New L J Institute of Engineering and Technology

Subject: Computer Networks
Subject Code: 3150710
Branch: CSE
Semester: V

- **Faculty Name:**
  - **Assistant Professor: Bhaumik Gelani**

- **Teaching and Examination Scheme:**

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE (E)	PA (M)	ESE (V)	PA (I)	
4	0	2	5	70	30	30	20	150

Unit No.	Unit Title	% Weightage
1	Introduction to computer networks and Internet	15
2	Application Layer	17
3	Transport Layer	25
4	Network Layer	25
5	The Link layer and Local Area Networks	18

Unit – 1 Introduction to computer networks and Internet

1. **What is Topology? List out and explain various network topology.**
2. **Explain Wired media.**

   OR

   Q. Explain Twisted -pair cable, Coaxial cable and Fiber Optics cable.
3. **What is Transmission Media? Explain Unguided media.**

   OR

   Q. Explain Radio waves, Micro waves and Infrared.
4. **What is Transmission Media? Explain Switched Networks.**

   OR

   Q. Explain Circuit & Packet Switching
5. **Explain OSI Reference Model with Diagram. (Brief Description of Each Layer).**
6. **Explain TCP/IP Reference Model with Diagram. (Brief Description of Each Layer).**
7. **What is Delay? Explain types of Delays.**
8. **Write a short note on Botnet.**
9. **Explain Different types of Networking Connecting Devices (Repeater, Hub, Switch, Bridge, Router and Gateways).**
10. **Difference Between:**
    a. **Simplex, Half Duplex, and Full Duplex (Transmission modes)**
    b. **LAN, MAN and WAN**
    c. **Circuit & Packet Switching (Explain Switched Networks)**
    d. **OSI and TCP/IP**

Unit - 2 Application Layer

11. **Draw Structure of Email. Explain Working of E-mail.**
12. **Write a short note on SMTP.**
13. **Explain MIME Header.**
14. **Draw and explain Working Diagram of MIME Protocol.**
15. **Write a short note following protocols:**
    a. **POP3 and IMAP.**
    b. **FTP and CMIP.**
    c. **SNMP and HTTP.**
16. **Explain Request Message and Response Message Format of HTTP.**
17. **What is DNS? List and explain types of DNS.**
18. **Write a short note: WWW and TFTP.**
19. **What is HTTP? Explain Types of HTTP Connections.**
20. **Write a short note: Socket Programming**
21. **Difference Between:**
    a. **FTP and TFTP**
    b. **Persistent and Non-Persistent Connections.**
    c. **POP3 and IMAP.**

Unit - 3 Transport Layer

22. **Write a short note: Transport Layer.**
23. **Explain Multiplexing and Demultiplexing.**
24. **Draw and explain UDP Header format.**
25. **Explain Stop and Wait Protocol.**
26. **Explain Sliding Window Protocols.**
27. **Explain Stop and Wait ARQ (Automatic Repeat Request).**
28. **Explain Go-Back-N ARQ**
29. **Explain Selective Reject ARQ.**
30. **Draw and explain TCP Header format.**
31. **Explain TCP Connection (A 3-way handshake).**
32. **Explain TCP Termination (A 4-way handshake).**
33. **What is Congestion Control? Explain Types of Congestion control algorithms.**

    OR

    Q. Explain Leaky Bucket Algorithm.
    Q. Explain Token bucket Algorithm.
34. **Write a short note: Piggybacking.**
35. **Write a short note: Proxy Server.**
36. **Difference Between:**
    a. **Stop and Wait Protocol and Sliding Window Protocols.**
    b. **GO-BACK-N and Selective Reject / Selective Repeat ARQ**
    c. **Stop and Wait, Go-Back-N and Selective Repeat**
    d. **Leaky Bucket and Token Bucket**
    e. **Flow Control and Congestion Control**

Unit - 4 Network Layer

37. **Explain Functions of Network Layer.**
38. **Explain Network Layer Design Issues.**
39. **What is Packet Forwarding? Explain Packet Forwarding Techniques.**
40. **What is Routing? Explain Types of Routing.**
41. **Write a short note: Network Service Models.**
42. **Draw and explain Router Architecture.**
43. **List out Network Layer Protocols. Explain ARP and RARP.**

OR

Q. Explain Physical addresses and Logical addresses.

44. **Write a short note: ICMP and IGMP.**
45. **Draw and explain IPv4 Datagram Header.**
46. **Draw and explain IPv6 Datagram Header.**
47. **Explain Classification of IP Addresses (Classful Addressing).**
48. **Explain Classless Addressing (CIDR).**
49. **Explain Classify Binary and Hexadecimal Representation of IPv6 address.**
50. **Explain Convert the given IPv4 address to IPv6 address.**
51. **Write a short note on Network Transmission Types.**
52. **Write a short note: NAT (Network Address Translation).**
53. **Explain Routing protocols: Distance vector routing, Link state routing and Path vector Routing.**

OR

Q. Explain Distance vector routing (Bellman ford) Algorithm with Example.

Q. Explain Link state routing (Dijsktra) Algorithm with Example.

Q. Explain Path vector Routing Algorithm with Example.

54.Difference between:

a. **Virtual Circuit and Datagram Networks**
b. **IPv4 and IPv6**
c. **Classful Addressing and Classless Addressing**
d. **Distance Vector Routing and Link State Routing**
e. **Broadcast and Multicast**

Unit - 5 The Link layer and Local Area Networks

55. Explain Functions of Data Link Layer and List out Services of Data Link Layer.
56. What is Error Detection? Explain Types of Errors.

OR

Q. Explain Single-Bit Error and Burst Error.

57. What is Error Detection? Explain Error Detecting Techniques.

OR

Q. Explain Single parity check and Two-dimensional parity check.

Q. Explain Checksum and Cyclic redundancy check.

58. Write a short note: Hamming Code.
59. Write a short note: High-Level Data Link Control (HDLC).

OR

Q. Draw and Explain HDLC frame format.

60. Explain HDLC frames types.
61. Write a short note: Multiple Access Protocols.

OR

Q. What is Aloha Protocol? Explain Types of Aloha Protocols.

Q. Explain Channelization Protocols (FDMA, TDMA and CDMA).

Q. Write a short note: CSMA (Carrier Sense Multiple Access).

Q. Write a short note: CSMA/CD and CSMA/CA.

62. Explain Ethernet (IEEE standards 802.3).
63. Explain Token bus (IEEE standards 802.4) and Token ring (IEEE standards 802.5)
64. Write a short note: FDDI and DQDB (IEEE standards 802.6).
65. Write a short note: VLAN (Virtual Local Area Network).

66. Explain Different types of Networking Connecting Devices (Repeater, Hub, Switch, Bridge, Router and Gateways).

67. Difference Between:

a. **Pure ALOHA and Slotted ALOHA**
b. **FDMA, TDMA, and CDMA**
c. **Token Bus and the Token Ring**

New L J Institute of Engineering and Technology

Subject: Computer Networks
Subject Code: 3150710
Branch: CSE
Semester: V

- **Faculty Name:**
  - **Assistant Professor: Bhaumik Gelani**

- **Teaching and Examination Scheme:**

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE (E)	PA (M)	ESE (V)	PA (I)	
4	0	2	5	70	30	30	20	150

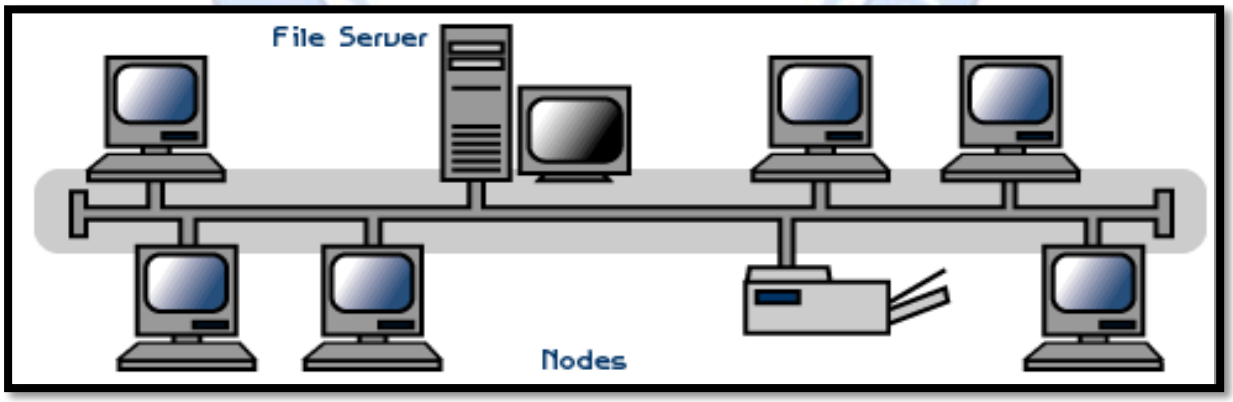
Unit No.	Unit Title	% Weightage
1	Introduction to computer networks and Internet	15
2	Application Layer	17
3	Transport Layer	25
4	Network Layer	25
5	The Link layer and Local Area Networks	18

Unit – 1 Introduction to computer networks and Internet

1. What is Topology? List out and explain various network topology.

Ans:

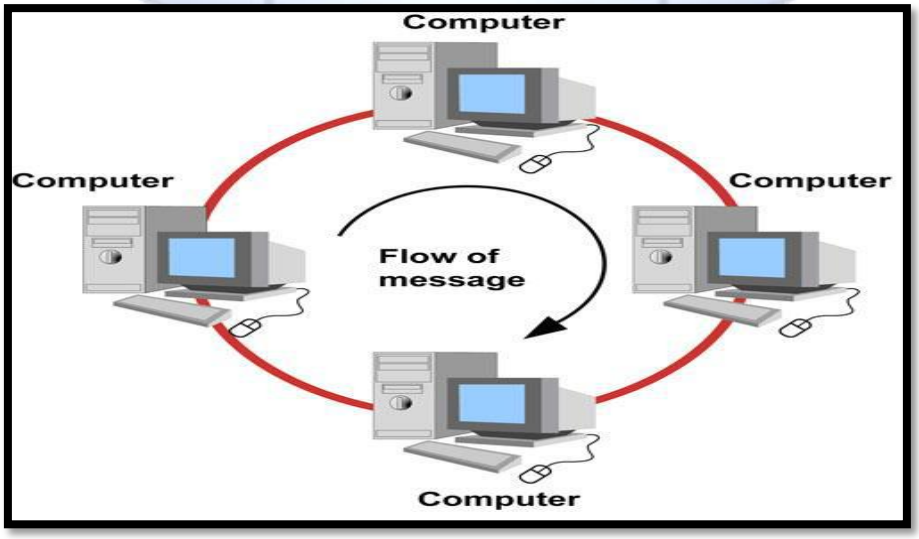
- **Topology:**
  - Topology described the **actual layout of network transmission media**.
  - Network topology is the arrangement of the various components (Links, Nodes, Printer etc.) of a computer network.
- **Types Network Topology:**
  - Bus Topology
  - Ring Topology
  - Tree Topology
  - Star Topology
  - Mesh Topology
  - Hybrid Topology
- **Bus Topology:**
  - The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
  - Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.



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

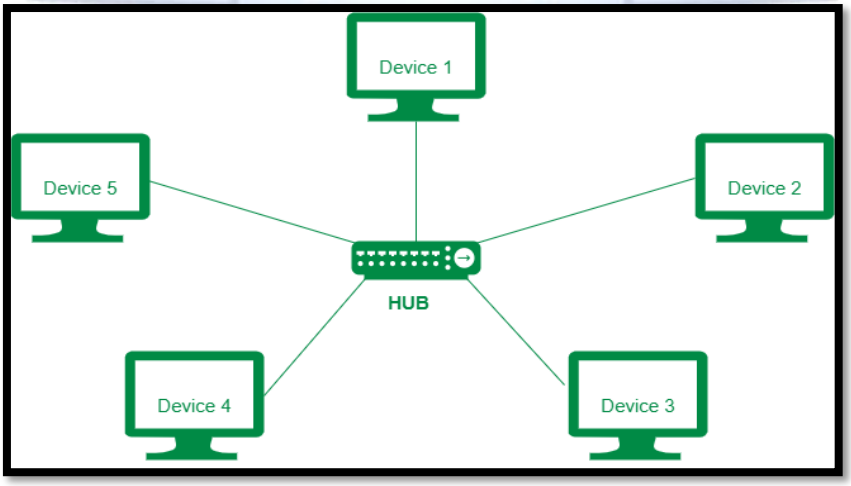
- **Advantages of Bus topology:**
  - **Low-cost cable:**
    - In bus topology, nodes are directly connected to the cable without passing through a hub.
  - **Moderate data speeds:**
    - Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
  - **Limited failure:**
    - 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.

- **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.



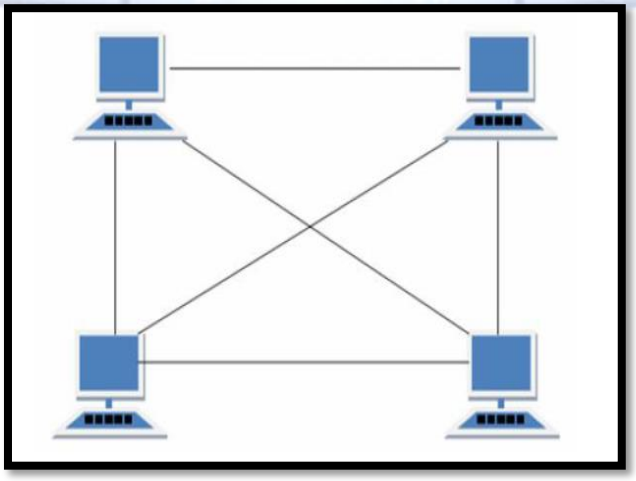
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token 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.
  - **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.

- **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.**



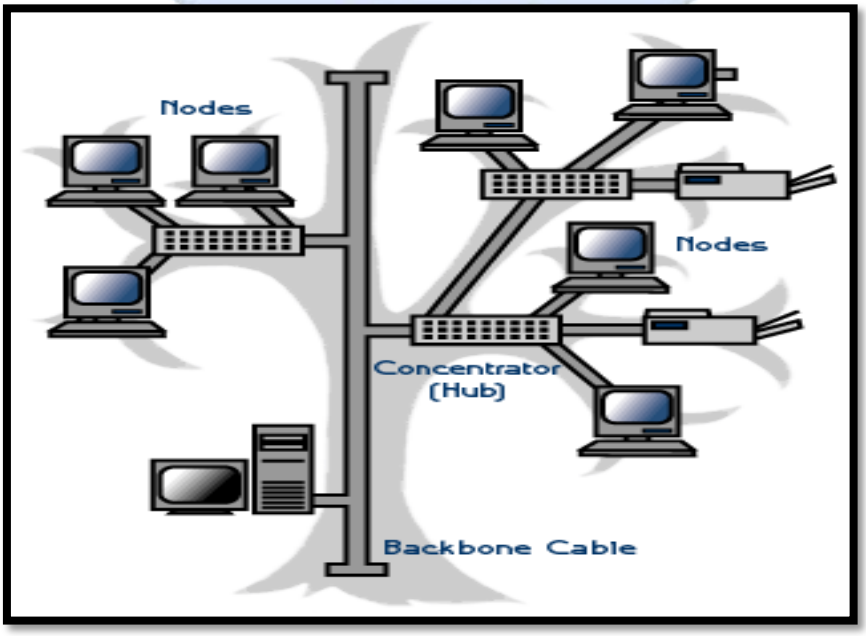
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology.**
- Star topology is the most popular topology in network implementation.
- **Advantages of Star topology:**
  - **Network control:**
    - Complex network control features can be easily implemented in the 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.
  - **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 of Star topology:**
  - **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.

- **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.



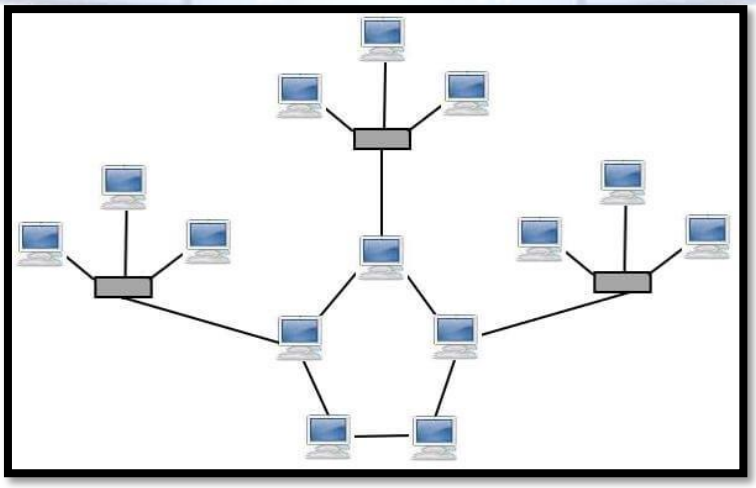
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for 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.

- **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:**
  - **Easily expandable:**
    - We can add the new device to the existing network.
    - Therefore, we can say that tree topology is easily expandable.
  - **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.

- **Hybrid Topology:**



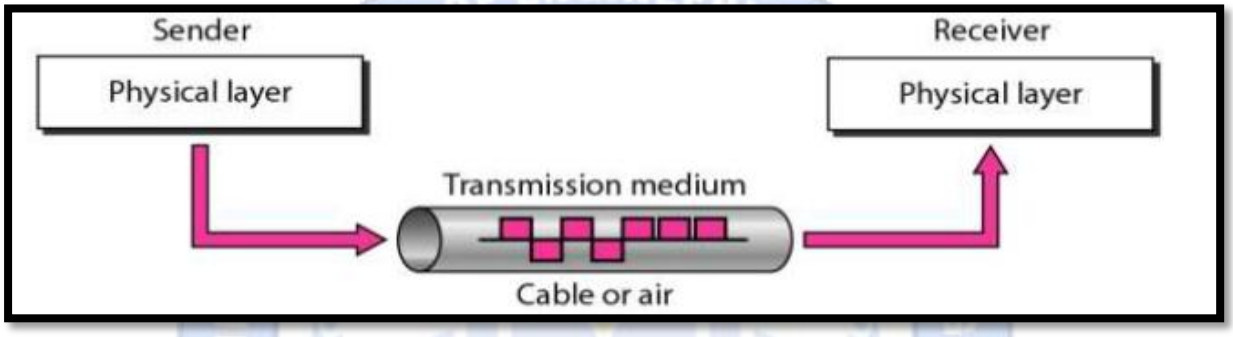
- A hybrid topology is a kind of network topology that is a combination of two or more network topologies, such as mesh topology, bus topology, and ring topology.
- Its usage and choice are dependent on its deployments and requirements like the performance of the desired network, and the number of computers, their location.
- However, a variety of technologies are needed for its physical implementation, and it offers a complex structure.
- Also, it includes an advantage as increasing flexibility; it can increase fault tolerance, and allows new basic topologies to be added or removed easily.
- The hybrid topology is more useful when you need to fulfill diversity in Computer Network.
- In this topology, all network sections can include the configuration of different Network Topology.

2. What is Transmission Media? Explain Wired media.

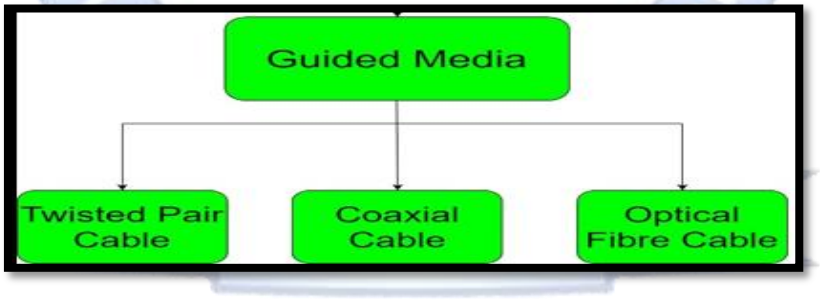
OR

Q. Explain Twisted -pair cable, Coaxial cable and Fiber Optics cable.

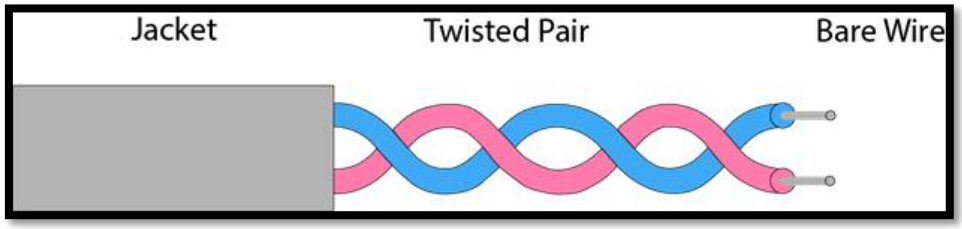
- **Transmission Media:**
  - Transmission media is a communication channel that carries the information from the sender to the receiver.
  - Data is transmitted through the electromagnetic signals.



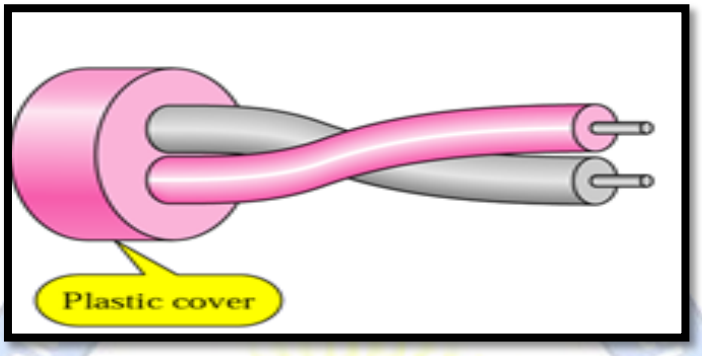
- **Guided media (Wired media):**
  - Guided media, the waves are guided along a solid medium.
  - Guided media are those that provide a wired-channel from one device to another.
  - Three Guided media commonly used for data transmission are:



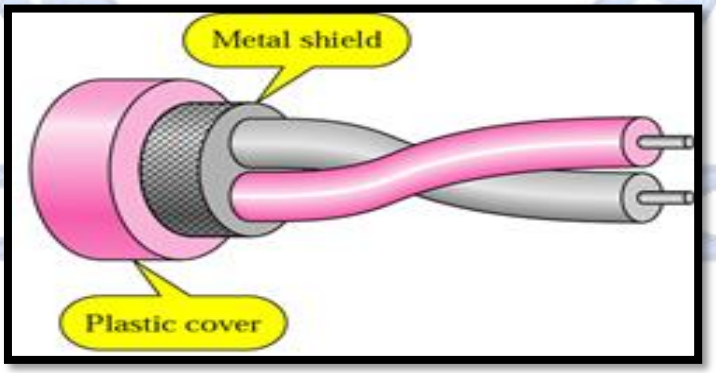
- **Twisted Pair Cable:**
  - Twisted pair is a physical media made up of a pair of cables twisted with each other.
  - A twisted pair cable is cheap as compared to other transmission media.
  - Installation of the twisted pair cable is easy, and it is a lightweight cable.
  - The frequency range for twisted pair cable is from 0 to 3.5KHz.



- **Types of Twisted pair:**
  - Unshielded Twisted Pair (UTP)
  - Shielded Twisted Pair (STP)
- **Unshielded Twisted Pair (UTP):**

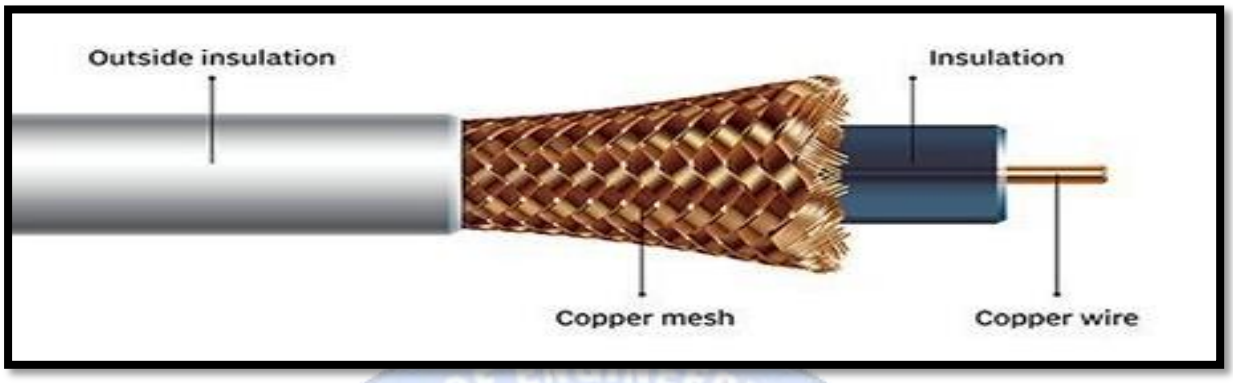


  - An unshielded twisted pair is widely used in telecommunication.
  - Ordinary telephone wired.
  - Less expensive.
  - Weak immunity against noise & interferences.
  - Most used in two categories: Cat-3 & Cat-5.
- **Shielded Twisted Pair (STP):**



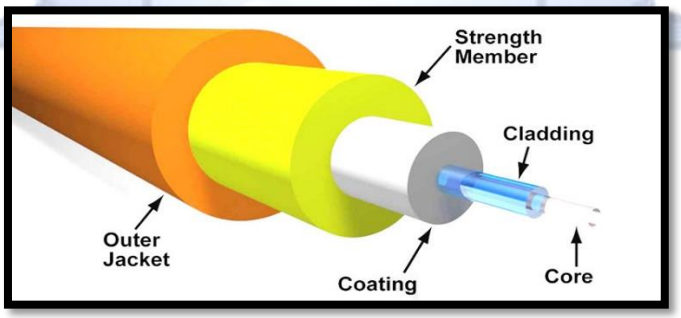
  - A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.
  - An extra metallic shield on each pair.
  - Relatively more expensive.
  - Better performance than UTP.

- **Coaxial Cable:**

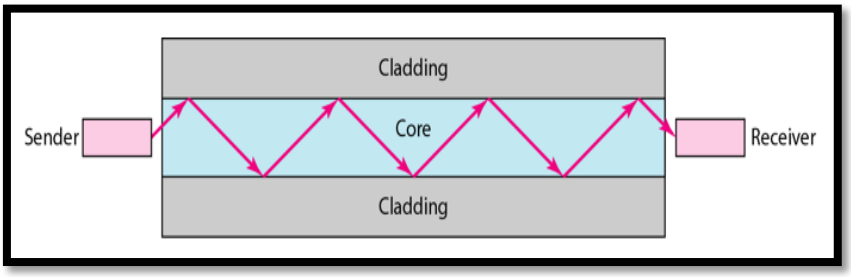


  - Coaxial cable is very commonly used transmission media.
  - Outer conductor is braided shield.
  - Inner conductor is solid metal.
  - Separated by insulating material.
  - Used in television, long distance telephone transmission.
  - High bandwidth and excellent noise immunity.
  - **Advantages Of Coaxial cable:**
    - The data can be transmitted at high speed.
    - It has better shielding as compared to twisted pair cable.
    - It provides higher bandwidth.
  - **Disadvantages Of Coaxial cable:**
    - It is more expensive as compared to twisted pair cable.
    - If any fault occurs in the cable causes the failure in the entire network.

- **Fiber-optic cable:**



  - Fibre optic cable is a cable that uses electrical signals for communication.
  - Fibre optic is a cable that holds the optical fibers coated in plastic that are used to send the data by pulses of light.
  - Fibre optics provide faster data transmission than copper wires.



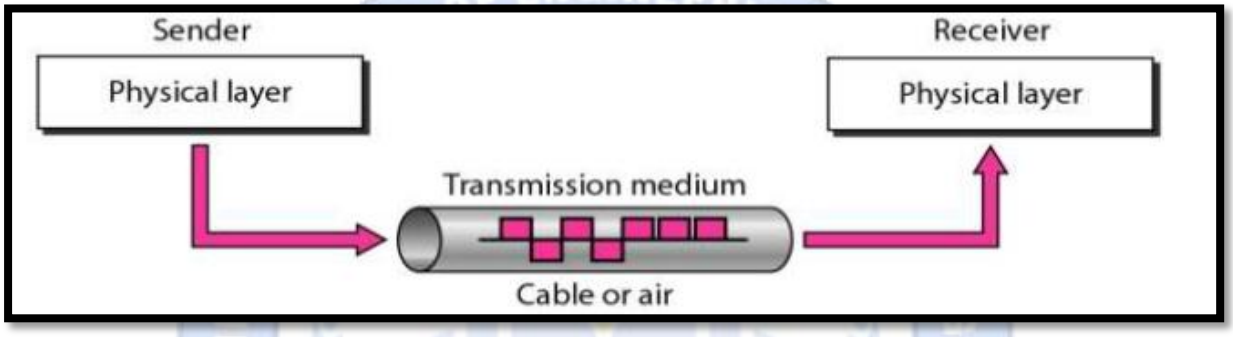
- **Advantages of Fibre Optic Cable:**
  - Faster speed
  - Used Longer distances
  - Increased capacity and bandwidth
  - Lightweight
  - Immunity to electromagnetic interference.
- **Disadvantages of Fibre Optic Cable:**
  - Difficult to install and maintain
  - High cost

3. What is Transmission Media? Explain Unguided media.

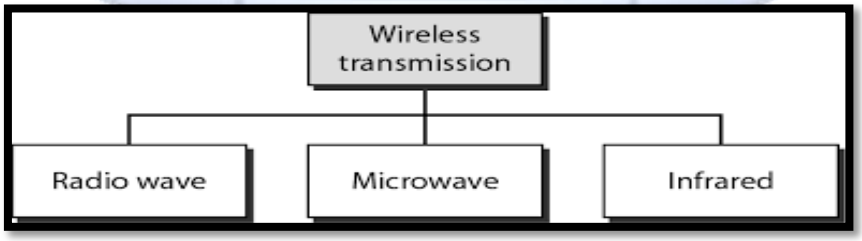
OR

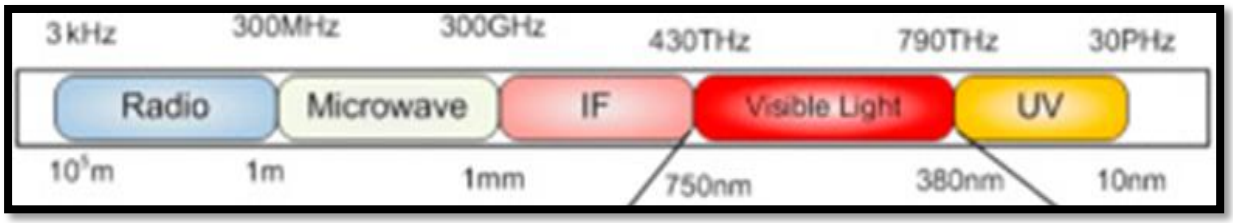
Q. Explain Radio waves, Micro waves and Infrared.

- **Transmission Media:**
  - Transmission media is a communication channel that carries the information from the sender to the receiver.
  - Data is transmitted through the electromagnetic signals.

