works ?

- **Client:** When we talk the word **Client**, it mean to talk of a person or an organization using a particular service. Similarly in the digital world a **Client** is a computer (**Host**) i.e. capable of receiving information or using a particular service from the service providers (**Servers**).
- **Servers:** Similarly, when we talk the word **Servers**, It mean a person or medium that serves something. Similarly in this digital world a **Server** is a remote computer which provides information (data) or access to particular services.

(cont..)

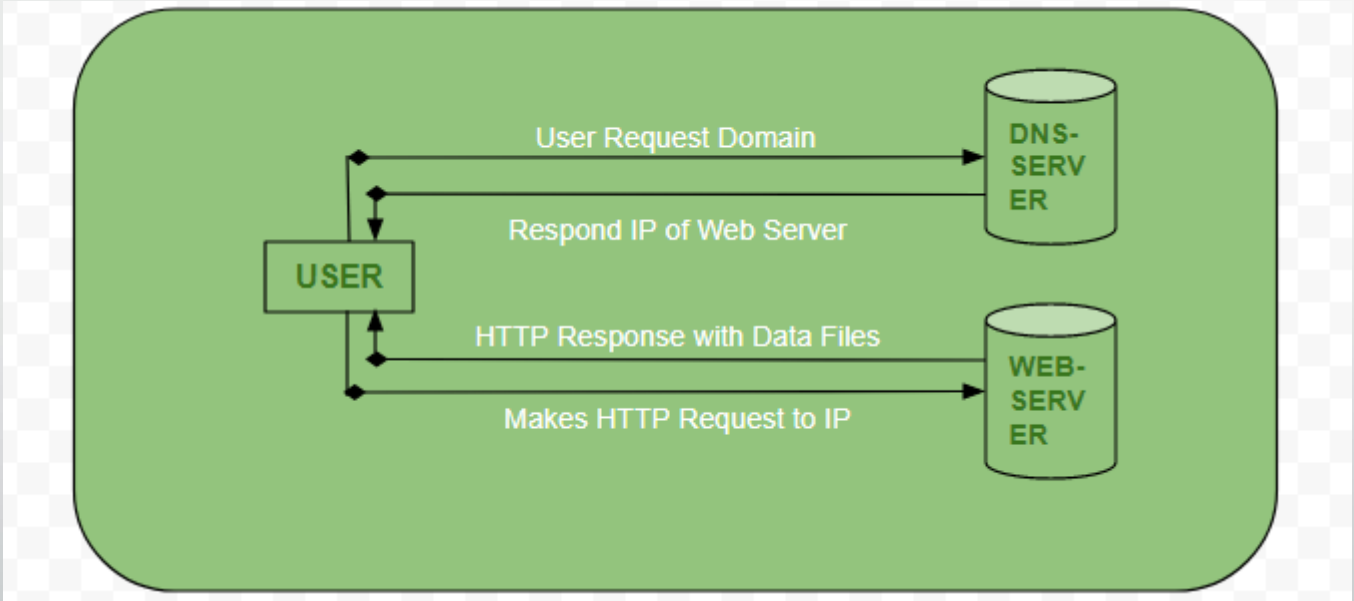
So, its basically the **Client** requesting something and the **Server** serving it as long as its present in the database.



How the browser interacts with the servers ?

- There are few steps to follow to interacts with the servers a client.
- User enters the **URL**(Uniform Resource Locator) of the website or file. The Browser then requests the **DNS**(DOMAIN NAME SYSTEM) Server.
- **DNS Server** lookup for the address of the **WEB Server**.
- **DNS Server** responds with the **IP address** of the **WEB Server**.
- Browser sends over an **HTTP/HTTPS** request to **WEB Server's IP** (provided by **DNS server**).
- Server sends over the necessary files of the website.
- Browser then renders the files and the website is displayed. This rendering is done with the help of **DOM** (Document Object Model) interpreter, **CSS** interpreter and **JS Engine** collectively known as the **JIT** or (Just in Time) Compilers.

- There are few steps to follow to interacts with the servers a client.
- User enters the **URL**(Uniform Resource Locator) of the website or file. The Browser then requests the **DNS**(DOMAIN NAME SYSTEM) Server.
- **DNS Server** lookup for the address of the **WEB Server**.
- **DNS Server** responds with the **IP address** of the **WEB Server**.
- Browser sends over an **HTTP/HTTPS** request to **WEB Server's IP** (provided by **DNS server**).
- Server sends over the necessary files of the website.
- Browser then renders the files and the website is displayed. This rendering is done with the help of **DOM** (Document Object Model) interpreter, **CSS** interpreter and **JS Engine** collectively known as the **JIT** or (Just in Time) Compilers.

