COMPUTER NETWORKS - PREPINSTA

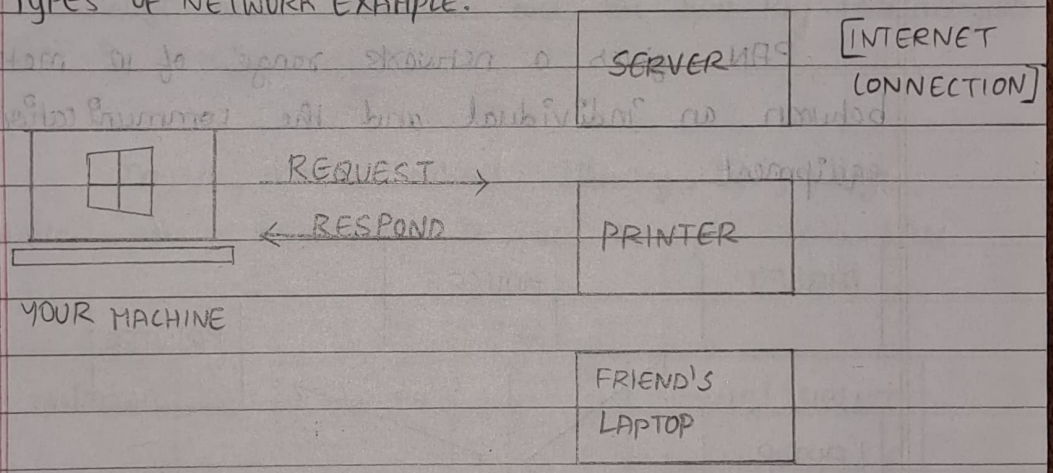
INTRODUCTION TO COMPUTER NETWORKS

WHAT IS A COMPUTER NETWORK?

Computer networking is the term for a network of connected computers devices that may communicate and share resources.

These networked devices transmit data through wireless or physical technologies using a set of guidelines known as communication protocols.

TYPES OF NETWORK EXAMPLE:



CLASSIFICATIONS AND NETWORK TYPES:

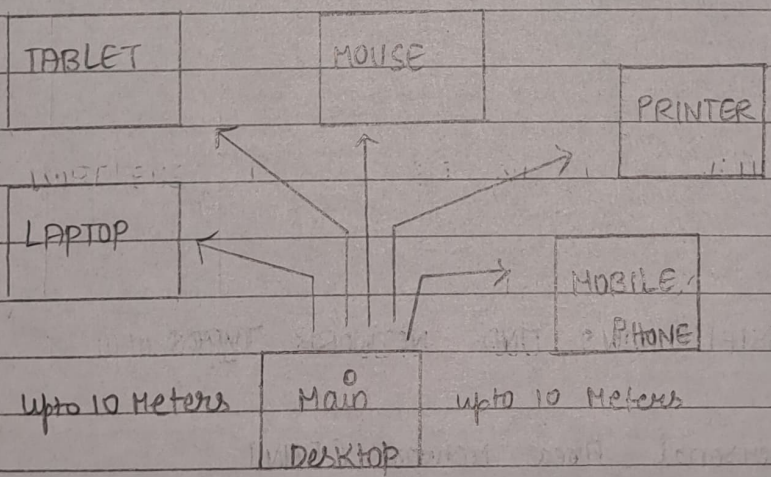
1. Personal Area Network [PAN]
2. Local Area Network [LAN]
3. Wide Area Network [WAN]
4. Wireless Local Area Network [WLAN]
5. Campus Area Network [CAN]
6. Metropolitan Area Network [MAN]
7. Storage Area Network [SAN]
8. System - Area Network [SAN]

9. Passive optical Local Area Network [POLAN]
10. Enterprise private Network [EPN]
11. Virtual private Network [VPN]
12. Home Area Network [HAN]

PERSONAL AREA NETWORK [PAN]

The most fundamental kind of computer network is called a PAN. This network is restricted to a single user, so that computing device communication is focused solely on the user's workspace.

PAN gives a network range of 10 metres between an individual and the communication equipment.



LOCAL AREA NETWORK [LAN]

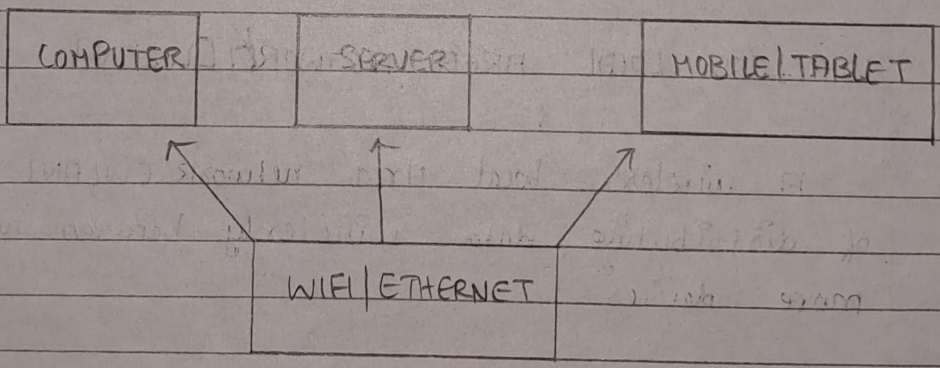
The most used network type is LAN. A local area network, or LAN, is a type of computer network that links computers locally.

Locally speaking, it joins them over a common communication line.

TWO or more computers joined by a server form a local area network [LAN].

Wifi and Ethernet are the two key technologies used in this network.

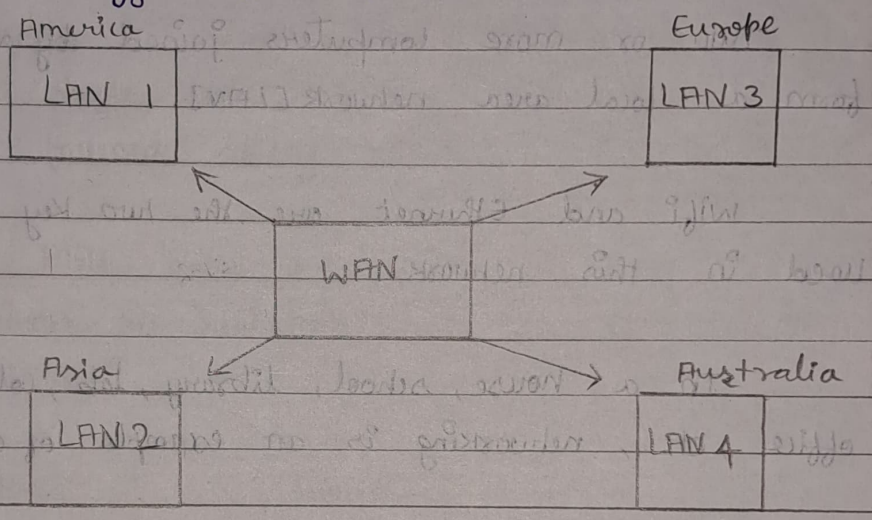
In a house, school, library, lab, college, office, etc., networking is an example of a LAN.



WIDE AREA NETWORK [WAN]

Any network that covers a vast geographic region and typically connects several local area networks (LAN's), is known as a wide area network [WAN].

As a collection of numerous worldwide networks connected to one another, the Internet is the biggest WAN in the world.



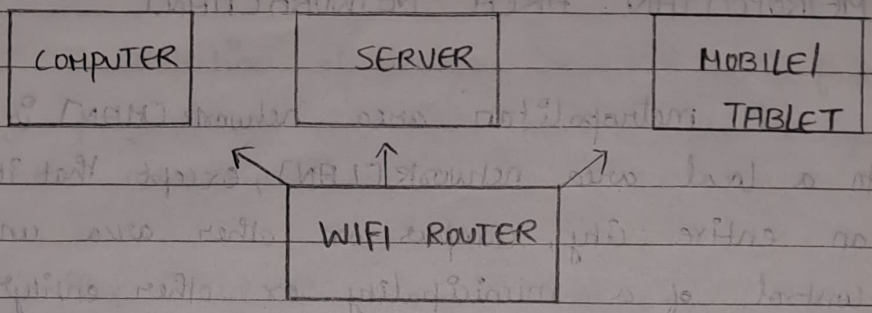
WIRELESS LOCAL AREA NETWORK [WLAN]

A wireless local area network [WLAN] is a way of distributing data wirelessly between two or more devices.

High-frequency radio waves are used by WLAN's, which frequently have an Internet access point built in.

Typically a home or small business, a WLAN enables users to wander about the coverage area while keeping a network connection.

WIRELESS LOCAL AREA NETWORK [WLAN]

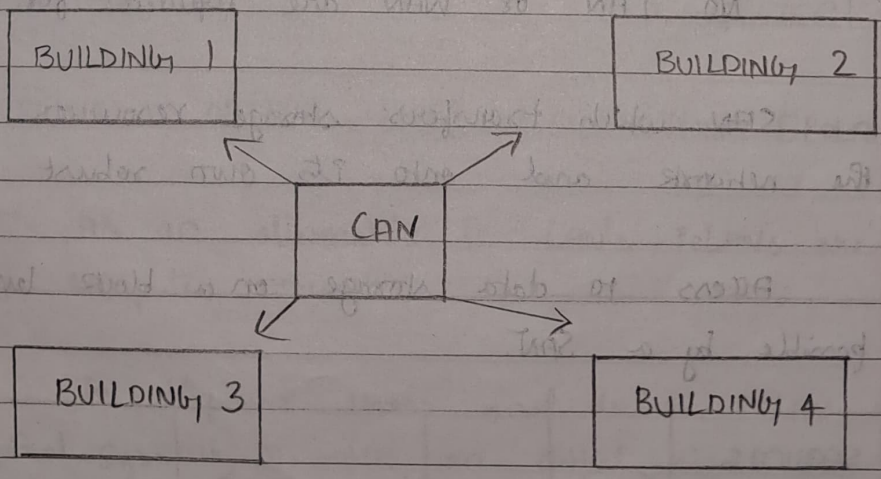


CAMPUS AREA NETWORK [CAN]

A Campus area network [CAN] is a collection of local area networks [LAN] that are all connected to one another within a sepecific geographic region.

A ~~can~~ CAN is less expensive than a wide area Network [WAN] or a metropolitan area network. [MAN].

Corporate Area Network [CAN] is another name for it.



METROPOLITAN AREA NETWORK [MAN]

A metropolitan area network [MAN] is comparable to a local area network [LAN], except that it covers an entire city, campus, or other area under the control of a municipality or other entity.

MANs are created by joining many LANs together. As a result, MANs are bigger than LANs, but smaller than wide area networks [WAN], which span a huge geographic region and occasionally directly connect users all over the world.

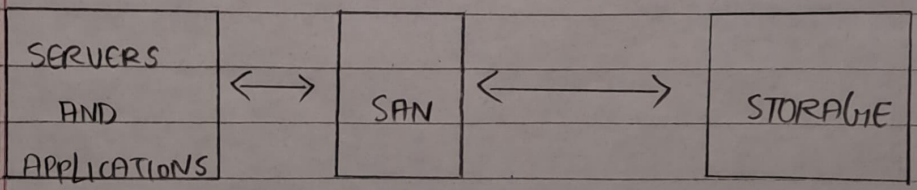
STORAGE AREA NETWORK [SAN]

Groups of storage devices are linked to numerous servers through a high-speed computer network called a storage Area Network [SAN]

NO LAN or WAN are required for this network.

SAN which transfers storage resources away from the network and onto its own robust network.

Access to data storage on a block level is made possible by a SAN.



Date
Page

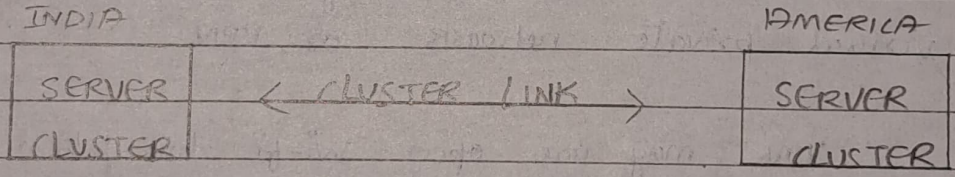
SYSTEM AREA NETWORK [SAN]

A collection of devices connected by a fast, high-performance connection together form a system area network [SAN].

The TCP/IP protocol assigns Internet Protocol [IP] addresses to each SAN network interface controller [NIC] and utilises those addresses to define the data routing for a SAN connection.

Additionally, data delivery is carried out using a dependable transport that is integrated into the SAN. clusters of client and server computers are one type of SAN.

Through a virtual interface adaptor, Microsoft SQL Server 2005 connects to the SAN.