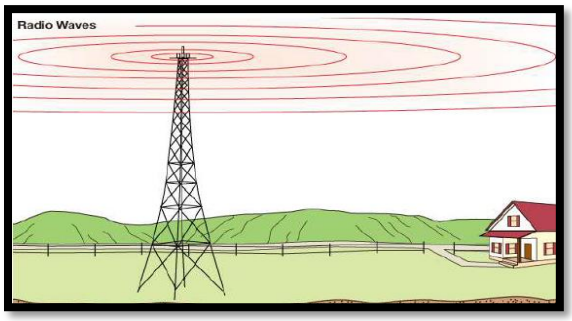


- **Unguided media (wireless):**
  - Unguided media, the waves propagate in the atmosphere and in outer space.
  - Unguided media transmit electromagnetic waves without using a physical conductor, This type of communication is often referred to as wireless communication.
    - Radio wave
    - Micro wave
    - Infrared Wave



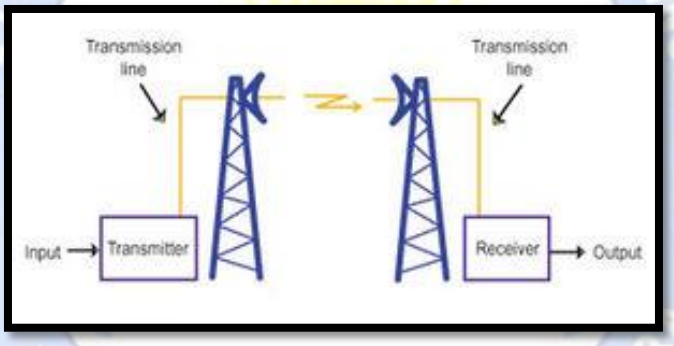


- **Radio wave:**



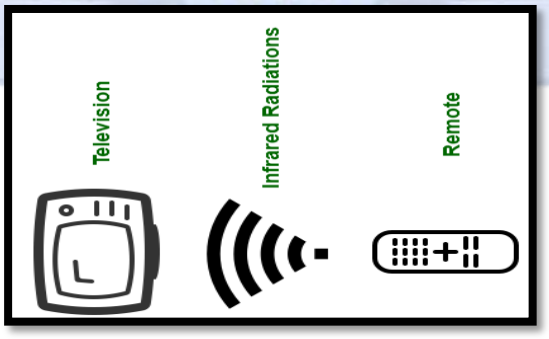
  - Highly regulated
  - Omnidirectional antennas
  - Radio waves are used for multicast communications, such as radio and television, and paging systems
  - Penetrate through walls

- **Micro Wave:**



  - Use directional antennas-point to point line of sight communications
  - Used for unicast communication such as cellular telephones, satellite networks
  - Higher frequency ranges can not efficiently penetrate walls

- **Infrared Wave:**



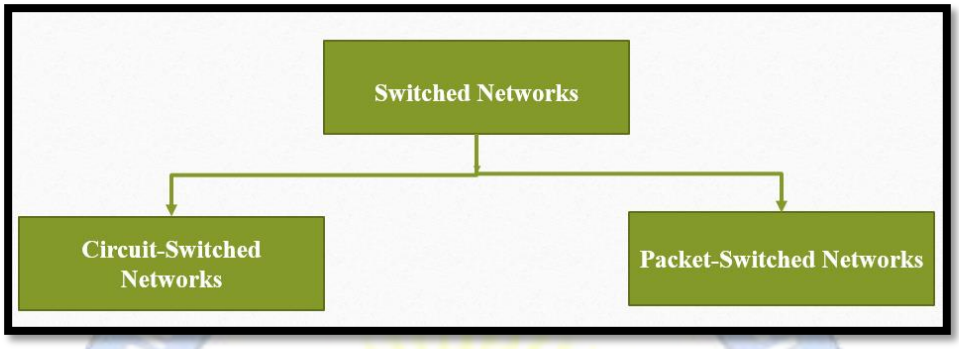
  - Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation
  - Used on Televisions, DVDs, and stereos all use infrared communication.
  - Cheap, Easy to build but they do not pass through solid objects
  - Relatively directional

4. Explain Switched Networks.

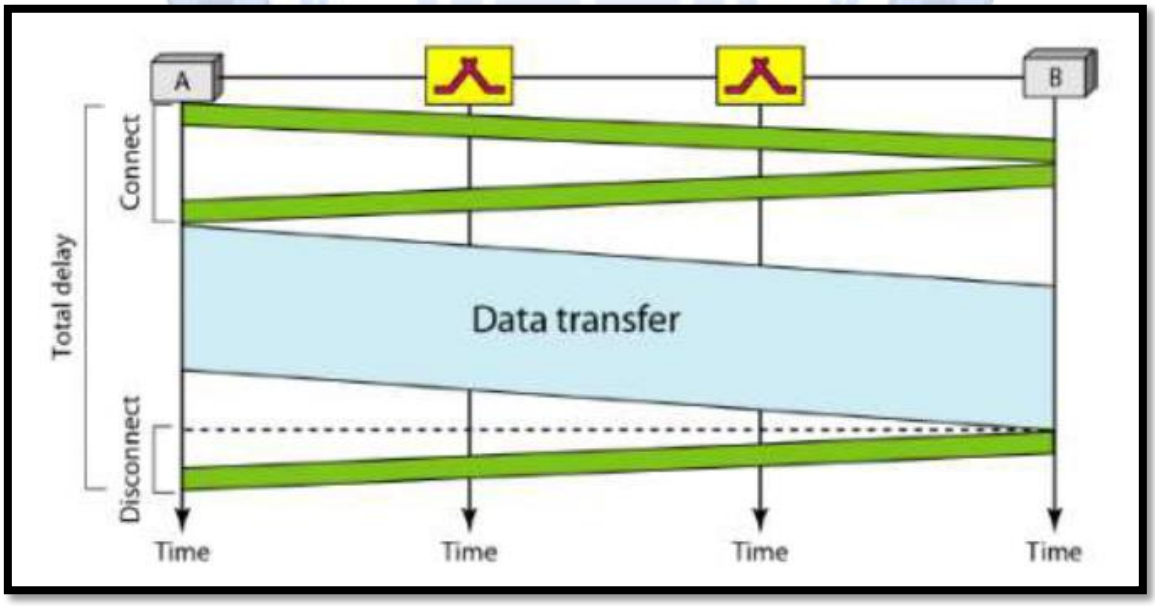
OR

Q. Explain Circuit & Packet Switching .

Ans:

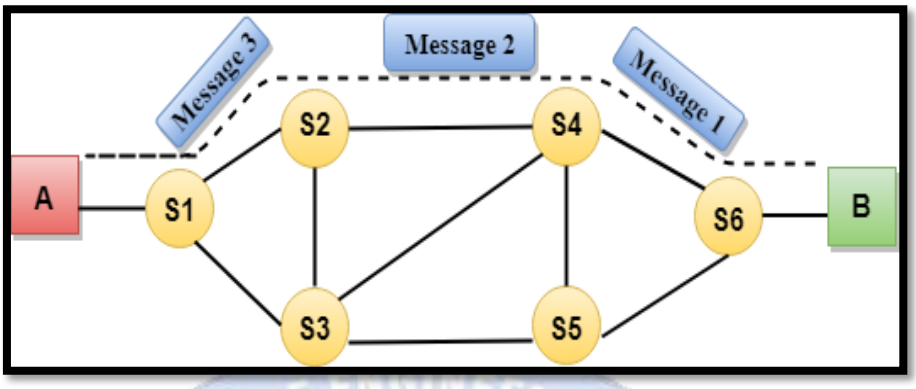


- **Circuit switching:**
  - **Communication via circuit switching involves three phases:**
    - Circuit Establishment
    - Data Transfer
    - Circuit Disconnect



  - Network resources (e.g., bandwidth) divided into "pieces"
    - Pieces allocated to calls
    - Resource piece *idle* if not used by owning call *(no sharing)*
    - Dividing link bandwidth into "pieces"
      - Frequency division
      - Time division

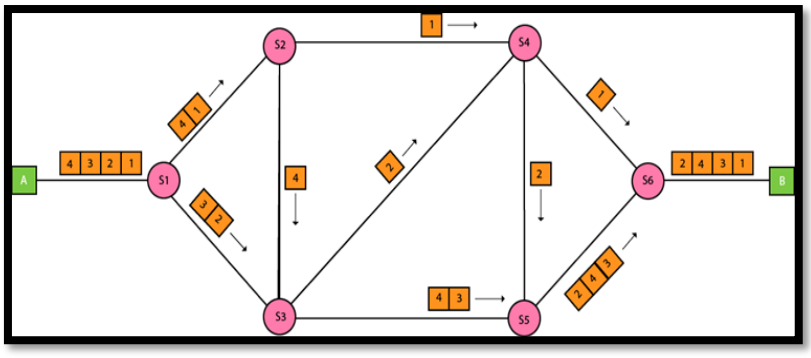
- **Circuit-Switched Networks:**



- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path.
- After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

• Packet Switching Network:

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- **Packet Switching:**

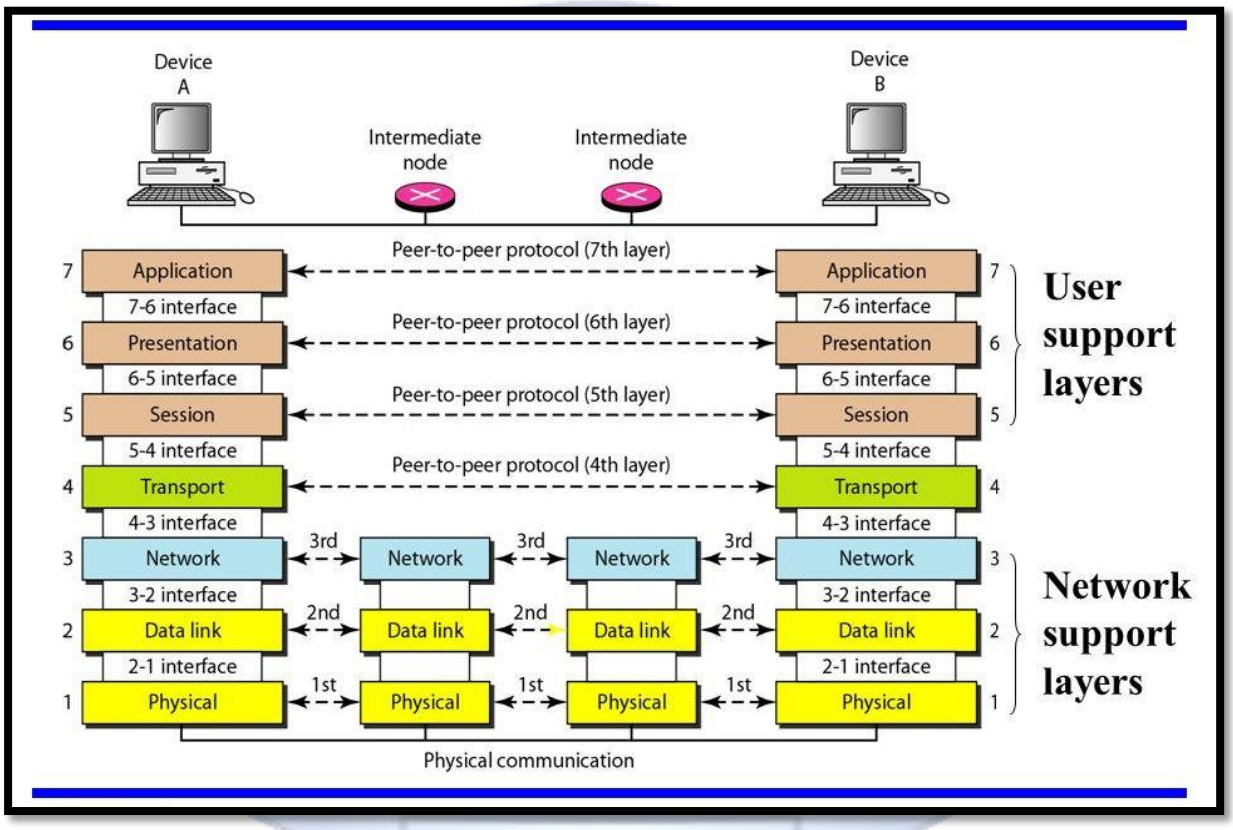


- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.
- **There are two approaches to Packet Switching:**
  - Datagram Packet switching
  - Virtual Circuit Switching
- **Datagram Packet switching:**
  - It is a packet switching technology in which packet is known as a datagram.
  - Datagram Packet Switching is also known as connectionless switching.
  - The packets are reassembled at the receiving end in correct order.
  - In Datagram Packet Switching technique, the path is not fixed.
  - Intermediate nodes take the routing decisions to forward the packets.
- **Virtual Circuit Switching:**
  - Virtual Circuit Switching is also known as connection-oriented switching.
  - In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
  - Call request and call accept packets are used to establish the connection between sender and receiver.
  - In this case, the path is fixed for the duration of a logical connection.

5. Explain OSI Reference Model with Diagram. (Brief Description of Each Layer).

Ans:

- **OSI** stands for **Open System Interconnect.**
- A system that implements open protocols is called an ***open system***
- A set of protocols is *open* if protocol details are publicly available.
- **OSI Reference Model:**



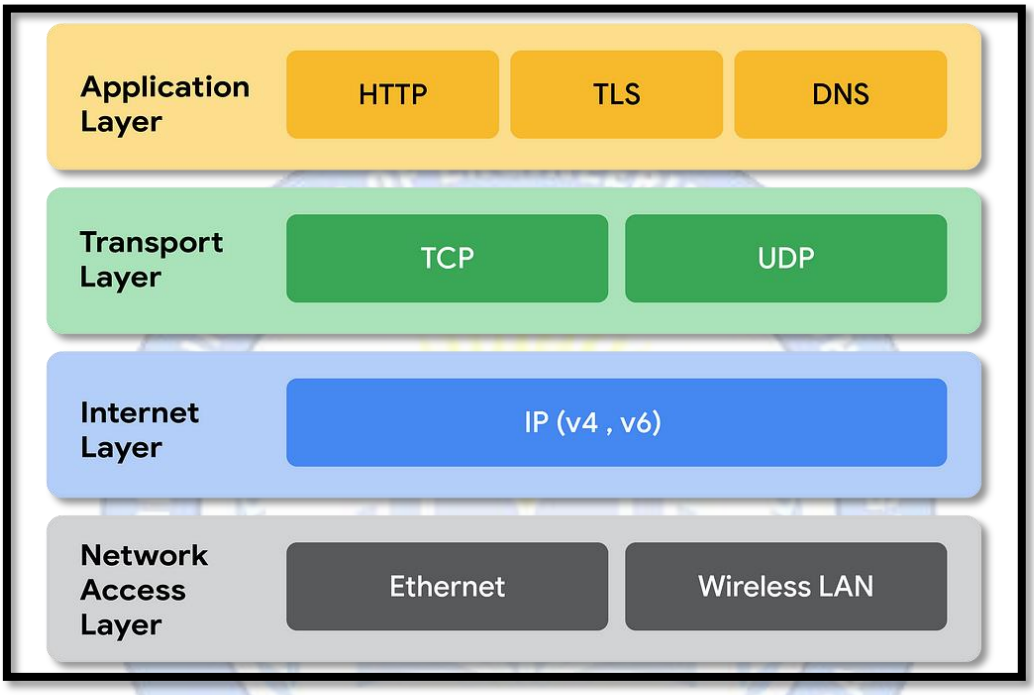
- **Physical layer**
  - The physical layer is responsible for movements of individual **bits** from one hop (node) to the next.
- **Data link layer**
  - The data link layer is responsible for moving frames from one hop (node) to the next.
  - Groups of bits its called **Frame.**
- **Network layer**
  - The network layer is responsible for the delivery of individual packets from the source host to the destination host.
  - Groups of Frame its called **Packets.**

- **Transport layer**
  - The transport layer is responsible for the delivery of a message from one process to another.
- **Session layer**
  - The session layer is responsible for dialog control and synchronization.
- **Presentation layer**
  - The presentation layer is responsible for translation, compression, and encryption.
  - Data translation ,compression and encryption.
  - Encrypt data to hide it.
  - Compress data from last message to small no of messages.
- **Application layer**
  - The application layer is responsible for providing services to the user.
  - Login password checking, file transfer are some of the application.
  - Provide direct access to network device.
  - Interface between user and system.
  - **Examples:** File transfer, Emails, www

6. Explain TCP/IP Reference Model with Diagram. (Brief Description of Each Layer).

Ans:

- **TCP/IP Reference Model:**



- **Physical layer**
  - The physical layer is responsible for movements of individual **bits** from one hop (node) to the next.
- **Data link layer**
  - The data link layer is responsible for moving frames from one hop (node) to the next.
  - Groups of bits its called **Frame.**
- **Network layer**
  - The network layer is responsible for the delivery of individual packets from the source host to the destination host.
  - Groups of Frame its called Packets.
  - **Network layer protocols :** IP, ICMP, ARP and RARP.
    - **IP (Internetwork Protocol):**
      - IP is transmission mechanism used. It is connectionless and unreliable protocol. packets in the IP layer called **datagram.**
    - **ICMP (Internet Control Message Protocol):**
      - ICMP used to handle, control and error message in the **IP** layer.

- **ARP (Address Resolution Protocol):**
  - ARP is used to find the **physical address** of the node when the **IP addres**s is known

- **RARP (Reverse Address Resolution Protocol):**
  - RARP is used to find the **IP Address** of the node when its physical address is known**.**

- **Transport layer:**
  - The transport layer is responsible for the delivery of a message from one process to another.
  - **Transport layer protocols** : TCP and UDP
  - Both Protocols Use Port to Port Communication
  - **TCP (Transmission Control Protocol) :**
    - TCP provides full transport layer to applications.
    - It is **Connection oriented** protocol .
    - The packet in this layer is called **segment**.
    - **TCP provides** error control, flow control, multiplexing.
  - **UDP (User Datagram Protocol) :**
    - UDP is **Connectionless** protocol.
    - The packet produces by UDP is called User Datagram.
    - UDP provides **only multiplexing**
- **Application layer**
  - The application layer is responsible for providing services to the user.
  - Login password checking, file transfer are some of the application.
  - Interface between user and system.
    - **Examples:** File transfer, Emails, www
  - **Application layer protocols:** SMTP, FTP, SNMP and TELNET
    - **SMTP (Simple Mail Transfer Protocol) :**
      - SMTP supports E-mail on the internet. SMTP is use Mailing.
    - **FTP (File Transfer protocol):**
      - FTP is provided for copy file form one computer to another computer.
      - To copy file some problem must occurs to solved by FTP
    - **SNMP (Simple Network Management Protocol) :**
      - SNMP provides a set of fundamental operations for monitoring and maintaining devices in internet.
    - **TELNET (Terminal Network) :**
      - TELNET is a general purpose Client – Server application program, TELNET is use Remote access login .

7. What is Delay? Explain types of Delays.

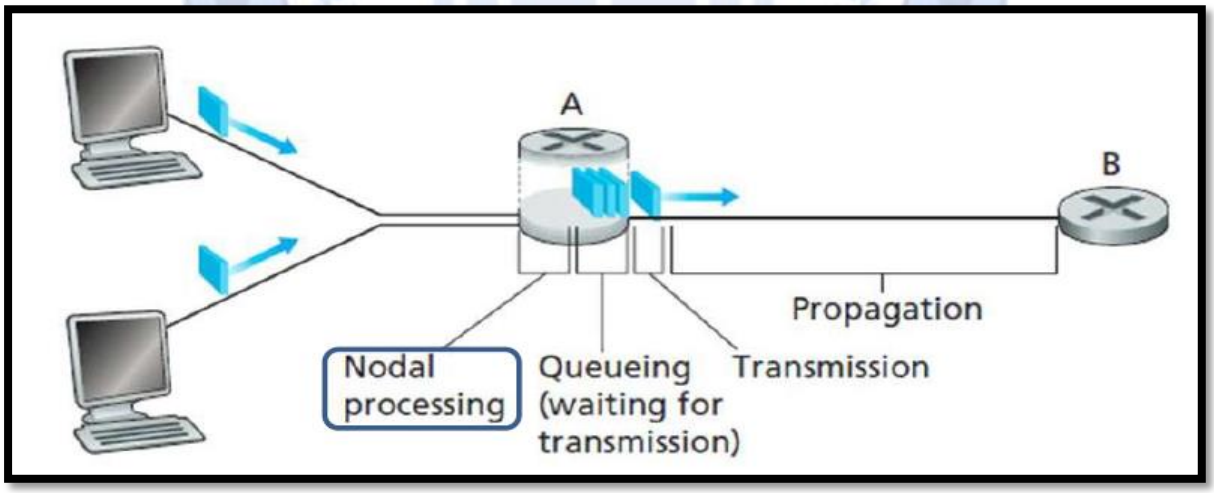
- **Delay:**
  - As a packet travels from one node (host or router) to the sub sequent node (host or router) along this path, the packet suffers from several types of delays at each node along the path.

$$d_{nodal} = d_{proc} + d_{queue} + d_{tran} + d_{prop}$$

Where

d_{nodal}	=	Total Delay
d_{proc}	=	Processing Delay
d_{queue}	=	Queuing Delay
d_{tran}	=	Transmission Delay
d_{prop}	=	Propagation Delay

- **Types of Delays:**



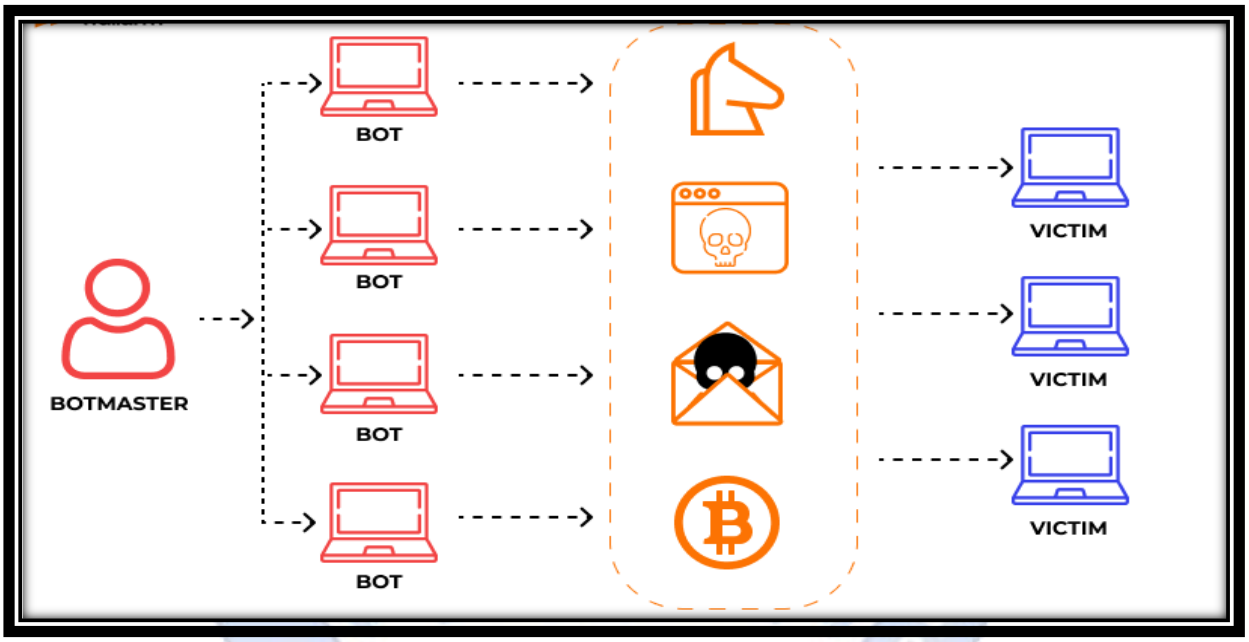
- **Processing Delay**
  - The time required to examine the packet sheared and determine where to direct the packet.
  - To check bit level error.
  - Determine output link.
  - Delay in terms of microseconds.

- **Queuing Delay**
  - A time to waits at output link for transmission.
  - Depends on congestion level of router.
  - If queue empty then delay will be zero.
  - If queue full–heavy traffic then delay will be long.
  - Delay in terms of microsecond to millisecond.
- **Transmission Delay**
  - An amount of time required for the router to transmit the packet.
  - Its depends on packet length(L) and transmission rate(R) of link.
- **Propagation Delay**
  - A time required to propagate from the beginning of the link to router B.
  - Depends on the length of physical medium(d) link and propagation speed(s) of link.
  - Delay in terms of millisecond.

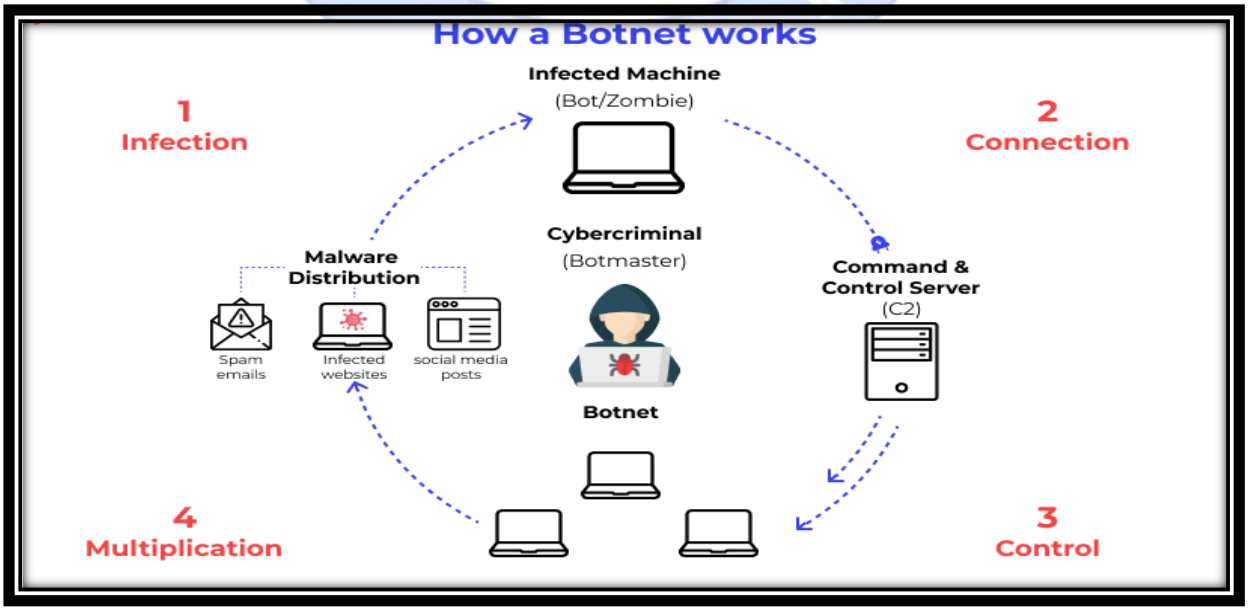
8. Write a short note on Botnet.

Ans:

- **Botnet:**
  - Botnet refers to a **network of hijacked internet-connected devices** that are **installed with malicious codes** known as **malware.**
  - Each of these **infected devices** is known as **Bots**, and a hacker/cybercriminal known as the "Bot herder" remotely controls them.
  - A **bot** is also called a **zombie**, and a **botnet** is referred to as a **zombie army.**



- **Working:**

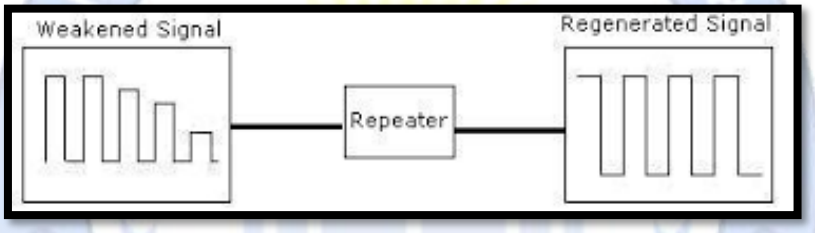


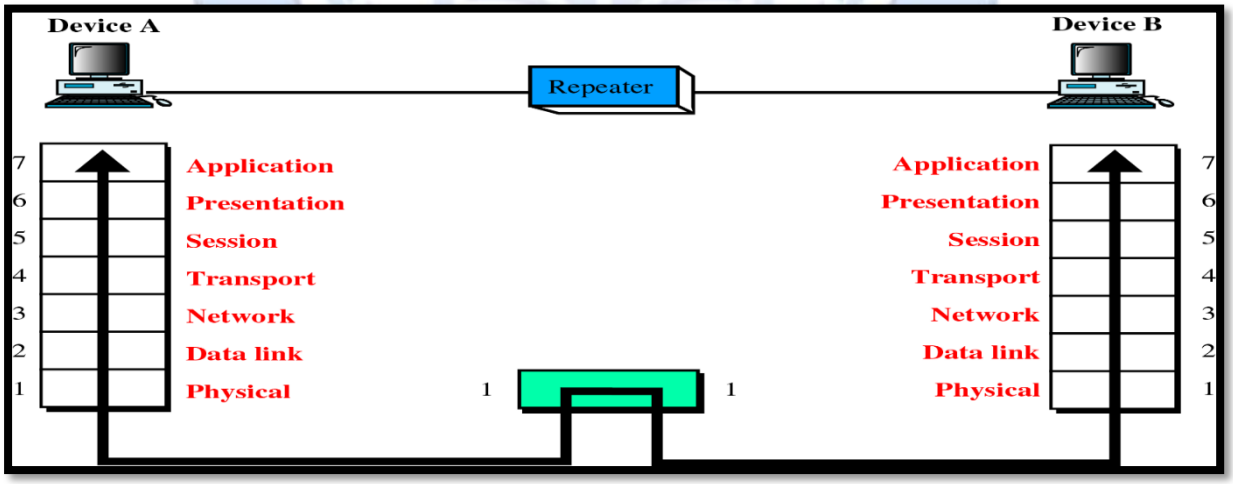
- **Stage 1 - Prepare and Expose**
  - At this stage, the bad actor figures out the vulnerability to introduce into the user's device.
  - The vulnerability hunting takes place in the website, human behavior, and application. By doing so, the hacker prepares a set-up to lure the target to get exposed to malware, knowingly or unknowingly.
  - Most commonly, hackers figure out the vulnerabilities in websites and the software.
  - Additionally, malware is delivered via emails or random messages.
- **Stage 2 - Infecting the user via malware**
  - The next action that the botnet performs is activating the malware so that the end-user is infected and has compromised security.
  - The process of infecting the device usually takes place via the Trojan virus or social engineering method.
  - Some attackers adopt a more hostile approach and deploy drive-by-download techniques to infect the device.
  - Using all these methods, attackers corrupt the targeted device with botnet malware.
- **Stage 3 - Controlling the targeted devices**
  - The last stage of botnet working methodology is gaining control over each device.
  - Hackers systematize the involved infected machines in the botnet and design a methodology to manage them remotely.
  - In general, around thousands of devices are controlled in the process via a huge zombie network.
  - Once the stage is successfully completed, the bad actor is able to gain admin-like access to the targeted devices or computers.

9. Explain Different types of Networking Connecting Devices (Repeater, Hub, Switch, Bridge, Router and Gateways).

Ans:

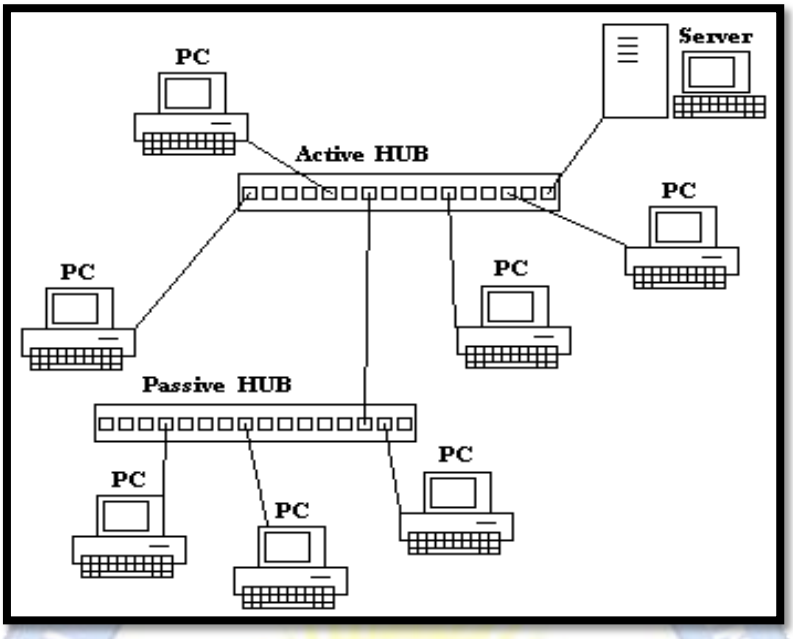
- Different types of Networking Connecting Devices are:
  1. Repeater
  2. Hub
  3. Switch
  4. Bridge
  5. Router
  6. Gateways
- **Repeater**:



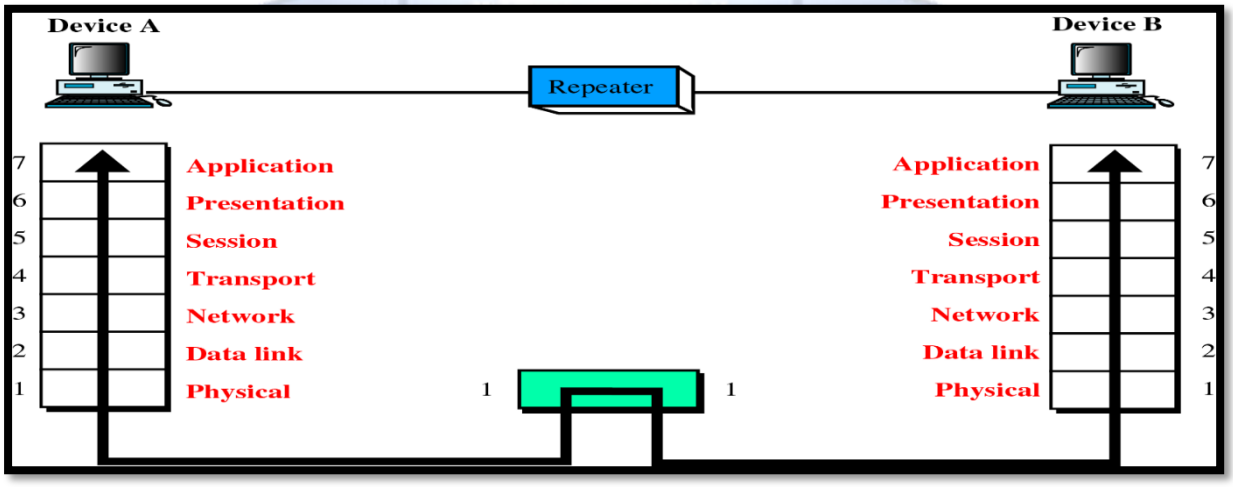


- A repeater operates at the physical layer.
- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
- An important point to be noted about repeaters is that they do not amplify the signal.
- When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.
- It is a 2-port device.