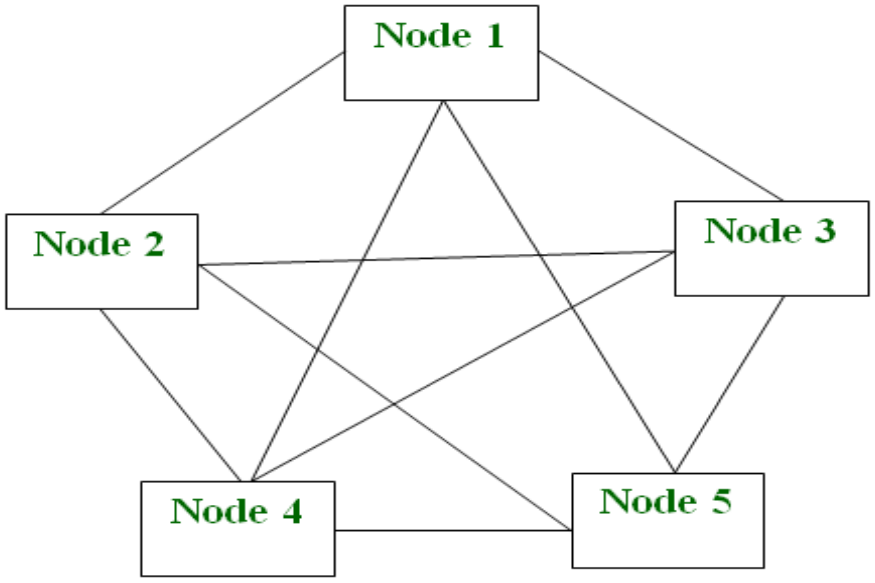

User Request Domain
DNS-SERVER
Respond IP of Web Server
USER
HTTP Response with Data Files
WEB-SERVER
Makes HTTP Request to IP

- **Advantages of Client-Server model:**
- Centralized system with all data in a single place.
- Cost efficient requires less maintenance cost and Data recovery is possible.
- The capacity of the Client and Servers can be changed separately.
- **Disadvantages of Client-Server model:**
- Clients are prone to viruses, Trojans and worms if present in the Server or uploaded into the Server.
- Server are prone to Denial of Service (DOS) attacks.
- Data packets may be spoofed or modified during transmission.
- Phishing or capturing login credentials or other useful information of the user are common and MITM(Man in the Middle) attacks are common.

P2P(peer-to-peer)

- A peer-to-peer network is a simple network of computers. Here each computer acts as a node for file sharing within the formed network. Here each node acts as a server and thus there is no central server in the network. This allows the sharing of a huge amount of data. The tasks are equally divided amongst the nodes. Each node connected in the network shares an equal workload. For the network to stop working, all the nodes need to individually stop working. This is because each node works independently.

(cont..)



P2P Architecture

- **Advantages of P2P Network**
- **Easy to maintain:** The network is easy to maintain because each node is independent of the other.
- **Less costly:** Since each node acts as a server, therefore the cost of the central server is saved. Thus, there is no need to buy an expensive server.
- **No network manager:** In a P2P network since each node manages his or her own computer, thus there is no need for a network manager.
- **Adding nodes is easy:** Adding, deleting, and repairing nodes in this network is easy.
- **Less network traffic:** In a P2P network, there is less network traffic than in a client/ server network.
- **Disadvantages of P2P Network**
- **Data is vulnerable:** Because of no central server, data is always vulnerable to getting lost because of no backup.
- **Less secure:** It becomes difficult to secure the complete network because each node is independent.
- **Slow performance:** In a P2P network, each computer is accessed by other computers in the network which slows down the performance of the user.
- **Files hard to locate:** In a P2P network, the files are not centrally stored, rather they are stored on individual computers which makes it difficult to locate the files

Features of P2P network

- These networks do not involve a large number of nodes, usually less than 12. All the computers in the network store their own data but this data is accessible by the group.
- Unlike client-server networks, P2P uses resources and also provides them. This results in additional resources if the number of nodes increases. It requires specialized software. It allows resource sharing among the network.
- Since the nodes act as clients and servers, there is a constant threat of attack.
- Almost all OS today support P2P networks.

Define www:-

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

Difference b/w internet and www

INTERNET	WWW
Internet is a global network of networks.	WWW stands for World wide
Internet is a means of connecting a computer to any other computer anywhere in the world.	World Wide Web which is a collection of information which is accessed via the Internet.
Internet is infrastructure.	WWW is service on top of that infrastructure.
Internet can be viewed as a big book-store.	Web can be viewed as collection of books on that store.
At some advanced level, to understand we can think of the Internet as hardware.	At some advanced level, to understand we can think of the WWW as software.
Internet is primarily hardware-based.	WWW is more software-oriented as compared to the Internet.
It is originated sometimes in late 1960s.	English scientist Tim Berners-Lee invented the World Wide Web in 1989.
Internet is superset of WWW.	WWW is a subset of the Internet.