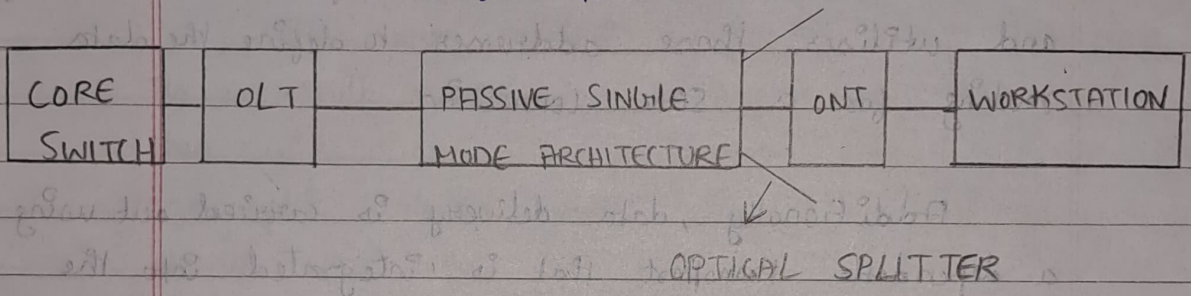
PASSIVE OPTICAL LOCAL AREA NETWORK [POLAN]

As an alternative to LAN's, POLANs are a sort of computer network.

To disperse users and devices, POLAN uses optical systems to split an optical signal from a single strand of single-mode optical fibre into several transmissions. In a nutshell, POLAN is a point-to-multipoint LAN architecture

British Telecommunications initially introduced PoL in 1987. PoL is made up of three main parts, namely:

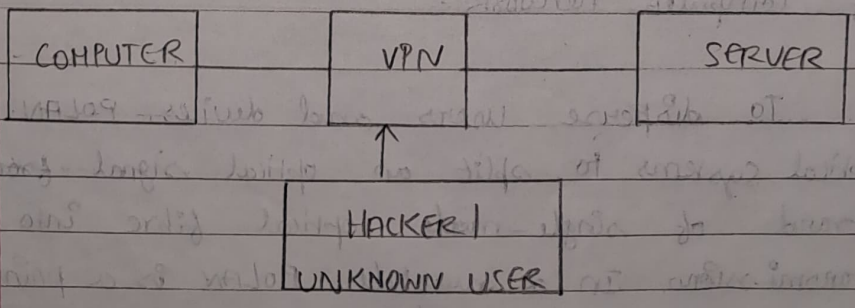
1. Fiber optic Terminal [OLT]
2. optical Splitter
3. Laser Network Terminal [ONT]



VIRTUAL PRIVATE NETWORK [VPN]

A service that safeguards your internet connection and online privacy is known as a virtual private network or VPN.

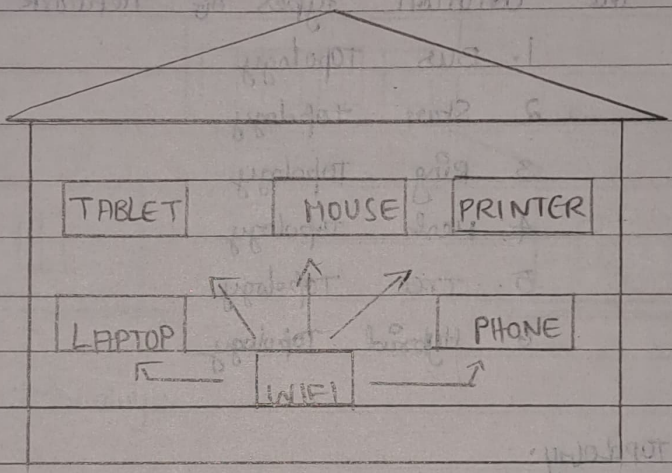
You may use open wi-fi hotspots with confidence since it turns your data into an encrypted tunnel, hides your IP address to safeguard your online identity, and generates an encrypted tunnel for your data.



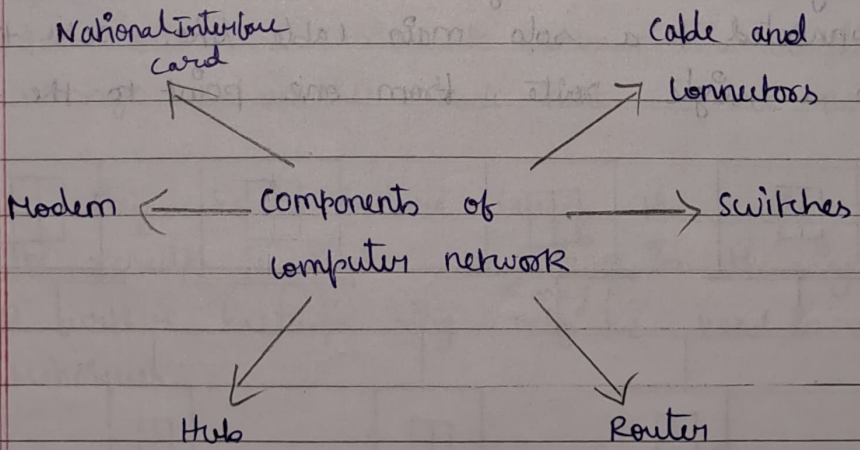
HOME AREA NETWORK [HAN]

A home area network [HAN] is a network that is installed and run inside a relatively small area, usually a home or small office [SOHO]

It makes it possible for computers, mobile devices, and other devices to communicate and share resources [like the internet] over a network connection.



COMPONENTS OF COMPUTER NETWORK



COMPUTER NETWORK TOPOLOGY

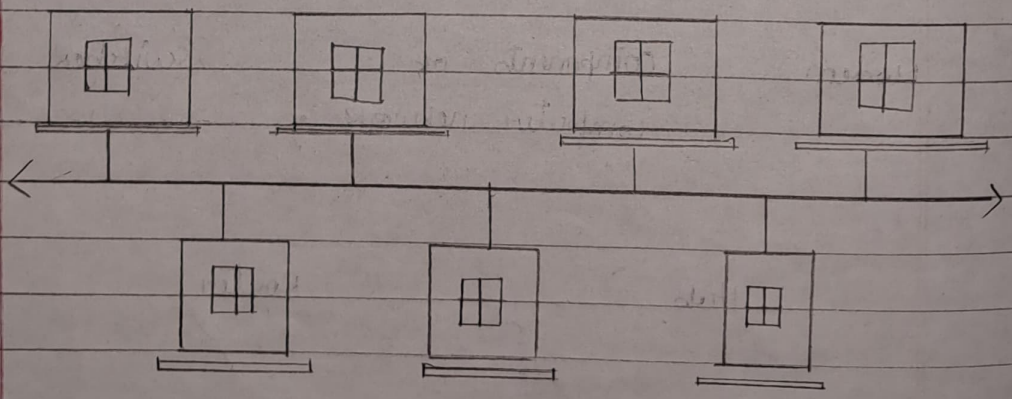
The way in which computers or other network devices are connected to one another is known as a topology of the network. Both the logical and physical aspects of a network may be defined by its topologies. A network may have identical or dissimilar logical and physical topologies.

The common types of network topologies are:

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

BUS TOPOLOGY:

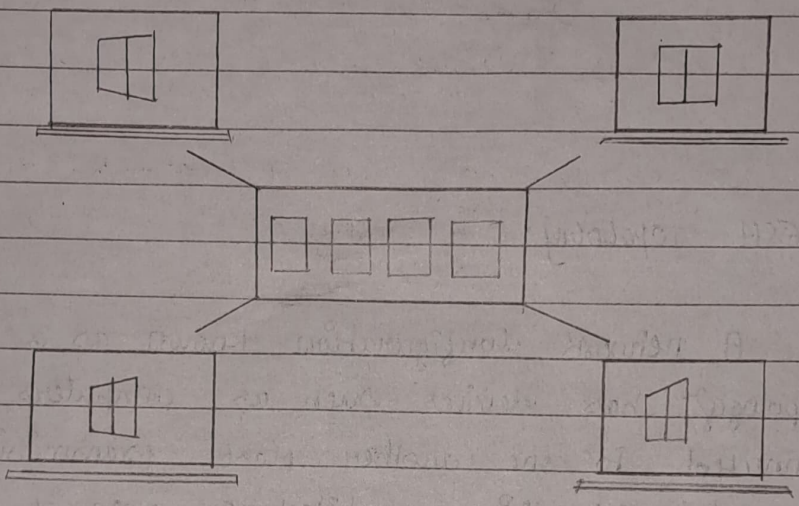
Bus topology is the kind of network topology where every node, ie every device on the network, is connected to a solo main cable line. Data transmitted in a single route, from one point to the other



Date
Page

STAR TOPOLOGY:

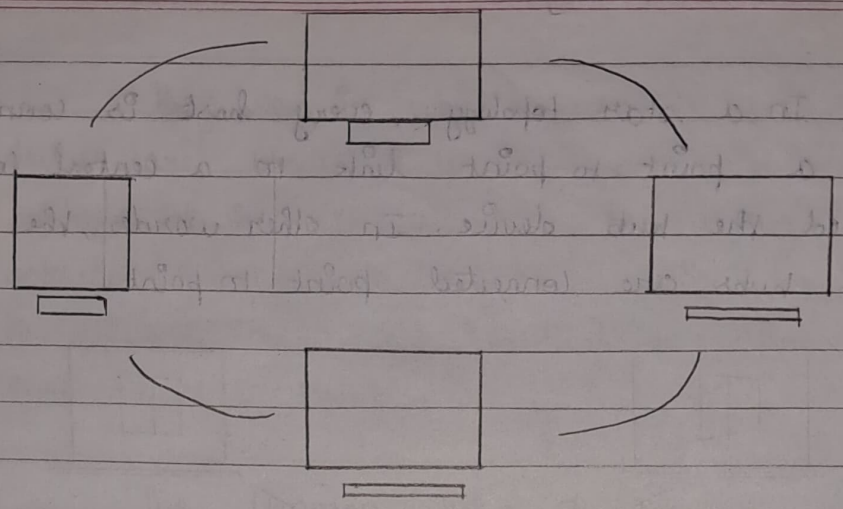
In a star topology, every host is connected via a point-to-point link to a central component called the hub device. In other words, the hosts and hubs are connected point to point.



RING TOPOLOGY:

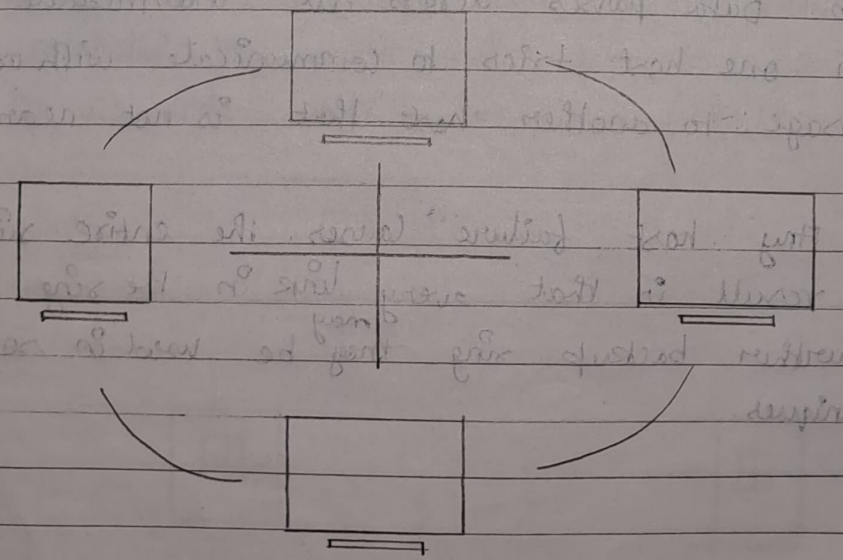
In a ring topology, a network structure is formed by connecting each host machine to exactly two more hosts. Data passes across all intermediate hosts when one host tries to communicate with or send a message to another host that is not nearby.

Any host failure causes the entire ring to fail. The result is that every link in the ring can fail. A further backup ring may be used in some techniques.



MESH TOPOLOGY:

A network configuration known as a mesh topology has devices such as computers and routers connected to one another. Most transmissions can be spread with this architecture even if one of the connection fails. It is a topology that wireless networks frequently employ. Here is a picture of a straightforward computer configuration on a mesh network.