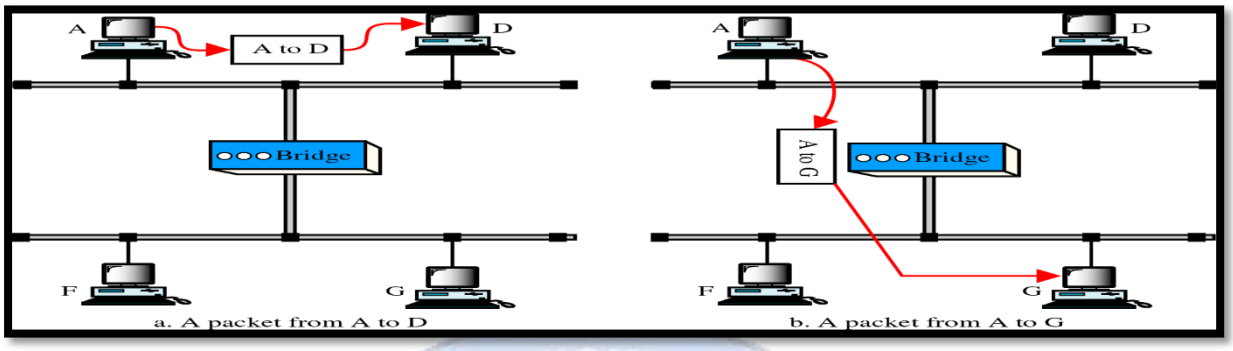
- **Hub:**

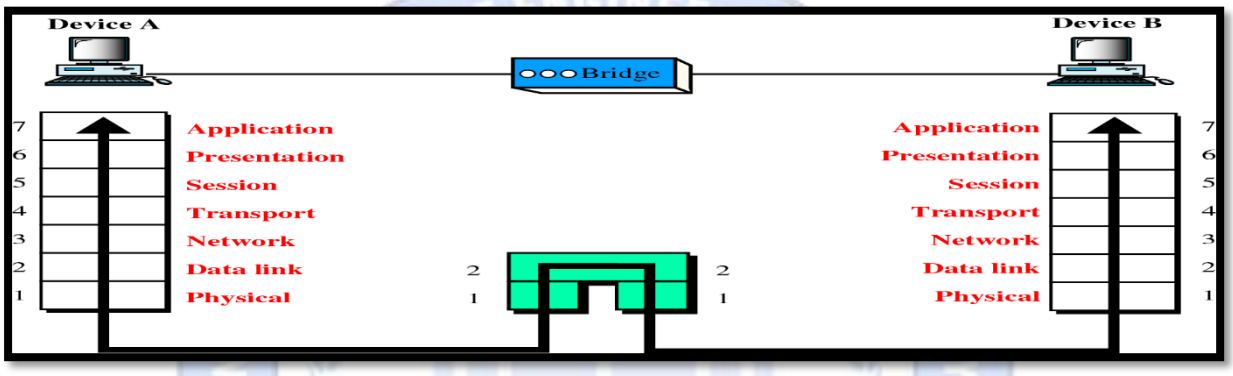


  - A hub is basically a multiport repeater.
  - A hub **works at** the **physical layer (layer 1)** of the OSI model.
  - A hub connects multiple wires coming from different branches.
  - **Types of Hub**
    - **Active Hub :-**
      - These are the hubs which have their own power supply and can clean , boost and relay the signal along the network.
      - These are used to extend maximum distance between nodes.
    - **Passive Hub :-**
      - These are the hubs which collect wiring from nodes and power supply from active hub.

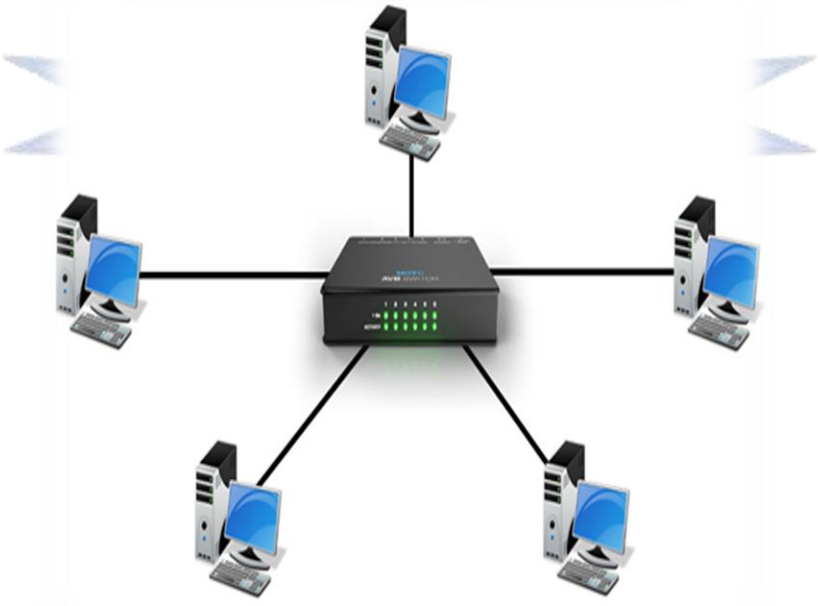


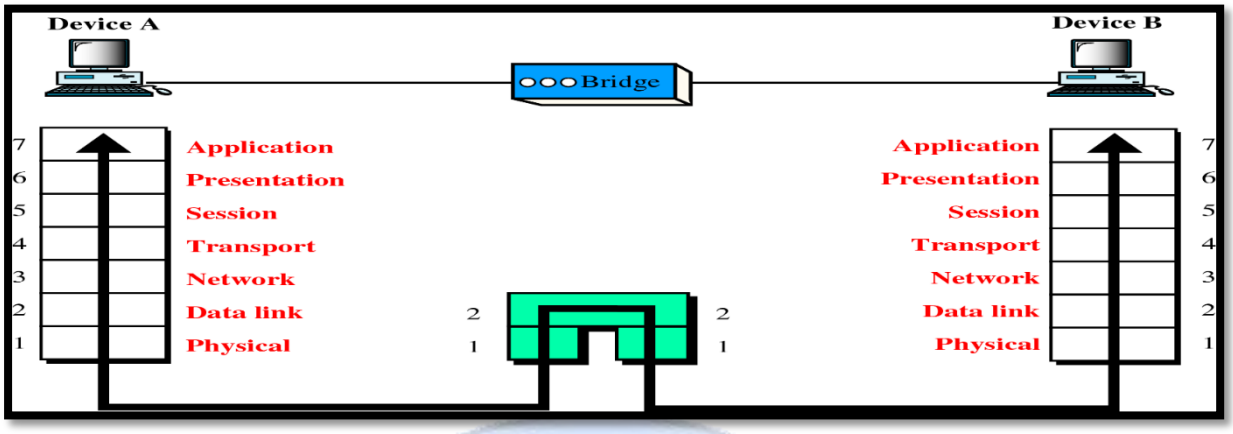
- **Bridge:**





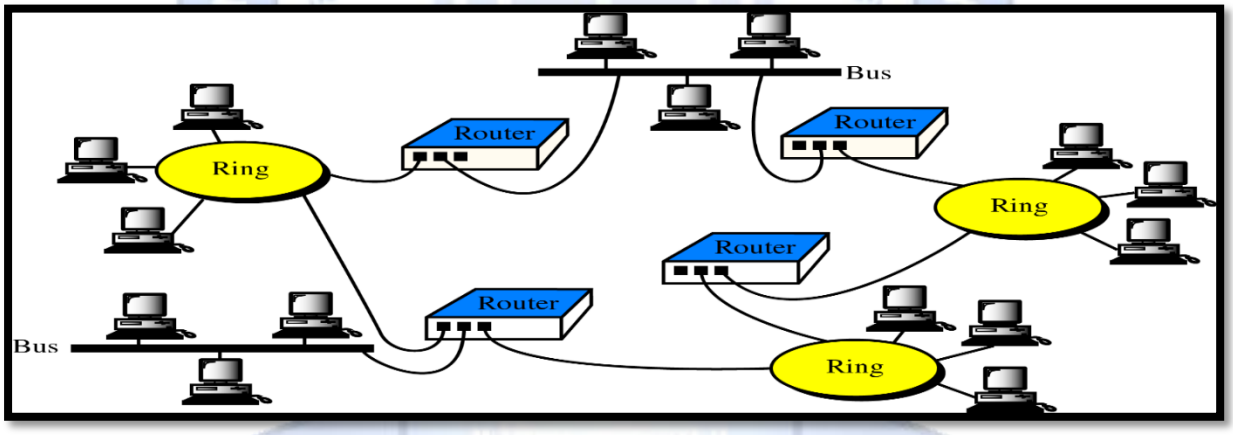
  - A bridge operates at **data link layer**.
  - A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination.
  - It is also used for interconnecting two LANs working on the same protocol.
  - It has a single input and single output port, thus making it a **2-port device**.
- **Switch**:

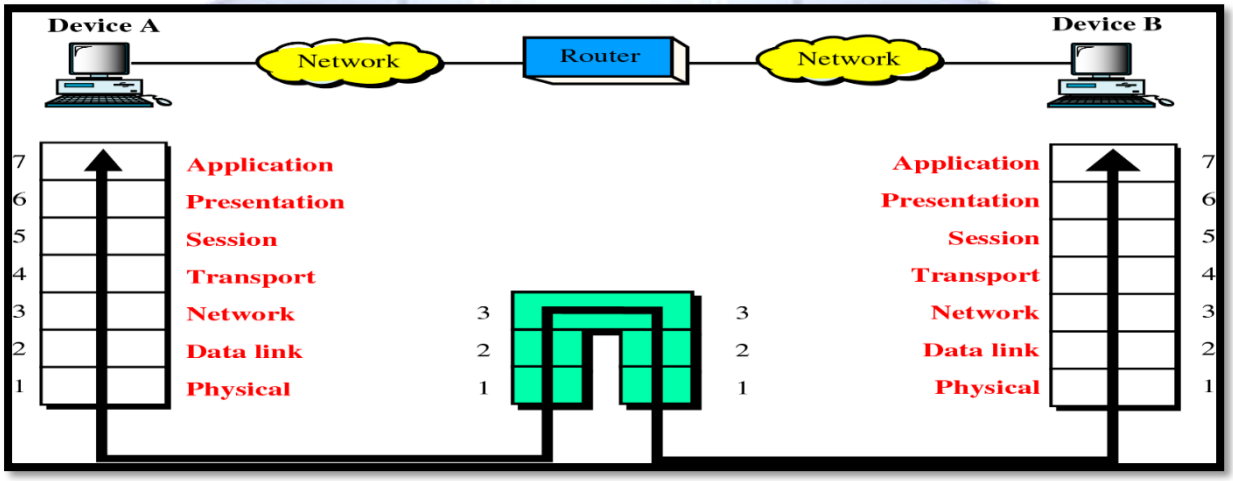




- Switch is **data link** layer device.
- A switch is a multi-port bridge with a buffer and a design that can boost its efficiency (large number of ports imply less traffic) and performance.
- Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.
- In other words, switch divides collision domain of hosts, but broadcast domain remains same.

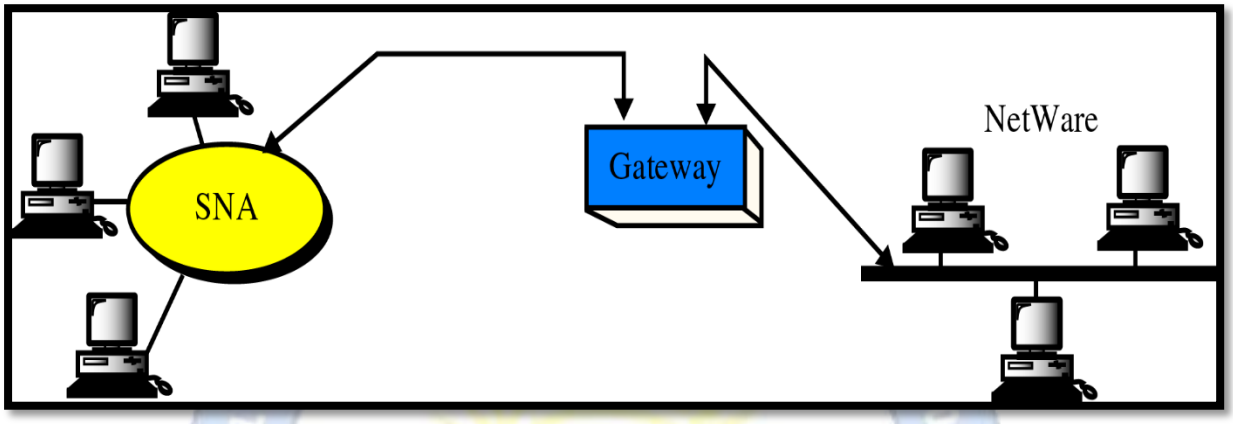
- **Routers:**

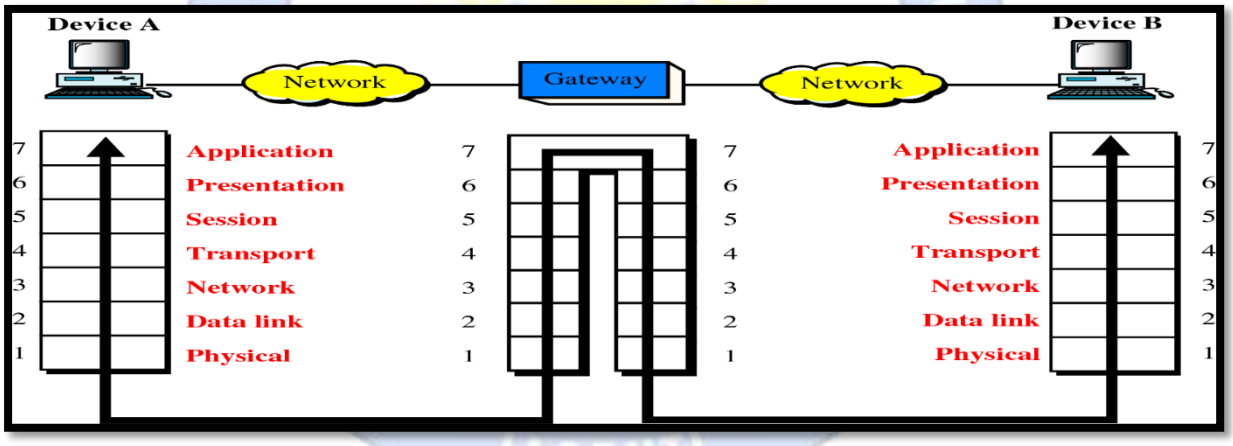




- Router is mainly a Network Layer device.
- A router is a device like a switch that routes data packets based on their IP addresses.
- Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.
- Router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

- **Gateway:**





- Gateway is mainly used All seven Layer in OSI Model.
- A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models.
- They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

10.Difference Between:

a. Simplex, Half Duplex, and Full Duplex (Transmission modes)

Basis for Comparison	Simplex	Half Duplex	Full Duplex
Direction of Communication	Unidirectional	Two-directional, one at a time	Two-directional, simultaneously
Send / Receive	Sender can only send data	Sender can send and receive data, but one a time	Sender can send and receive data simultaneously
Performance	Worst performing mode of transmission	Better than Simplex	Best performing mode of transmission
Example	Keyboard and monitor	Walkie-talkie	Telephone

b. LAN, MAN and WAN

BASIS OF COMPARISON	LAN	MAN	WAN
Stands form	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.
Ownership of Network	Private	Private or Public	Private or Public
Design and maintenance	Easy	Difficult	Difficult
Cost	Low	High	Higher
Network Size	Small	Larger	Largest
Speed	Fastest	Slower	Slowest
Range	1 to 10 km	10 to 100 km	Beyond 100 km

c. Circuit & Packet Switching (Explain Switched Networks)

BASIS FOR COMPARISON	CIRCUIT SWITCHING	PACKET SWITCHING
Orientation	Connection oriented.	Connectionless.
Purpose	Initially designed for Voice communication.	Initially designed for Data Transmission.
Flexibility	Inflexible, because once a path is set all parts of a transmission follows the same path.	Flexible, because a route is created for each packet to travel to the destination.
Order	Message is received in the order, sent from the source.	Packets of a message are received out of order and assembled at the destination.
Technology /Approach	Circuit switching can be achieved using two technologies, either **Space Division Switching or Time-Division Switching.**	Packet Switching has two approaches **Datagram Approach and Virtual Circuit Approach**.
Layers	Circuit Switching is implemented at **Physical Layer.**	Packet Switching is implemented at **Network Layer.**

d. OSI and TCP/IP

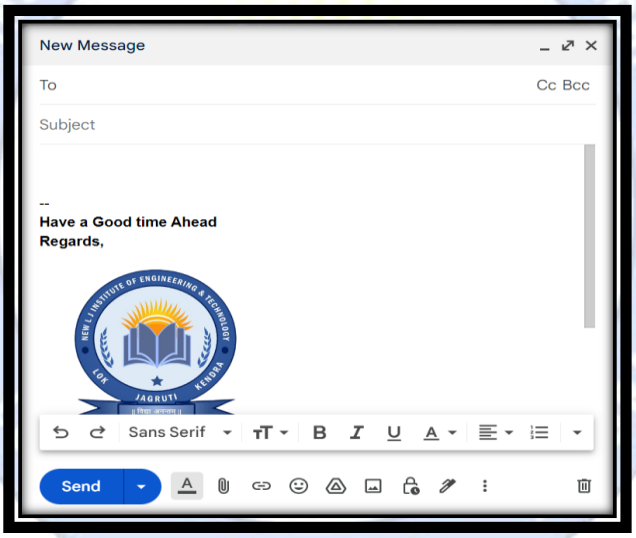
BASIS FOR COMPARISON	OSI Model	TCP/IP Model
Stands For	Open System Interconnection	Transmission Control Protocol / Internet Protocol
Approach	Vertical Approach.	Horizontal Approach.
Presentation Layer and Session Layer	Presents	absents
Transport Layer	Connection Oriented.	Connection Oriented and Connection less.
Network Layer	Connection Oriented and Connection less.	Connection less.
Protocol	Independent.	Dependent.
Number Of Layers	7 layers	5 layers

Unit - 2 Application Layer

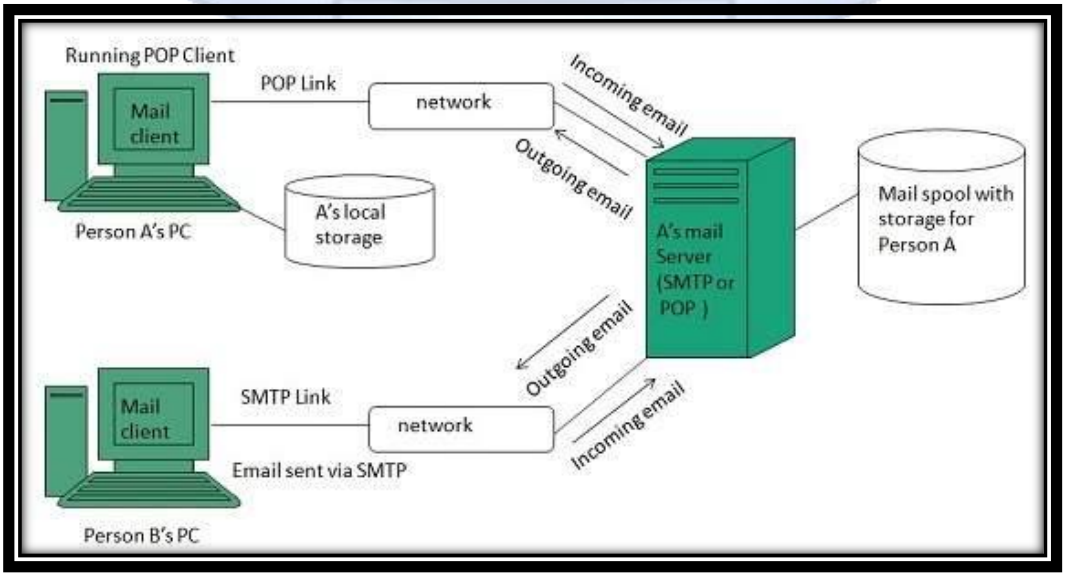
11. Draw Structure of Email. Explain Working of E-mail.

Ans:

- **Structure of Email:**
  - Electronic mail is often referred to as E-mail and it is a method used for **exchanging digital messages**.
  - Electronic mail is mainly designed for **human use**.
  - It allows a message to includes **text, image, audio** as well as **video**.
  - This service allows one message to be **sent to one or more than one recipient**.



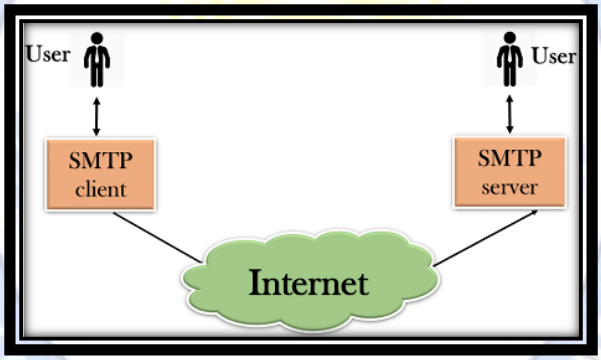
- **Working of E-mail:**



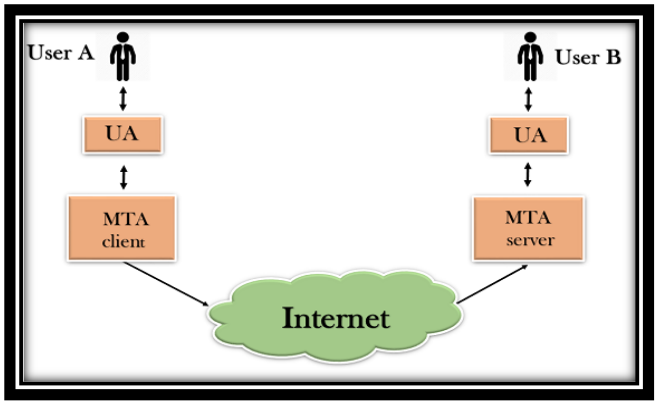
- Email working follows the client server approach. In this client is the mailer i.e. the mail application or mail program and server is a device that manages emails.
- Following example will take you through the basic steps involved in sending and receiving emails and will give you a better understanding of working of email system:
  - Suppose person A wants to send an email message to person B.
  - Person A composes the messages using a mailer program i.e. mail client and then select Send option.
  - The message is routed to **Simple Mail Transfer Protocol** to person B's mail server.
  - The mail server stores the email message on disk in an area designated for person B.
  - Now, suppose person B is running a POP client and knows how to communicate with B's mail server.
  - It will periodically poll the POP server to check if any new email has arrived for B.As in this case, person B has sent an email for person B, so email is forwarded over the network to B's PC. This is message is now stored on person B's PC.

12. Write a short note on SMTP.

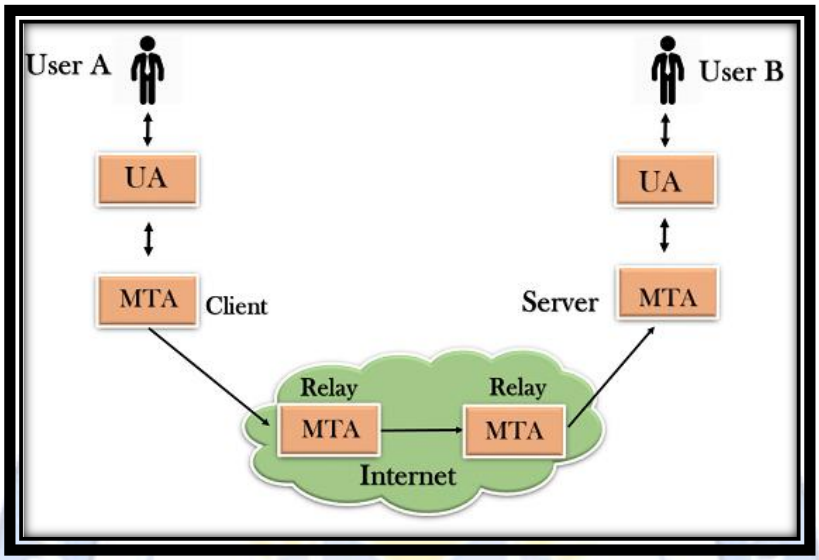
- **SMTP:**
  - SMTP stands for **Simple Mail Transfer Protocol.**
  - SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.
  - It is a program used for sending messages to other computer users based on e-mail addresses.
  - It provides a mail exchange between users on the same or different computers, and it also supports:
    - It can send a single message to one or more recipients.
    - Sending message can include text, voice, video or graphics.
    - It can also send the messages on networks outside the internet.
  - The **main purpose** of SMTP is used to **set up communication rules between servers.**



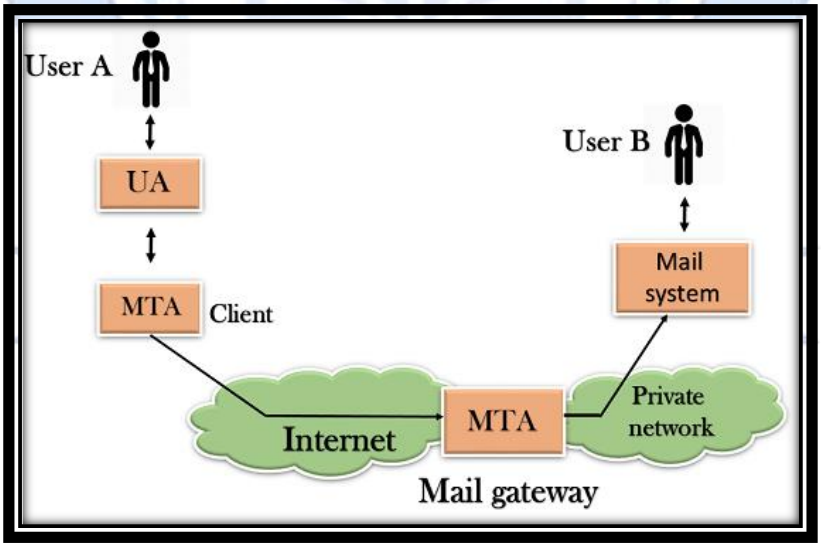
  - **Components of SMTP:**
    - First, we will break the **SMTP client** and **SMTP server** into two components such as **user agent (UA)** and **mail transfer agent (MTA).**
    - The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.



- SMTP allows a more complex system by adding a relaying system.
- Instead of just having one MTA at sending side and one at receiving side, more MTAs can be added, acting either as a client or server to relay the email.



- The relaying system without TCP/IP protocol can also be used to send the emails to users, and this is achieved by the use of the mail gateway.
- The mail gateway is a relay MTA that can be used to receive an email.

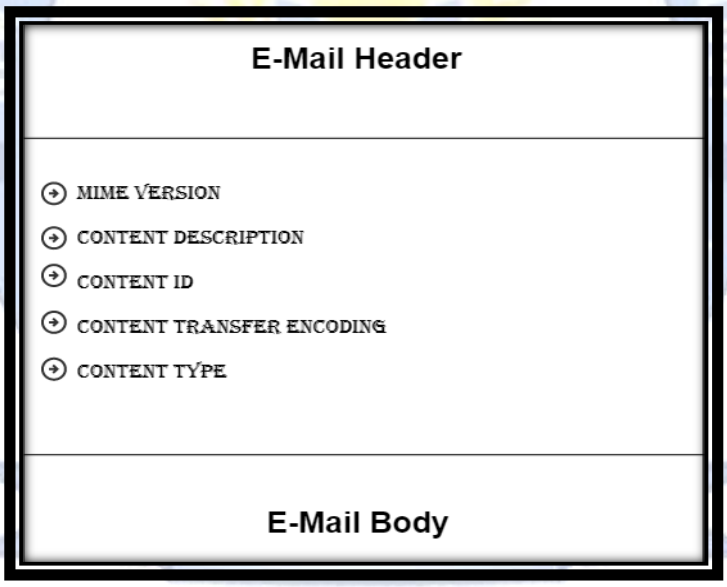


13. Explain MIME Header.

Ans:

- MIME stands for **Multipurpose Internet Mail Extensions.**
- It is used to extend the capabilities of Internet e-mail protocols such as SMTP.
- The MIME protocol allows the users to exchange various types of digital content such as:
  - Pictures, audio, video, and various types of documents and files in the e-mail.
- MIME is an e-mail extension protocol, i.e., it does not operate independently, but it helps to extend the capabilities of e-mail in collaboration with other protocols such as SMTP.

- **MIME Header:**
  - MIME adds five additional fields to the header portion of the actual e-mail to extend the properties of the simple email protocol.



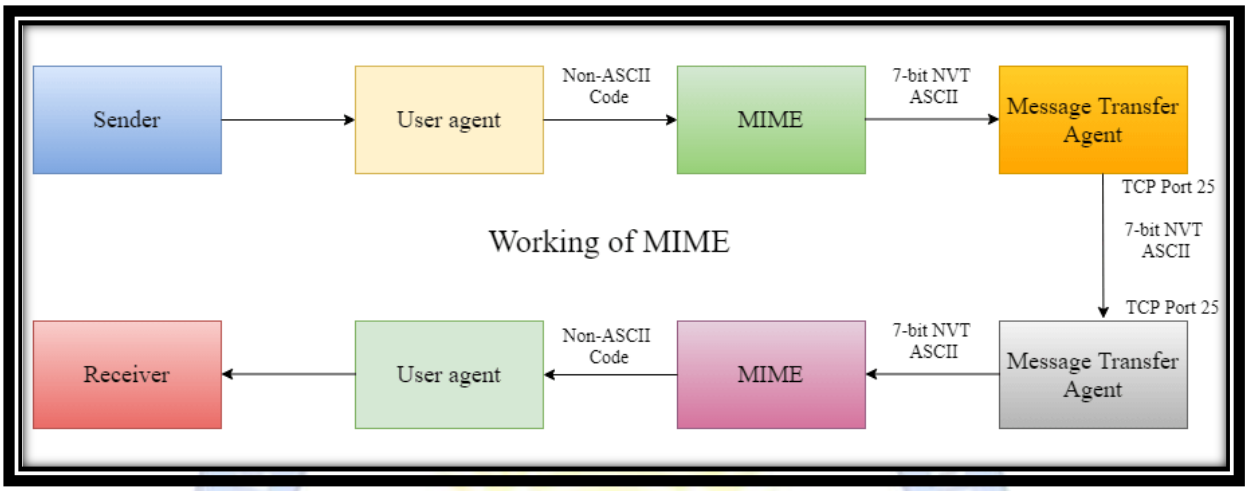
- **These fields are as follows:**
  1. MIME Version
  2. Content Type
  3. Content Type Encoding
  4. Content Id
  5. Content description
- **MIME-Version:**
  - Defines the version of the MIME protocol.
  - It must have the parameter Value 1.0, which indicates that message is formatted using MIME.

- **Content-Type:**
  - Type of data used in the body of the message.
  - They are of different types like text data (plain, HTML), audio content, or video content.
- **Content-Type Encoding:**
  - It defines the method used for encoding the message.
  - Like 7-bit encoding, 8-bit encoding, etc.
- **Content Id:**
  - It is used for uniquely identifying the message.
- **Content description:**
  - It defines whether the body is actually an image, video, or audio.

14. Draw and explain Working Diagram of MIME Protocol.

Ans:

- **Working Diagram of MIME Protocol:**



  - **MIME-Version:**
    - Defines the version of the MIME protocol.
    - It must have the parameter Value 1.0, which indicates that message is formatted using MIME.
  - **Content-Type:**
    - Type of data used in the body of the message.
    - They are of different types like text data (plain, HTML), audio content, or video content.
  - **Content-Type Encoding:**
    - It defines the method used for encoding the message.
    - Like 7-bit encoding, 8-bit encoding, etc.
  - **Content Id:**
    - It is used for uniquely identifying the message.
  - **Content description:**
    - It defines whether the body is actually an image, video, or audio.

- **Features of MIME Protocol**
  - It supports multiple attachments in a single e-mail.
  - It supports the non-ASCII characters.
  - It supports unlimited e-mail length.
  - It supports multiple languages.

15. Write a short note following protocols:

a. POP3 and IMAP.

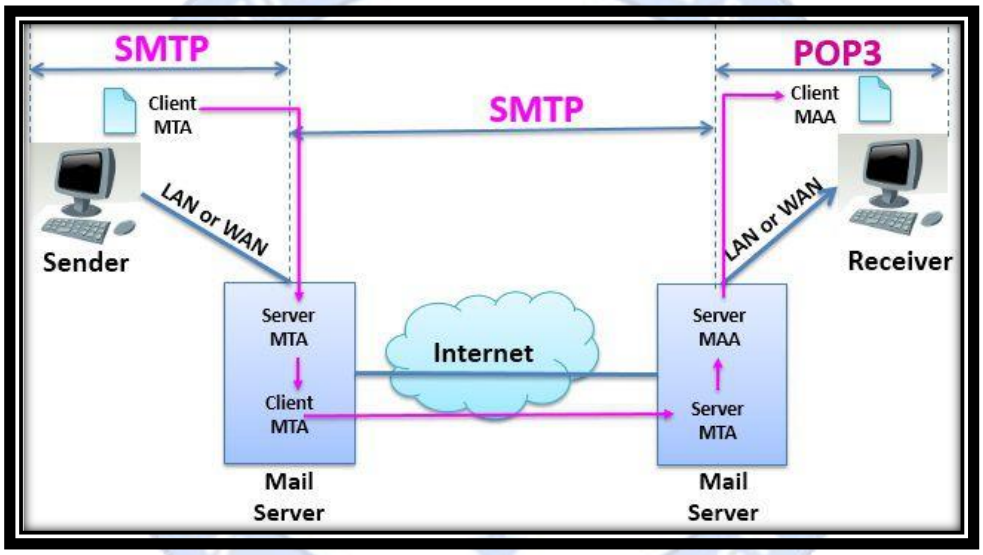
b. FTP and CMIP.

c. SNMP and HTTP.

Ans:

a. POP3 and IMAP.