Domain name system (DNS)

- Domain Name System (DNS) is a hostname for **IP address** translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers. It is required for the functioning of the Internet.
- **What is the Need of DNS?**
- Every host is identified by the IP address but remembering numbers is very difficult for people also the IP addresses are not static therefore a mapping is required to change the domain name to the IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

Note:The Domain Name System (DNS) is the phonebook of the Internet.

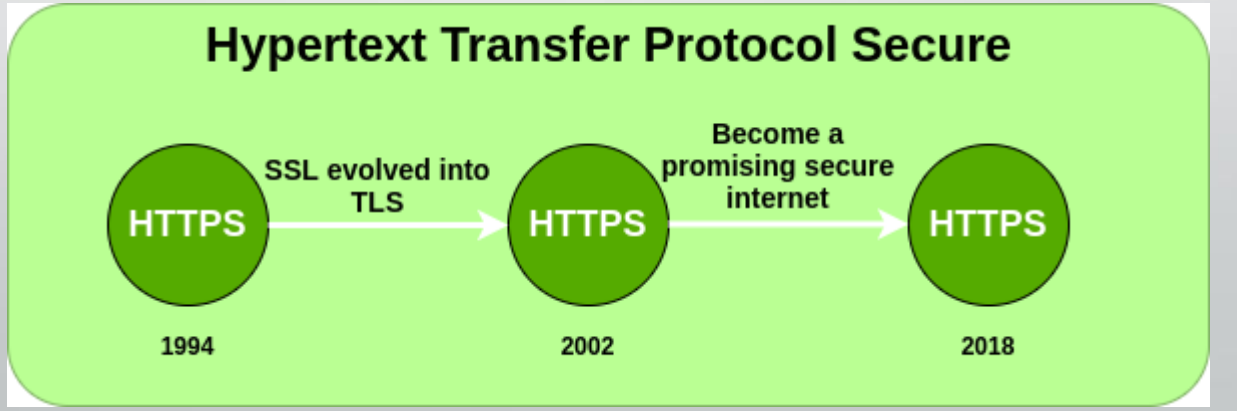
Figure 12.1 Domain Name System

HTTP

- HTTP stands for HyperText Transfer Protocol. It is invented by Tim Berner. HyperText is the type of text which is specially coded with the help of some standard coding language called HyperText Markup Language (HTML).
- HTTP provides a standard between a web browser and a web server to establish communication. It is a set of rules for transferring data from one computer to another.
- Data such as text, images, and other multimedia files are shared on the World Wide Web. Whenever a web user opens their web browser, the user indirectly uses HTTP. It is an application protocol that is used for distributed, collaborative, hypermedia information systems.
- **Characteristics of HTTP**
- HTTP is IP based communication protocol that is used to deliver data from server to client or vice-versa.
- Any type of content can be exchanged as long as the server and client are compatible with it.
- It is a request and response protocol based on client and server requirements.

HTTPS

- HTTPS stands for Hyper Text Transfer Protocol Secure. HTTP Secure (HTTPS), could be a combination of the Hypertext Transfer Protocol with the SSL/TLS convention to supply encrypted communication and secure distinguishing proof of an arranged web server. HTTPS is more secure than HTTP because HTTPS is certified by the SSL(Secure Socket Layer). Whatever website you are visiting on the internet, if its URL is HTTP, then that website is not secure.



DNS Server Types

- There are several server types involved in completing a DNS resolution. The following list describes the four name servers in the order a query passes through them. They provide the domain name being sought or referrals to other name servers.