TREE TOPOLOGY

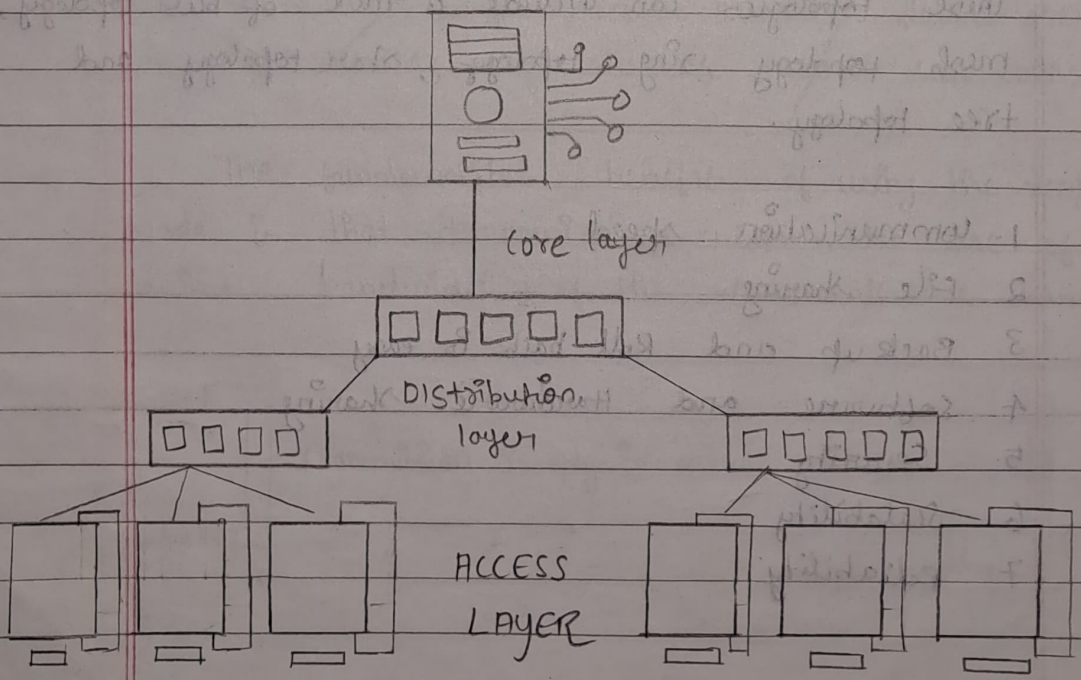
This topology emulates expanded star topology and incorporates bus topology's attributes.

This network is divided into numerous tiers or layers by this topology. A network is divided into three different types of network devices, mostly in LAN's.

Access-layer is the lowest layer, where computers are connected

The intermediate layer, often referred to as the distribution layer, serves as a bridge between the top and lower layers.

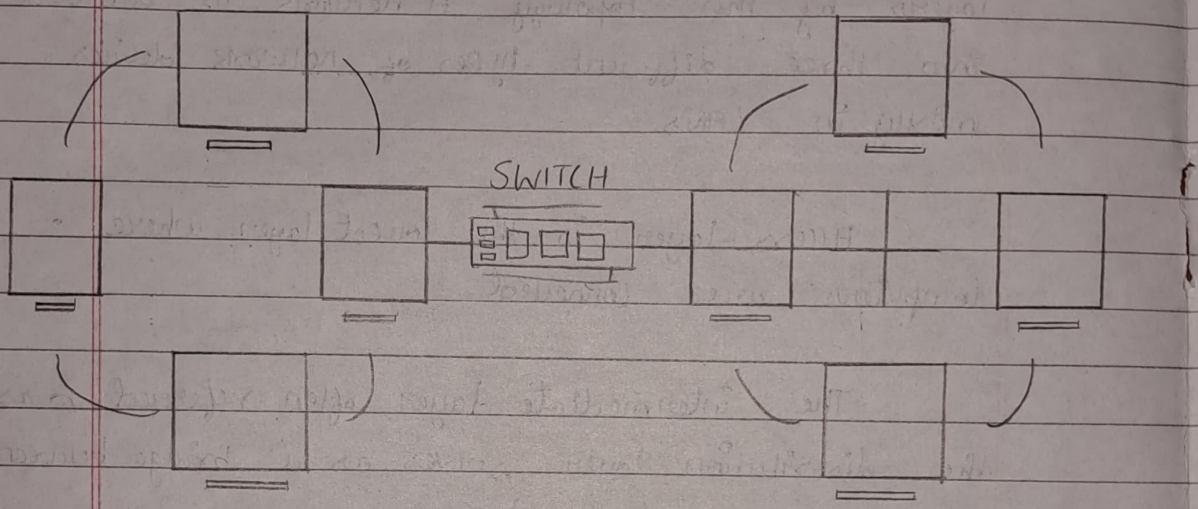
The core layer, which is the topmost layer and the layer from which all other layers branch out, serves as the network's centre node.



Date
Page

HYBRID TOPOLOGY

A hybrid topology is a type of network topology that uses two or more differing network topologies. These topologies can include a mix of bus topology, mesh topology, ring topology, star topology and tree topology.



FEATURES OF COMPUTER NETWORK

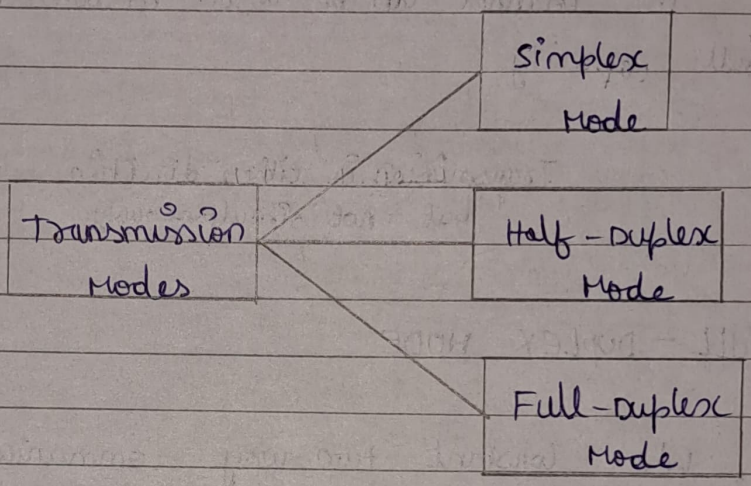
A hybrid topology is a type of network topology that uses two or more differing network topologies. These topologies can include a mix of bus topology, mesh topology, ring topology, star topology and tree topology.

1. Communication speed
2. File sharing
3. Back up and Roll back is easy
4. Software and Hardware sharing
5. Security
6. Scalability
7. Reliability

TRANSMISSION MODES

Transmission mode refers to the process of moving data from one device to another.

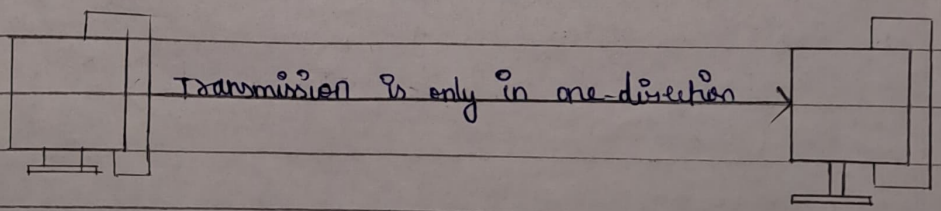
The communication mode is another name for the transmission mode.



SIMPLEX MODE:

Communication in simplex mode is unidirectional, like on a one-way street. The other device on a link can only receive; only one of the two can transmit.

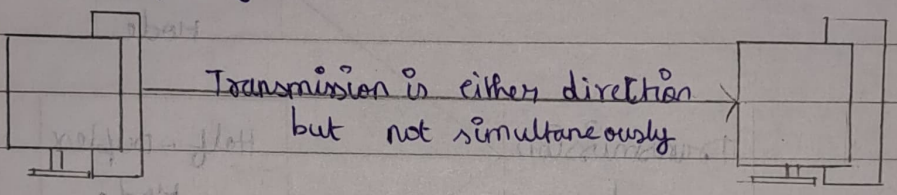
The fundamental benefit of using the simplex mode is that transmissions can make use of the entire bandwidth of the communication channel.



HALF-DUPLEX MODE:

Each station in half-duplex mode is capable of both transmitting and receiving, just not simultaneously. The ability of both devices to send and receive is inversely correlated while one is sending.

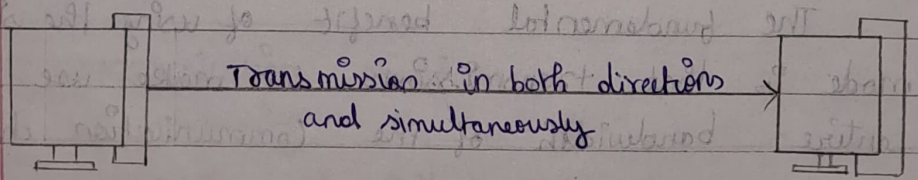
The channel can be used in both directions to its full capacity



FULL-DUPLEX MODE

When constant two-way communication is needed, full-duplex mode is employed. However, the channel's capacity must be shared equally between the two directions.

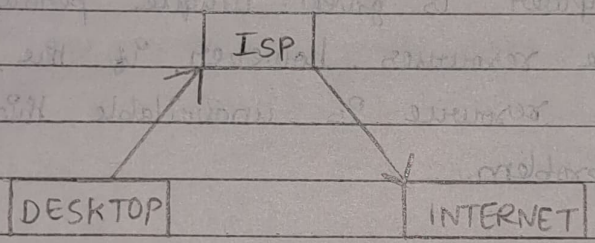
The Full-duplex mode is the fastest mode of communication between devices.



INTERNET SERVICE PROVIDER

Internet service provider is known by the acronym ISP. This business offers virtual hosting, website creation, and other related services, including access to the internet.

For instance, when you connect to the internet, the link between your Internet-capable equipment and the internet is established using a particular transmission mechanism that entails the transfer of data packets via an Internet protocol route.



COMPUTER NETWORK ARCHITECTURE:

The Physical and logical design of the software, hardware, protocols, and media used for data transfer constitutes computer network architecture. Simply expressed, we may say that this refers to how computers are set up and how duties are distributed among them.

There are two varieties of network architectures in use:

1. Peer-To-Peer network
2. client/server network

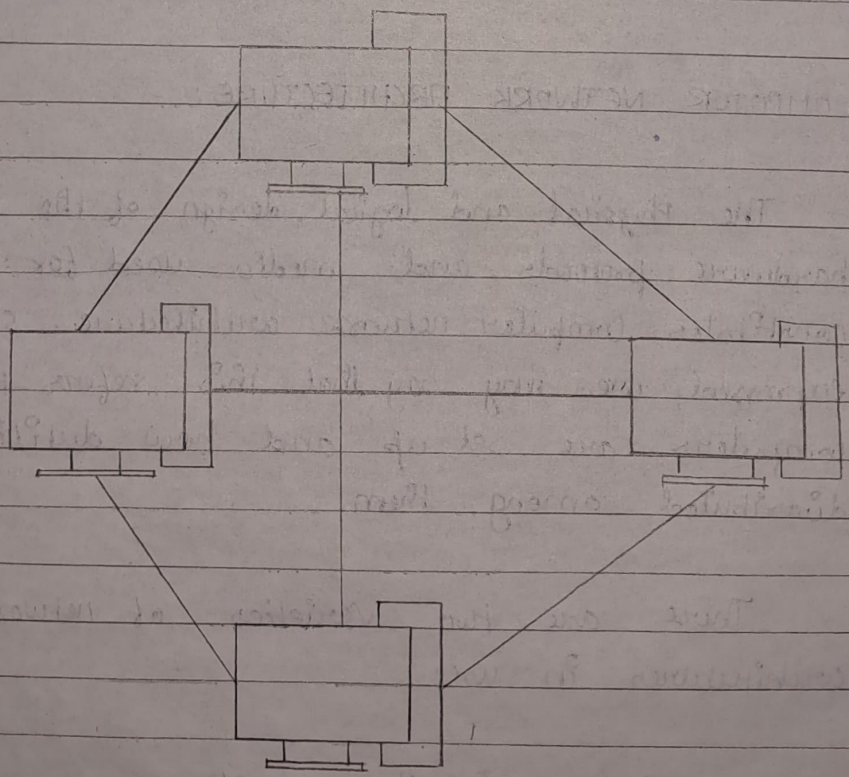
PEER-TO-PEER NETWORK

A Peer-to-peer network is one in which all the computers are connected and have an equal opportunity to process data

Peer-to-Peer networks, which typically have up to 10 computers, are beneficial in smaller settings.

A dedicated server is not present in a peer-to-peer network

Each computer is given unique permissions for sharing the resources, however if the computer hosting the resource is unavailable, this could cause a problem.