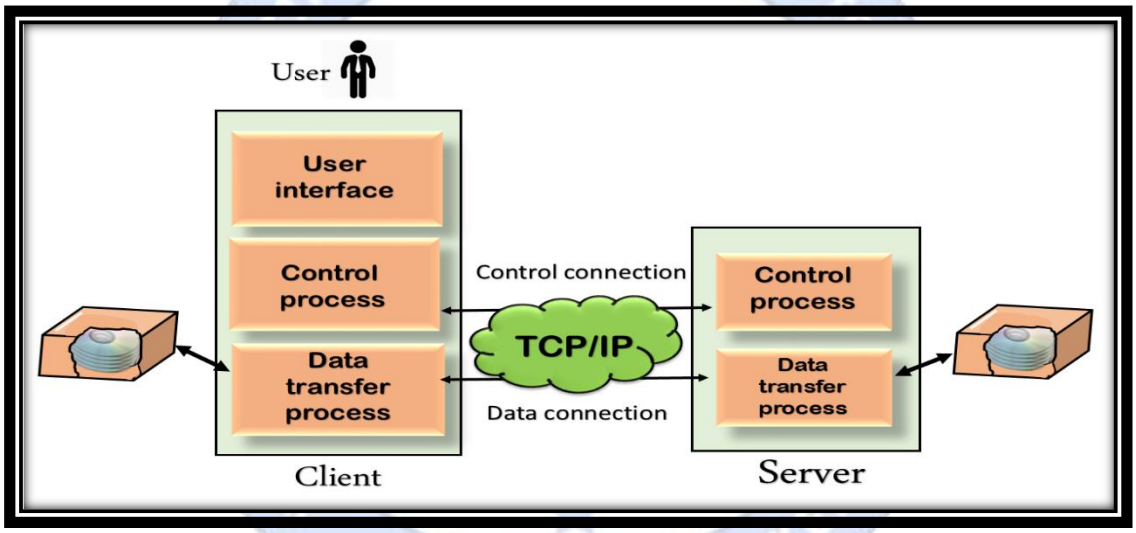
- **POP:** Post Office Protocol – Version 3
- **IMAP:** Internet Mail Access Protocol



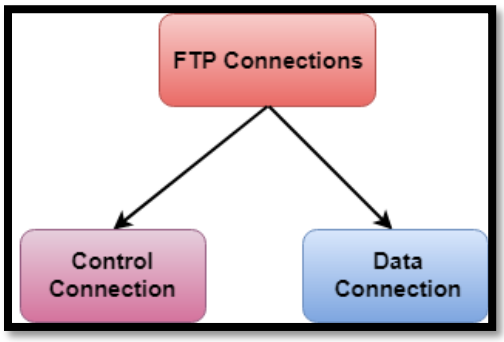
- POP3 and IMAP are the protocols that are used to retrieve mail from the mailbox at the mail server to the recipient's computer. Both are message accessing agents (MAA).
- The two protocols POP3 and IMAP are used when both the sender and recipient of mail are connected to the mail server by **WAN or LAN**.
- The SMTP protocol transfers the mail from client's computer to the mail server and from one mail server to another mail server.
- POP3 has a limited functionality whereas, the IMAP has extra features over POP3.
- IMAP follows Client-server Architecture and is the most commonly used email protocol.
- It is a combination of client and server process running on other computers that are connected through a network.
- This protocol resides over the TCP/IP protocol for communication.
- Once the communication is set up the server listens on port 143 by default which is non-encrypted.
- For the secure encrypted communication port, 993 is used.

b. FTP and CMIP.

- FTP stands for **File transfer protocol.**
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.
- **Objectives of FTP**
  - It provides the sharing of files.
  - It is used to encourage the use of remote computers.
  - It transfers the data more reliably and efficiently.



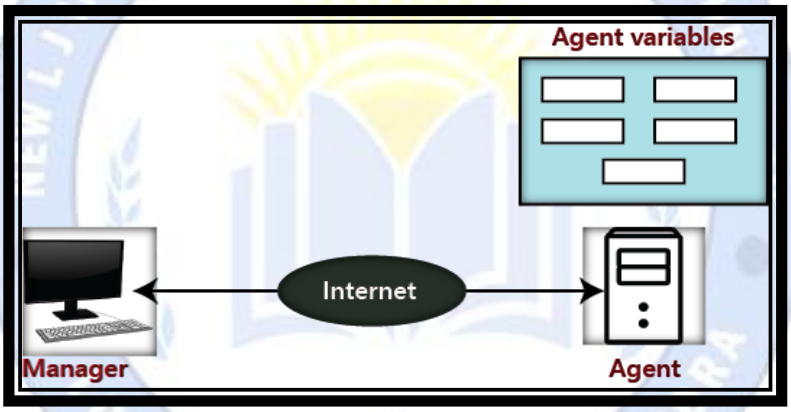
- **The FTP client has three components:**
  - The user interface, control process, and data transfer process.
- **The server has two components:**
  - The server control process and the server data transfer process.
- **There are two types of connections in FTP:**



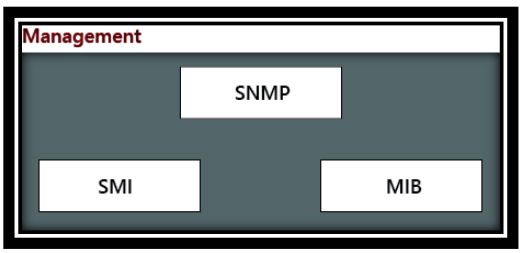
- **Control Connection:**
  - The control connection uses very simple rules for communication.
  - Through control connection, we can transfer a line of command or line of response at a time.
  - The control connection is made between the control processes.
  - The control connection remains connected during the entire interactive FTP session.
- **Data Connection:**
  - The Data Connection uses very complex rules as data types may vary.
  - The data connection is made between data transfer processes.
  - The data connection opens when a command comes for transferring the files and closes when the file is transferred.

c. SNMP and HTTP.

- **SNMP**
  - **SNMP** Stand for **Simple Network Management Protocol.**
  - SNMP was defined by **IETF (Internet Engineering Task Force).**
  - It is used to manage the network. It is an internet standard protocol that monitors devices in IP networks and collects and organizes the information (data) of these devices.
  - SNMP is **supported** by most network devices such as the **hub, switch, router, bridge, server, modem, and printer, etc.**
  - The concept of SNMP is based on the manager and agent.
  - A manager is like a host that controls a group of agents, such as routers.

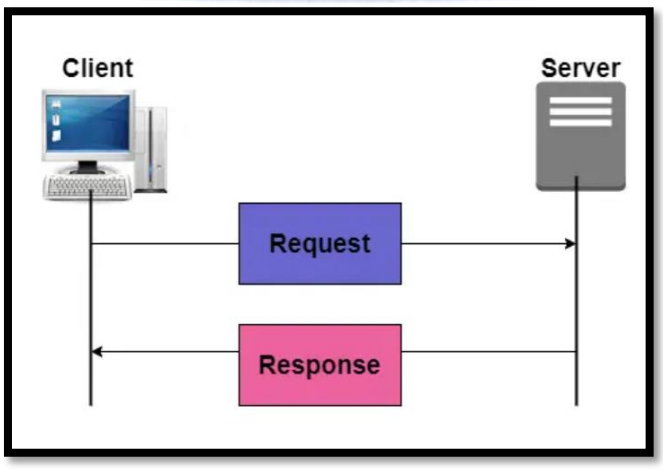


  - **SNMP Manager:**
    - It is a computer system that monitors network traffic by the SNMP agent, and it queries these agents, takes answers, and controls them.
  - **SNMP Agent:**
    - It is a software program that is located in a network element.
    - It collects real-time information from the device and passes this information to the SNMP manager.
  - **Management components**
    - It has two components
      - SMI
      - MIB



- **SNMP:**
  - It defines the structure of packets that is shared between a manager and an agent.
- **SMI (Structure of Management Information):**
  - SMI is a network management component that defines the standard rules for the naming object and object type (including range and length) and also shows how to encode objects and values.
- **MIB (Management Information Base):**
  - MIB is the second component of the network management.
  - It is virtual information storage where management information is stored.

- **HTTP:**
  - **HTTP** is one of the protocols used at the **Application Layer**.
  - The **HTTP** is similar to **FTP** because **HTTP** is used to transfer the files and it mainly uses the services of **TCP.**
  - Also, **HTTP** is much simpler than **FTP** because there is only **one TCP connection**.
  - In **HTTP,** there is no separate control connection, as only data is transferred between the client and the server.
  - **SMTP** messages are **stored and then forwarded** while the **HTTP** messages are **delivered immediately.**
  - The **HTTP** mainly uses the services of the **TCP** on the well-known port that is **port 80.**
  - **HTTP** is a **stateless protocol.**
  - In **HTTP, the** client initializes the transaction by sending a request message, and the server replies by sending a response.
  - **Working of HTTP:**

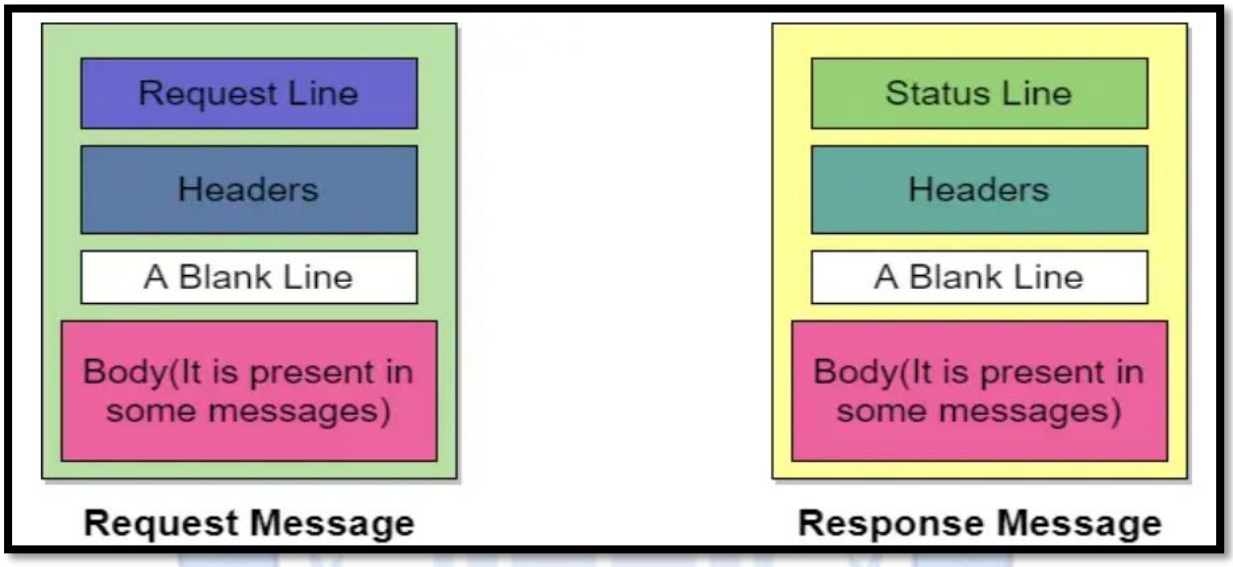


- The HTTP makes use of Client-server architecture.
- As we have already told you that the browser acts as the HTTP client and this client mainly communicates with the webserver that is hosting the website.
- The format of the request and the response message is similar.
- The Request Message mainly consists of a request line, a header, and a body sometimes.
- A Response message consists of the status line, a header, and sometimes a body.
- At the time when a client makes a request for some information (say client clicks on the hyperlink) to the webserver.
- The browser then sends a request message to the HTTP server for the requested objects.

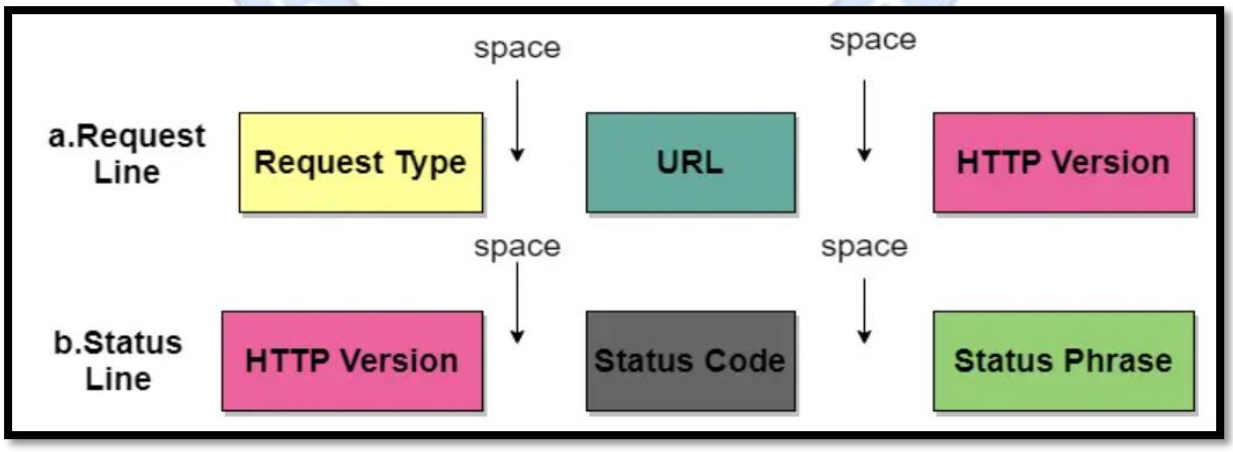
16. Explain Request Message and Response Message Format of HTTP.

Ans:

- **Request Message and Response Message Format of HTTP:**



- **Request Line and Status line**
  - The first line in the Request message is known as the request line, while the first line in the Response message is known as the Status line.



- **Request Type**
  - This field is used in the request line.
  - The are several request types that are defined and these are mentioned in the table given below;

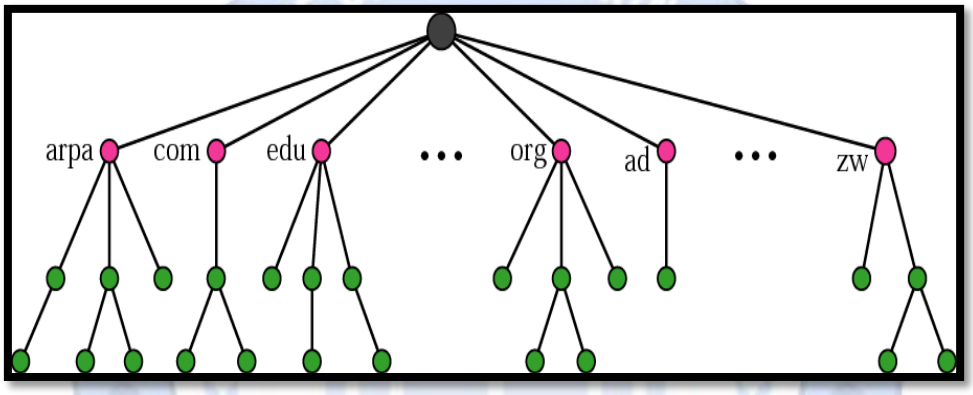
Name of Method	Actions
GET	• This method is used to request a document from the server.
HEAD	• This method mainly requests information about a document and not the document itself
POST	• This method sends some information from the client to the server.
PUT	• This method sends a document from the server to the client.
TRACE	• This method echoes the incoming request.
CONNECT	• This method means reserved
OPTION	• In order to inquire about the available options.

- **URL:**
  - URL is a Uniform Resource locator and it is mainly a standard way of specifying any kind of information on the Internet.
- **HTTP Version:**
  - The current version of the HTTP is 1.1.
- **Status Code:**
  - The status code is the field of the response message.The status code consists of three digits.
- **Status Phrase:**
  - This field is also used in the response message and it is used to explain the status code in the form of text.

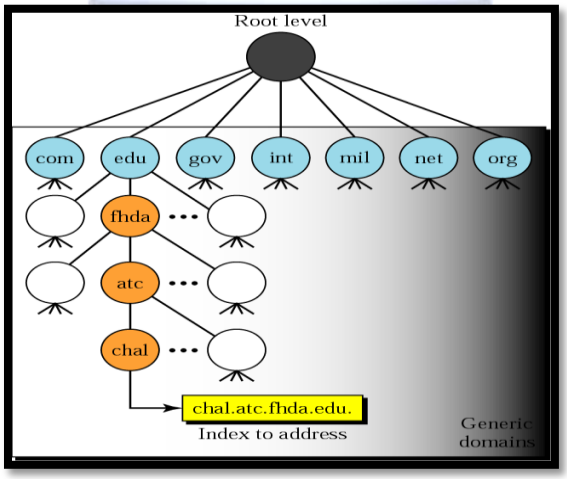
17. What is DNS? List and explain Types of DNS.

Ans:

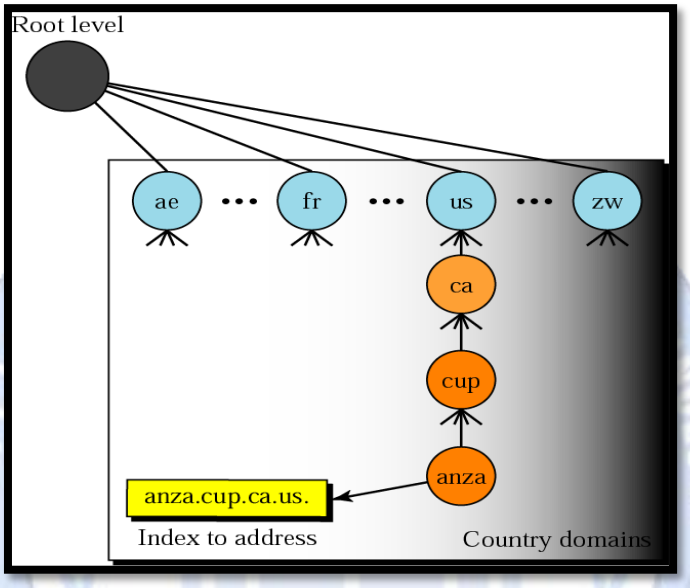
- **DNS:**
  - **DNS** stands for **Domain Name System**.
  - DNS is a directory service that provides a **mapping between** the **name of a host on the network and its numerical address**.
  - Each node in a **tree has a domain name**, and a full domain name is a sequence of symbols specified by (.) **dots.**
  - DNS is a **service** that **translates** the **domain name** into **IP addresses**.



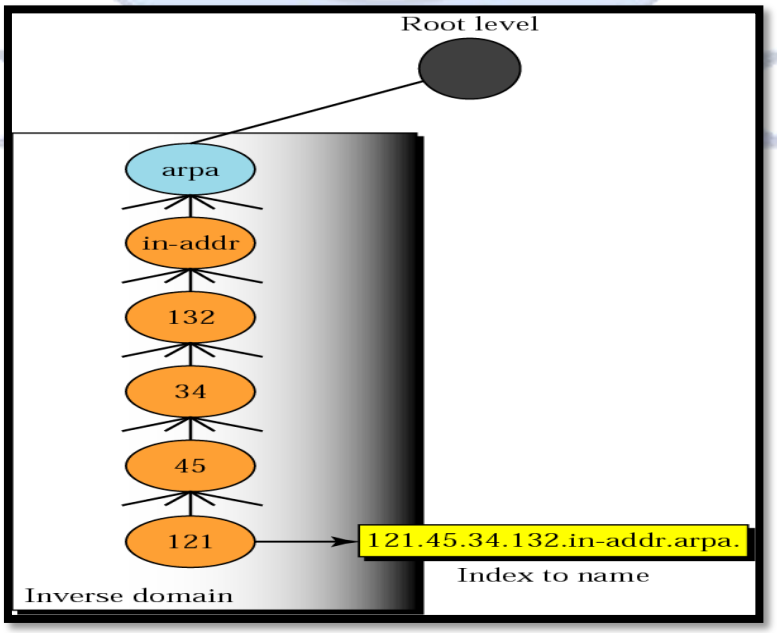
- **Types of DNS:**
  - The domain name space is **divided into three different sections:**
    - Generic Domains.
    - Country Domains.
    - Inverse Domain.
- **Generic Domains:**
  - It defines the registered hosts according to their generic behavior.
  - Each node in a tree defines the domain name, which is an index to the DNS database.
  - It uses t**hree-character** labels, and these **labels describe** the **organization type.**



- **Country Domains:**
  - The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.
  - Country domain uses **two character** country abbreviations.
  - Second labels can be more specific, national designation.
  - **For example,**
  - **Australia** the country domain is "**.au**", **Inida** is "**.in"** and UK is "**.uk**"etc.



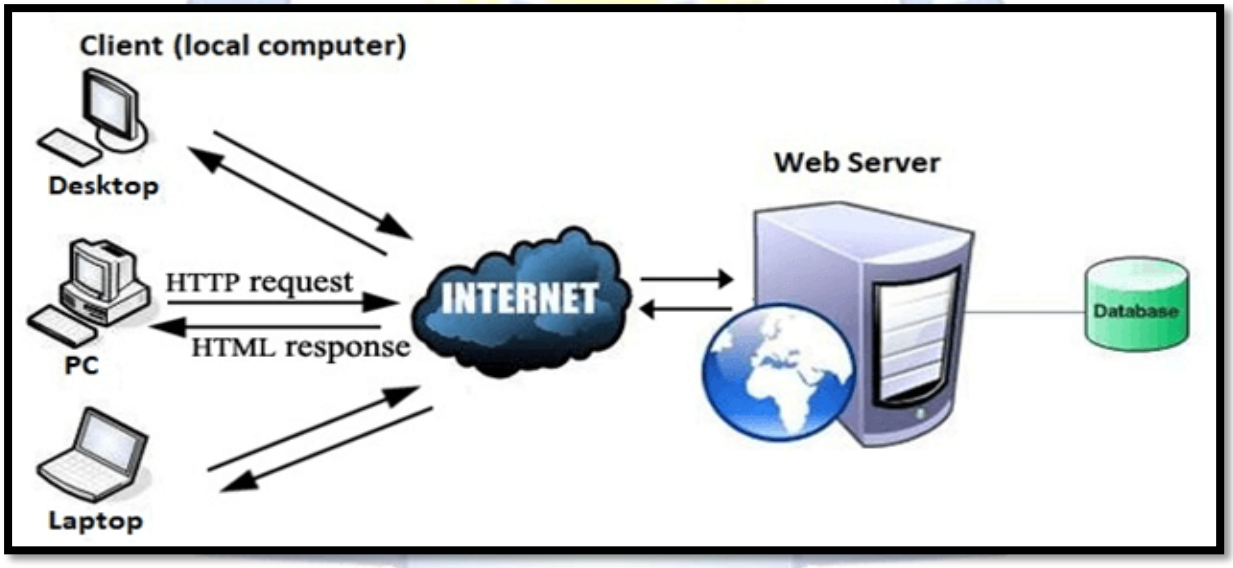
- **Inverse Domains:**
  - The inverse domain is used for mapping an address to a name.
  - When the server has received a request from the client, and the server contains the files of only authorized clients.
  - To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.



18. Write a short note: WWW and TFTP.

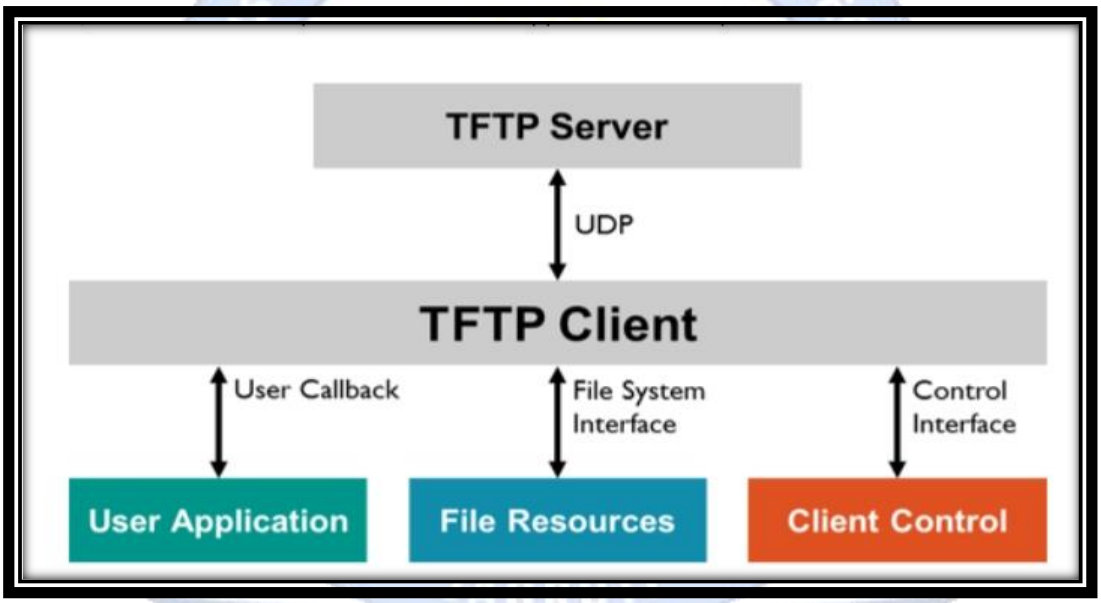
Ans:

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



  - **Components of the Web:**
    - There are 3 components of the web:
      - **Uniform Resource Locator (URL):**
        - serves as a system for resources on the web.
      - **HyperText Transfer Protocol (HTTP):**
        - specifies communication of browser and server.
      - **Hyper Text Markup Language (HTML):**
        - defines the structure, organization and content of a webpage.

- **TFTP:**
  - **Trivial File Transfer Protocol (TFTP)** is a simple protocol used for transferring files.
  - TFTP uses the User Datagram Protocol (UDP) which enables data to be sent between communication partners without sharing a fixed connection.
  - TFTP is mostly used to read and write files/mail to or from a remote server.
  - It is also possible to implement the TFTP based on other protocols.
  - TFTP is a simpler version of FTP and it doesn't have all its functions for example, you cannot list, delete or rename files or directories on a remote server.
  - In fact, TFTP can only be used to send and receive files between the two computers.
  - TFTP doesn't support user authentication and all data is sent in clear text.
- **TFTP messages:**

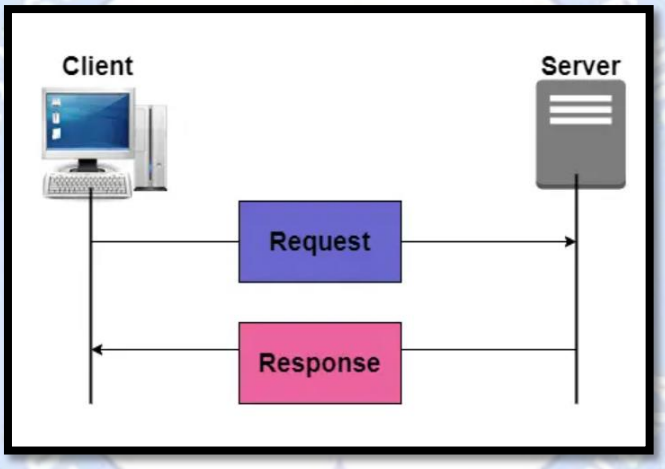


- **TFTP messages come in five types:**
  - **RRQ (read request):** to request devices to read files
  - **WRQ (write request):** to request devices to write files
  - **DATA:** to carry file blocks
  - **ACK (acknowledge):** to acknowledge received file blocks
  - **ERROR:** to tell the sending device when an operation cannot be performed.
- **Advantages:**
  - It utilizes the User Datagram Protocol (UDP) protocol.
  - It is very easy to use and implement.
  - It needs minimum memory utilization.
  - It is a faster file transfer protocol.

19. What is HTTP? Explain Types of HTTP Connections.

Ans:

- **HTTP:**
  - **HTTP** is one of the protocols used at the **Application Layer**.
  - The **HTTP** is similar to **FTP** because **HTTP** is used to transfer the files and it mainly uses the services of **TCP.**
  - In **HTTP,** there is no separate control connection, as only data is transferred between the client and the server.
  - **HTTP** port number is **80.**
  - **HTTP** is a **stateless protocol.**
  - In **HTTP, the** client initializes the transaction by sending a request message, and the server replies by sending a response.
  - **Working of HTTP:**



- **HTTP connections are broadly categorized into two types:**
  - Persistent
  - Non-Persistent

*****Explanation Referred Difference Between*****

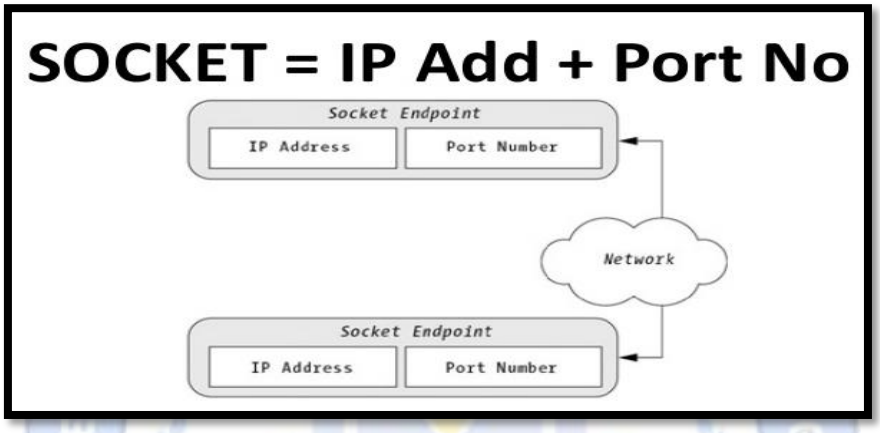
Persistent and Non-Persistent Connections

Q.21 (B)

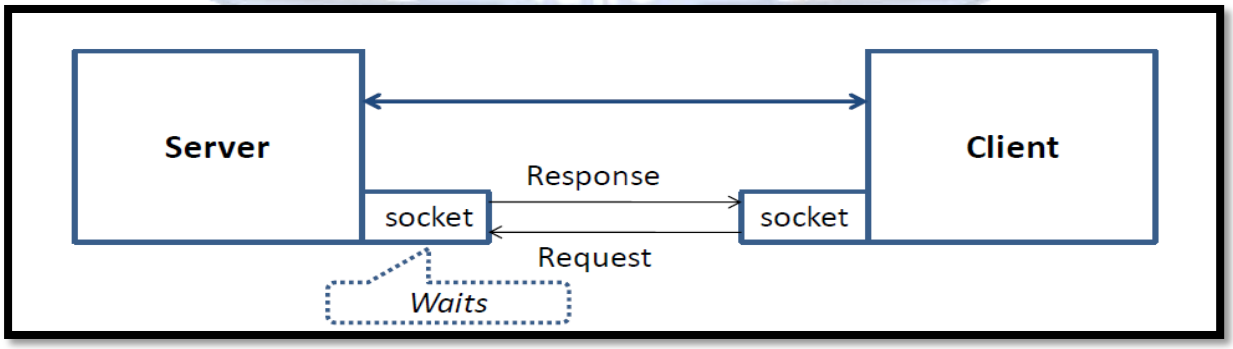
20. Write a short note: Socket Programming.

Ans:

- **Socket**
  - "A **socket** is one endpoint of a two-way communication link between two programs running on the network."
  - An Socket is combination of an IP address and a port number.



- **Network connection identified by a 5-tuple:**
  - src ip, src port, dst ip, dst port, protocol.
- **Client – Server Communication:**
  - Two machines must connect
  - Server waits for connection
  - Client initiates connection
  - Server responds to the client request



- **Two kinds of Internet transport services provided to applications.**
  - Connection-oriented (TCP)
  - Connectionless (UDP)

- **TCP/IP Server Program:**

MyServer.java

```
1. import java.io.*;  // required data input/output stream
2. import java.net.*; //required for Socket Class
3.  public class MyServer {
4.      public static void main(String[] args){
5.      try{
6.              ServerSocket ss=new ServerSocket(1111);
7.                 Socket s=ss.accept();//establishes connection
8.              DataInputStream dis=
9.                      new DataInputStream (s.getInputStream());
10.             String  str=(String)dis.readUTF();
11.             System.out.println("message= "+str);
12.             ss.close();
13.     }
14.     catch(Exception e){System.out.println(e);}
15.     }
16.}
```

Output

```
message= Hello Server
```

- **TCP/IP Client Program:**

```
1. import java.net.*; //required for Socket Class
2. import java.io.*; // required data input/output stream
3. public class MyClient {
4.      public static void main(String[] args)
5.      {  try{
6.              Socket s = new Socket("localhost",1111);
7.              DataOutputStream dout= new
                    DataOutputStream(s.getOutputStream());
8.              dout.writeUTF("Hello Server");// Writes a
                        string to the underlying output stream
9.            }catch(Exception e)
10.           {System.out.println(e);}
11.     }
12.}
```

Object of Socket class

21. Difference Between:

a. **FTP and TFTP**

b. **Persistent and Non-Persistent Connections.**

c. **POP3 and IMAP.**

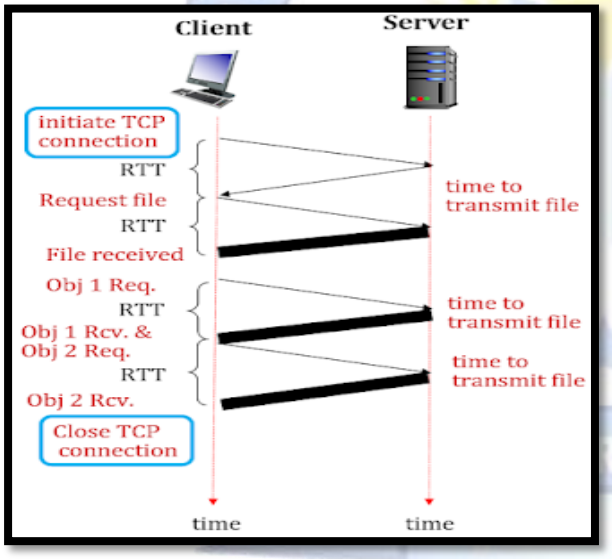
Ans:

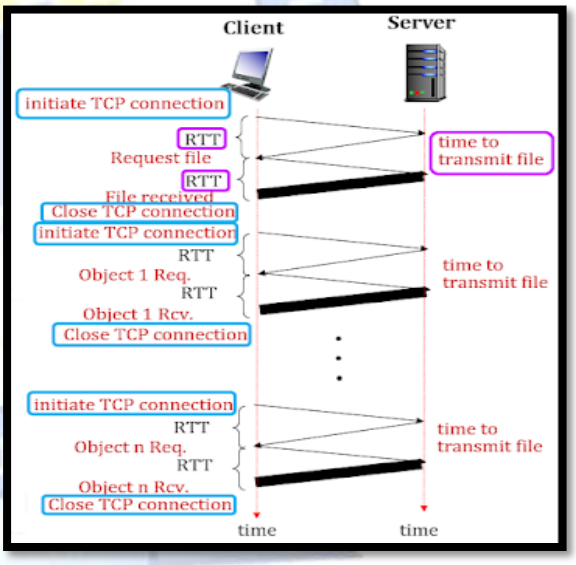
a. **FTP and TFTP**

COMPARISON	FTP	TFTP
Full-Form	File Transfer Protocol.	Trivial File Transfer Protocol.
Authentication	Authentication is required in FTP for communication between client and server.	No authentication is required in TFTP.
Service	FTP uses TCP service which is a connection-oriented service.	TFTP uses UDP service which is connection-less service.
Software	FTP software is larger than TFTP.	TFTP software is smaller than FTP and fits into readonly memory of the diskless workstation.
Commands/Message	FTP have many commands.	TFTP have only five messages.
Connection	FTP establishes two connections one for data(TCP port no. 21) and one for control(TCP port no. 20).	TFTP establishes a single connection for its file transfer (UDP port no. 69).
Complexity	FTP is more complex	TFTP is less complex.
Security	Encrypts data transfer	Does not encrypt data transfer
Error handling	Can recover from errors during transfer	Does not have error recovery
File transfer mode	Supports both ASCII and binary transfer modes	Only supports binary transfer mode

b. Persistent and Non-Persistent Connections.