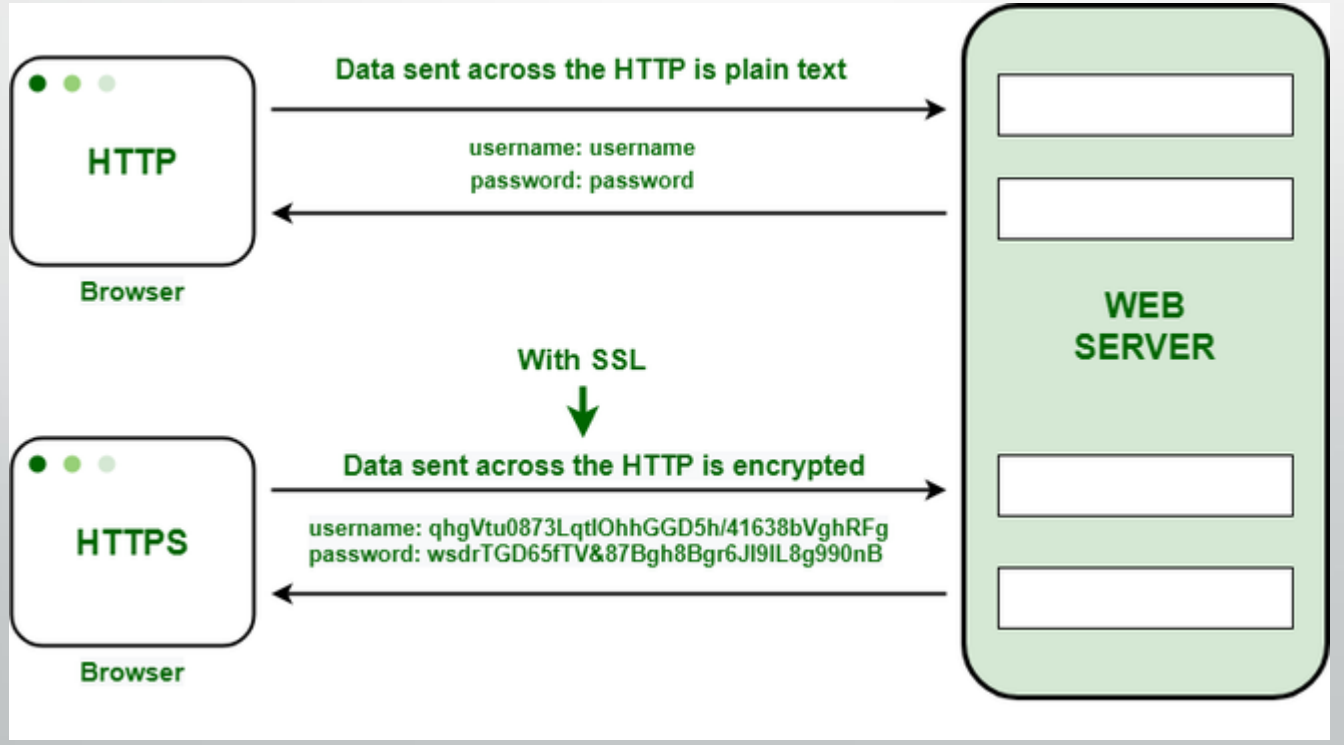
1. **Recursive server.** The recursive server takes DNS queries from an application, such as a web browser. It's the first resource the user accesses and either provides the answer to the query if it has it cached or accesses the next-level server if it doesn't. This server may go through several iterations of querying before returning an answer to the client.
2. **Root name server.** This server is the first place the recursive server sends a query if it doesn't have the answer cached. The root name server is an index of all the servers that will have the information being queried. These servers are overseen by the Internet Corporation for Assigned Names and Numbers, specifically a branch of ICANN called the Internet Assigned Numbers Authority.
3. **TLD server.** The root server directs the query based on the top-level domain -- the .com, .edu or .org in the URL. This is a more specific part of the lookup.
4. **Authoritative name server.** The authoritative name server is the final checkpoint for the DNS query. These servers know everything about a given domain and deal with the subdomain part of the domain name. These servers contain DNS resource records with specific information about a domain, such as the A record. They return the necessary record to the recursive server to send back to the client and cache it closer to the client for future lookups.

Characteristics of HTTPS

- HTTPS encrypts all message substance, including the HTTP headers and the request/response data. The verification perspective of HTTPS requires a trusted third party to sign server-side digital certificates.
- HTTPS is presently utilized more frequently by web clients than the first non-secure HTTP, fundamentally to ensure page genuineness on all sorts of websites, secure accounts and to keep client communications.

Difference between HTTP and HTTPS

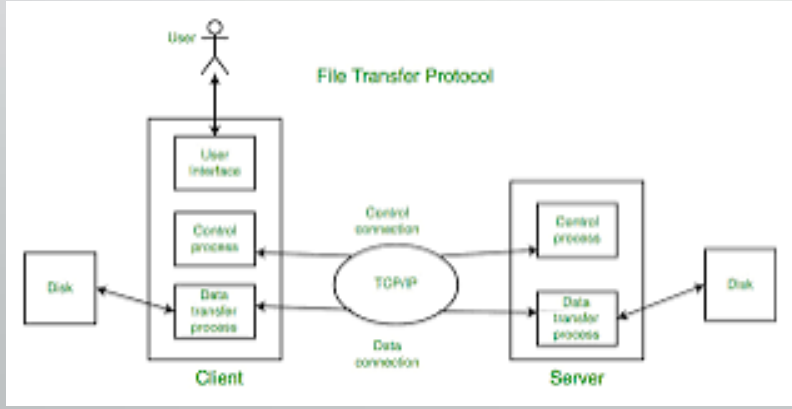
Hypertext Transfer Protocol (HTTP) is a protocol using which hypertext is transferred over the Web. Due to its simplicity, HTTP has been the most widely used protocol for data transfer over the Web but the data (i.e. hypertext) exchanged using HTTP isn't as secure as we would like it to be. Cryptographic protocols such as SSL and/or TLS turn HTTP into HTTPS i.e. **HTTPS = HTTP + Cryptographic Protocols**.