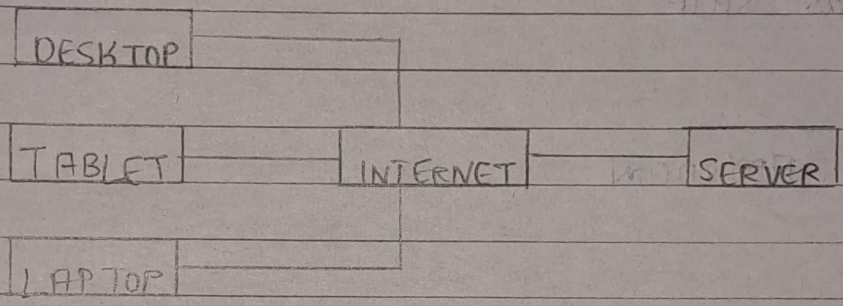


Date
Page

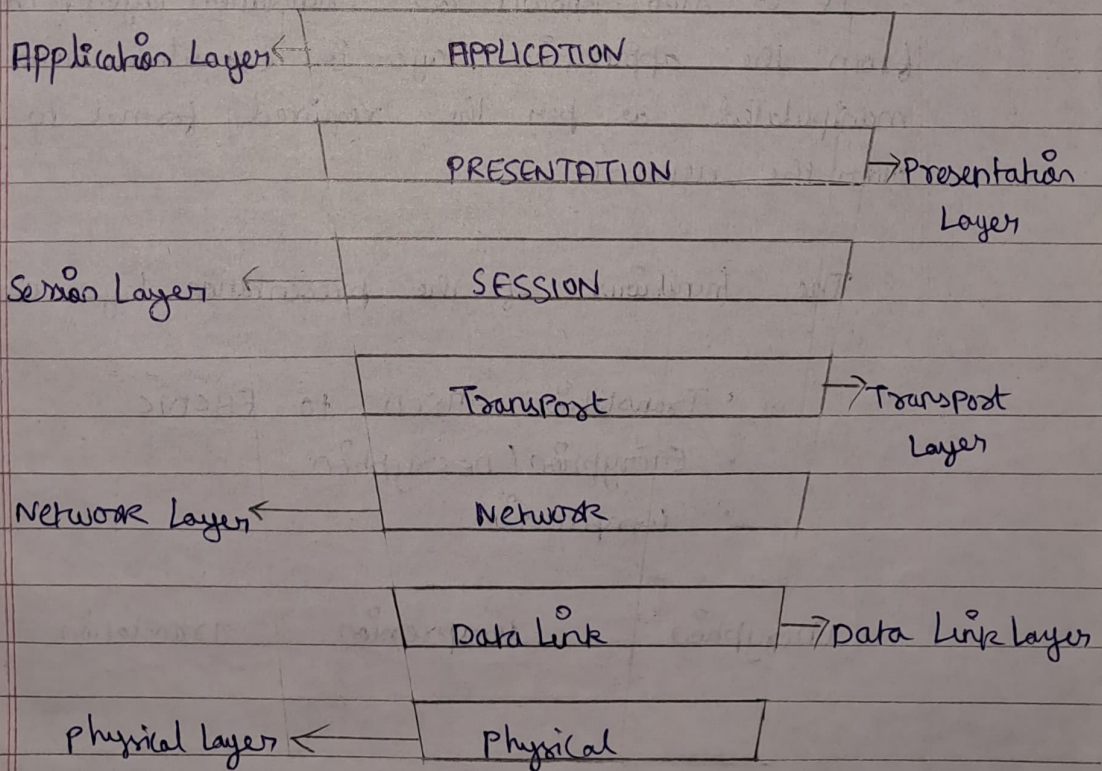
CLIENT / SERVER NETWORK

A client/server network is a form of computer network in which numerous workstations or less powerful personal computers are connected to a single, centrally located server.

It is a system in which clients are linked to the server just for resource sharing or utilisation.



THE OSI REFERENCE MODEL

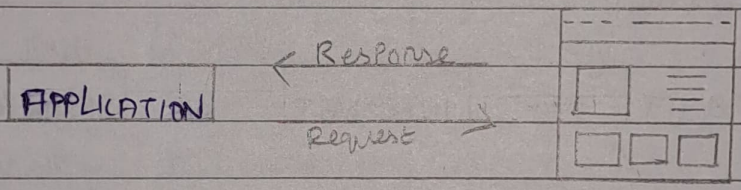


APPLICATION LAYER

It implemented by network applications and located at the very top of the OSI.

This layer also acts as a portal for application services to access the network and present information to the user.

Application Layer protocols include HTTP as well as SMTP.

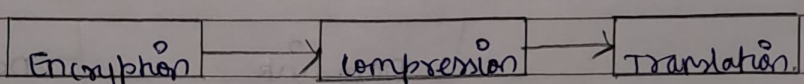


PRESENTATION LAYER

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

The functions of the presentation layer are:

- Translation - ASCII to EBCDIC
- Encryption / Decryption
- Compression.



SESSION LAYER

Establishing connections, keeping track of sessions, authenticating users, and ensuring security are all handled by this layer.

The functions of the ~~transport~~ session layer are:

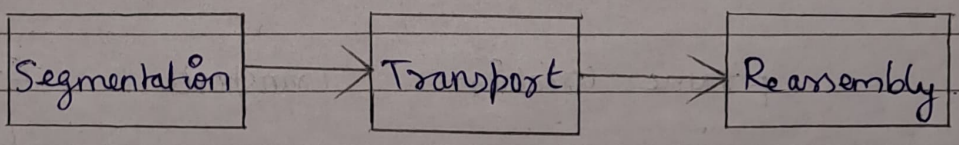
- Establishing, maintaining, and ending sessions
- Synchronization
- Dialog controller

TRANSPORT LAYER

The data transfers in the form of Segments. The full message must be delivered from beginning to end under its control. A successful data transmission is also acknowledged by the it, which also retransmits the data if an error is discovered.

The functions of the transport layer are:

- Segmentation and Reassembly
- Service point Addressing.

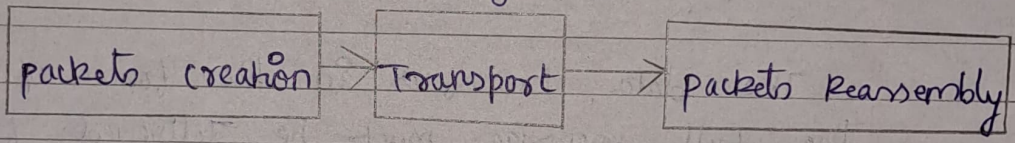


NETWORK LAYER

It handles packet routing by selecting the shortest route from a variety of options to transmit the packet. It inserts the IP addresses of the sender and receiver in the header.

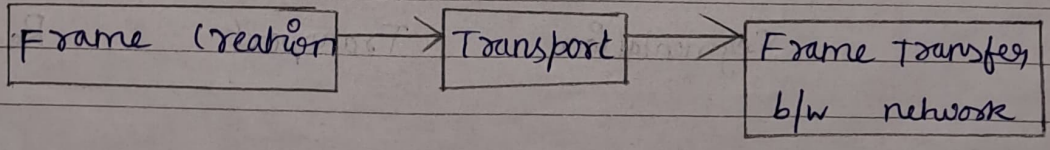
The functions of the transport layer are:

- Routing
- Logical Addressing



DATA LINK LAYER

- It enables data flow between two devices connected to the SAME network.
- It divides packets from the network layer into smaller units known as frames.
- It is in charge of flow control and error control during intra-network communication.

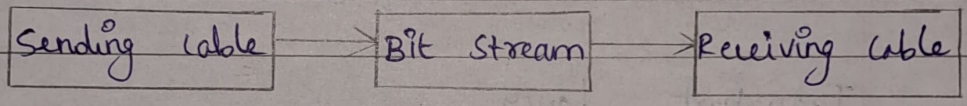


Date
Page

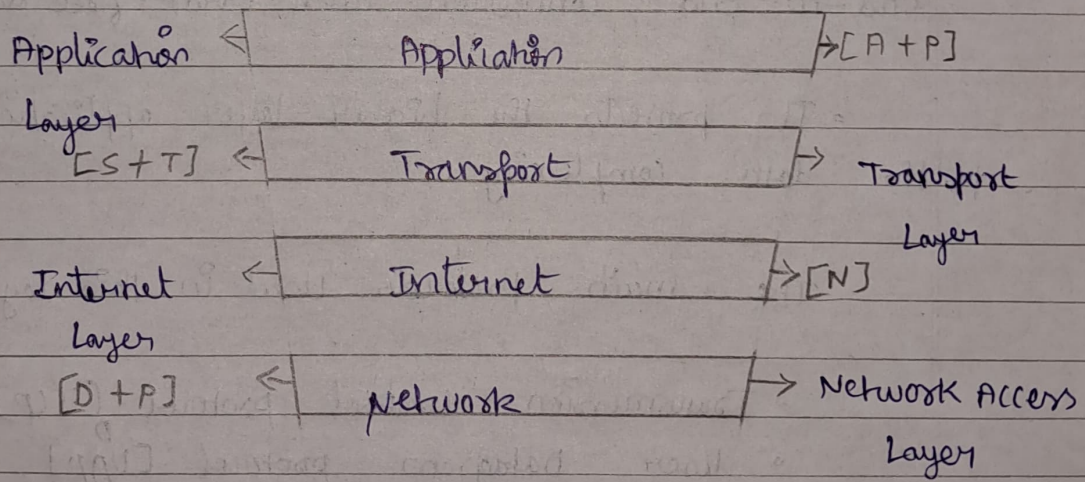
PHYSICAL LAYER

- This layer includes the actual hardware used for data transmission, such as cables and switches. Additionally, it is at this layer that the data is transformed into a bit stream, which is a series of ones and zeros.

- In order to differentiate the 1's from the 0's on both devices, the physical layer of both devices must also agree on a signal protocol.



TCP/IP MODEL:

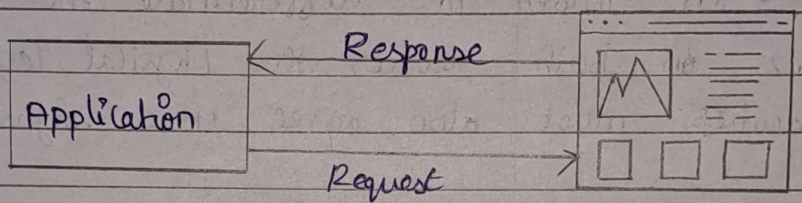


Date
Page

APPLICATION LAYER

- It is responsible for node-to-node communication and controls user-interface specifications.

- Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X window, LPD.



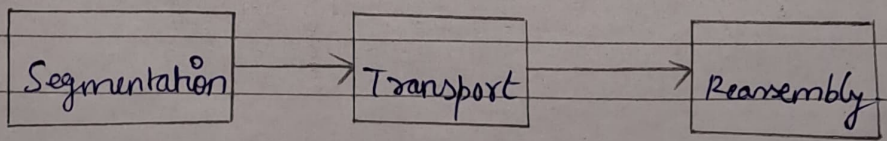
Transport Layer

- It is in charge of ensuring seamless end-to-end connection and error-free data transfer.

- It protects the higher-layer applications from the data complexity.

The main protocols used in this layer are:

- Transmission control protocol [TCP]
- User Datagram protocol [UDP]

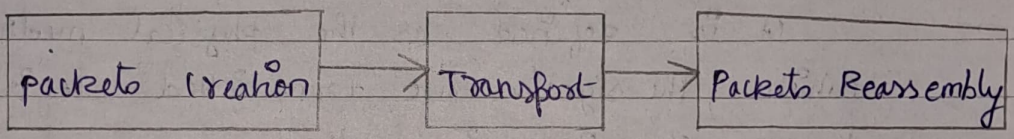


INTERNET LAYER

This layer performs similar tasks as the Network Layer of the OSI model. It outlines the protocols in charge of logical data transmission over the whole network.

The main protocols used in this layer are:

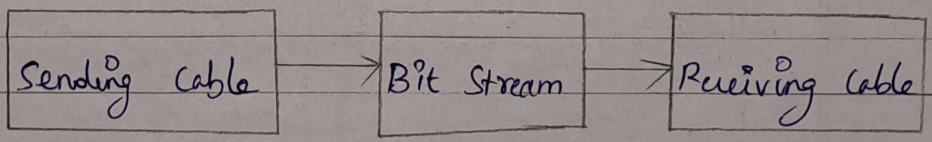
- Ip
- ICMP
- ARP



NETWORK ACCESS LAYER

- It is a combination of physical Layer and Data link Layer of OSI model.

- It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.



TRANSMISSION MEDIA

It is the channel through which data is sent from one place to another.

It is classified into two categories.