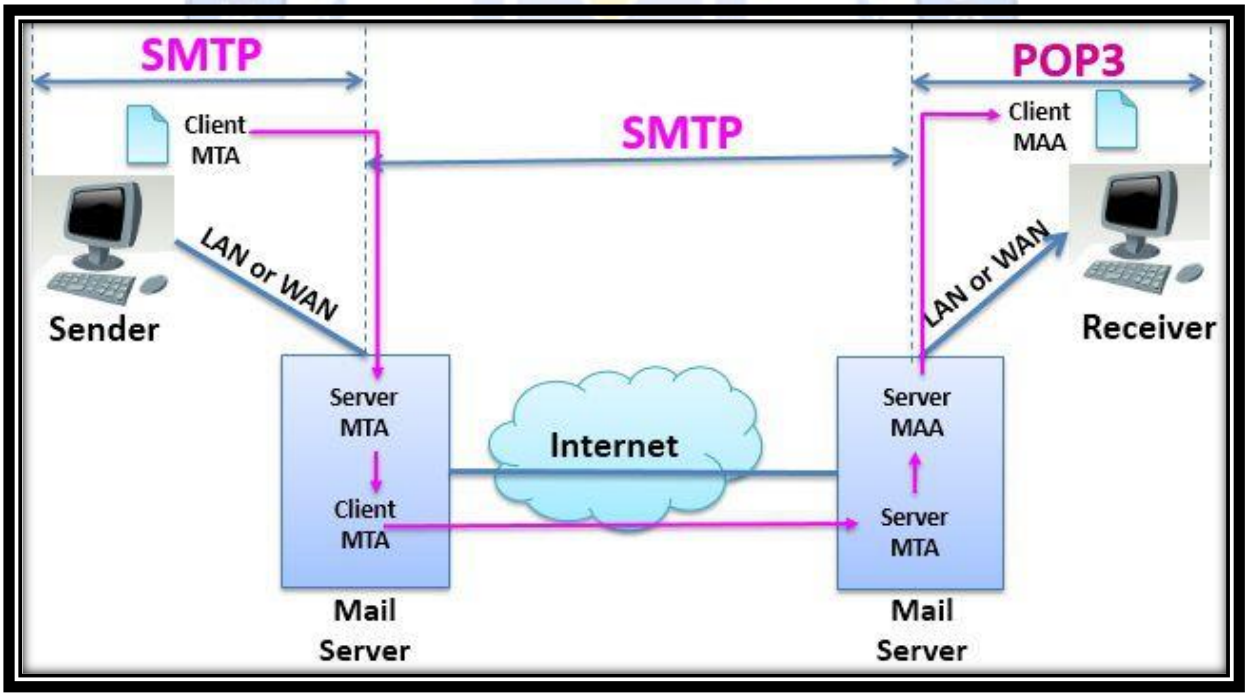
HTTP Version	HTTP Version 1.1	HTTP Version 1.0
Mode	It is default mode	It is not default mode
No. of RTT use	It uses one RTT for each object	It uses 2 RTT for each object
TCP Connection	TCP connection is not closed	closed after every request response
No. of request on TCP Connection	Multiple request over the single TCP connection.	Multiple request over the multiple TCP connection
Request Method	Request method are GET, HEAD, POST, PUT, DELETE, etc....	Request methods are used GET, POST and HEAD





c. POP3 and IMAP.

BASIS FOR COMPARISON	POP3	IMAP
Basic	To read the mail ithas to be downloaded first.	The mail content can be checked partially before downloading.
Organize	The user can not organize mails in the mailbox of the mail server.	The user can organize the mails on the server.
Folder	The user can not create, delete or rename mailboxes on a mail server.	The user can create, delete or rename mailboxes on the mail server.
Content	A user can not search the content of mail for prior downloading.	A user can search the content of mail for specific string of character before downloading.
Partial Download	The user has to download the mail for accessing it.	The user can partially download the mail if bandwidth is limited.
Functions	POP3 is simple and has limited functions.	IMAP is more powerful, more complex and has more features over POP3.

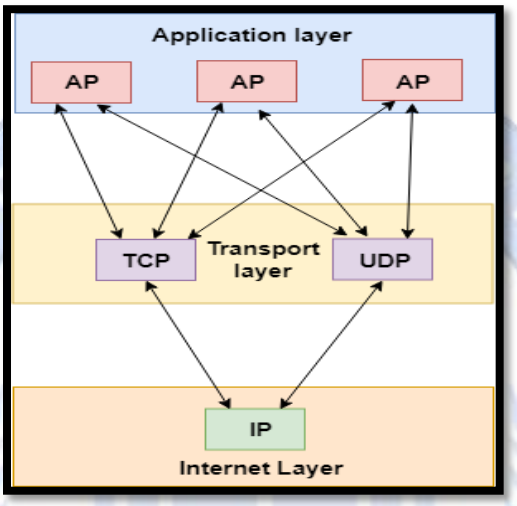


Unit - 3 Transport Layer

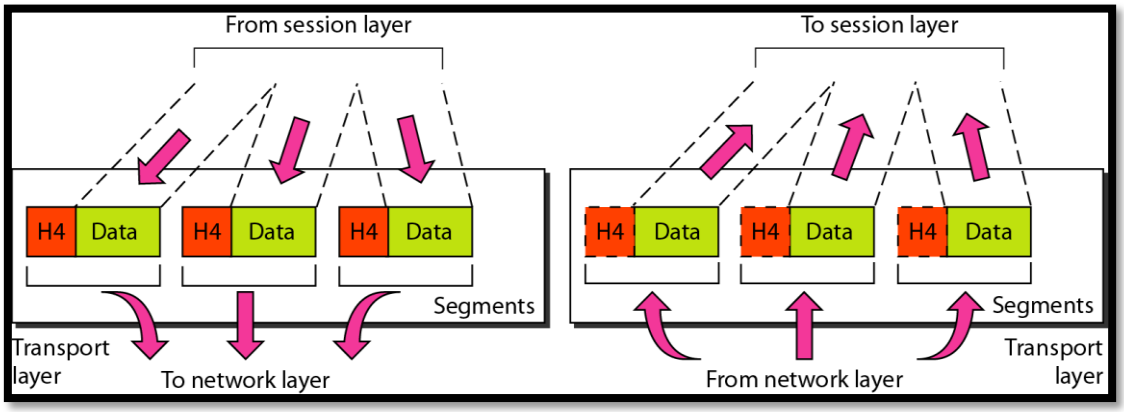
22. Write a short note: Transport Layer.

Ans:

- **Transport Layer:**



  - The transport layer is responsible for the **delivery of a message** from one process to another.
  - Transport Layer is the **fourth layer** from the **top in OSI Model** which provide communication services to the application processes that was running on different hosts.
  - Transport Layer provides the services to the **session layer** and it receives the services from **network layer**.
  - The **services** provided by transport layer includes **error correction** as well as **segmenting and De-segmenting** data before and after it's sent on the network.
  - Transport layer also provides the **flow control functionality** and **ensures that segmented data is delivered across** the network in the **right sequence.**

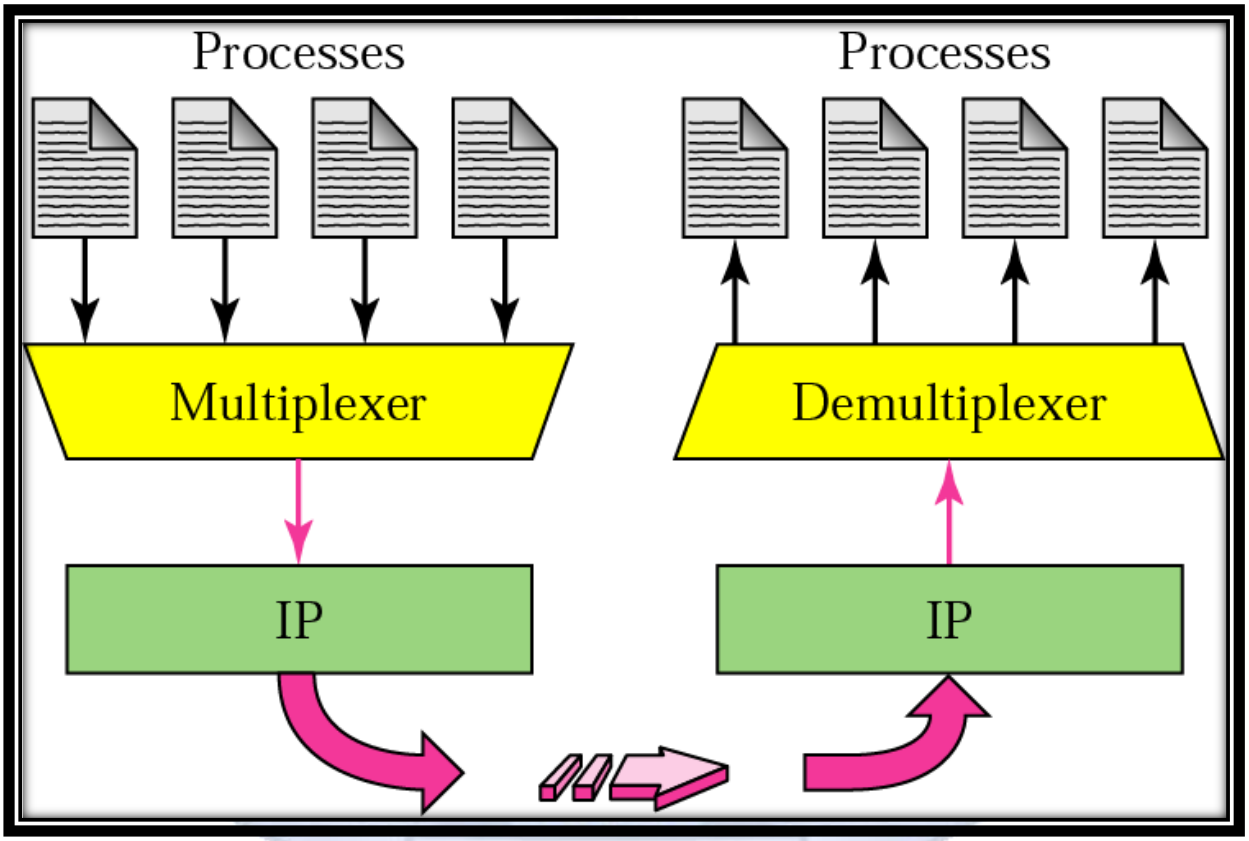


- **At the sender's side:**
  - At the sender's end, transport layer **collect data from application layer** i.e message and performs segmentations to divide the message into segments and then adds the port number of source and destination in header and send that message to network layer.
- **At the receiver's side:**
  - At the receiver's end, **transport layer collects data from network layer** and then reassembles the segmented data and identifies port number by reading its header to send that message to appropriate port in the session layer.
- **The two main Transport layer protocols are:**
  - **Transmission Control Protocol**
    - It provides reliable communication between two hosts.
  - **User Datagram Protocol**
    - It provides unreliable communication between two hosts.
- The services provided by the transport layer protocols can be **divided into five categories:**
  - End-to-end delivery
  - Addressing
  - Reliable delivery
  - Flow control
  - Multiplexing

23. Explain Multiplexing and Demultiplexing.

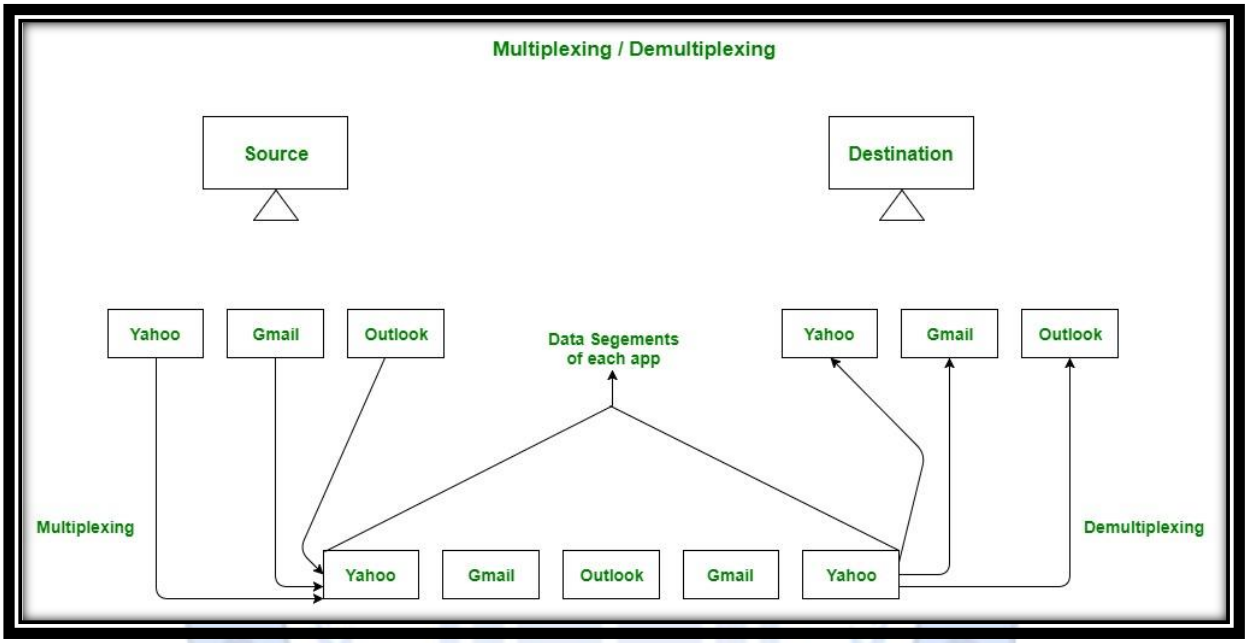
Ans:

- Multiplexing and Demultiplexing services are provided in almost every protocol architecture ever designed.
- UDP and TCP perform the demultiplexing and multiplexing jobs by including **two special fields** in the **segment headers**: the **source port number field** and the **destination port number field**.



- **Multiplexing:**
  - **Multiplexing** is the process of collecting the data from multiple application processes of the sender, enveloping that data with headers and sending them as a whole to the intended receiver.
  - In Multiplexing at the Transport Layer, the data is collected from various application processes. These segments contain the source port number, destination port number, header files, and data.
  - These segments are passed to the Network Layer which adds the source and destination IP address to get the datagram.
- **Demultiplexing**
  - Delivering the received segments at the receiver side to the correct app layer processes is called demultiplexing.

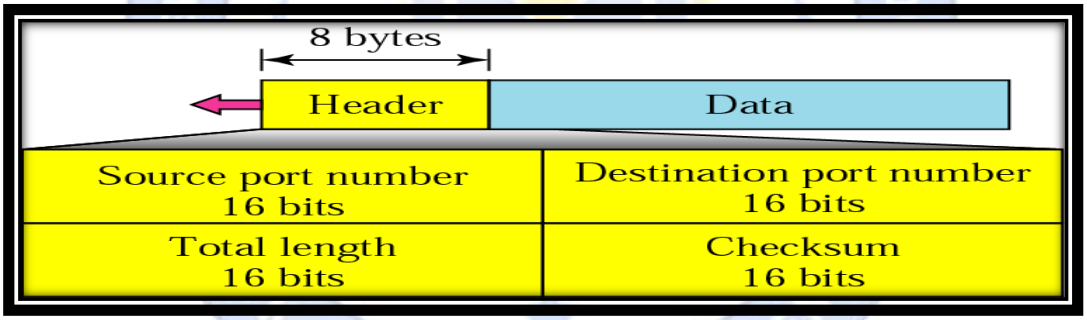
- The destination host receives the IP datagrams; each datagram has a source IP address and a destination IP address.
- Each datagram carries 1 transport layer segment.
- Each segment has the source and destination port number.
- The destination host uses the IP addresses and port numbers to direct the segment to the appropriate socket.



24. Draw and explain UDP Header format.

Ans:

- **Connection Less Transport (UDP)**
  - UDP stands for **User Datagram Protocol**.
  - UDP is a simple protocol and it provides non-sequenced transport functionality.
  - UDP is a connectionless protocol.
  - This type of protocol is used when reliability and security are less important than speed and size.
  - UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
  - The packet produced by the UDP protocol is known as a user datagram.
  - **UDP Header**
    - UDP header is **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes.
    - First 8 Bytes contains all necessary header information and remaining part consist of data.

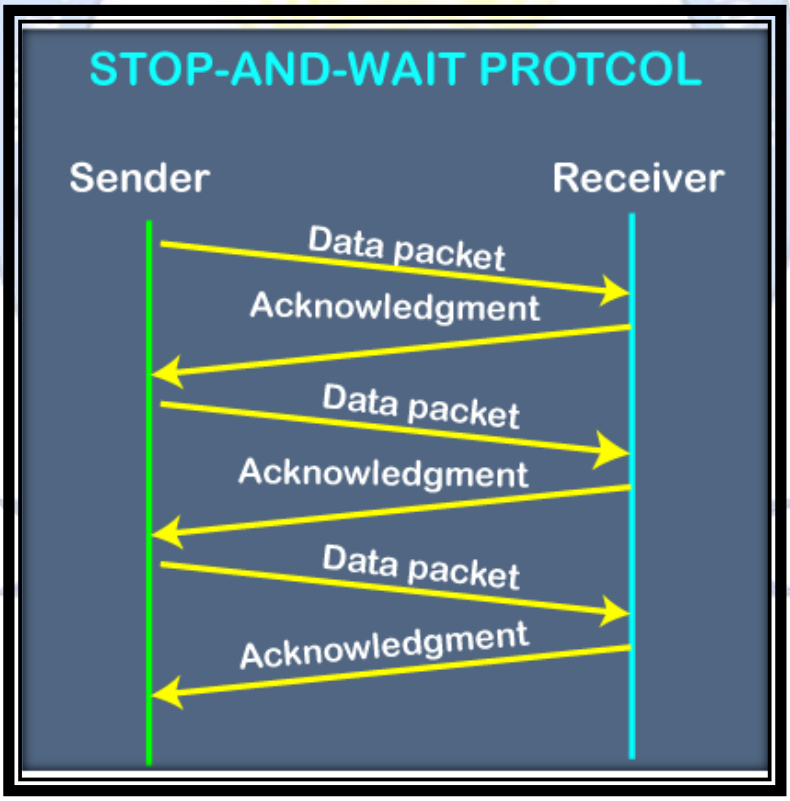


  - UDP port number fields are each 16 bits long, therefore range for port numbers defined from 0 to 65535; port number 0 is reserved.
  - Port numbers help to distinguish different user requests or process.
  - **Source port address:**
    - It defines the address of the application process that has delivered a message.
    - The source port address is of 16 bits address.
  - **Destination port address:**
    - It defines the address of the application process that will receive the message.
    - The destination port address is of a 16-bit address.
  - **Total length:**
    - It defines the total length of the user datagram in bytes.
    - It is a 16-bit field.
  - **Checksum:**
    - The checksum is a 16-bit field which is used in error detection.

25. Explain Stop and Wait Protocol.

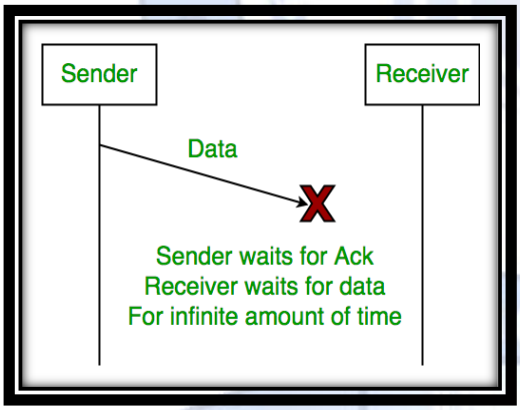
Ans:

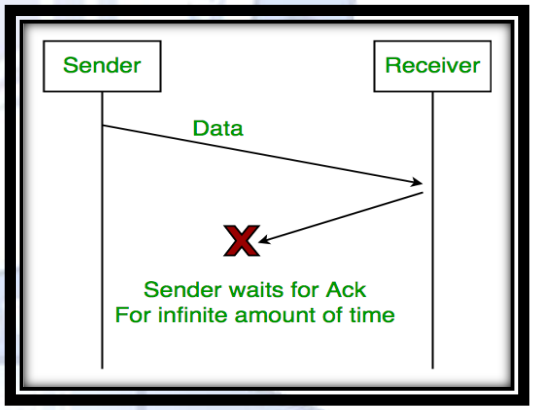
- stop and wait means, whatever the data that sender wants to send, he sends the data to the receiver.
- After sending the data, he stops and waits until he **receives the acknowledgment from the receiver**.
- The stop and wait protocol is a flow control protocol where flow control is one of the services of the data link layer.
- It is a data-link layer protocol which is used **for transmitting the data over the noiseless channels.**
- It provides **unidirectional data transmission** which means that either **sending or receiving of data will take place at a time**.
- It provides flow-control mechanism but **does not provide any error control mechanism.**



- **The primitives of stop and wait protocol are:**
  - **Sender side:**
    - **Rule 1:** Sender sends one data packet at a time.
    - **Rule 2:** Sender sends the next packet only when it receives the acknowledgment of the previous packet.

- Therefore, the idea of stop and wait protocol in the sender's side is very simple, i.e., send one packet at a time, and do not send another packet before receiving the acknowledgment.
    - **Receiver side**
        - **Rule 1:** Receive and then consume the data packet.
        - **Rule 2:** When the data packet is consumed, receiver sends the acknowledgment to the sender.
- Stop-and-Wait is a simple protocol used for transmitting data between two devices over a communication channel.
- In this protocol, the sender sends a packet of data to the receiver and then waits for the receiver to acknowledge the packet before sending the next packet.
- The receiver sends an acknowledgement to the sender indicating that the packet has been received and is error-free.
- **Problems:**
    - Lost Data
    - Lost Acknowledgement

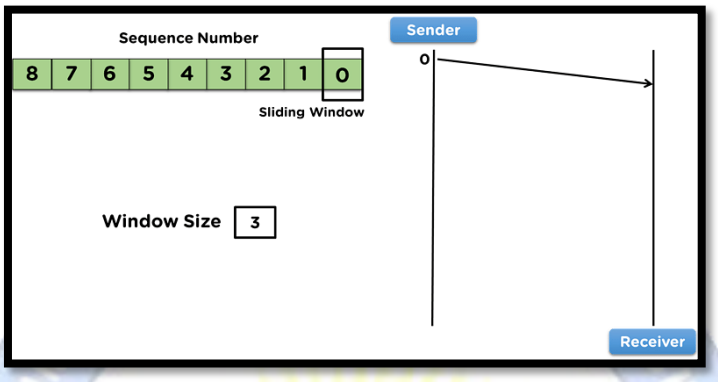




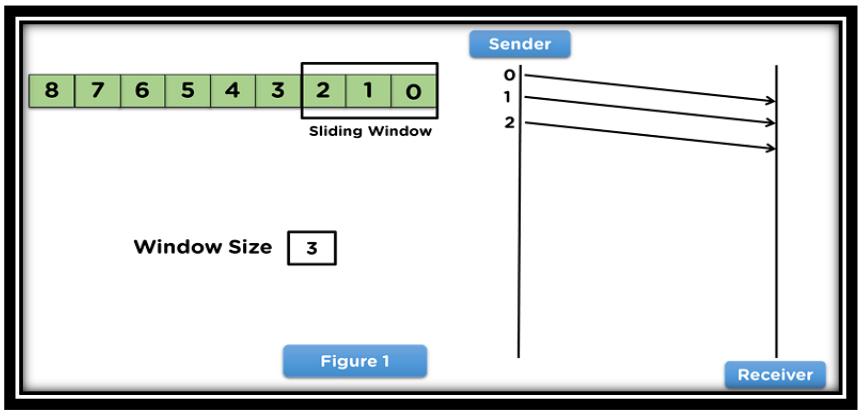
26. Explain Sliding Window Protocols.

Ans:

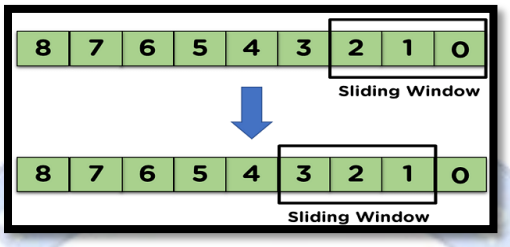
- The sliding window protocol is a method designed in the network model that allows data exchange more efficiently and within the scope of clearly defined steps in the channel.



- The sliding window protocol is a method designed in the network model that allows data exchange more efficiently and within the scope of clearly defined steps in the channel.
- This protocol allows sharing multiple data frames from the sender before receiving any acknowledgment from the receiver side.
- Each of the frames in the network model is assigned a sequence number to increase the transmission efficiency.
- **Working of the Sliding Window Protocol:**
  - The working of the sliding window protocol can be divided into two steps sender steps, and the receiver steps and also some important values are needed in a network model for smooth transmission of the data frames are:
  - Sender and the receiver side
  - Window Size
  - The total data frames to be transmitted
  - Proper sequencing of the frames
- **Steps for the Sender Side:**



- To begin with, the sender side will share data frames with the receiver side per the window size assigned to the model.
- The sliding window will appear on the frames transmitted over to the receiver side.
- Then the sender will wait for an acknowledgment from the receiver side for the shared frames, as mentioned in figure 1.



- When the receiver transmits the acknowledgment of the first transmitted frame, the sliding window will shift from the acknowledged frame.

- **Steps for the Receiver Side:**

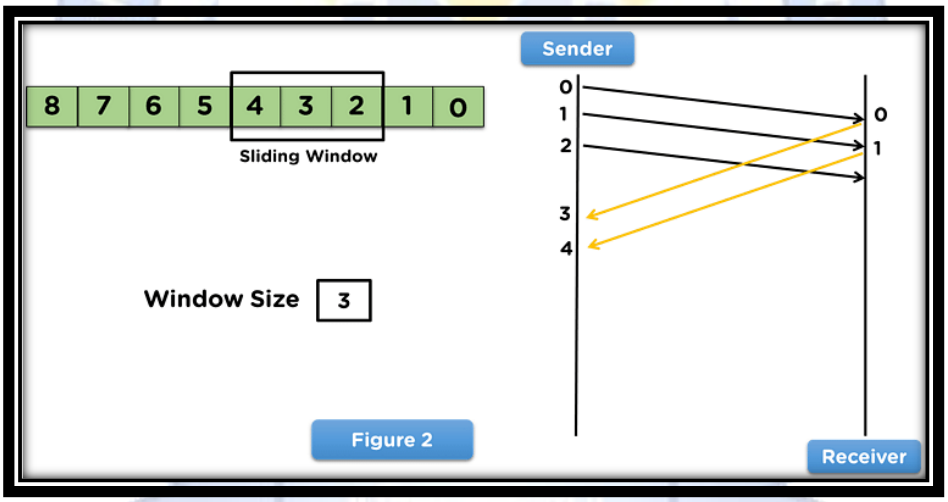


Figure 2

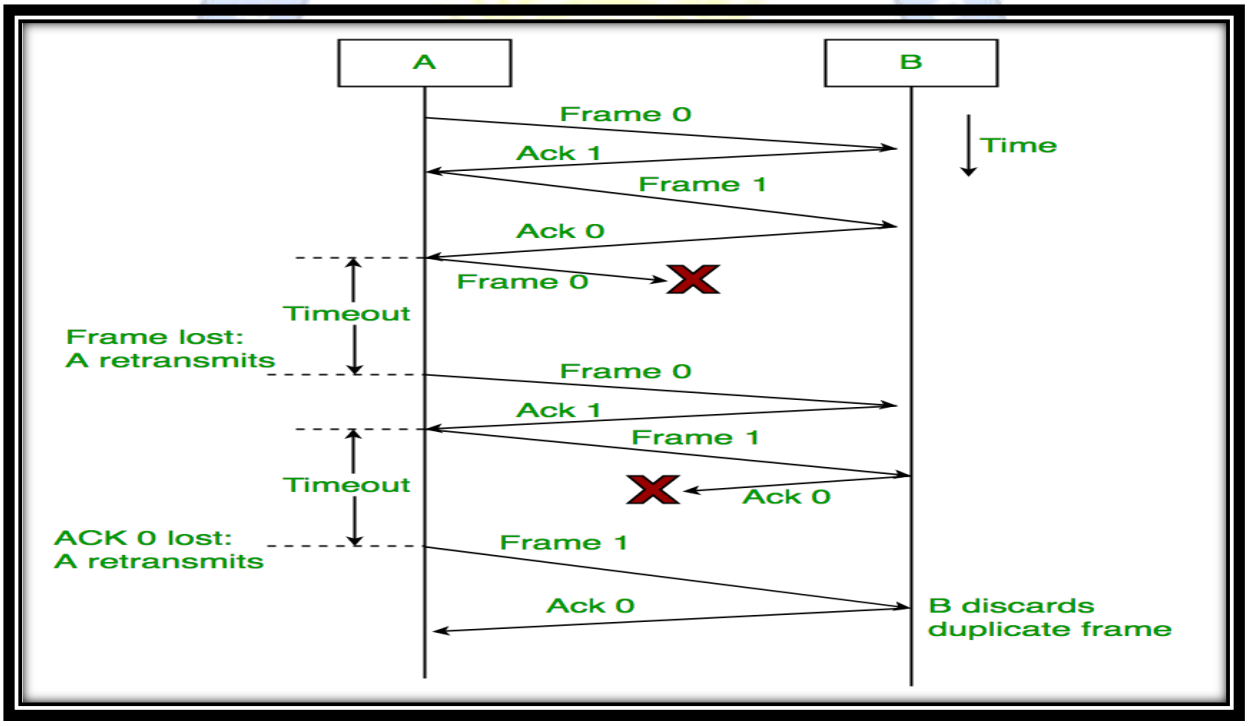
- On receiving the data frames from the sender side, the receiver will use the frames in the network model.
- After the receiver uses the frame, it will transmit the acknowledgement to the sender side for that data frame.
- Then, the receiver side will receive the next data frame from the sender side, as mentioned in figure2.
- This process continues until all the frames are transmitted from the sender side to the receiver side, and the receiver side transmits the acknowledgment of all the received frames.

27. Explain Stop and Wait ARQ (Automatic Repeat Request).

Ans:

- **Problems:**
  - Lost Data
  - Lost Acknowledgement
- Above 2 problems are resolved by Stop and Wait ARQ (Automatic Repeat Request) that does both error control and flow control.

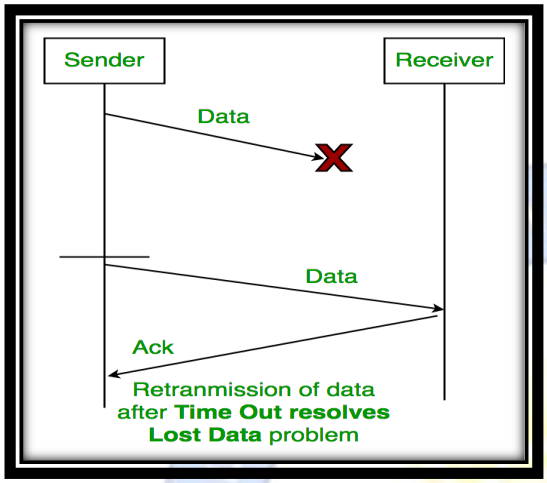
- **Stop and Wait ARQ (Automatic Repeat Request):**

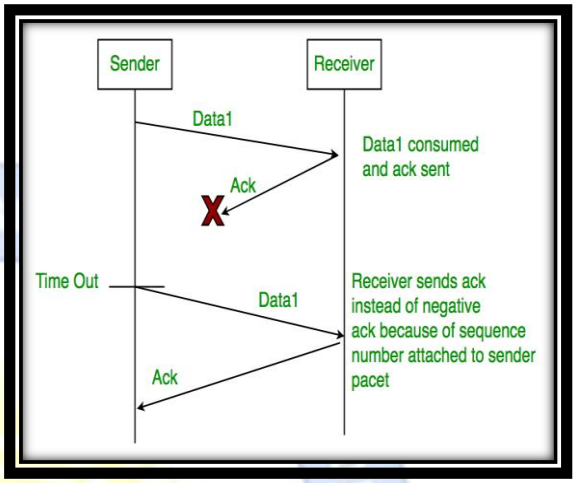


- Sender A sends a data frame or packet with sequence number 0.
- Receiver B, after receiving data frame, sends and acknowledgement with sequence number 1 (sequence number of next expected data frame or packet)
- There is only one bit sequence number that implies that both sender and receiver have buffer for one frame or packet only.
- **Characteristics:**
  - Used in Connection-oriented communication.
  - It offers error and flow control

- It is used in Data Link and Transport Layers
- Stop and Wait ARQ mainly implements Sliding Window Protocol concept with Window Size 1.