HTTP	HTTPS
HTTP stands for HyperText Transfer Protocol. In HTTP, the URL begins with “http://”.	HTTPS stands for HyperText Transfer Protocol Secure. In HTTPS, the URL starts with “https://”.
HTTP uses port number 80 for communication.	HTTPS uses port number 443 for communication.
Hyper-text exchanged using HTTP goes as plain text i.e. anyone between the browser and server can read it relatively easily if one intercepts this exchange of data and due to which it is Insecure.	HTTPS is considered to be secure but at the cost of processing time because Web Server and Web Browser need to exchange encryption keys using Certificates before actual data can be transferred.
HTTP Works at the Application Layer.	HTTPS works at Transport Layer.
HTTP does not use encryption, which results in low security in comparison to HTTPS.	HTTPS uses Encryption which results in better security than HTTP.
HTTP speed is faster than HTTPS.	HTTPS speed is slower than HTTP.
HTTP does not use data hashtags to secure data.	HTTPS will have the data before sending it and returning it to its original state on the receiver side.
HTTP is used to transfer text, video, and images via web pages.	HTTPS is used to transfer data securely via a network.

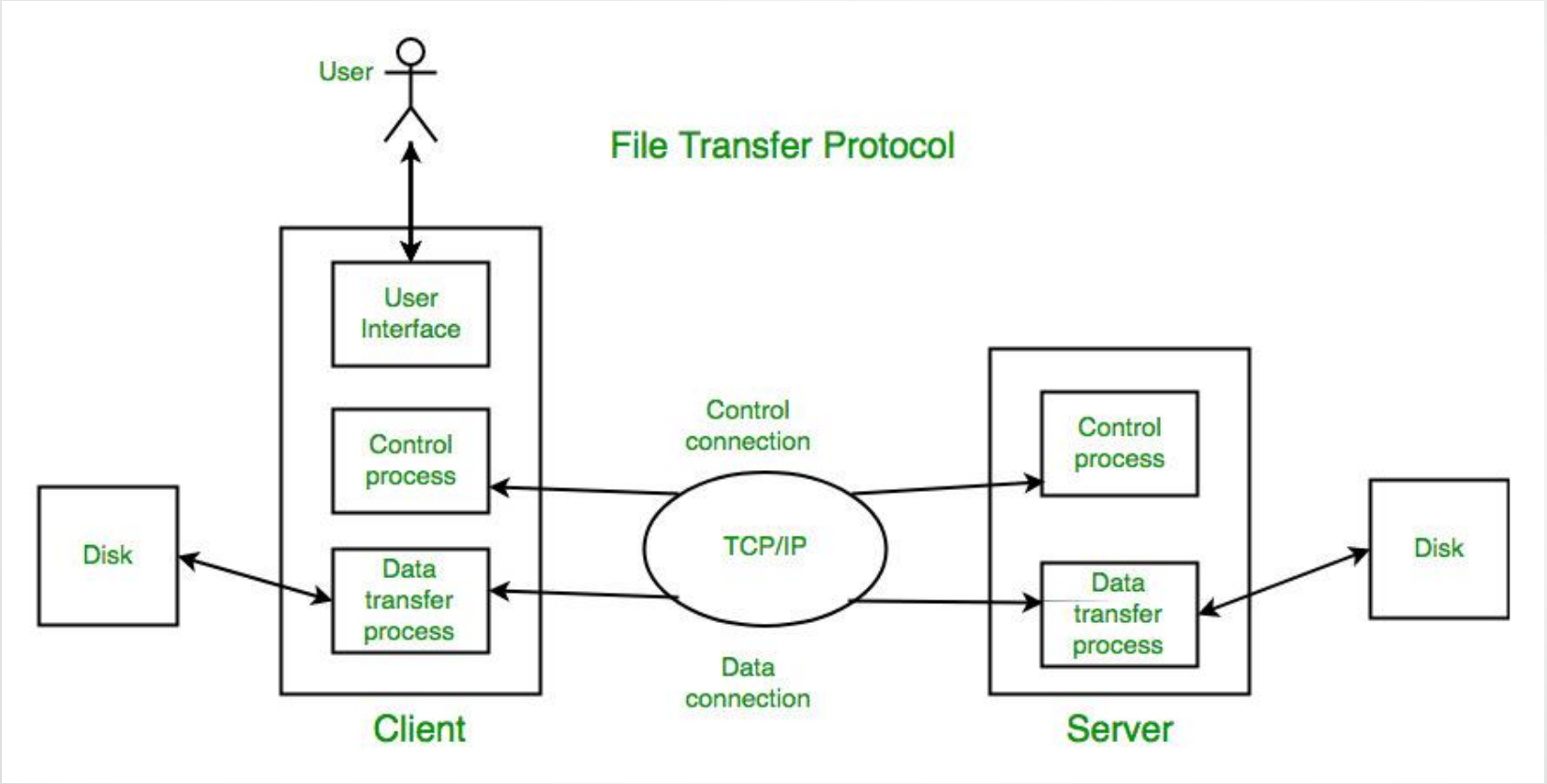
FTP(File Transfer Protocol)