1. Guided Transmission Media Wired
2. Unguided Transmission Media. Wireless

GUIDED TRANSMISSION MEDIA

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

Types of Guided Media:

1. Twisted pair
2. Coaxial cable
3. Fibre optic.

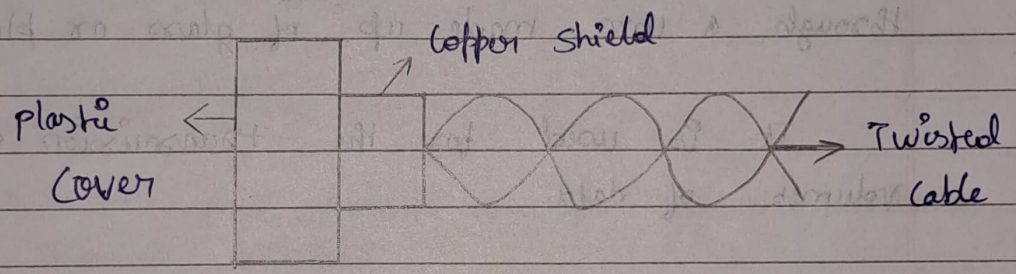
Date
Page

TWISTED PAIR:

It is made up of two wires with distinct insulated conductors that are looped around one another. Usually, a protective sheath is wrapped around multiple such pairs.

ADVANTAGES:

- Cost Effective.
- Easy Instalation.

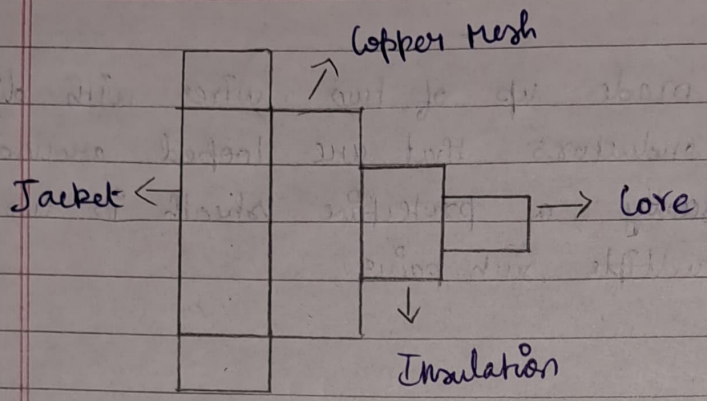


COAXIAL CABLE

It has two parallel conductors, each with a separate insulated protection cover, and an exterior plastic covering with an insulating layer composed of PVC or Teflon.

ADVANTAGES:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive.



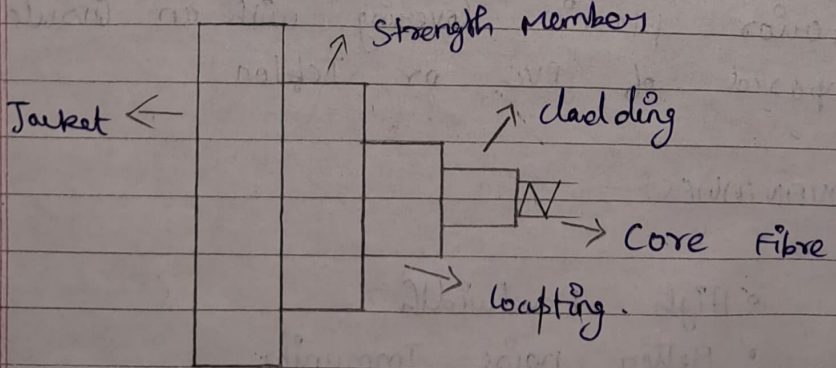
OPTICAL FIBRE

It uses the concept of refraction of light through a core made up of glass or plastic.

It is used for the transmission of large volumes of data.

ADVANTAGES:

- Increased capacity and bandwidth
- Immunity to electromagnetic interference
- Resistance to corrosive materials



UN-GUIDED TRANSMISSION MEDIA

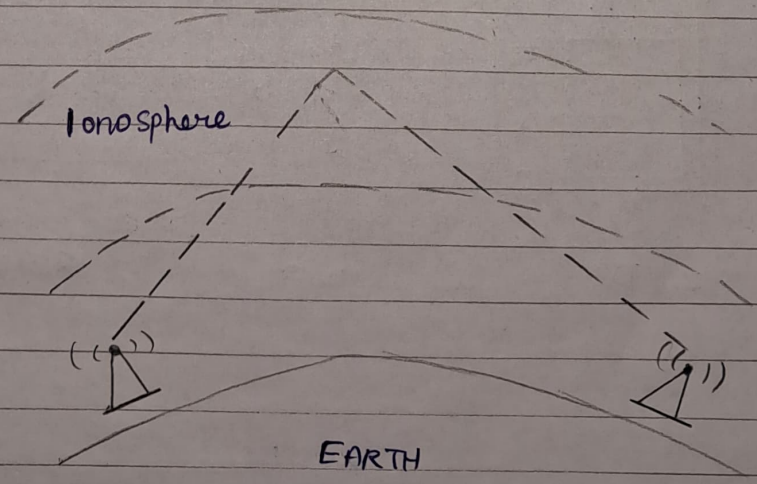
It is also referred to as wireless or unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

Types of un-guided media:

1. Radio waves
2. Micro waves
3. Infrared.

RADIO WAVES

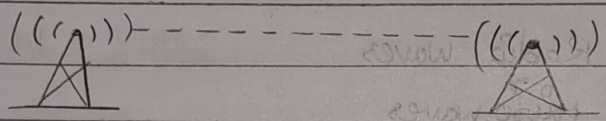
- These are easy to generate and can penetrate through buildings.
- The sending and receiving antennas need not be aligned
- Frequency Range : 3KHz - 1GHz.
- Example : AM and FM radios and cordless phones.



Date
Page

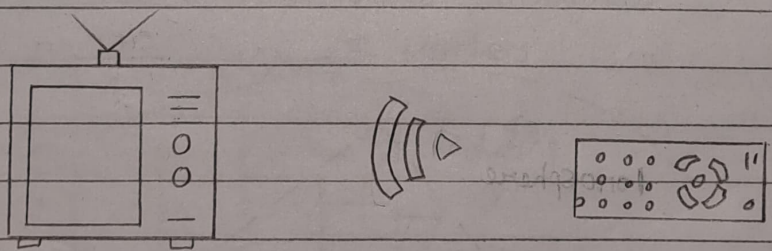
MICROWAVES

- The transmitter and reception stations need to be precisely positioned in relation to one another.
- The signal's range is directly inversely related to the antenna's height
- Frequency Range : 1 GHz - 300 GHz
- Example : Television and mobile phone communication.



INFRARED

- It is used to communicate over small distances, and obstacles are insurmountable to them.
- Frequency Range : 300 GHz - 400 THz
- Example : printers, wireless mice, TV remote controls, and wireless keyboards.



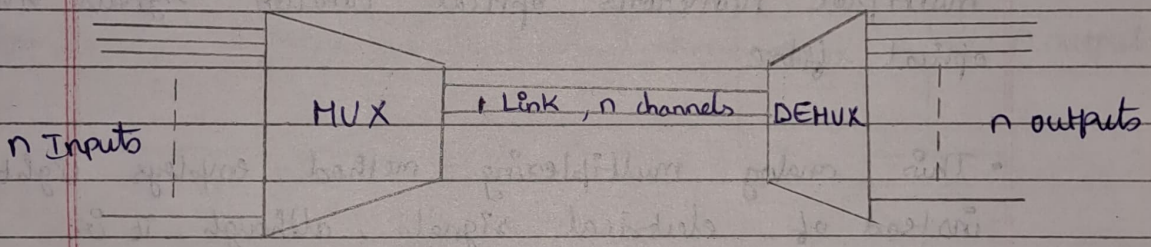
TV WIFI REMOTE

MULTIPLEXING

Sharing a resource, like bandwidth, is known as multiplexing. In this process several signals from various sources are integrated and delivered across a single communication or physical line.

TYPES OF MULTIPLEXING:

1. Frequency Division Multiplexing [FDM]
2. Wavelength Division Multiplexing [WDM]
3. Time - Division Multiplexing [TDM]

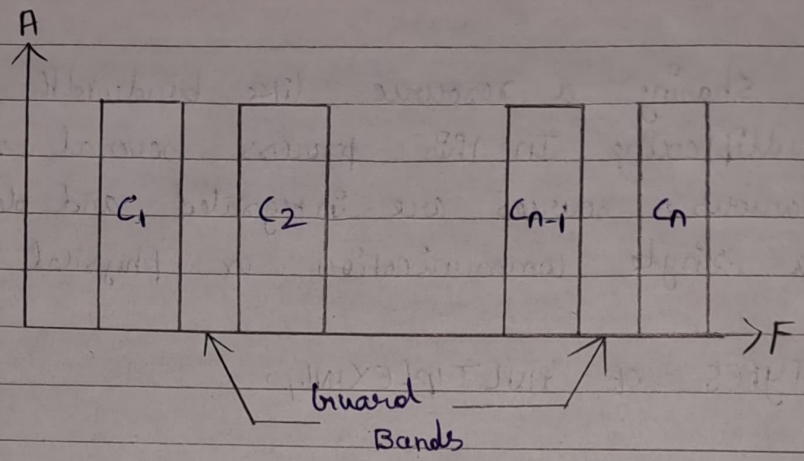


FREQUENCY DIVISION MULTIPLEXING [FDM]:

- It divides the bandwidth of a single physical medium into a number of smaller, independent frequency channels.

- FDM is an analog technology

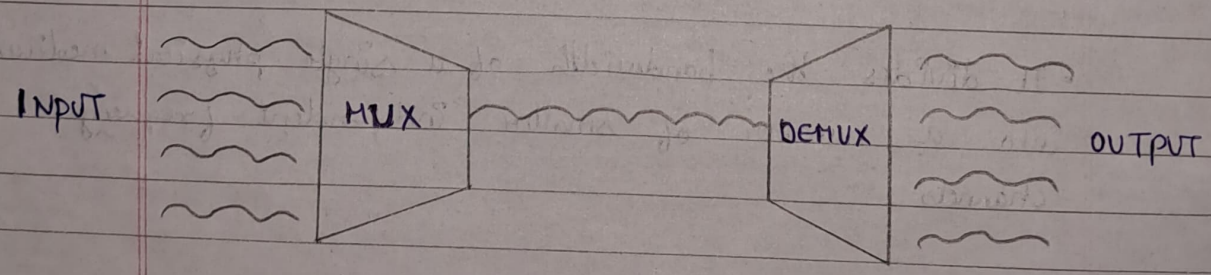
- It uses guard band, which is a frequency that neither channel uses.



WAVELENGTH DIVISION MULTIPLEXING [WDM].

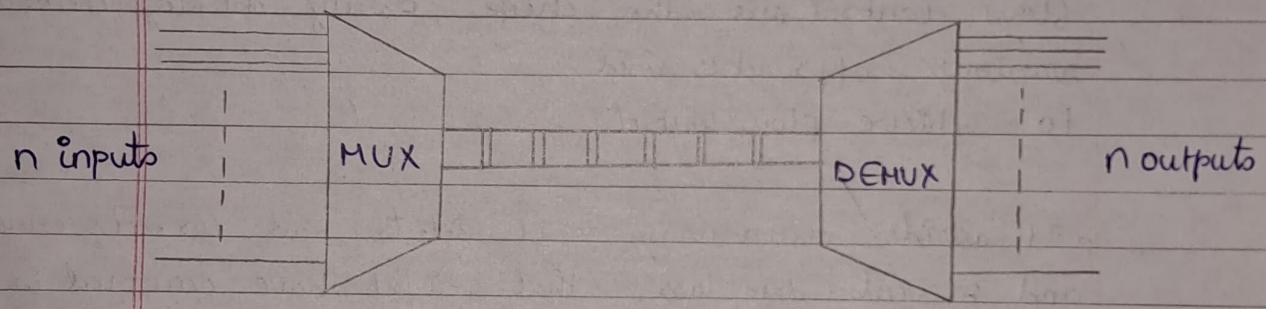
- This involves employing several wavelengths to multiplex numerous optical carrier signals onto one optical fibre.

- This analog multiplexing method employs light instead of electrical signals, although it is fundamentally similar to FDM.



TIME DIVISION MULTIPLEXING [TDM]

- TDM uses time slots to allocate the shared channel among its users.
- Each user is limited to sending data during the allotted time period.
- In this, the frequency (bandwidth) of all transmissions is the same at all times.