- **Resolved Problems:**
  - Time Out
  - Sequence Number

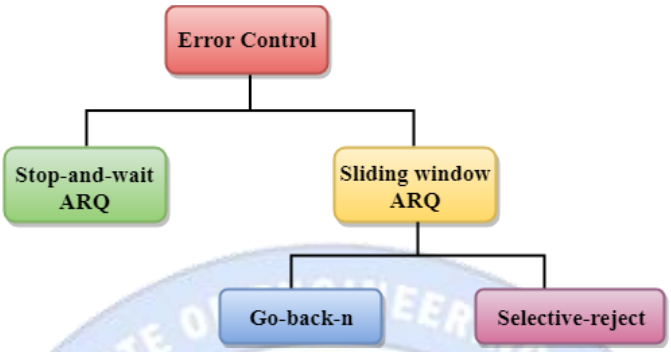




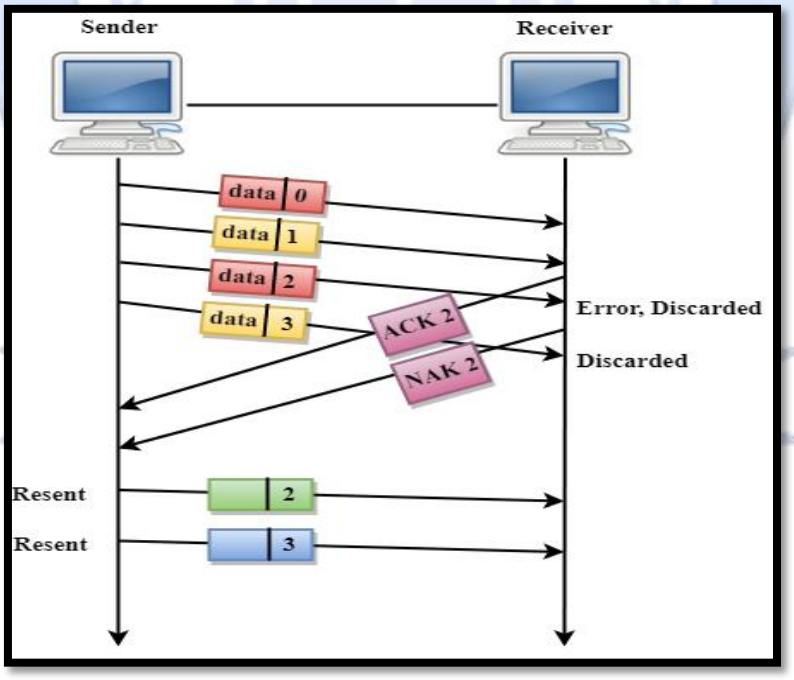
28. Explain Go-Back-N ARQ.

Ans:

- **Error Control** is a technique of error detection and retransmission.



- **Go-Back-N ARQ:**
  - In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.
  - **Three possibilities can occur for retransmission:**
    - Damaged Frame
    - Lost Data Frame
    - Lost Acknowledgement



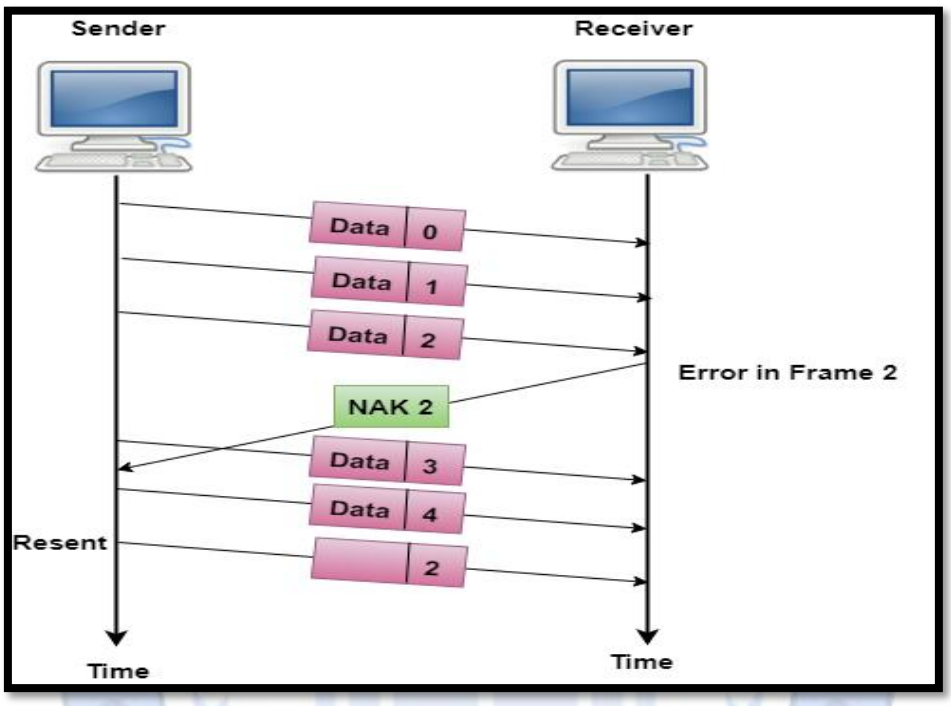
- **Damaged Frame:**
  - When the frame is damaged, then the receiver sends a NAK frame.
  - In the above figure, three frames have been transmitted before an error discovered in the third frame.

- In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error.
- The receiver discovers the error in data 2 frame, so it returns the NAK 2 frame.
- The frame 3 is also discarded as it is transmitted after the damaged frame.
- Therefore, the sender retransmits the frames 2,3.

- **Lost Data Frame:**
  - In Sliding window protocols, data frames are sent sequentially.
  - If any of the frames is lost, then the next frame arrive at the receiver is out of sequence.
  - The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame.
  - The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame.
- **Lost Acknowledgement:**
  - The sender can send as many frames as the windows allow before waiting for any acknowledgement.
  - Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement.
  - If the acknowledgement is lost, then the sender could wait forever.
  - To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached.
  - If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

29. Explain Selective Reject ARQ.

Ans:

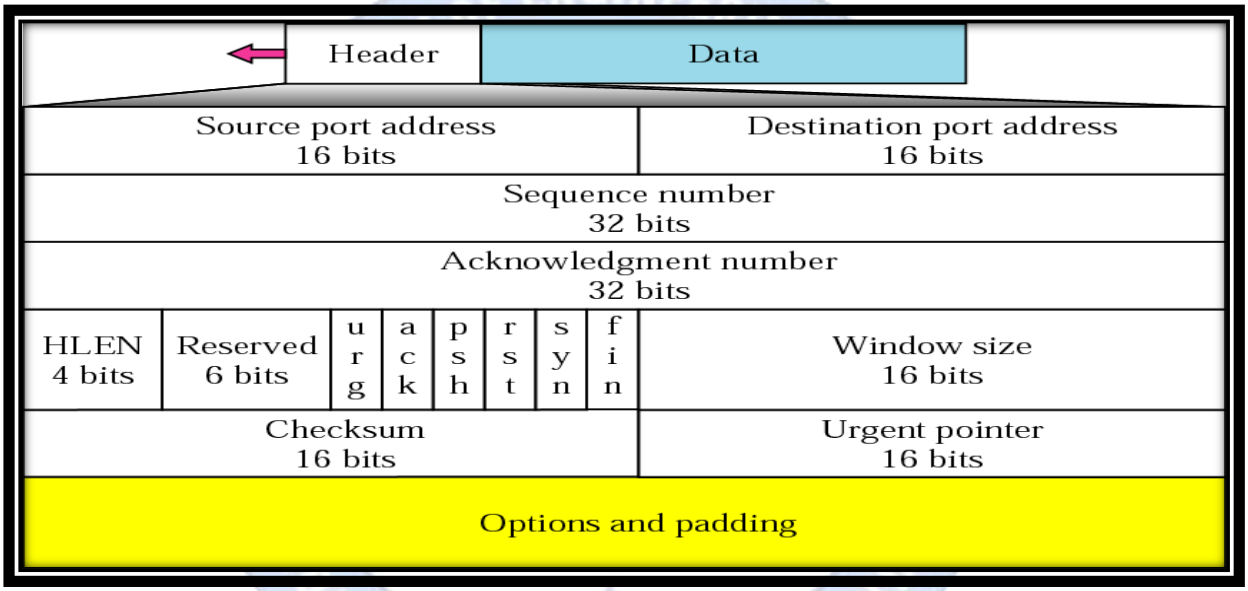


- Selective Repeat ARQ technique is more efficient than Go-Back-n ARQ.
- Selective Repeat is also the sliding window protocol **which detects or corrects the error occurred in the datalink layer.**
- The selective repeat protocol **retransmits only that frame which is damaged or lost.**
- In selective repeat protocol, the retransmitted framed is received out of sequence.
- **The selective repeat protocol can perform the following actions:**
    a. In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.
    b. The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
    c. The receiver must have an appropriate logic for reinserting the frames in a correct order.
    d. The sender must consist of a searching mechanism that selects only the requested frame for retransmission.

30. Draw and explain TCP Header format.

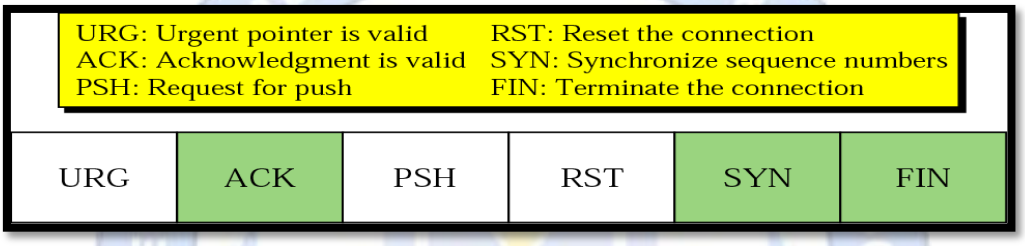
Ans:

- **Connection Oriented Transport (TCP):**
  - TCP stands for Transmission Control Protocol.
  - It provides full transport layer services to applications.
  - It is a connection-oriented protocol means the connection established between both the ends of the transmission.
  - TCP segment consists of data bytes to be sent and a header that is added to the data by TCP as shown:



  - **Source port address:**
    - It is used to define the address of the application program in a source computer.
    - It is a 16-bit field.
  - **Destination port address:**
    - It is used to define the address of the application program in a destination computer.
    - It is a 16-bit field.
  - **Sequence number:**
    - A stream of data is divided into two or more TCP segments.
    - The 32-bit sequence number field represents the position of the data in an original data stream.
  - **Acknowledgement number:**
    - A 32-field acknowledgement number acknowledge the data from other communicating devices.
    - If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.

- **Header Length (HLEN):**
  - It specifies the size of the TCP header in 32-bit words.
  - The minimum size of the header is 5 words, and the maximum size of the header is 15 words.
  - Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
- **Reserved:**
  - It is a six-bit field which is reserved for future use.
- **Control bits:**
  - Each bit of a control field functions individually and independently.
  - A control bit defines the use of a segment or serves as a validity check for other fields.
  - **There are total six types of flags in control field**:



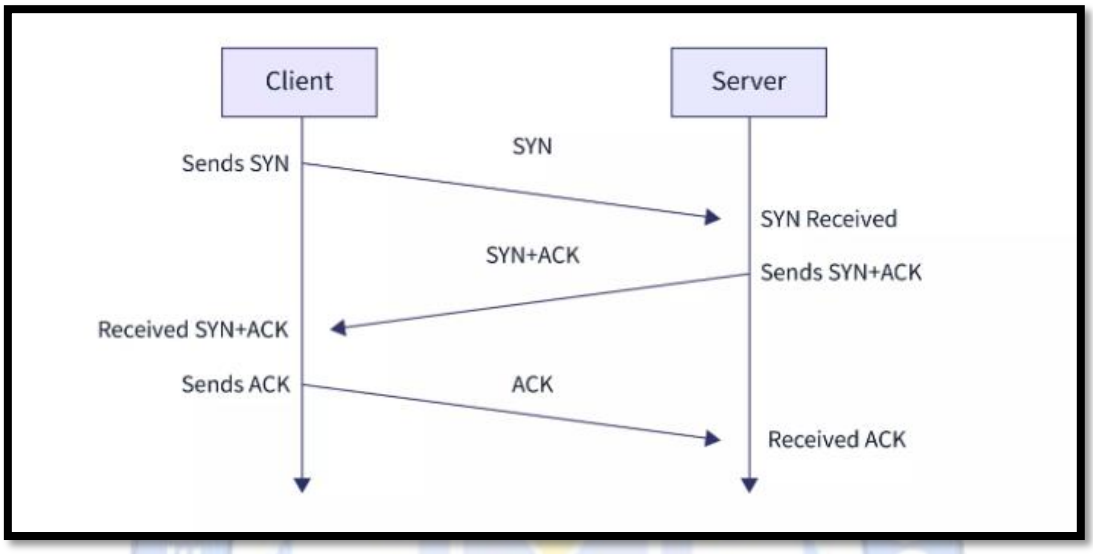
Flag	Description
URG	The value of the urgent pointer field is valid.
ACK	The value of the acknowledgment field is valid.
PSH	Push the data.
RST	The connection must be reset.
SYN	Synchronize sequence numbers during connection.
FIN	Terminate the connection.

- **Window Size:**
  - The window is a 16-bit field that defines the size of the window.
- **Checksum:**
  - The checksum is a 16-bit field used in error detection.
- **Urgent pointer:**
  - If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
- **Options and padding:**
  - It defines the optional fields that convey the additional information to the receiver.

31. Explain TCP Connection (A 3-way handshake).

Ans:

- **TCP Connection (A 3-way handshake):**

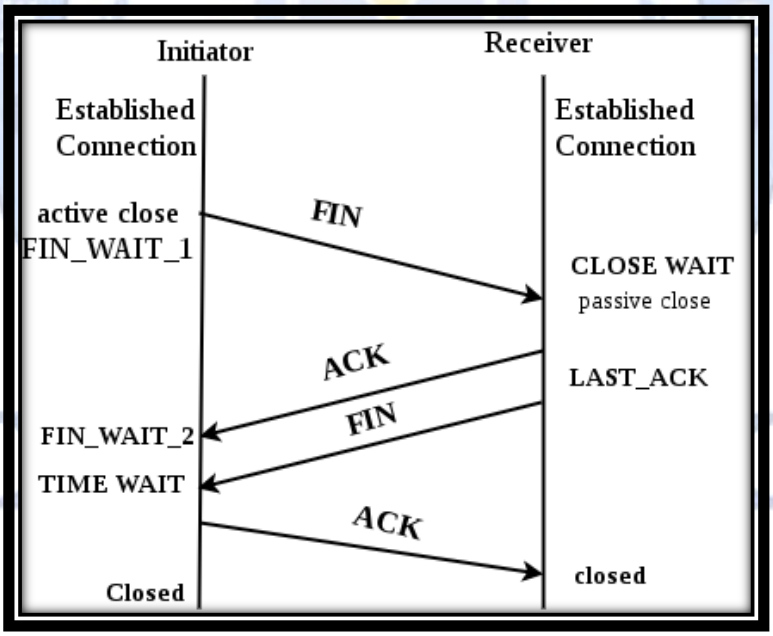


  - Handshake refers to the process to establish connection between the client and server.
  - Handshake is simply defined as the process to establish a communication link.
  - To transmit a packet, TCP needs a three way handshake before it starts sending data.
  - The reliable communication in TCP is termed as PAR (Positive Acknowledgement Re-transmission).
  - The positive acknowledgement from the receiver establishes a successful connection.
  - **Step 1 (SYN):**
    - In the first step, the client wants to establish a connection with a server, so it sends a **segment with SYN(Synchronize Sequence Number)** which informs the **server** that the **client is likely to start communication** and with what sequence number it starts segments with.
  - **Step 2 (SYN + ACK):**
    - **Server responds** to the **client request with SYN-ACK signal bits set**.
    - Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with.
  - **Step 3 (ACK):**
    - In the final part **client acknowledges the response of the server and they both establish a reliable connection** with which they will start the **actual data transfer,**

32. Explain TCP Termination (A 4-way handshake).

Ans:

- **TCP Termination (A 4-way handshake):**
  - Any device establishes a connection before proceeding with the termination.
  - TCP requires 3-way handshake to establish a connection between the **client and server before sending the data.**
  - Similarly, to **terminate or stop the data transmission**, it requires a **4-way handshake.**
  - The segments required for TCP termination are similar to the segments to build a TCP connection (ACK and SYN) except the **FIN segment**.
  - The **FIN segment** specifies a **termination request sent** by **one device to the other.**
  - The **client is the data transmitter** and the **server is a receiver in a data transmission process** between the **sender and receiver.**



a. Firstly, from one side of the connection, either from the client or the server the FIN flag will be sent as the request for the termination of the connection.
b. In the second step, whoever receives the FIN flag will then be sending an ACK flag as the acknowledgment for the closing request to the other side.
c. And, at the Later step, the server will also send a FIN flag as the closing signal to the other side.
d. In the final step, the TCP, who received the final FIN flag, will be sending an ACK flag as the final Acknowledgement for the suggested connection closing.

33. What is Congestion Control? Explain Types of Congestion control algorithms.

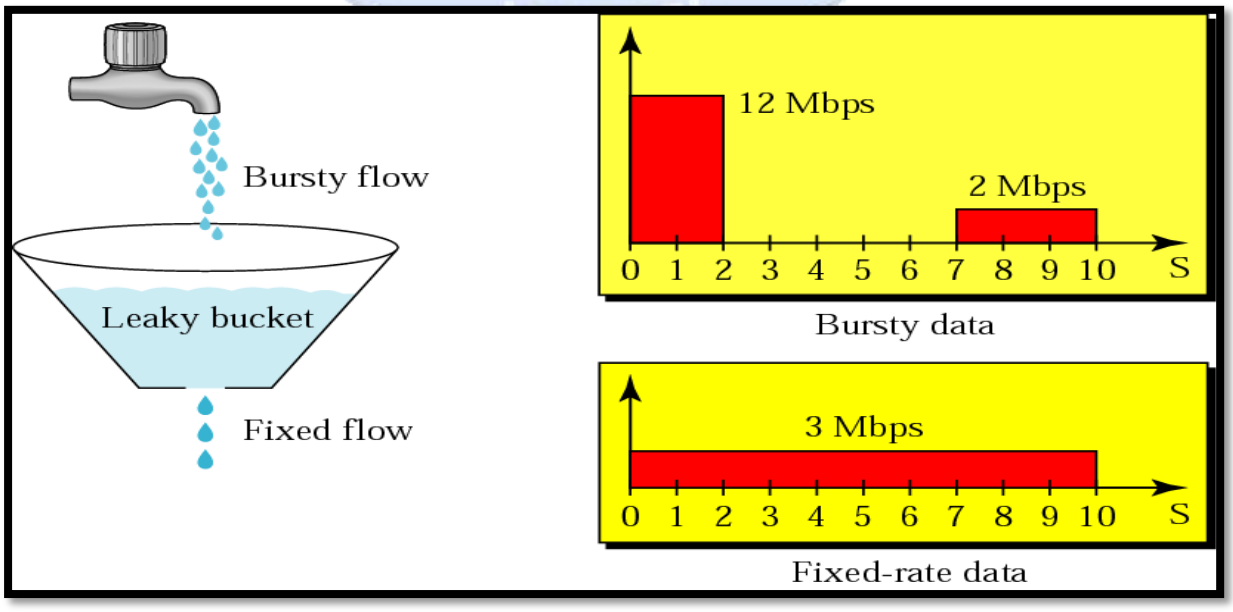
OR

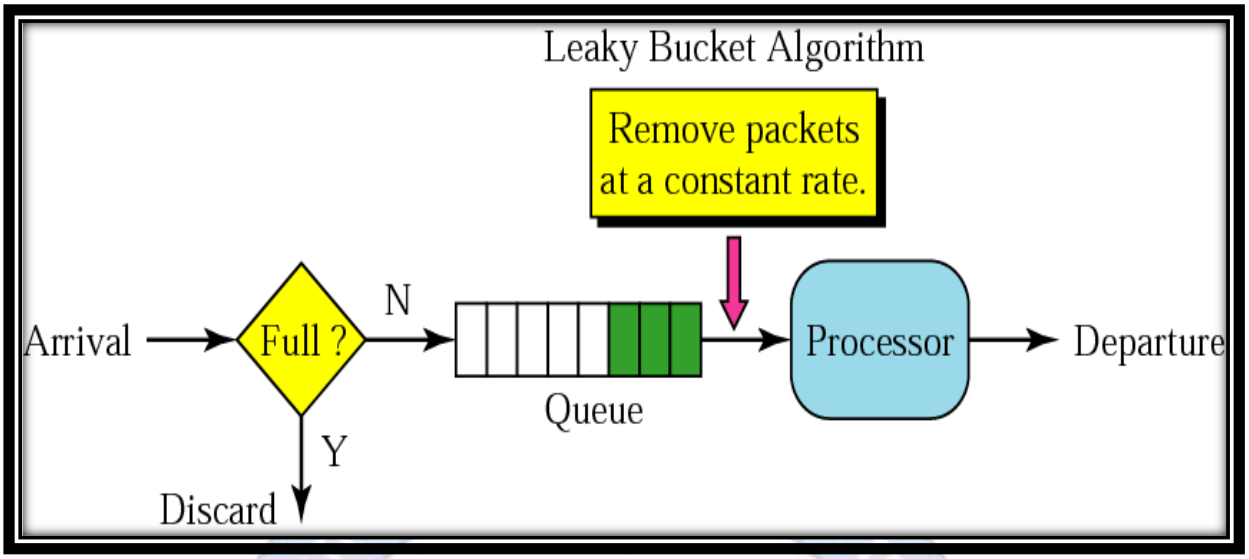
Q. Explain Leaky Bucket Algorithm.

Q. Explain Token bucket Algorithm.

Ans:

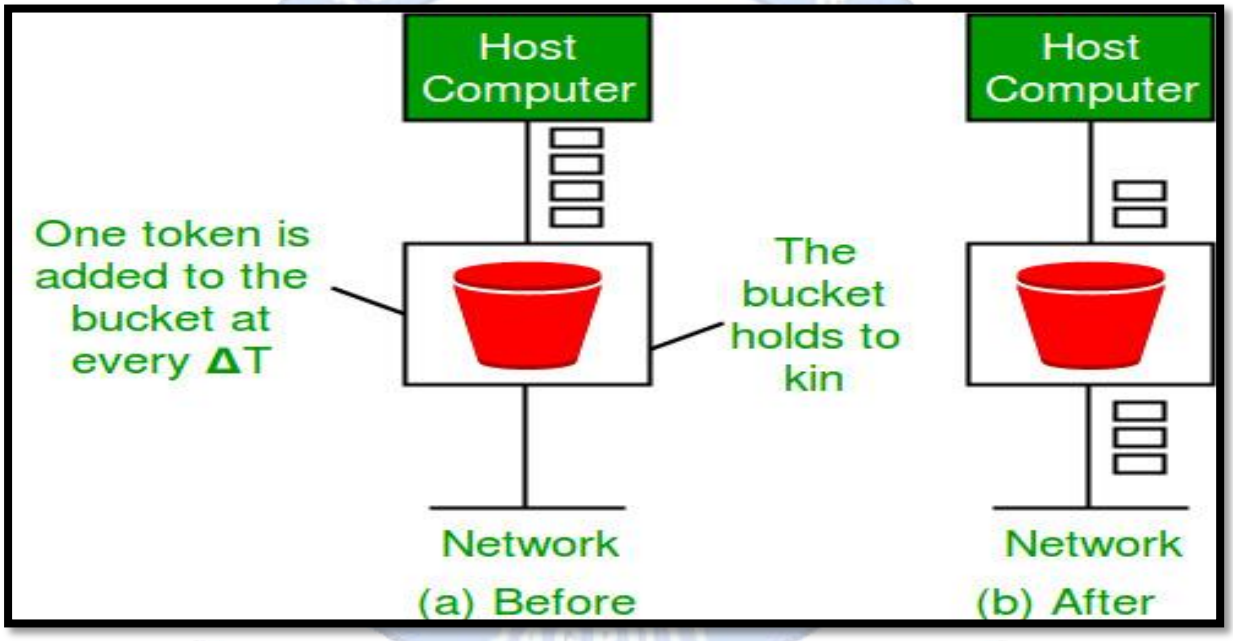
- A **state occurring in network layer** when the **message traffic is so heavy** that it **slows down network response time**.
- **Effects of Congestion:**
  - As delay increases, performance decreases.
  - If delay increases, retransmission occurs, making situation worse.
- **Congestion control algorithms:**
  - Leaky Bucket Algorithm
  - Token bucket Algorithm
- **Leaky Bucket Algorithm:**
  - The leaky bucket algorithm discovers its use in the **context of network traffic shaping or rate-limiting.**
  - A leaky bucket execution and a token bucket execution are predominantly used for traffic shaping algorithms.
  - This algorithm is used to control the rate at which traffic is sent to the network and shape the burst traffic to a steady traffic stream.
  - The **disadvantages** compared with the leaky-bucket algorithm are the **inefficient use of available network resources**.
  - The large area of network resources such as **bandwidth is not being used effectively.**

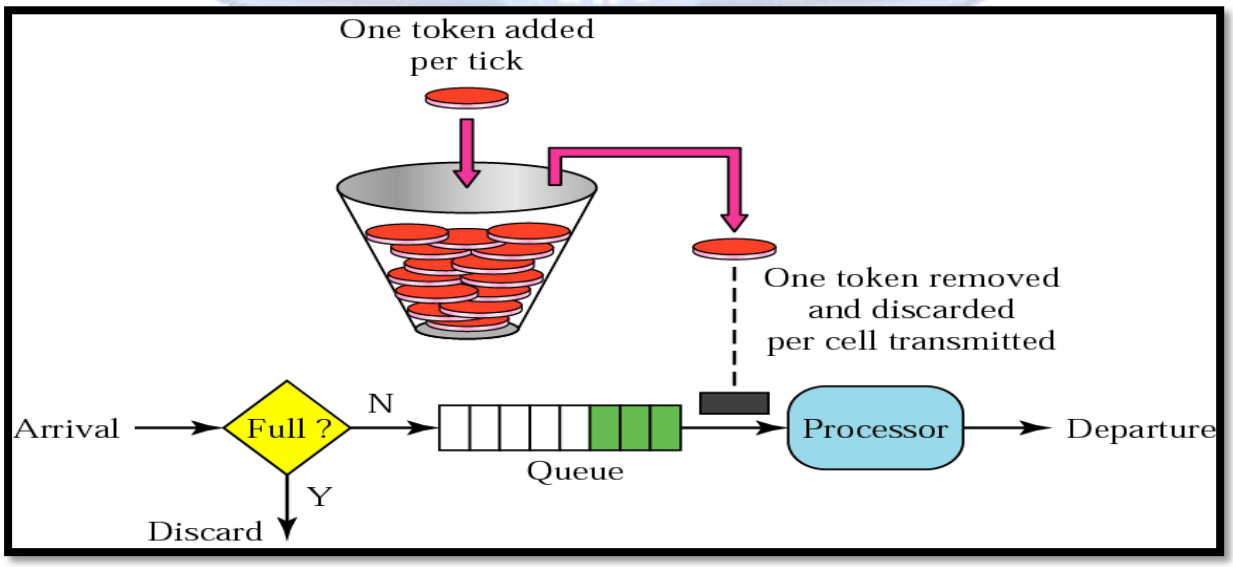




- **Steps are involved in leaky bucket algorithm:**
  - When **host** wants to **send packet, packet is thrown into the bucket**.
  - The bucket leaks at a **constant rate**, meaning the network interface transmits packets at a constant rate.
  - **Bursty traffic** is **converted to a uniform traffic** by the **leaky bucket**.
  - In practice the bucket is a **finite queue** that **outputs at a finite rate**.

- **Token bucket Algorithm**
  - The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is.
  - So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost.
  - One such algorithm is token bucket algorithm.
- **Steps of this algorithm can be described as follows:**
  - In regular intervals tokens are thrown into the bucket. *f*
  - The bucket has a maximum capacity. *f*
  - If there is a ready packet, a token is removed from the bucket, and the packet is send.
  - If there is no token in the bucket, the packet cannot be send.





- **Let's understand with an example,**
  - **In figure (A)** we see a bucket holding three tokens, with five packets waiting to be transmitted.
  - For a packet to be transmitted, it must capture and destroy one token.
  - **In figure (B)** We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

- **Formula:**

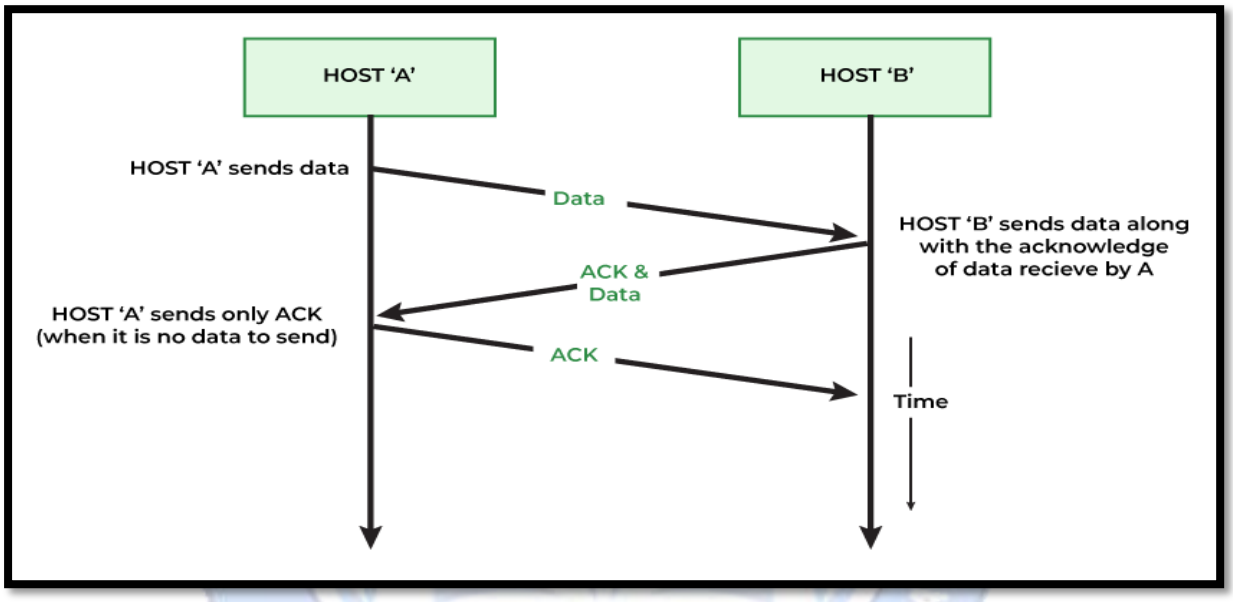
$$M * s = C + \rho * s$$

  - Where,
    - **S –** is time taken
    - **M –** Maximum output rate
    - **ρ –** Token arrival rate
    - **C –** Capacity of the token bucket in byte

34. Write a short note: Piggybacking.

Ans:

- **Piggybacking** is a **process of attaching acknowledgment with the data packet to be sent.**
- It is an **efficient solution** for **reducing the bandwidth utilization** of the **network.**
- TCP is a **full-duplex communication protocol**, so piggybacking is used to transmit packets.

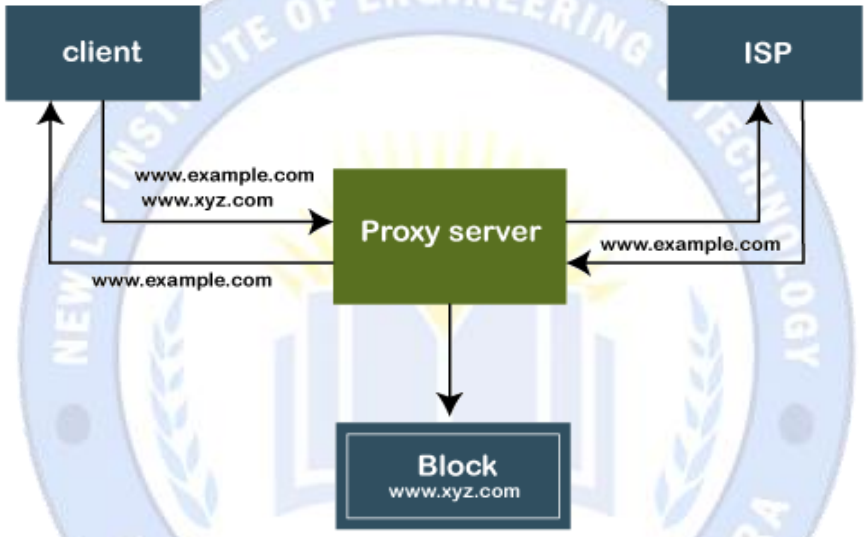


- As we can see in the figure, we can see with piggybacking, **a single message (ACK + DATA) over the wire in place of two separate messages**.
- Piggybacking **improves the efficiency of the bidirectional** protocols.
    - If **Host A** has **both acknowledgment and data**, which **it wants to send**, then the data frame will be sent with the ack field which contains the **sequence number of the frame**.
    - If **Host A contains only one acknowledgment**, then it will **wait for some time**, then in the case, if it finds any data frame, it piggybacks the acknowledgment, otherwise, **it will send the ACK frame**.
    - If **Host A left with only a data frame**, then it will **add the last acknowledgment** to it. **Host A** can **send a data frame with an ack field containing no acknowledgment bit.**

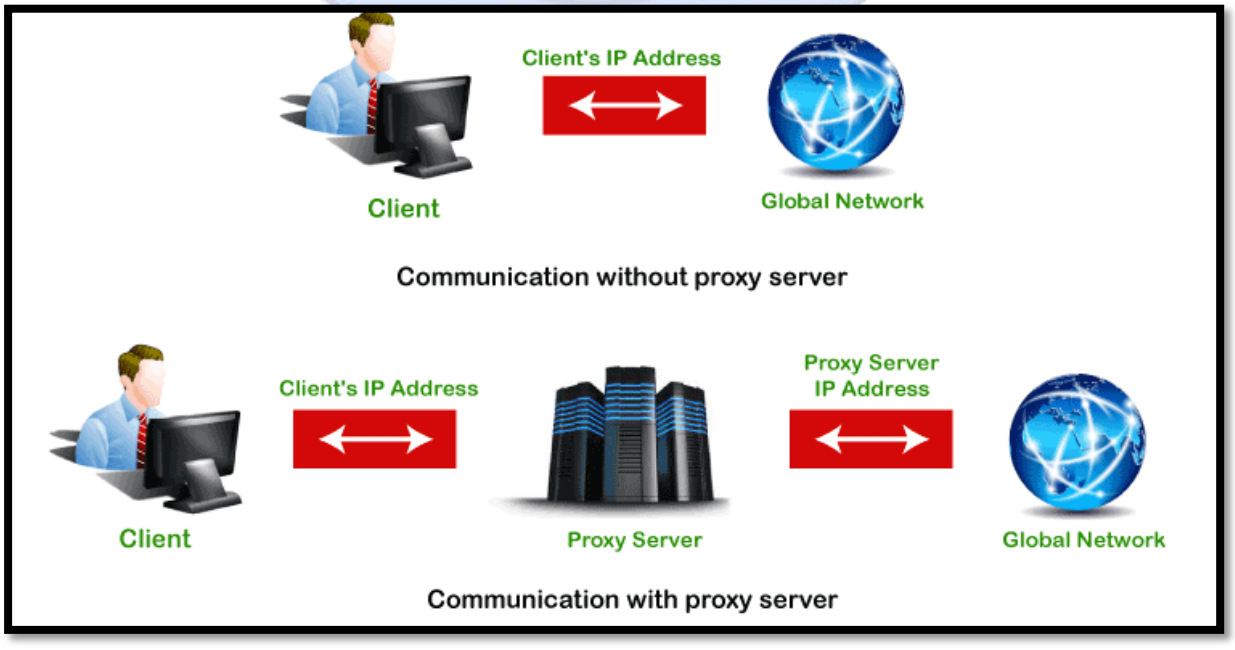
35. Write a short note: Proxy Server.