- FTP is a standard communication protocol. There are various other protocols like HTTP which are used to transfer files between computers, but they lack clarity and focus as compared to FTP. Moreover, the systems involved in connection are heterogeneous, i.e. they differ in operating systems, directories, structures, character sets, etc the FTP shields the user from these differences and transfers data efficiently and reliably. FTP can transfer ASCII, EBCDIC, or image files.



How Does FTP Work?

- FTP is a client server protocol that has two communication channel, command channel for conversation control and data channel for file content.
- Here are steps mentioned in which FTP works:
- A user has to log in to FTP Server first, there may be some servers where you can access to content without login, known as anonymous FTP.
- Client can start a conversation with server, upon requesting to download a file.
- The user can start different functions like upload, delete, rename, copy files, etc. on server.



Types of Connection in FTP

•Control Connection

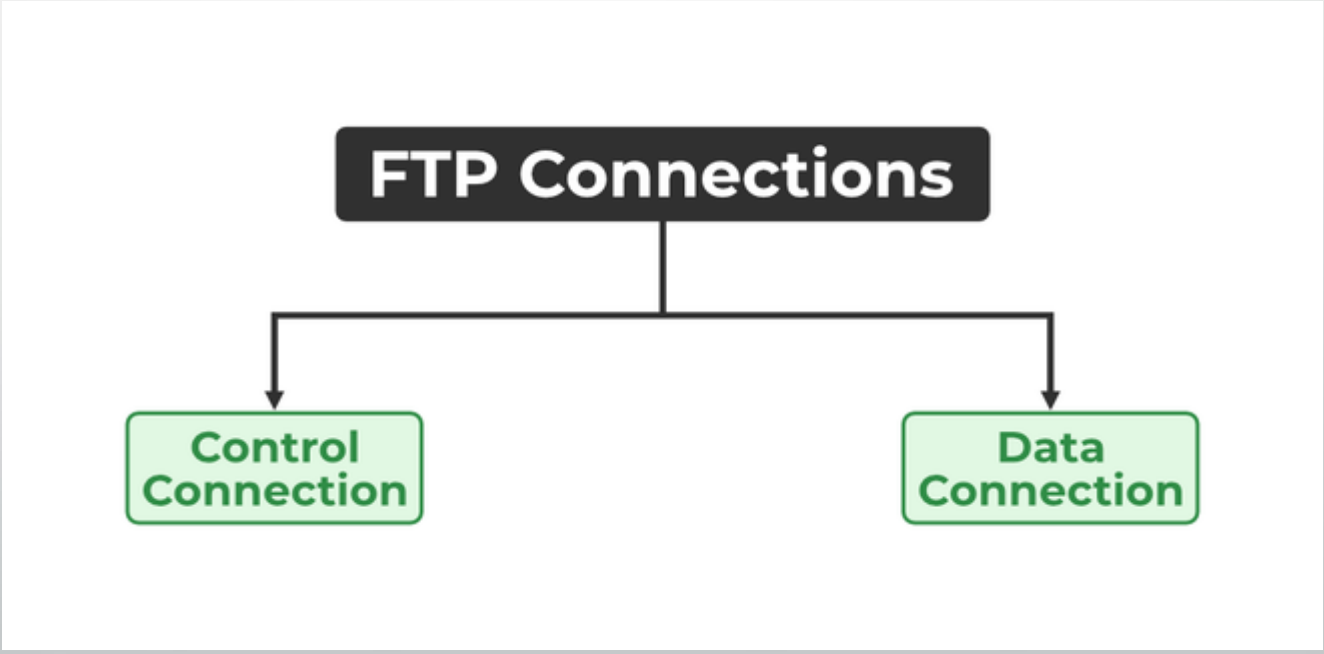
•Data Connection

Control Connection

For sending control information like user identification, password, commands to change the remote directory, commands to retrieve and store files, etc., FTP makes use of a control connection. The control connection is initiated on port number 21.