DATA LINK LAYER:

FLOW CONTROL:

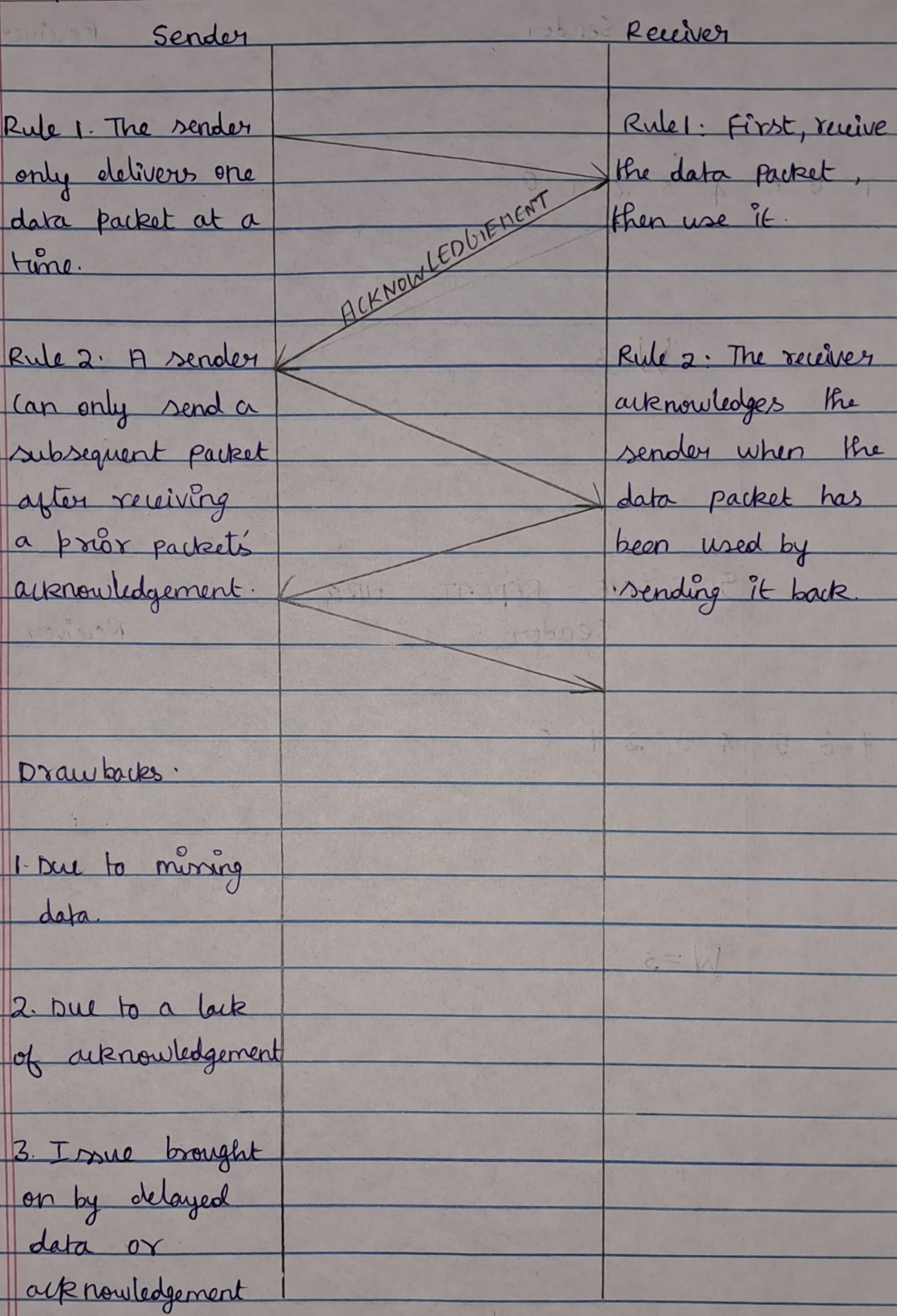
It is an important function of the Data Link Layer. It refers to a set of procedures that tells the sender how much data it can transmit before waiting for acknowledgement from the receiver.

ERROR CONTROL:

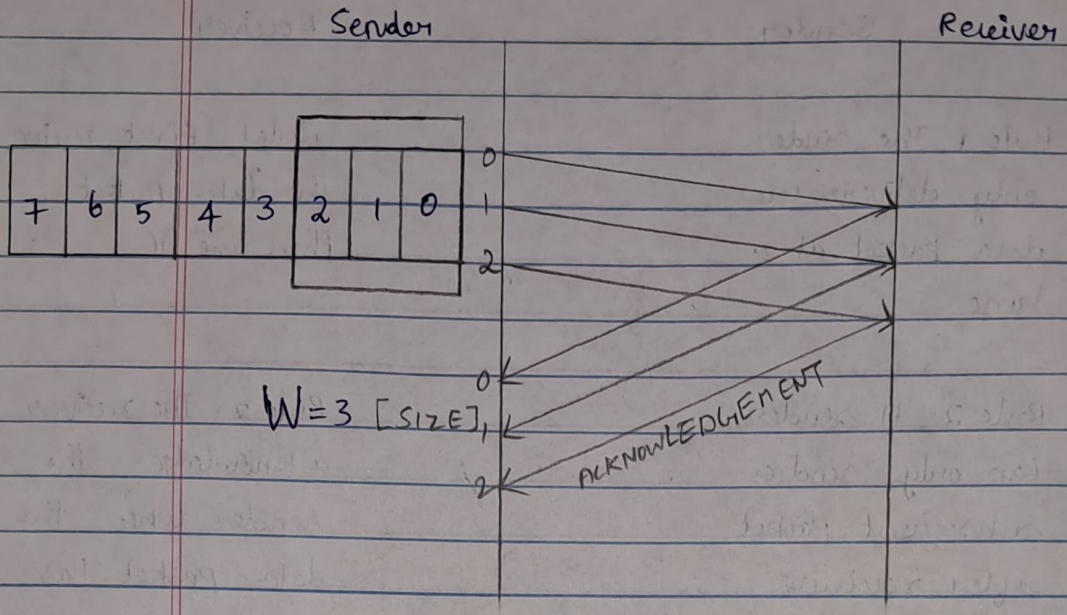
The error control function of data link layer detects the errors in transmitted frames and retransmit all the erroneous frames.

FLOW CONTROL	ERROR CONTROL
• It is a method used to maintain proper transmission of the data from sender to the receiver.	• It is used to ensure that error-free data is delivered from sender to receiver.
• Feedback-based flow control and rate-based flow control are the various approaches used to achieve flow control	• Many methods can be used here like Cyclic Redundancy check, parity checking, checksum.
• It avoids overrunning and prevents data loss.	• It detects and corrects errors that might have occurred in transmission.
• Examples: Stop-and-wait and Sliding Window	• Examples: Stop-and-wait ARQ, Go-Back-N ARQ, Selective-Repeat ARQ

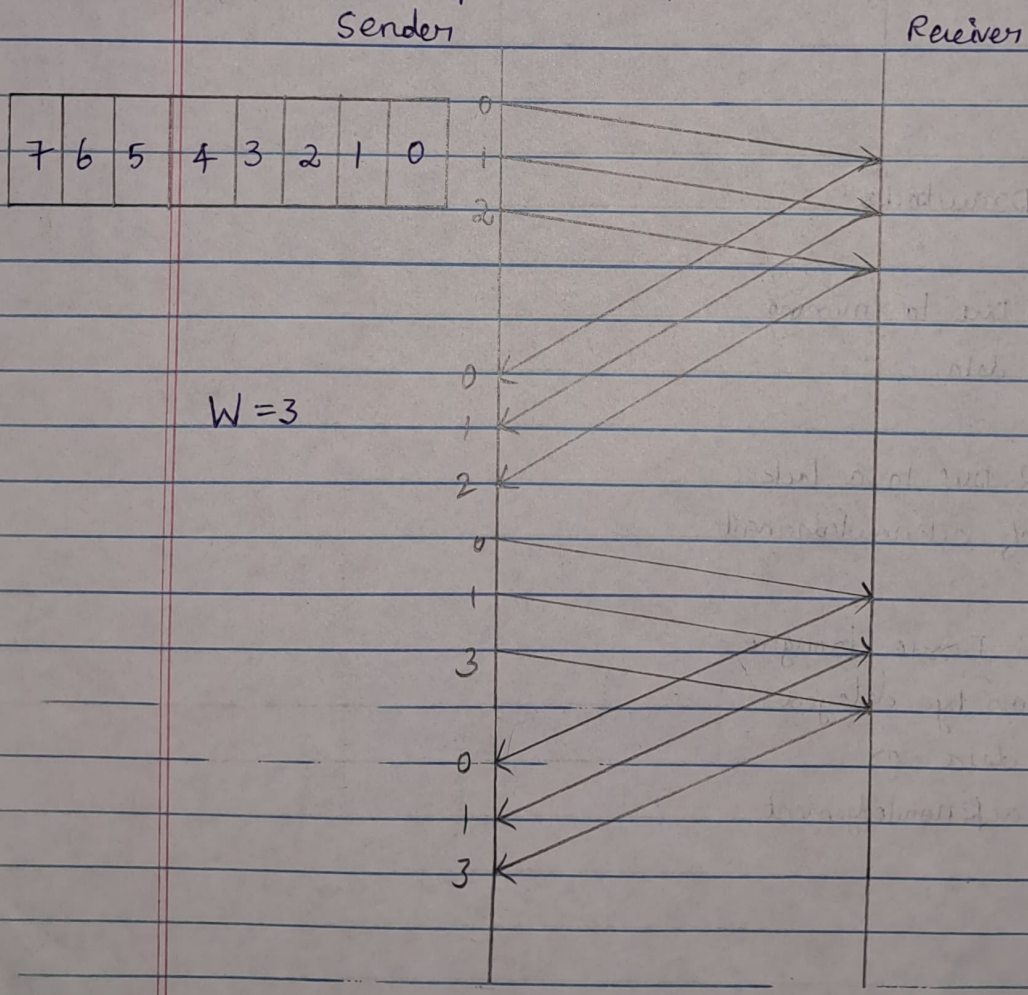
STOP AND WAIT PROTOCOL



GO-BACK-N ARQ

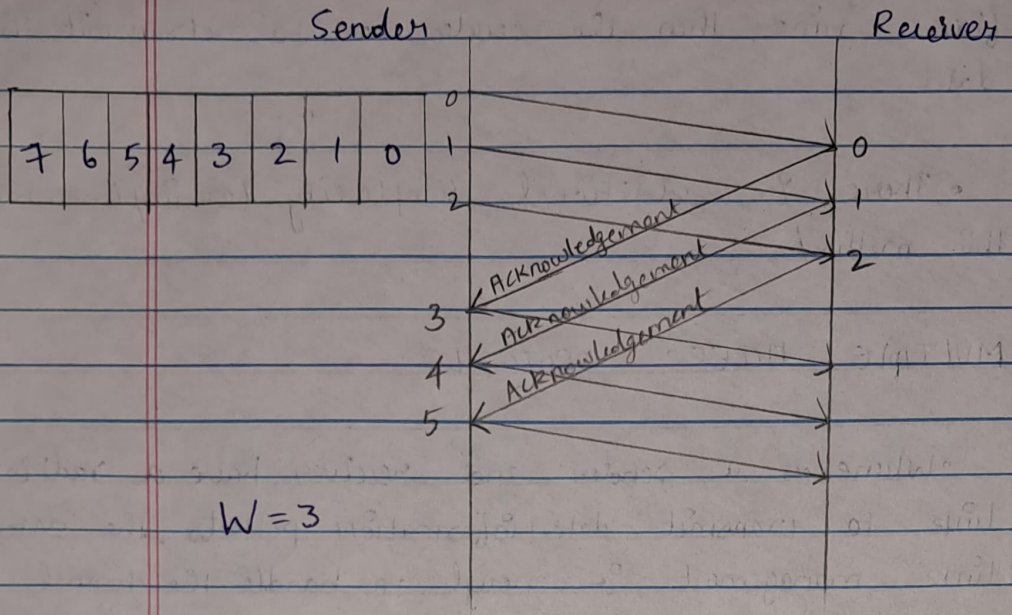


SELECTIVE REPEAT ARQ



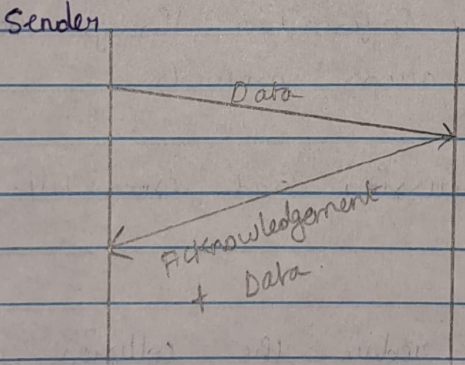
ITERATION GOES ON.....

SLIDING WINDOW



PIGGYBACKING

Piggybacking is a method of attaching acknowledgement to the outgoing data packet.



ADVANTAGES:

- The available channel bandwidth is used efficiently.