Ans:

- The **proxy server is a computer on the internet that accepts the incoming requests from the client and forwards** those **requests to the destination server**.
- It **works as a gateway between** the **end-user and the internet**.
- It has **its own IP address**.
- It **separates** the **client system and web server** from the **global network**.



Mechanism of Proxy Server



- If the requested data or page already exists in the local cache, the proxy server itself provides the required retrieval to the client.
- If the requested data or page does not exist in the local cache, the proxy server forwards that request to the destination server.
- The proxy servers transfer the replies to the client and also being cached to them.
- **Need of Proxy Server**
  - It reduces the chances of data breaches.
  - It adds a subsidiary layer of security between server and outside traffic.
  - It also protects from hackers.
  - It filters the requests.
- **Advantages of Proxy Server:**
  - It improves the security and enhances the privacy of the user.
  - It hides the identity (IP address) of the user.
  - It controls the traffic and prevents crashes.
  - Also, saves bandwidth by caching files and compressing incoming traffic.
  - Protect our network from malware.
  - Allows access to the restricted content.

36. Difference Between:

a. **Stop and Wait Protocol and Sliding Window Protocols.**
b. **GO-BACK-N and Selective Reject / Selective Repeat ARQ**
c. **Stop and Wait, Go-Back-N and Selective Repeat**
d. **Leaky Bucket and Token Bucket**
e. **Flow Control and Congestion Control**

Ans:

a. **Stop and Wait Protocol and Sliding Window Protocols.**

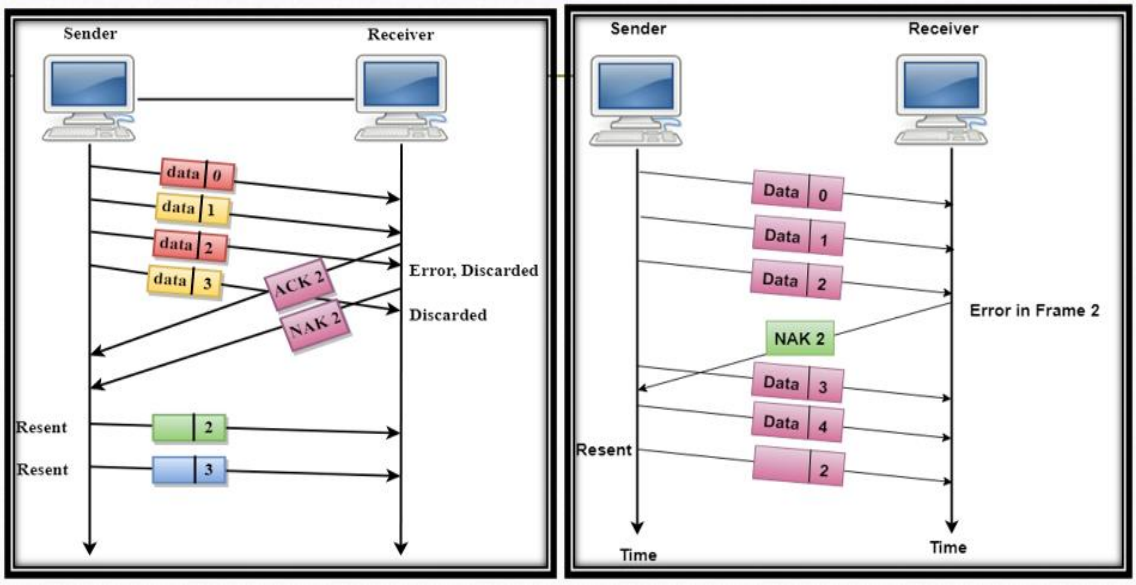
BASIS FOR COMPARISON	STOP-AND-WAIT PROTOCOL	SLIDING WINDOW PROTOCOL
Behaviour	Request and reply	Simultaneous transmit
Number of transferrable frames	Only one	Multiple
Efficiency	Less	More comparatively
Acknowledgement	Sent after each arriving packet	Window of acknowledgement is maintained
Type of transmission	Half duplex	Full duplex
Propagation delay	Long	Short
Link utilisation	Poor	Better

b. **GO-BACK-N and Selective Reject / Selective Repeat ARQ**

BASIS FOR COMPARISON	GO-BACK-N	SELECTIVE REPEAT
Basic	Retransmits all the frames that sent after the frame which suspects to be damaged or lost.	Retransmits only those frames that are suspected to lost or damaged.
Bandwidth Utilization	If error rate is high, it wastes a lot of bandwidth.	Comparatively less bandwidth is wasted in retransmitting.
Complexity	Less complicated.	More complex.
Window size	N-1	<= (N+1)/2
Sorting	Sorting is neither required at sender side nor at receiver side.	Receiver must be able to sort as it has to maintain the sequence of the frames.

BASIS FOR COMPARISON	GO-BACK-N	SELECTIVE REPEAT
Searching	No searching of frame is required neither on sender side nor on receiver	The sender must be able to search and select only the requested frame.
ACK Numbers	NAK number refer to the next expected frame number.	NAK number refer to the frame lost.
Use	It more often used.	It is less in practice because of its complexity.

GO-BACK-N	SELECTIVE REPEAT



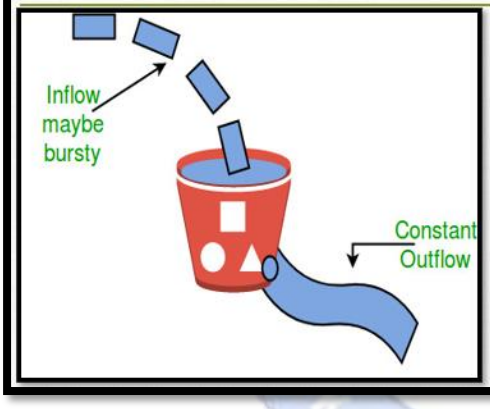
c. Stop and Wait, Go-Back-N and Selective Repeat

PROPERTIES	STOP AND WAIT	GO-BACK-N	SELECTIVE REPEAT
Sender window size	1	N	N
Receiver Window size	1	1	N
Minimum Sequence number	2	N+1	2N
Efficiency	1/(1+2*a)	N/(1+2*a)	N/(1+2*a)
Type of Acknowledgement	Individual	Cumulative	Individual
Supported order at Receiving end	–	In-order delivery only	Out-of-order delivery as well

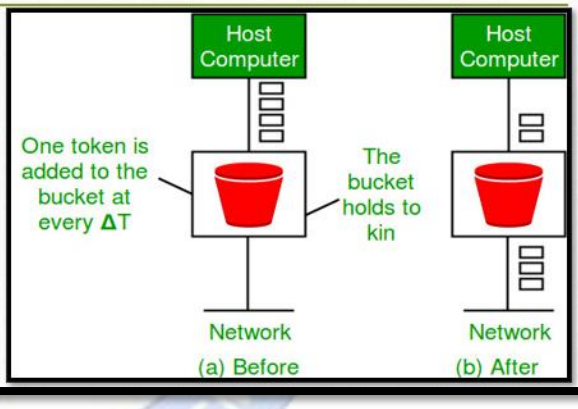
d. Leaky Bucket and Token Bucket

BASIS FOR COMPARISON	Leaky Bucket	Token Bucket
Basic	A leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full.	The token bucket allows bursty traffic at a regulated maximum rate.
Token	Independent	Dependent
If Bucket is Full	Packet or Data is Discarded	Token are Discarded But Not the Packet.
Sends The Packets	Average Rate	Faster
Save Token	No	Yes

- **Leaky Bucket:**



- **Token Bucket:**



e. Flow Control and Congestion Control

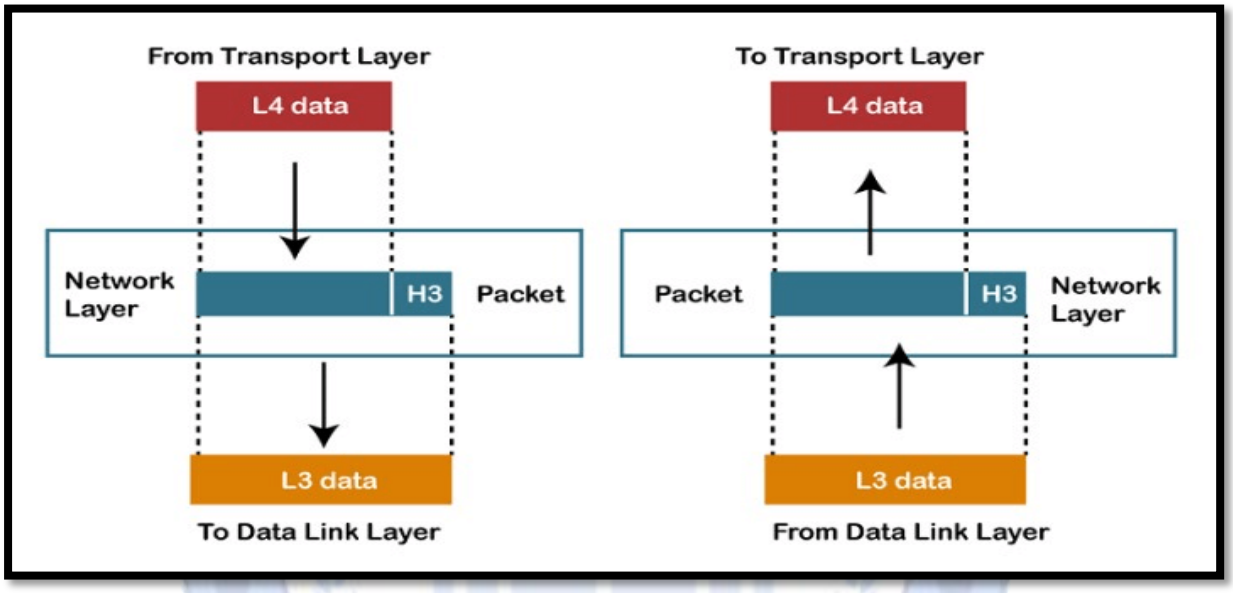
BASIS FOR COMPARISON	FLOW CONTROL	CONGESTION CONTROL
Basic	It controls the traffic from a particular sender to a receiver.	It controls the traffic entering the network.
Purpose	It prevents the receiver from being overwhelmed by the data.	It prevents the network from getting congested.
Responsibility	Data Link Layer and Transport Layer.	Network Layer and Transport Layer.
Responsible	The sender is responsible for transmitting extra traffic at receivers side.	The transport layer is responsible transmitting extra traffic into the network.
Preventive measures	The sender transmits the data slowly to the receiver.	Transport layer transmits the data into the network slowly.
Methods	Feedback-based flow control and Rate-based flow control	Provisioning, traffic-aware routing and admission control

Unit - 4 Network Layer

37. Explain Functions of Network Layer.

Ans:

- **Network Layer:**

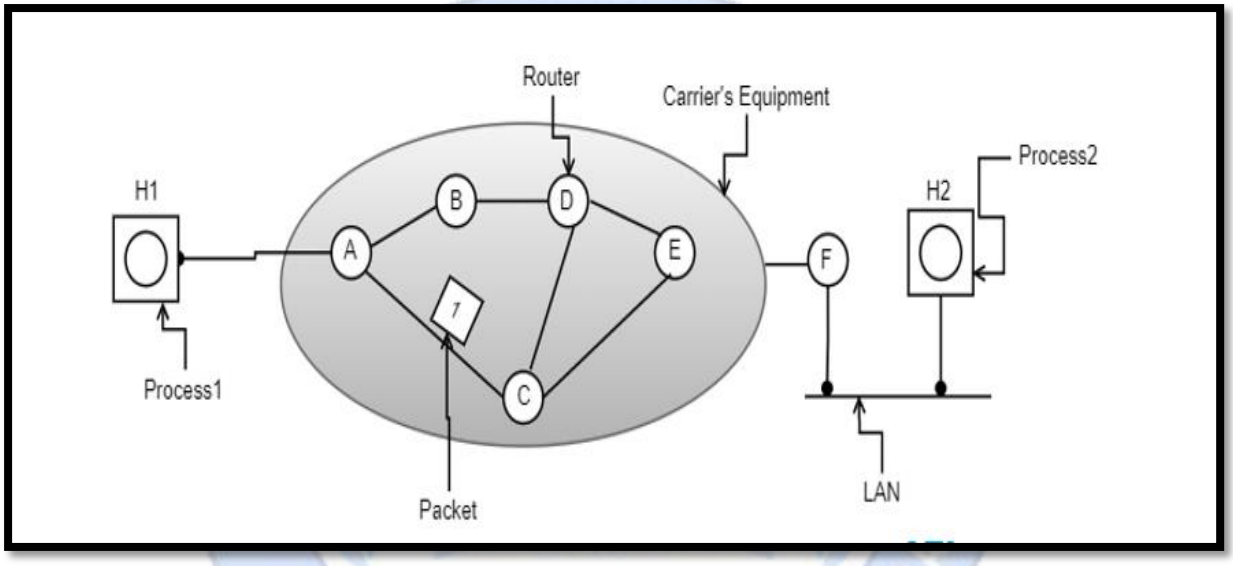


- The **Network Layer** is responsible for **facilitating data transfer between two different networks.**
- If the two devices communicating are on the same network, then the network layer is **unnecessary.**
- The network layer **breaks up segments from the transport layer into smaller units**, called **packets**, on the sender's device, and reassembling these packets on the receiving device.
- **Addressing:**
  - Maintains both the source and destination addresses at the frame header.
  - The network layer performs addressing to find out the specific devices on the network.
- **Packetizing:**
  - The network layer works on the conversion of packets those received from its upper layer.
  - This feature is accomplished by Internet Protocol (IP).
- **Routing:**
  - Being considered as the major functionality, the network layer chooses the best path for data transmission from a source point to the destination.
- **Internetworking:**
  - Internetworking works to deliver a logical connection across multiple devices.

38. Explain Network Layer Design Issues.

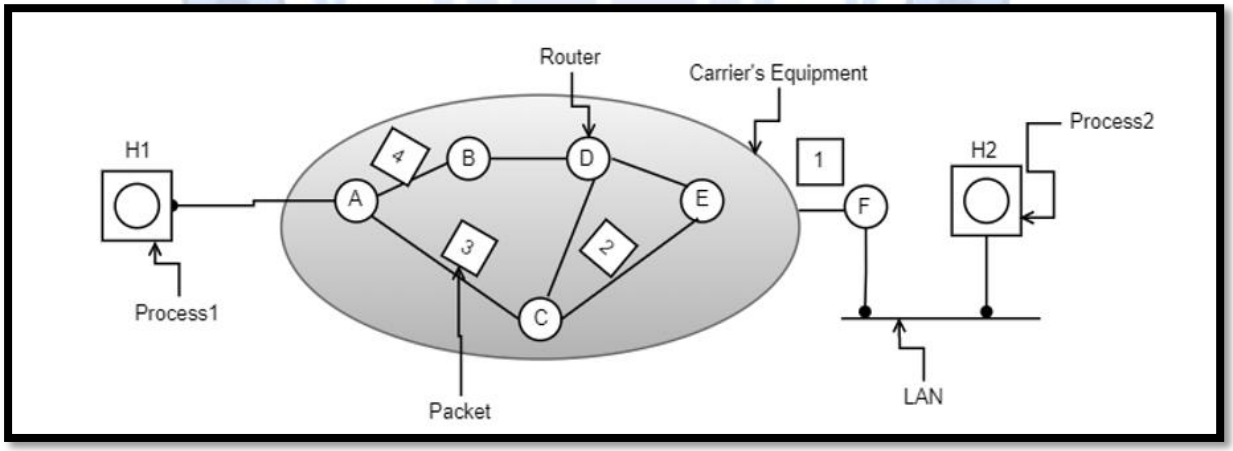
Ans:

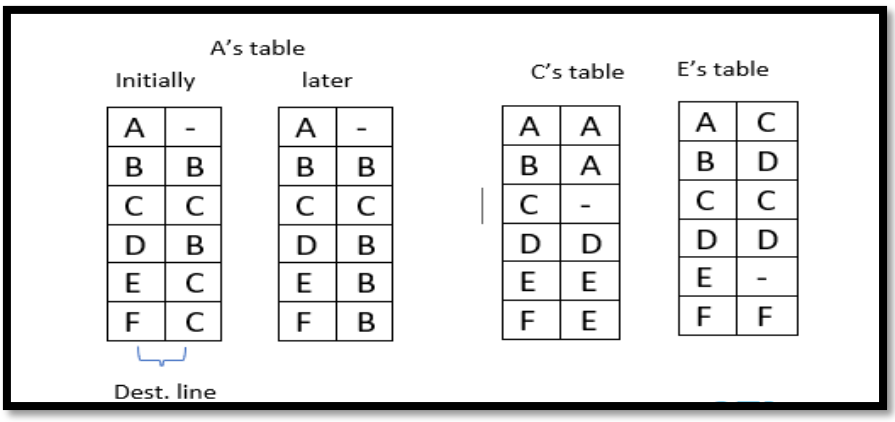
- **Network Layer Design Issues:**
  - Store-and-Forward Packet Switching
  - Services Provided to the Transport Layer
  - Implementation of Connectionless Service
  - Implementation of Connection-Oriented Service
- **Store-and-Forward Packet Switching**



  - Here, the foremost elements are the carrier's equipment (the connection between routers through transmission lines) and the customer's equipment.
  - H1 has a direct connection with carrier router 'A', while H2 is connected to carrier router 'F' on a LAN connection.
  - One of the carrier router 'F', is pointed outside the carrier's equipment as it does not come under the carrier, whereas considered as protocols, software, and construction.
  - This switching network performs as Transmission of data happens when the host (H1) with a packet transfers it to the nearby router through LAN (or) point-to-point connection to the carrier.
  - The carrier stores the packet until it completely arrives thus confirms the checksum.
  - Then after, the packet is transmitted over the path until H2 is reached.

- **Services Provided to the Transport Layer**
  - Through the network/transport layer interface, the network layer delivers its services to the transport layer.
  - Services offered by the network layer are outlined considering few objectives. Those are:
  - Offering services must not depend on router technology
  - The transport layer needs to be protected from type, number and the topology of the available routers.
  - Network addressing the transport layer needs to follow a consistent numbering scenario also at LAN and WAN connections.
  - **Connectionless:**
    - Here, routing and insertion of packets into subnet is accomplished individually. No additional setup is necessary
  - **Connection-Oriented:**
    - Subnet must offer reliable service and all the packets are transmitted over a single route.
- **Implementation of Connectionless Service:**
  - In this scenario, packets are termed as datagrams and the corresponding subnet is termed as datagram subnet.
  - Routing in datagram subnet is as follows:





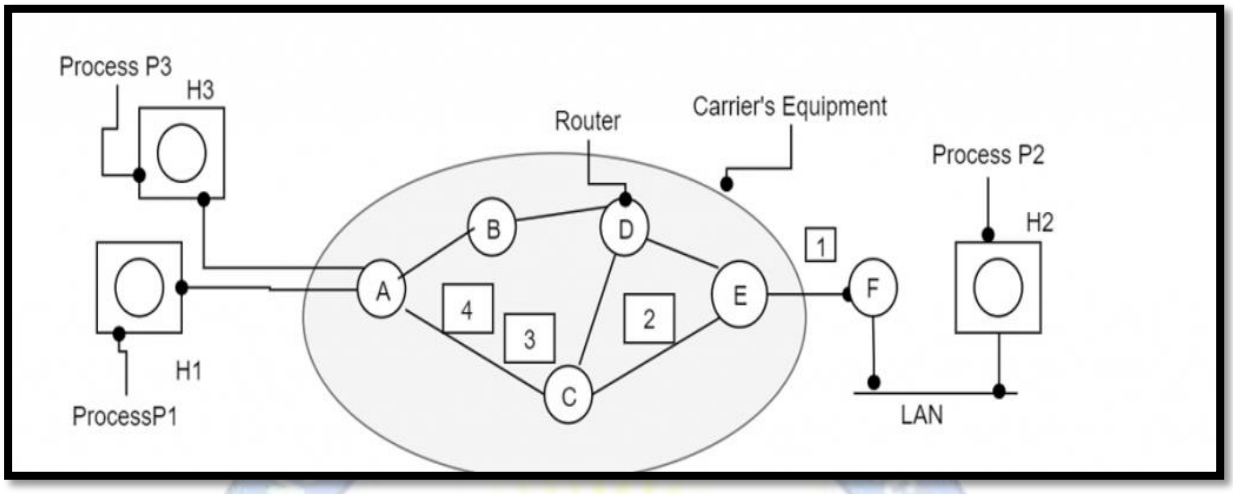
A	-
B	B
C	C
D	B
E	C
F	C

A	-
B	B
C	C
D	B
E	B
F	B

A	A
B	A
C	-
D	D
E	E
F	E

A	C
B	D
C	C
D	D
E	-
F	F

- **Implementation of Connection-Oriented Service**
  - The below diagram shows the routing algorithm in the virtual subnet.

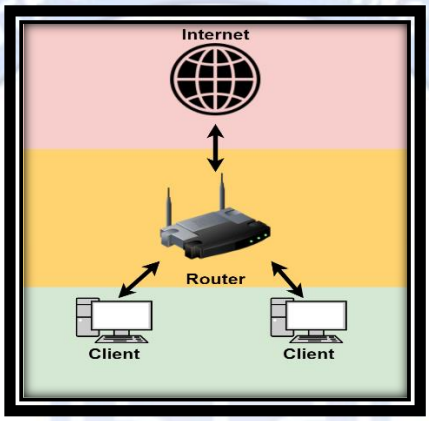


  - Here, the functionality of connection-oriented service works on the virtual subnet.
  - A virtual subnet performs the operation of avoiding a new path for each packet transmission.
  - As a substitute for this, when there forms a connection, a route from a source node to a destination node is selected and maintained in tables.
  - This route performs its action at the time of traffic congestion.
  - At the time when the connection is released, the virtual subnet also gets dismissed.
  - In this service, every packet carries its own identifier that states the exact address of the virtual circuit.

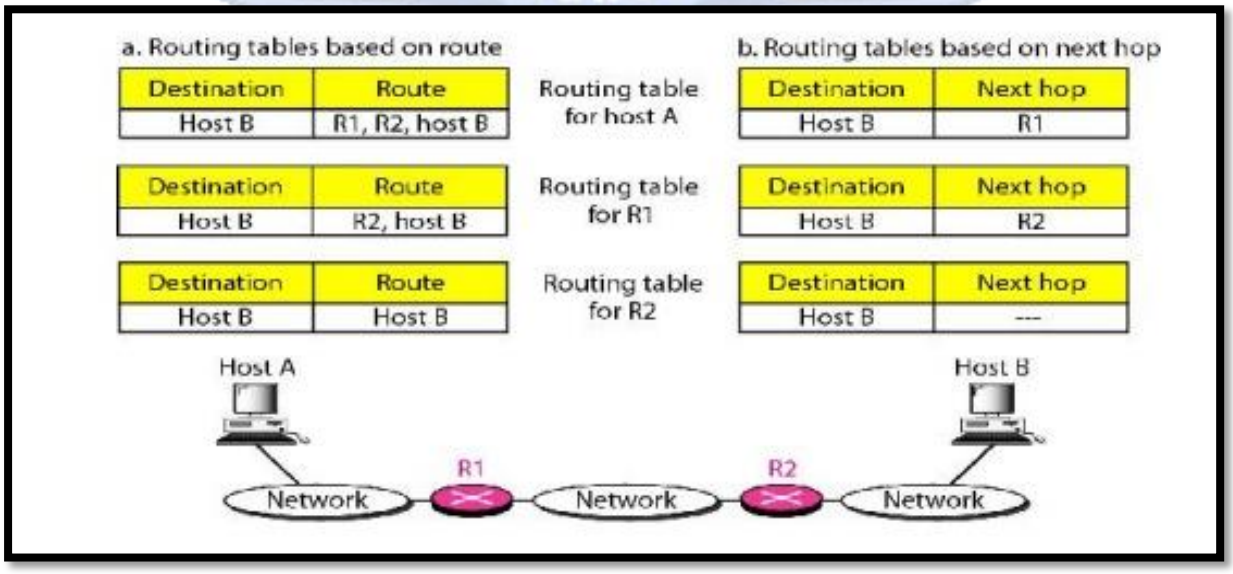
39. What is Packet Forwarding? Explain Packet Forwarding Techniques.

Ans:

- **Forwarding** is the **process of collecting data from one device and sending it to another device.**
- This process differs from routing because it doesn't manage moving data from one device to another.
- Forwarding means to place the packet in its route to its destination.
- Forwarding requires a host or a router to have a **routing table.**

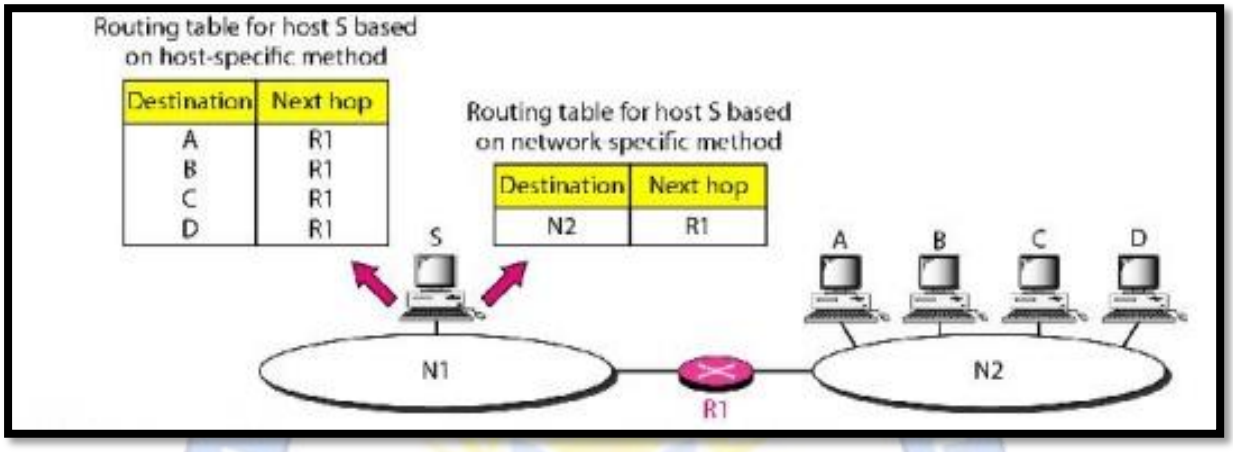


- **Packet Forwarding Techniques:**
  - Next-Hop Method versus Route Method
  - Network-Specific Method versus Host-Specific Method
  - Default Method
- **Next-Hop Method versus Route Method:**



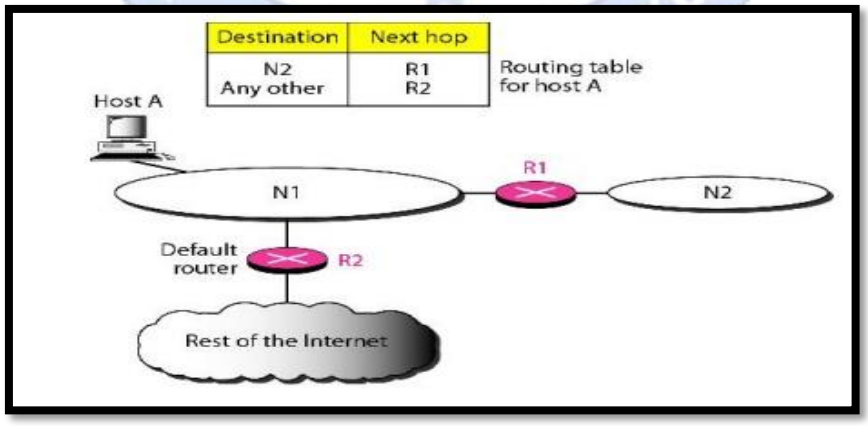
- One technique to reduce the contents of a routing table is called the next-hop method.
- In this technique, the routing table holds only the address of the next hop instead of information about the complete route (route method).
- The entries of a routing table must be consistent with one another.

- **Network-Specific Method versus Host-Specific Method:**



- A second technique to reduce the routing table and simplify the searching process is called the network-specific method.
- Here, instead of having an entry for every destination host connected to the same physical network (host-specific method), we have only one entry that defines the address of the destination network itself.
- Host-specific routing is used for purposes such as checking the route or providing security measures.

- **Default Method:**

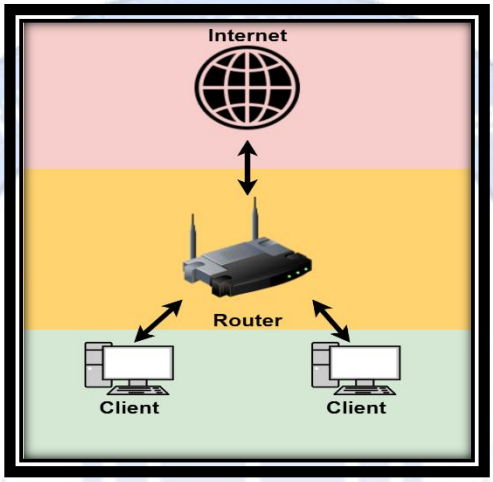


- Another technique to simplify routing is called the default method.
- Host A is connected to a network with two routers.
- Router R1 routes the packets to hosts connected to network N2.
- However, for the rest of the Internet, router R2 is used. So instead of listing all networks in the entire Internet, host A can just have one entry called the default (normally defined as network address 0.0.0.0).

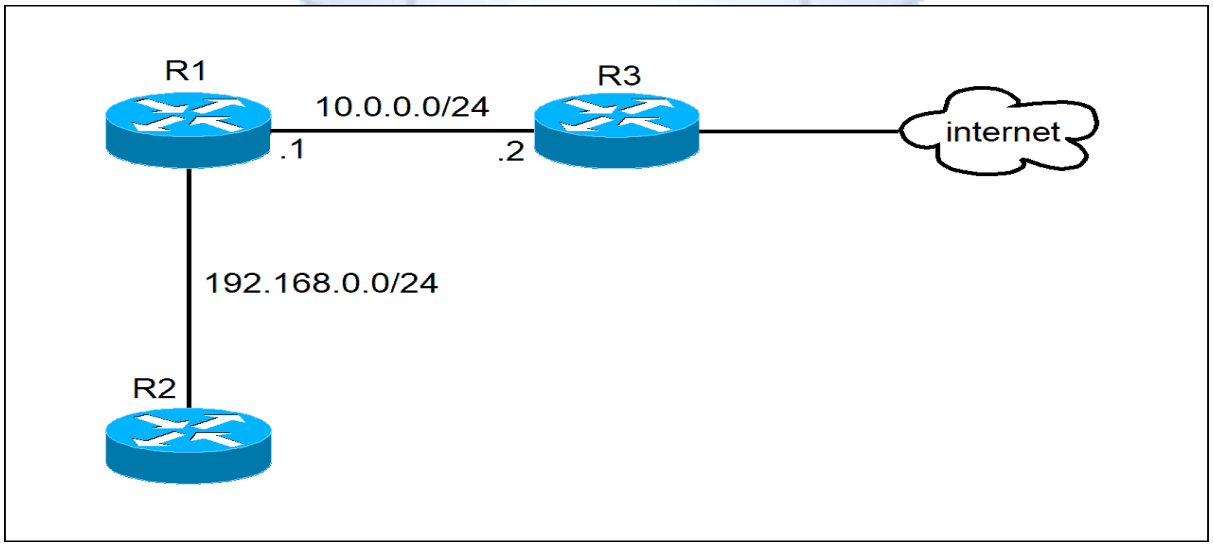
40. What is Routing? Explain Types of Routing.

Ans:

- A Router is a **process of selecting path along which the data can be transferred from source to the destination.**
- Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.