Data connection

- For sending the actual file, FTP makes use of a data connection. A data connection is initiated on port number 20.
  FTP sends the control information out-of-band as it uses a separate control connection. Some protocols send their request and response header lines and the data in the same TCP connection. For this reason, they are said to send their control information in-band. HTTP and SMTP are such examples.



Advantages of FTP

- File sharing also comes in the category of advantages of FTP in this between two machines files can be shared on the network.
- Speed is one of the main benefits of FTP.
- Since we don’t have to finish every operation to obtain the entire file, it is more efficient.
- Using the username and password, we must log in to the FTP server. As a result, FTP might be considered more secure.
- We can move the files back and forth via FTP.

Disadvantages of FTP

- File size limit is the drawback of FTP only 2 GB size files can be transferred.
- More then one receivers are not supported by FTP.
- FTP does not encrypt the data this is one of the biggest drawbacks of FTP.
- FTP is unsecured we use login IDs and passwords making it secure but they can be attacked by hackers.

Telnet (Teletype Network)

- **TELNET** stands for **Tel**etype **Net**work. It is a type of protocol that enables one computer to connect to the local computer. It is used as a standard **TCP/IP protocol** for virtual terminal service which is provided by **ISO**. The computer which starts the connection is known as the **local computer**.
- The computer which is being connected to i.e. which accepts the connection known as the **remote computer**.
- During telnet operation, whatever is being performed on the remote computer will be displayed by the local computer. Telnet operates on a client/server principle. The local computer uses a telnet client program and the remote computers use a telnet server program.

- **Advantages of Telnet**

1. It provides remote access to someone's computer system.
2. Telnet allows the user for more access with fewer problems in data transmission.
3. Telnet saves a lot of time.
4. The oldest system can be connected to a newer system with telnet having different operating systems.

- **Disadvantages of Telnet**

1. As it is somehow complex, it becomes difficult to beginners in understanding.
2. Data is sent here in form of plain text, that's why it is not so secured.
3. Some capabilities are disabled because of not proper interlinking of the remote and local devices.

- **Modes of Operation**

- Email stands for Electronic Mail. It is a method to send messages from one computer to another computer through the Internet. It is mostly used in business, education, technical communication, and document interactions.
- It allows communicating with people all over the world without bothering them. In 1971, a test email was sent Ray Tomlinson to himself containing text.
- It is the information sent electronically between two or more people over a network. It involves a sender and receiver/s.

- **Types of Email**
- **Newsletters**
- It is a type of email sent by an individual or company to the subscriber. It contains an advertisement, product promotion, updates regarding the organization, and marketing content. It might be upcoming events, seminars, or webinars from the organization.
- **Onboarding emails**
- It is an email a user receives right after the subscription. These emails are sent to buyers to familiarize and tell them about using a product. It also contains details about the journey in the new organization.
- **Transactional**
- These types of emails might contain invoices for recent transactions and details about transactions. If transactions failed then details about when the amount will be reverted. We can say that transaction emails are confirmation of purchase.
- **Plain-Text Emails**
- These types of emails contain just simple text similar to other text message services. It does not include images, videos, documents, graphics, or any attachments. Plain-text emails are also used to send casual chatting like other text message services.

- **Advantages of Email Services**
- These are the following advantages of email services:
- Easy and Fast:
- Secure:
- Mass Sending:
- Multimedia Email:

Disadvantages of Email Services

Malicious Use:

Spam:

Time-Consuming:

Popular Email Services

- **Gmail:**
- **Outlook:**

SMTP

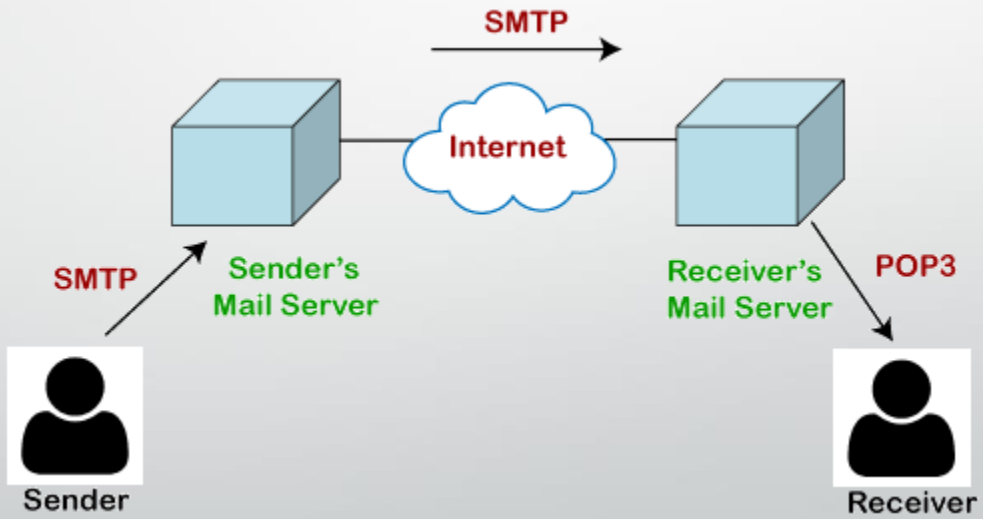
- **Components of SMTP**

1. Mail User Agent (MUA)
2. Mail Submission Agent (MSA)
3. Mail Transfer Agent (MTA)
4. Mail Delivery Agent (MDA)

- **1. Mail User Agent (MUA):** It is a computer application that helps you in sending and retrieving mail. It is responsible for creating email messages for transfer to the mail transfer agent(MTA).
- **2. Mail Submission Agent (MSA):** It is a computer program that basically receives mail from a Mail User Agent(MUA) and interacts with the Mail Transfer Agent(MTA) for the transfer of the mail.
- **3. Mail Transfer Agent(MTA):** It is basically software that has the work to transfer mail from one system to another with the help of SMTP.
- **4. Mail Delivery Agent(MDA): A mail** Delivery agent or Local Delivery Agent is basically a system that helps in the delivery of mail to the local system

POP (Post Office Protocol)

- The POP protocol stands for Post Office Protocol. As we know that SMTP is used as a message transfer agent. When the message is sent, then SMPT is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the Message Access Agent. The Message Access Agent contains two types of protocols, i.e., POP3 and IMAP.



- POP is an application layer protocol in the OSI model that provides end users the ability to fetch and receive email.

Internet Message Access Protocol (IMAP)

- **Internet Message Access Protocol (IMAP)** is an application layer protocol that operates as a contract for receiving emails from the mail server. It was designed by Mark Crispin in 1986 as a remote access mailbox protocol, the current version of IMAP is IMAP4. It is used as the most commonly used protocol for retrieving emails. This term is also known as Internet mail access protocol, Interactive mail access protocol, and Interim mail access protocol

MIME

- **Multipurpose Internet Mail Extension (MIME)** is a standard that was proposed by Bell Communications in 1991 in order to expand the limited capabilities of email. MIME is a kind of add-on *or a supplementary protocol* that allows non-ASCII data to be sent through SMTP. It allows the users to exchange different kinds of data files on the Internet: audio, video, images, application programs as well.
- **Features of MIME –**

1. It is able to send multiple attachments with a single message.
2. Unlimited message length.
3. Binary attachments (executables, images, audio, or video files) may be divided if needed.
4. MIME provided support for varying content types and multi-part messages.

U19NU23S0005

DCCA – 303

III Semester B.C.A. Degree Examination, April/May 2023
(NEP Scheme)
COMPUTER APPLICATION
DSC9 : Computer Communication and Networks

Time : 2½ Hours

Max. Marks : 60

Instruction : *Answer* ***all*** *the Sections.*

SECTION – A

I. Answer **any six** questions. **Each** question carries **two** marks. **(6×2=12)**

1) Define Computer Networks.

2) What is MAN ?

3) Define Message Switching.

4) What is multiplexing ?

5) What is byte stuffing ?

6) Mention the design issues of data link layer.

7) What is hierarchical routing ?

8) Define protocol.

9) Mention the services provided to Transport layer.

SECTION – B

II. Answer **any four** questions. **Each** question carries **six** marks. **(4×6=24)**

10) Explain the OSI reference model.

11) Compare LAN, WAN and MAN.

12) Explain the following :
   i) Twisted pair
   ii) Coaxial cable.

P.T.O.

DCCA – 303

13) Explain Checksum with an example.

14) Explain token bucket algorithm.

15) Write a note on internet transport protocol.

SECTION – C

III. Answer **any three** questions. **Each** question carries **8** marks. **(3×8=24)**

16) Explain any four topologies with neat diagram. **8**

17) Write a note on switching. **8**

18) a) Write a note on CRC. **4**

b) Explain Hamming code with an example. **4**

19) Write a note on distance vector routing with an example. **8**

20) a) Write a note on Electronic Mailing. **4**

b) Write a note on WWW. **4**