DISADVANTAGES:

- As there is delayed transmission of acknowledgement so if the acknowledgement is not received within the

fixed time then the sender has to retransmit the data.

- There is additional complexity for implementing this method.

MULTIPLE ACCESS PROTOCOLS:

- Whenever a sender and receiver have a radical link to transmit data/information packets, the data link management is enough to handle the channel.

- Assume that the data transmission between the two devices doesn't use a committed route.

- The channel in this instance simultaneously sends the information through the channel while using different access protocols.

- Collision and cross-talk are likely to result from it.

- To reduce the collision and prevent channel disruption, various access procedures are therefore required.

TYPES OF MULTIPLE ACCESS PROTOCOLS

1. Random Access protocol	2. Controlled Access
• Aloha • CSMA • CSMA/CD • CSMA/CA	• Reservation • Polling • Token passing

3. Channelization

- FDMA
- TDMA
- CDMA

WHAT IS ALOHA?

Although Aloha is intended for wireless LAN [Local Area Network], it may also be used to send data via a shared media.

In aloha, any station may at any moment provide information to a channel.

There is no need for carrier sensing.

Types of ALOHA:

1. pure ALOHA
2. Slotted ALOHA

S.no.	On the basis of	pure Aloha	Slotted Aloha
1.	Basic	In pure aloha, data can be transmitted at any time by any station.	In slotted aloha, data can be transmitted at the beginning of the time slot.
2.	Introduced by	It was introduced under the leadership of Norman Abramson in 1970 at the University of Hawaii.	It was introduced by Robert in 1972 to improve pure aloha's capacity.
3.	Time	Time is not synchronized in pure aloha. Time is continuous in it.	Time is globally synchronized in slotted aloha. Time is discrete in it.
4.	Number of collisions	It does not decrease the number of collisions to half.	On the other hand, slotted aloha enhances the efficiency of pure aloha. It decreases the number of collisions to half.
5.	Vulnerable time	In pure aloha, the vulnerable time is $= 2 \times Tt$	Whereas, in slotted aloha, the vulnerable time is $= Tt$.

S. no.	On the basis of	pure Aloha	Slotted Aloha
6.	Sucessful transmission	In pure aloha, the probability of the sucessful transmission of the frame is - $S = G * e^{-2G}$	In slotted aloha, the probability of the sucessful transmission of the frame is - $S = G * e^{-G}$
7.	Throughput	The maximum throughput in pure aloha is about 18%.	The maximum throughput in slotted aloha is about 37%.

CSMA/CD

The Carrier Sense Multiple Access / Collision Detection protocol is used to detect a collision in the media access control (MAC) layer.

Once the collision was detected, the CSMA CD immediately stopped the transmission by sending the signal so that the sender does not waste all the time to send the data packet.

ADVANTAGES:

- It is utilized for quick collision detection on a shared channel.
- For collision detection, CSMA/CD is superior to CSMA

- To prevent the transfer of trash in any way, CSMA/CD is utilized.

- It is used to consume or share the same amount of bandwidth at each station as necessary

- Compared to CSMA CA, it has reduced CSMA CD overhead.

DISADVANTAGES:

- Due to the fact that CSMA/CD's efficiency declines with increasing distance, it is not appropriate for long-distance networks.

- Beyond this range, it is unable to detect collisions. It can only detect collisions up to 2500 meters.

- performance of collision detection is decreased when more devices are added to a CSMA CD.

CSMA/CA:

- The Carrier Sense Multiple Access / Collision Avoidance protocol is used whenever a station sends a data frame to a channel, it checks whether it is in use.

- If the shared channel is busy, the station waits until the channel enters idle mode.

- Hence, we can say that it reduces the chances of collisions and make better use of the medium to send data packets more efficiently.

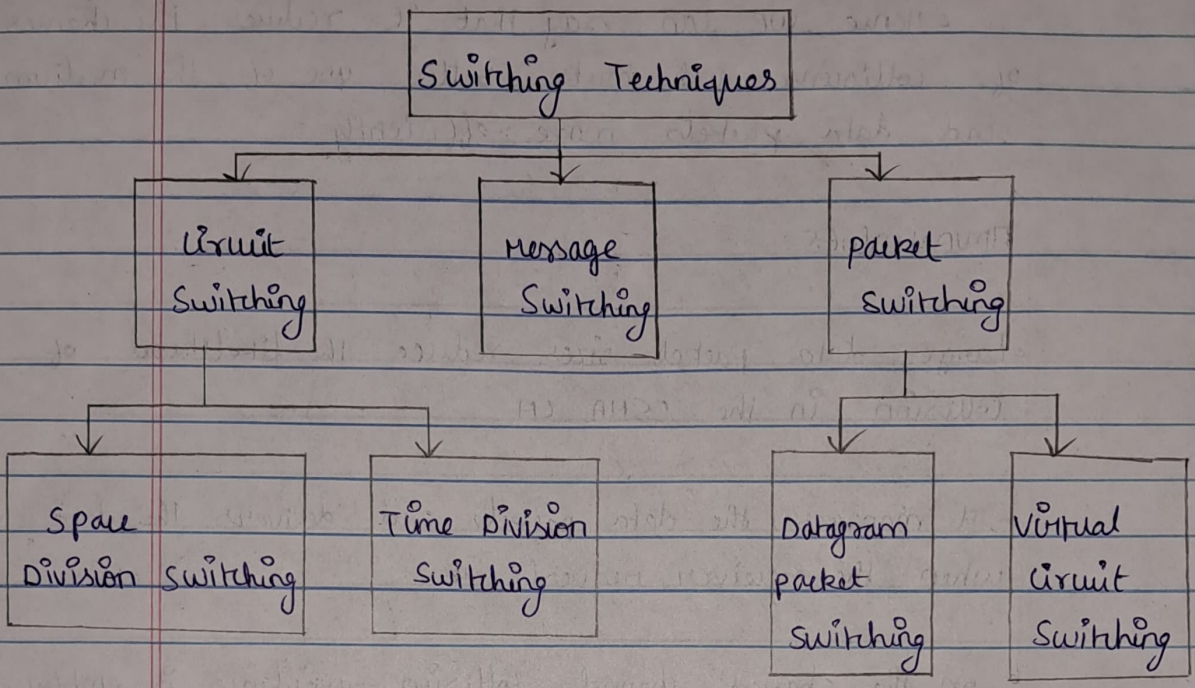
ADVANTAGES:

- Large data packet sizes reduce the likelihood of collision in the CSMA CA.
- It manages the data packets and delivers the data only when the receiver requests it.
- on the shared channel, collision avoidance is employed instead of collision detection.
- By using CSMA CA, unnecessary data transmissions over the channel is avoided.
- It works well for wireless transmission within a network.
- With the aid of the RTS/CTS extension, it prevents needless data traffic on the network

DISADVANTAGES:

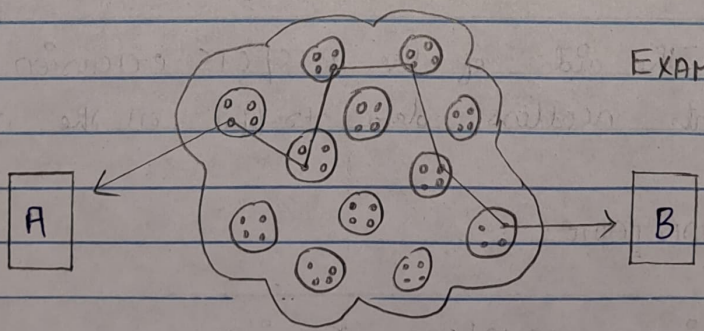
- Sometimes CSMA/CA requires more waiting time than typical before transmitting a data packet.
- Each station uses extra bandwidth because of it.
- It's efficiency is lower than that of a CSMA CD.

SWITCHING TECHNIQUES - NETWORK LAYER



CIRCUIT SWITCHING

- This switching technique establishes a dedicated channel between the transmitter and the receiver
- until the connection is terminated, the dedicated way will continue to exist.



EXAMPLE: Telephone

SPACE DIVISION SWITCHING

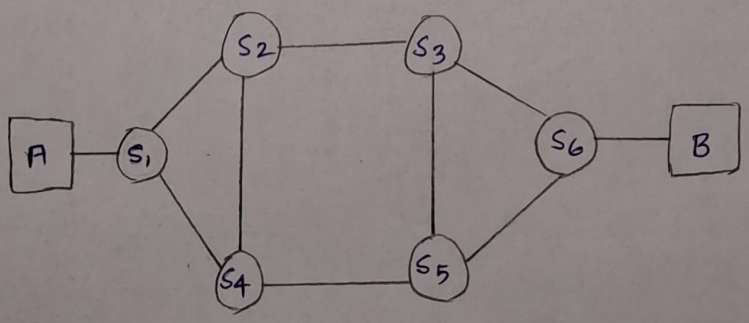
- To produce a single transmission channel in a switch, this technique employs a physically unique set of crosspoints.
- The switches used in space division switching are quick, reliable, and non blocking.
- Types of switches used:
  1. crossbar switch
  2. multi stage switch

TIME DIVISION SWITCHING:

- Time division switching refers to the process of receiving and re-transmitting incoming and outgoing messages in a separate time slot.
- The digitized message/data is divided into time periods or slots.

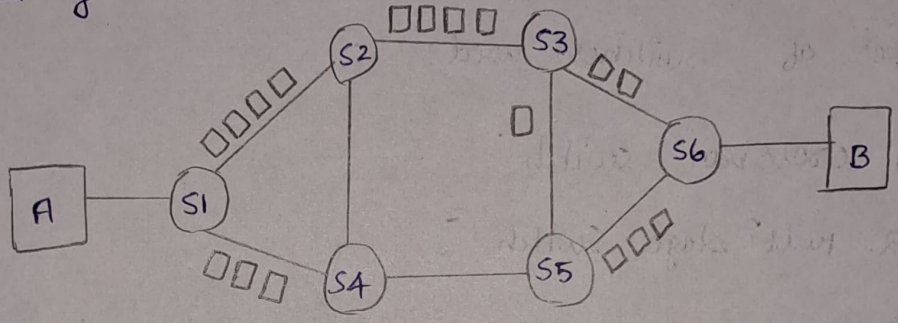
MESSAGE SWITCHING:

- This technique does not provide a specific route between the sender and receiver.
- Store and Forward Network.



PACKET SWITCHING

- It divides the data into packets, and these packets are identified using their sequence number.
- These packets contains source address, destination address, intermediate node address, etc. for routing independently.



DATAGRAM PACKET SWITCHING	VIRTUAL CIRCUIT PACKET SWITCHING
• Connectionless	• Connection oriented
• NO Reservation	• Reservation
• out of order	• Same order
• High overhead	• Less overhead
• Packet Lost [↑]	• Packet lost [↓]
• used in internet	• used in ATM

ATM – Asynchronous Transfer Mode

LOGICAL ADDRESSING

- It is the way through which a host is uniquely identified in an entire network by assigning an IP address to it.
- A 32 bit IP address are used in it, and are divided into network ID and host ID.
- Internet protocol is used for logical addressing
- IP provides two types of addressing:
    1. IPV4
    2. IPV6

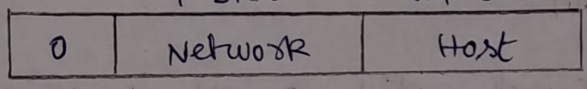
CLASSFUL ADDRESSING:

Classful IP addressing is an IPV4 addressing architecture that is divided into five classes as follows:

1. class A
2. class B
3. class C
4. class D
5. class E

CLASS A

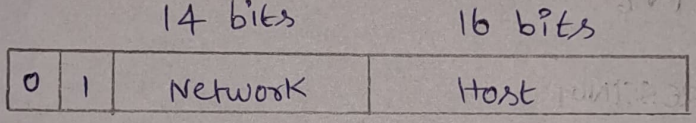
In class A, the first 8 bits of the address are used for the network portion, and the final 24 bits are set aside for the host portion. The 8 octet's leading initial bit is fixed.



- Network addresses : $2^{7} - 2 = 128 - 2 = 126$
- Host addresses : $2^{24} - 2 = 1,67,77,216 - 2 = 16777214$

CLASS B

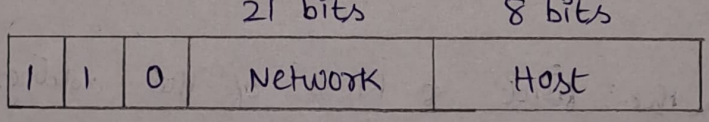
In class B, the first 16 bits of the address are used for the network portion, and the latter 16 bits are set aside for the host portion. The octet's first two bits are fixed.



- Network addresses : $2^{14} = 16384$
- Host addresses : $2^{16} - 2 = 65536 - 2 = 65534$

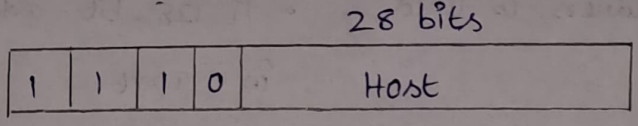
CLASS C

In class C, the first 24 bits of the address are set aside for the network portion, while the final 8 bits are set aside for the host portion. The octet's first three bits are fixed.

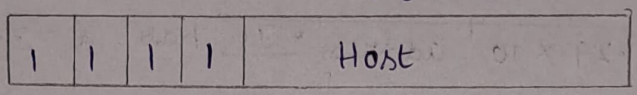


- Network addresses = $2^{21} = 2097152$
- Host addresses : $2^{8} - 2 = 256 - 2 = 254$

CLASS D



CLASS E



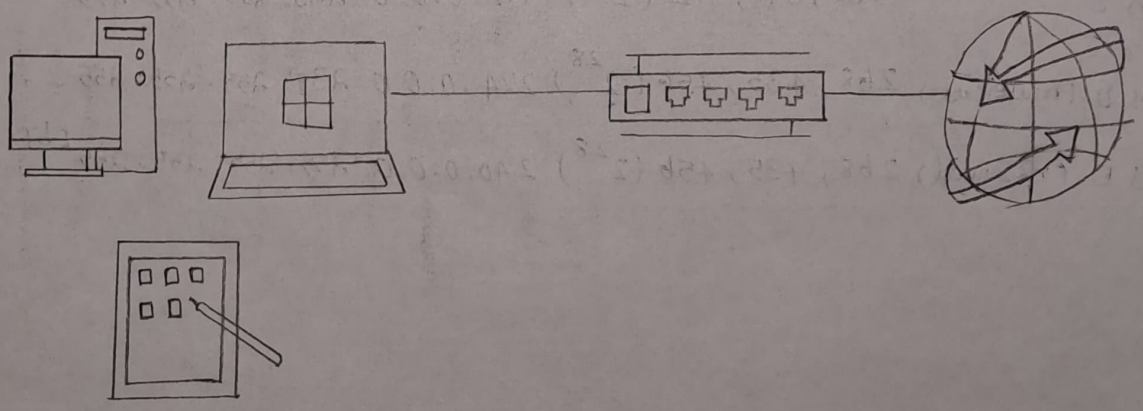
Class	Leading bits	Size of network number bit field	Size of rest bit field	Number of networks	Addresses per network
class A	0	8	24	128 (2^7)	16,777,216 (2^{24})
class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})
class C	110	24	8	2,097,152 (2^{21})	256 (2^8)
class D (multicast)	1110	not defined	not defined	not defined	not defined
class E (reserved)	1111	not defined	not defined	not defined	not defined

class	Total addresses in class	Start address	End address
class A	2,147,483,648 (2^{31})	0.0.0.0	127.255.255.255 [a]
class B	1,073,741,824 (2^{30})	128.0.0.0	191.255.255.255
class C	536,870,912 (2^{29})	192.0.0.0	223.255.255.255
class D (multicast)	268,435,456 (2^{28})	224.0.0.0	239.255.255.255
class E (reserved)	268,435,456 (2^{28})	240.0.0.0	255.255.255.255 [b]

IPV4	IPV6
• A 32-bit address is used in IPV4	• A 128-bit address is used in IPV6
• End-to-end connection integrity is not possible.	• End to end, connection integrity is possible.
• It has a 4.29×10^9 address space generation capacity.	• It has a 3.4×10^{38} address space generation capacity.
• Application determines the security feature.	• IPSEC is a built-in security element of the IPV6 protocol.
• IPV4 addresses are represented as decimal numbers	• IPV6 addresses are represented using hexadecimal numbers.
• It's header is 20-60 bytes long.	• It has a fixed header size of 40 bytes
• It is possible to switch from IPV4 to IPV6.	• IPV4 conversion is not possible for every IPV6.

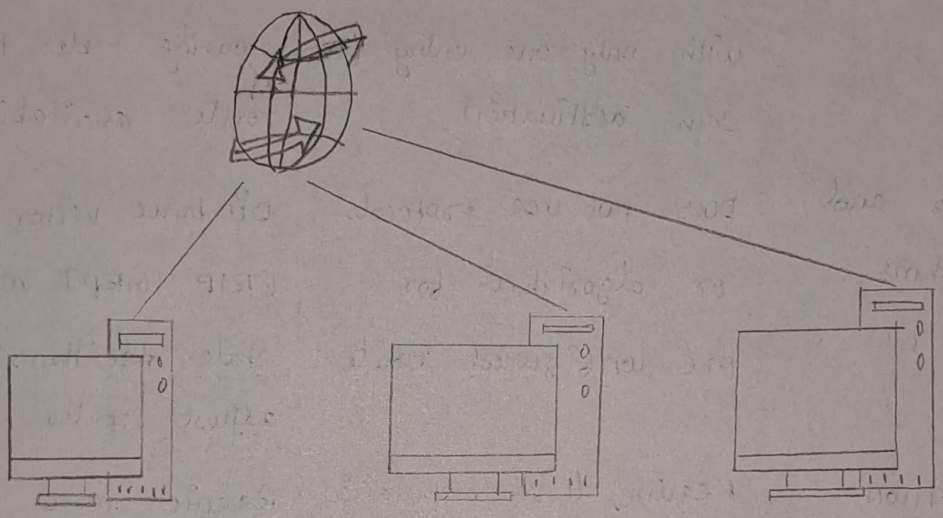
NETWORK ADDRESS TRANSLATION

NAT makes it possible for several devices to access the internet using a single public address.



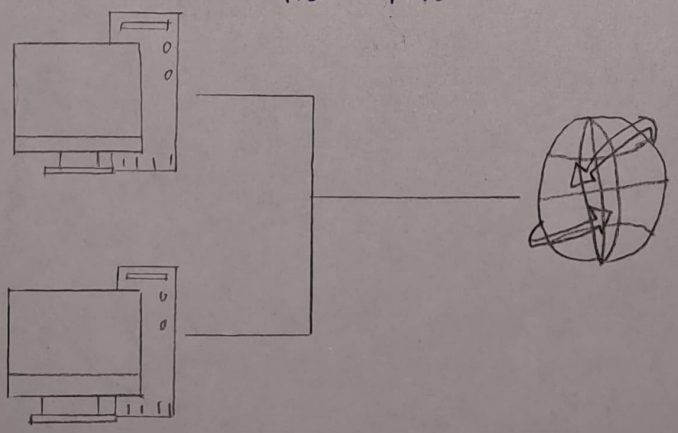
ADDRESS RESOLUTION PROTOCOL [ARP]

- This process maps a dynamic IP address to a machine's MAC address in a network.
- ARP's primary function is to convert 48-bit addresses from 32-bit formats and the reverse.



DYNAMIC HOST CONFIGURATION PROTOCOL [DHCP]

1. DHCPDiscover - Looks for a DHCP server
2. DHCP offer - The DHCP server offers an address
3. DHCPRequest - The host requests to lease the address
4. DHCPack - DHCP server sends the IP addresses to the host.



	Static routing	Dynamic routing
Path Selection	one pre-configured route to destination	Multiple available routes to destination
Route updates	Engineers must reconfigure to make route changes	Algorithms automatically update with preferred route changes
Routing tables	Smaller routing table with only one entry for each destination.	Routers send out entire routing tables to identify route availability.
Protocols and Algorithms	Does not use protocols or algorithms for pre-configured route	Distance vector algorithm [RIP, IGRP] and link state algorithms [OSPF, IS-IS] adjust routes
COMPUTATION AND BANDWIDTH	Requires less computation time and bandwidth	Requires more computation and bandwidth
Security	Better security	Less security
Use cases	used in smaller networks with fewer routers and unchanging network architecture.	used in larger networks and in networks that change frequently.

TRANSPORT LAYER

USER DATAGRAM PROTOCOL [UDP]

- UDP is a communication protocol that is utilised on the internet for time-sensitive transfers, such as video playing.
- By avoiding a formal connection establishment before data is delivered, it speeds up communications.
- This enables data to be transported incredibly fast, but it may also lead to packets being lost in transit, opening up potential for exploitation in the form of DDoS attacks. [connection-less-protocol]

ADVANTAGES OF UDP:

- UDP packets are often smaller than TCP.
- Connectionless Transmission.
- It is quicker, easier, and more effective.

DISADVANTAGES OF UDP:

- There is no assurance that the data will reach the sender.
- Inadequate error checking techniques.
- The missing shipments won't be sent again.
- Receiving packets that are out of sequence is possible.

TRANSMISSION CONTROL PROTOCOL [TCP]

- TCP is a connection-oriented protocol, the connection will stay active as long as the sender and receiver are still in contact.
- The data is then divided into a number of packets, given a number, and finally transmitted to the destination.
- on the receiver end, the TCP will reassemble the packets and send them to the application layer.

FEATURES OF TCP:

1. Connection-oriented and Reliable
2. Flow control
3. Error control
4. Congestion control
5. Full Duplex.

WHAT IS CONGESTION?

A condition when network response times are slowed by high message flow at the network layer.

CONGESTION CONTROL

- Congestion Control is a method that regulates how data packets enter the network, allowing for more efficient use of a shared network infrastructure and preventing congestive collapse
- Congestion Control algorithms are used at the TCP layer as a method to prevent congestive collapse in a network.

1. Leaky Bucket Algorithm
2. Token Bucket Algorithm

LEAKY BUCKET ALGORITHM

The network's transmission rate is managed, and the bursty traffic is transformed into a continuous stream using this algorithm.

TOKEN BUCKET ALGORITHM

- Tokens are tossed into the bucket at predetermined intervals
- The bucket can hold a maximum of 6.
- If the packet is prepared, a token is taken out of the bucket and it is transmitted.
- Assume that the packet cannot be forwarded if there is no token in the bucket.

APPLICATION LAYER

DOMAIN NAME SYSTEM

- A host's name and its IP address are mapped using the directory services DNS.
- The internet cannot function without DNS.
- DNS is a service that converts domain names into IP addresses. This enables network users to locate other hosts by using familiar names rather than their memory of IP addresses.

WORLD WIDE WEB COMMUNICATION:

- The World Wide Web is about communication between web clients and web servers.
- clients are often browsers (Chrome, Edge, Safari), but they can be any type of program or device.
- servers are most often computers in the cloud.

HTTP REQUEST / RESPONSE

The requests and answers used in communication between clients and servers are as follows:

1. An HTTP request is sent to the web by a client (a browser).
2. The query is sent to a web server.
3. To handle the request, the server executes a programme.
4. The browser receives an HTTP response (output) from the server.
5. The browser serves as the client and gets the answer.

TELNET:

- A text-based, two-way communication channel between two computers is provided by the network protocol known as Telnet, which allows for virtual computer access.
- Network control program (NCP) protocols were initially used by TELNET. Later on, it was given the name Teletype over Network protocol, or TONP.

- Although it has been used indiscriminately for some time, on March 5, 1973, it was formally established in articles that were published.

FIREWALL:

- A firewall is a network security device that can be hardware - or software - based. It analyses all incoming and outgoing traffic and ~~devices~~ decides whether to accept, reject, or discard that particular traffic based on a predetermined set of security rules.

- Recognize: permit the traffic
- Blocking the traffic while sending a "unreachable error" in response to rejection
- Stop the traffic without responding: drop.

ELECTRONIC MAIL:

- E-mail is defined as the transmission of messages on the Internet. It is one of the most commonly used features over communications network that may contain text, files, images, or other attachments.
- The basic components of an email system are:

* User Agent [UA]
* Message Transfer Agent [MTA]
* Mail Box
* Spool file

NETWORK MANAGEMENT:

- Network management is a broad subject that gives network administrators access to tools, protocols and techniques for managing networks in order to enable optimal network operations.
- In order to optimize the network and maintain continued availability, a number of features are included in network management.
- Among the essential elements of network administration are the following:
  - * network performance monitoring
  - * network monitoring
  - * network maintenance
  - * network configuration management
  - * network provisioning.

CRYPTOGRAPHY - BASIC CONCEPTS

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.

OBJECTIVES OF CRYPTOGRAPHY ARE:

CONFIDENTIALITY: Anyone for whom the information was not meant cannot understand it.

INTEGRITY: The information cannot be changed while being stored or being transported between the sender and the intended recipient without the change being noticed.

NON-REPUDIATION: The person who created or sent the material cannot afterwards deny that they had any motivation for doing so.

AUTHENTICATION: Both the sender and the recipient are able to verify each other's identities and the information's source and destination.

TYPES OF CRYPTOGRAPHY:

1. Symmetric Key cryptography
2. Asymmetric Key cryptography