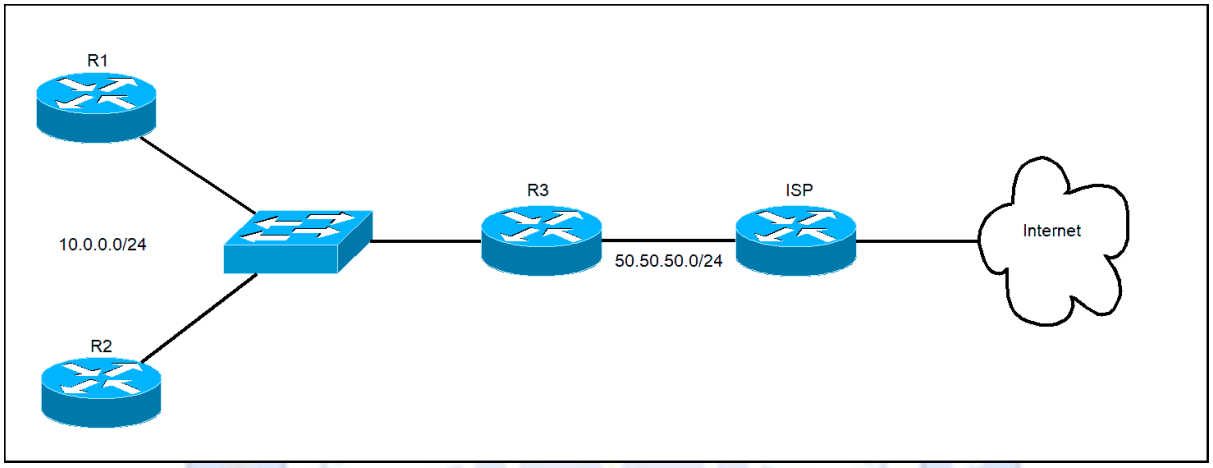


- **Types of Routing:**
  - Routing can be classified into three categories:
    - Static Routing
    - Default Routing
    - Dynamic Routing
- **Static Routing:**



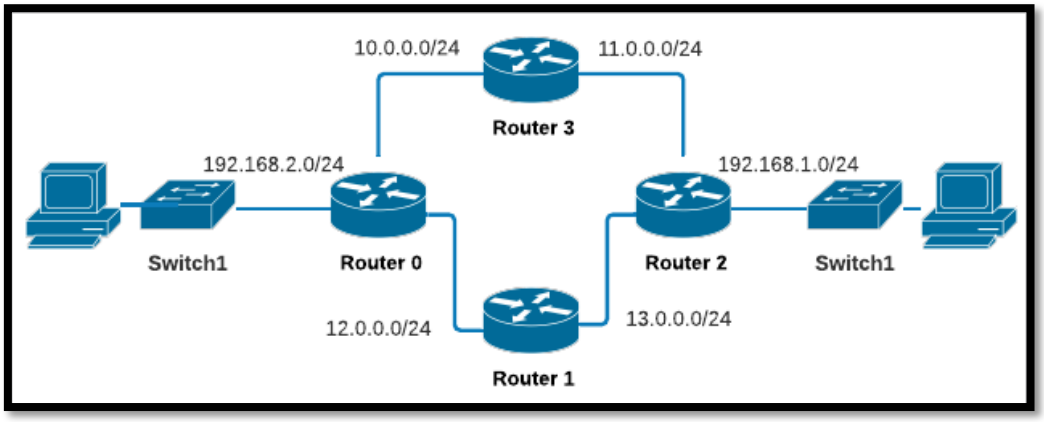
- Static Routing is also known as Nonadaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the condition or topology of the networks

- **Default Routing:**



- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not.
- A Packet is transmitted to the device for which it is configured in default routing.
- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.
- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route.
- The default route is chosen only when a specific route is not mentioned in the routing table.

- **Dynamic Routing:**

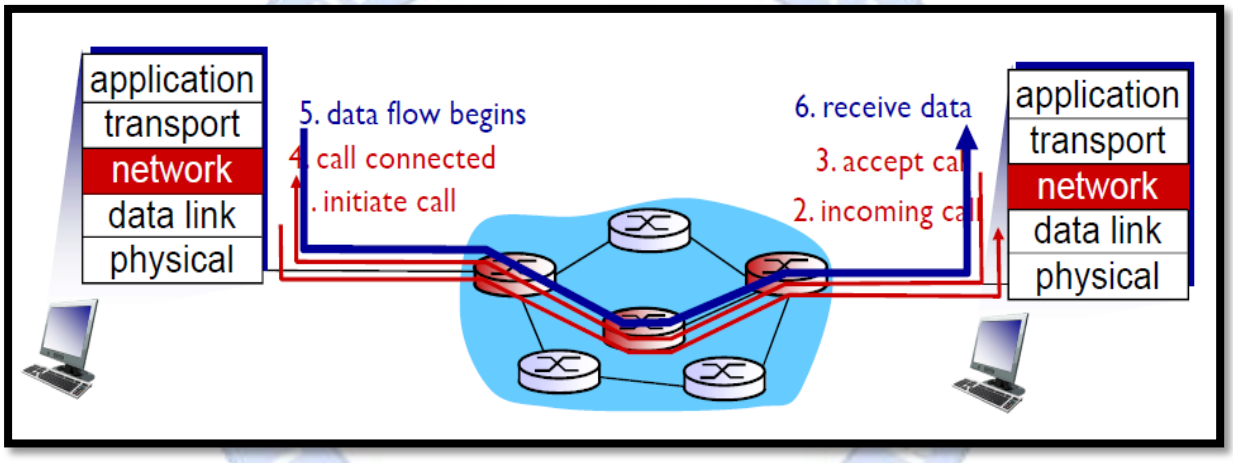


- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

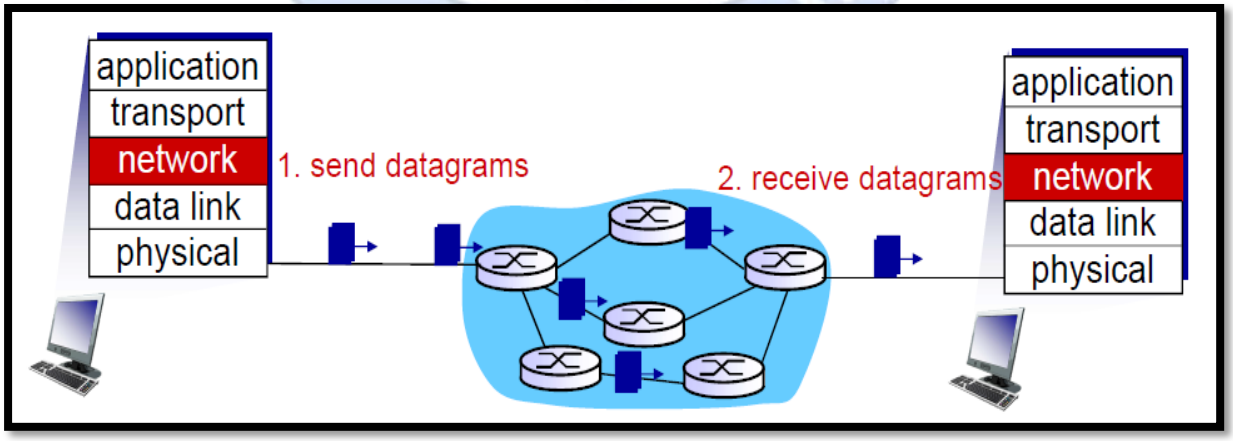
41. Write a short note: Network Service Models.

Ans:

- The **network-service model** defines the characteristics of end-to-end transport of data between one "edge" of the network and the other, that is, between sending and receiving end systems.
- **Network Service Models:**
  - Virtual-circuit service model
  - Datagram service model
- **Virtual-circuit service model**



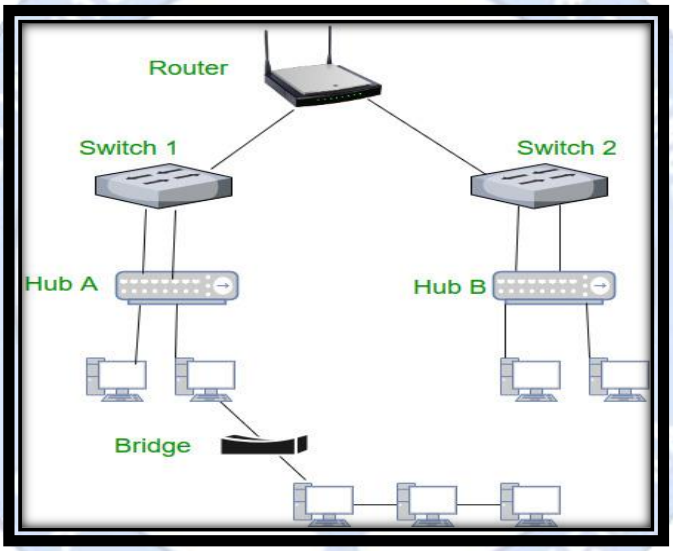
- **Datagram service model**



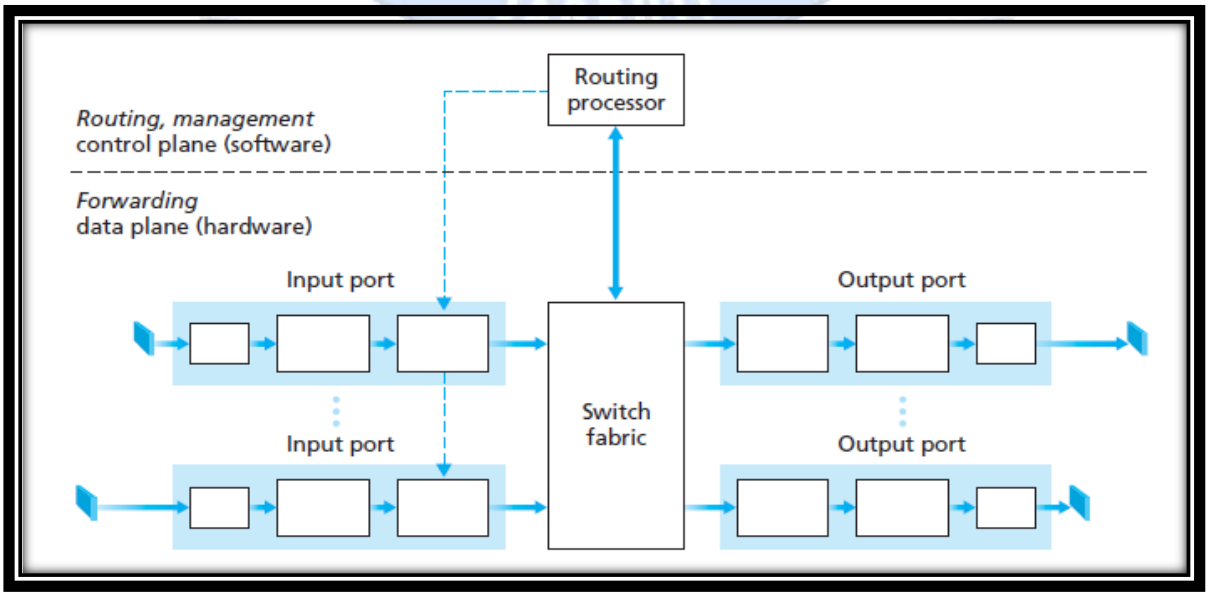
42. Draw and explain Router Architecture.

Ans:

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



- **Router Architecture:**



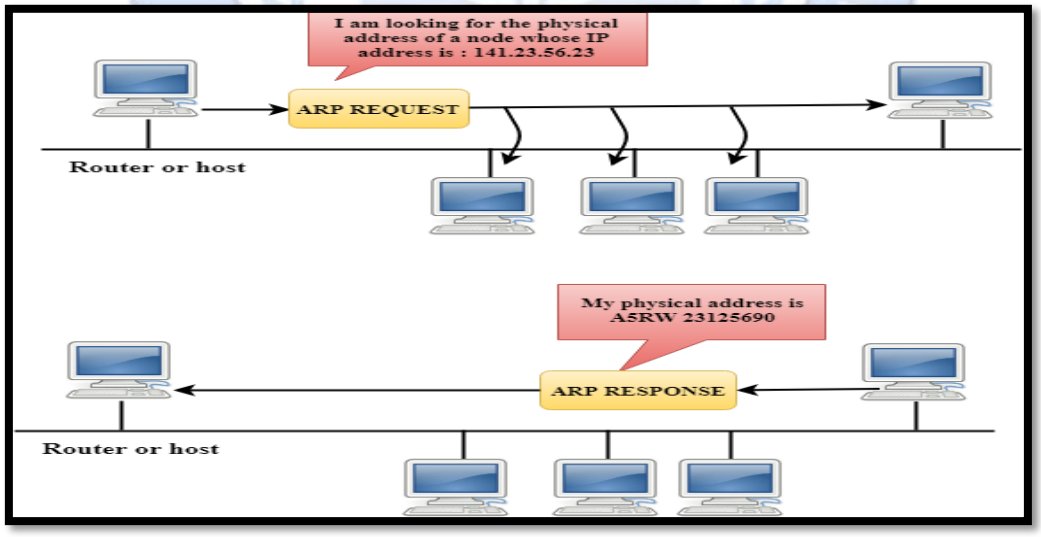
43. List out Network Layer Protocols. Explain ARP and RARP.

OR

Q. Explain Physical addresses and Logical addresses.

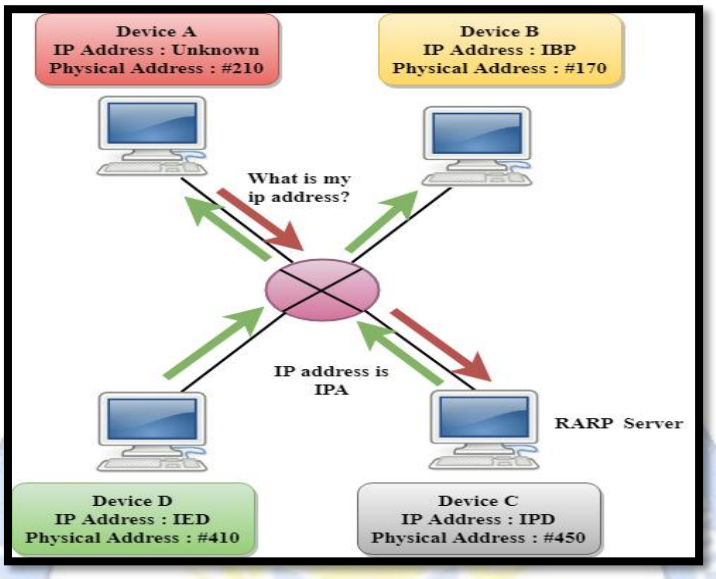
Ans:

- **ARP:**
  - ARP stands for **Address Resolution Protocol.**
  - It is used to associate an IP address with the MAC address.
  - Each device on the network is recognized by the MAC address imprinted on the NIC.
  - Therefore, we can say that devices need the MAC address for communication on a local area network.
  - MAC address can be changed easily.
- **MAC address:**
  - The MAC address is used to identify the actual device.
- **IP address:**
  - It is an address used to locate a device on the network.



- If the host wants to know the physical address of another host on its network, then it sends an ARP query packet that includes the IP address and broadcast it over the network.
- Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes the IP address and sends back the physical address.
- The host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends back to the sender.

- **RARP:**



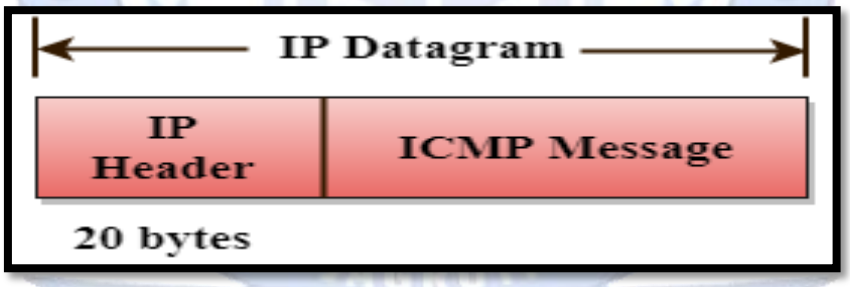
- RARP stands for **Reverse Address Resolution Protocol**.
- If the host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network.
- A RARP server on the network recognizes the RARP packet and responds back with the host IP address.
- The protocol which is used to obtain the IP address from a server is known as **Reverse Address Resolution Protocol**.
- The message format of the RARP protocol is similar to the ARP protocol.
- Like ARP frame, RARP frame is sent from one machine to another encapsulated in the data portion of a frame.

44. Write a short note: ICMP and IGMP.

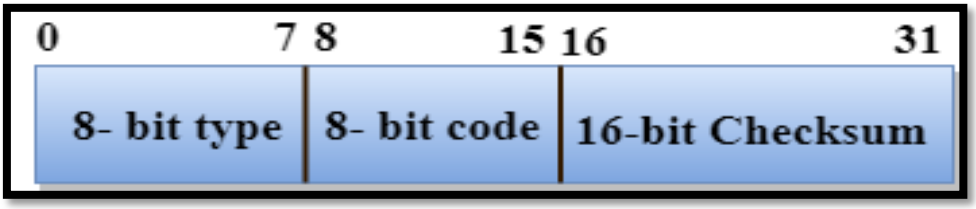
Ans:

- **ICMP:**
  - ICMP stands for **Internet Control Message Protocol.**
  - The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender.
  - ICMP uses echo test/reply to check whether the destination is reachable and responding.
  - ICMP handles both control and error messages, but its main function is to report the error but not to correct them.
  - An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which it has been passed.
  - Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.
  - ICMP protocol communicates the error messages to the sender.
  - ICMP messages cause the errors to be returned back to the user processes.

  - **ICMP messages are transmitted within IP datagram.**

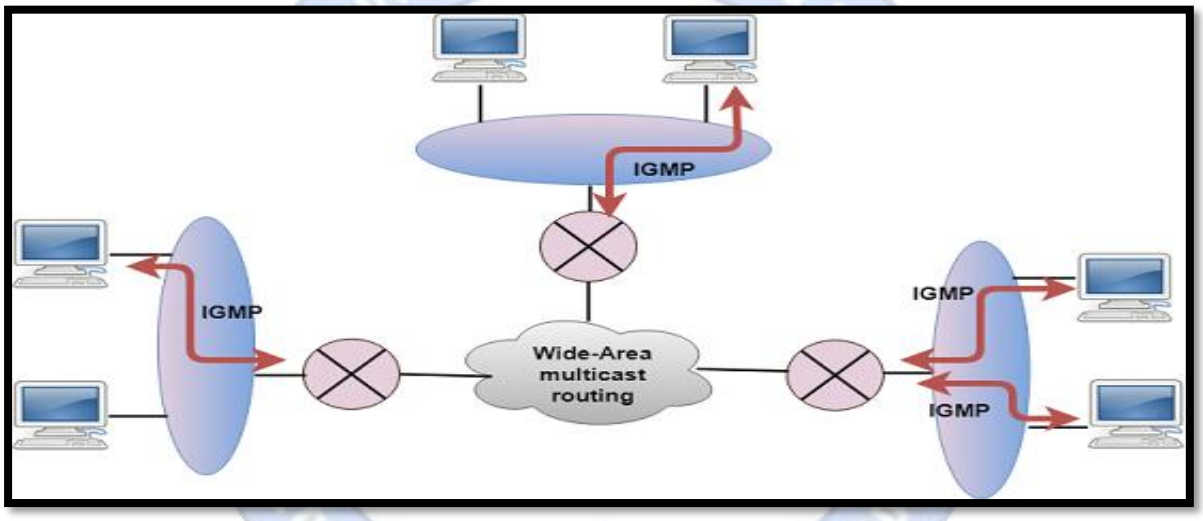


  - **The Format of an ICMP message:**

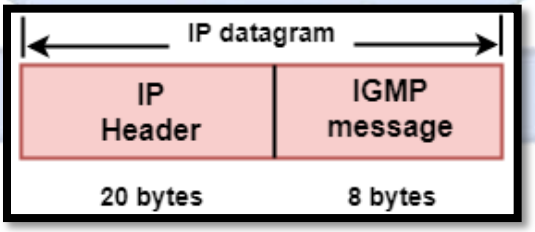


    - The first field specifies the type of the message.
    - The second field specifies the reason for a particular message type.
    - The checksum field covers the entire ICMP message.

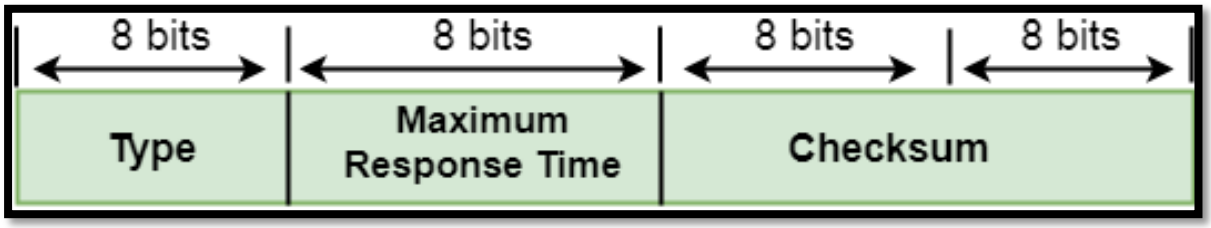
- **IGMP:**
  - IGMP stands for **Internet Group Message Protocol**.
  - The IP protocol supports two types of communication:
    - **Unicasting:** It is a communication between one sender and one receiver. Therefore, we can say that it is one-to-one communication.
    - **Multicasting:** Sometimes the sender wants to send the same message to a large number of receivers simultaneously. This process is known as multicasting which has one-to-many communication.
  - The IGMP protocol is used by the hosts and router to support multicasting.
  - The IGMP protocol is used by the hosts and router to identify the hosts in a LAN that are the members of a group.



- IGMP is a part of the IP layer, and IGMP has a fixed-size message.
- **The IGMP message is encapsulated within an IP datagram.**



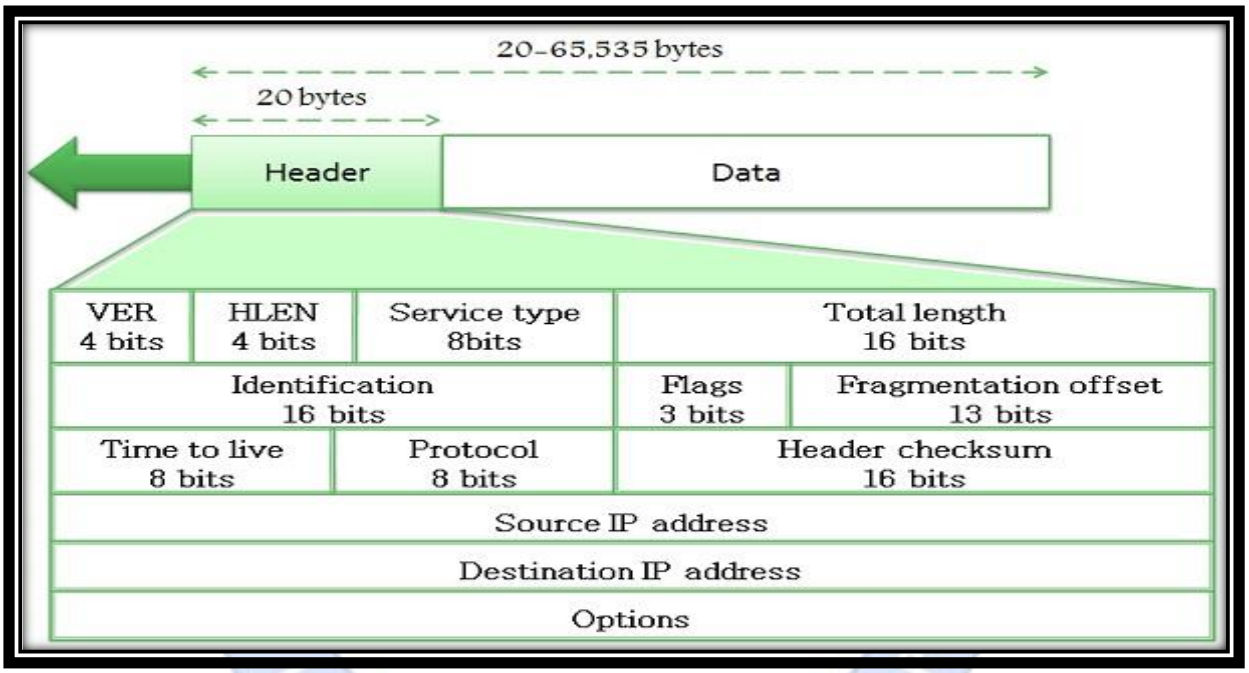
- **The Format of an IGMP message**



45. Draw and explain IPv4 Datagram Header.

Ans:

- **IP** stands for **Internet Protocol** and **v4** stands for **Version Four** (IPv4).
- IP version four addresses are 32-bit integers which will be expressed in decimal notation.
- **IPv4 Datagram Header**: Size of the header is 20 to 60 bytes.
- Example: 192.0.2.126 could be an IPv4 address.



- **VERSION:**
  - Version of the IP protocol (4 bits), which is 4 for IPv4
- **HLEN:**
  - IP header length (4 bits), which is the number of 32 bit words in the header.
  - The minimum value for this field is 5 and the maximum is 15
- **Type of service:**
  - Low Delay, High Throughput, Reliability (8 bits)
- **Total Length:**
  - Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes
- **Identification:**
  - Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)

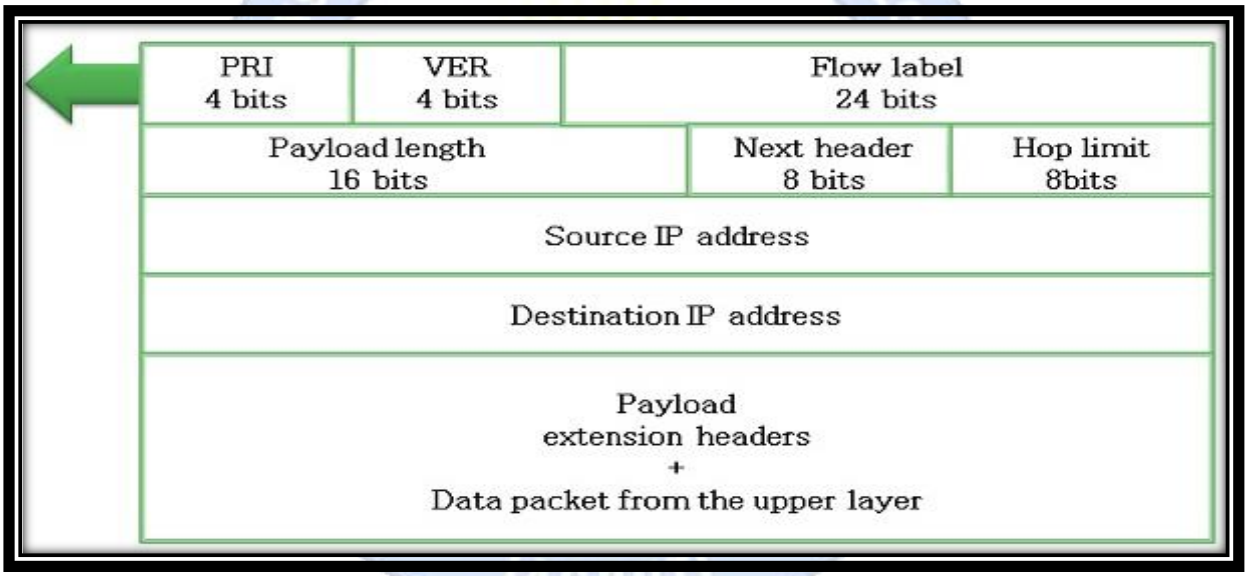
- **Flags:**
  - 3 flags of 1 bit each :
    - reserved bit (must be zero),
    - do not fragment flag,
    - more fragments flag (same order)
- **Fragment Offset:**
  - Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes
- **Time to live:**
  - Datagram's lifetime (8 bits), It prevents the datagram to loop through the network
- **Protocol:**
  - Name of the protocol to which the data is to be passed (8 bits)
- **Header Checksum:**
  - 16 bits header checksum for checking errors in the datagram header
- **Source IP address:**
  - 32 bits IP address of the sender
- **Destination IP address:**
  - 32 bits IP address of the receiver
- **Option:**
  - Optional information such as source route, record route.

46. Draw and explain IPv6 Datagram Header.

Ans:

- **IP** stands for **Internet Protocol** and **v6** stands for **Version six** (IPv6).
- Each packet is consist of a mandatory base header succeeded by the payload.
- **IPv6** Address Length 128 bits (16 bytes).
- The payload includes two parts namely optional extension headers and data from an upper layer.
- The base header consumes 40 bytes, inversely the extension headers and data from the top layer usually hold up to 65,535 bytes of information.

- **IPv6 Datagram Header**:



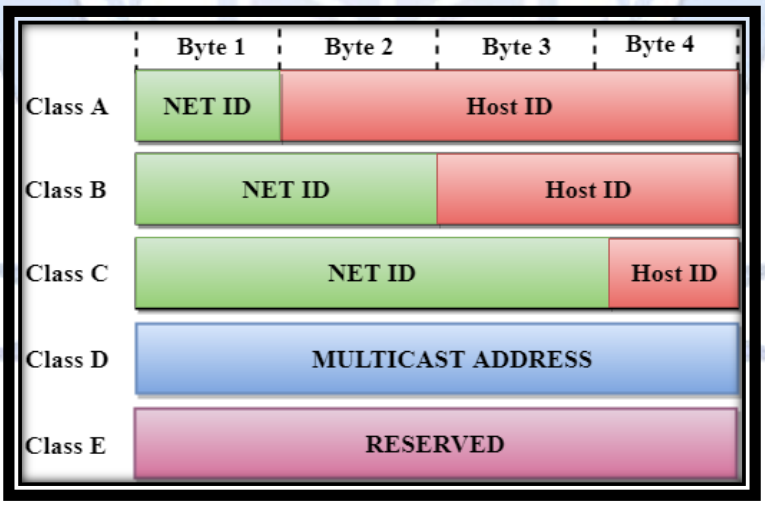
- **Version:**
  - This four-bit field specifies the version of the IP, i.e., 6 in this case.
- **Priority:**
  - It defines the priority of the packet concerning traffic congestion.
- **Flow label:**
  - The reason for designing this protocol is to facilitate with special controlling for a certain flow of data.
- **Payload length:**
  - It defines the total length of the IP datagram excepting the base header.
- **Next header:**
  - It's an eight-bit field describe the header that trails the base header in the datagram.
  - The next header is one of the optional extension headers which IP uses or the header for an upper layer protocol such as UDP or TCP.

- **Hop limit:**
  - This eight-bit hop limit field assist with the same functions at the TTL field in IPv4.
- **Source address:**
  - It is a 16 bytes internet address identifies the source of the datagram.
- **Destination address:**
  - This is 16-byte internet address that generally describes the final destination of the datagram.

47. Explain Classification of IP Addresses (Classful Addressing).

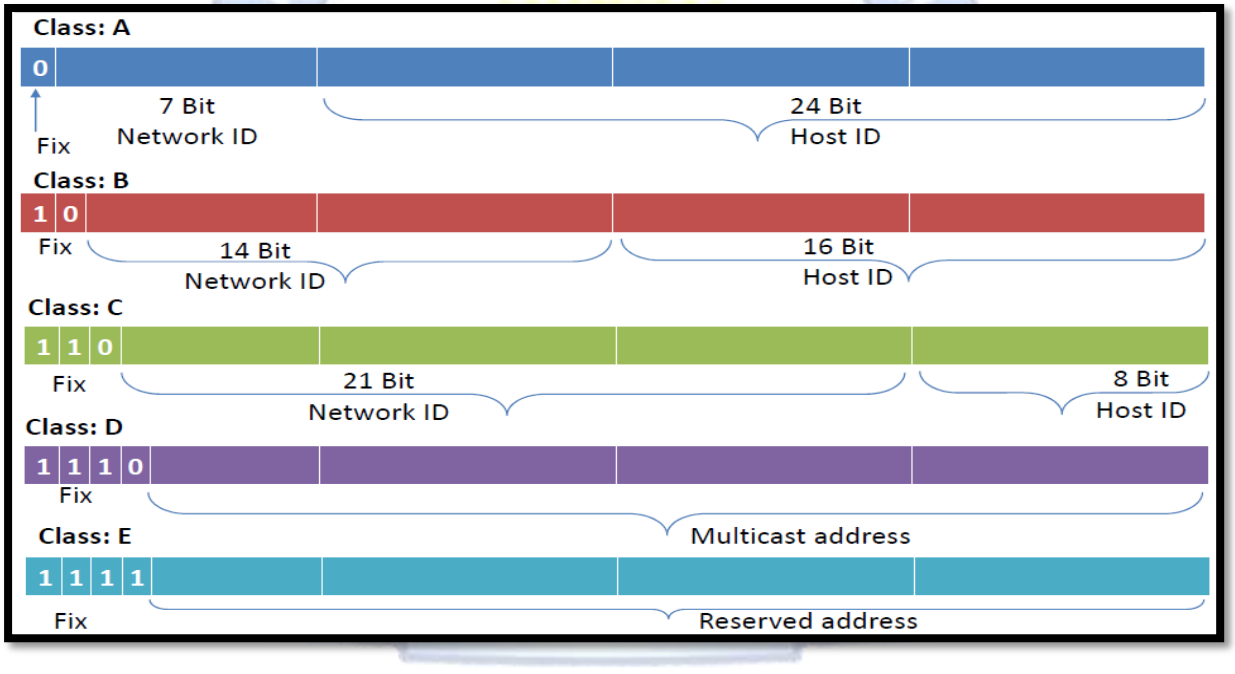
Ans:

- The 32 bit IP address is divided into five sub-classes. These are:
  - Class A
  - Class B
  - Class C
  - Class D
  - Class E
- Each of these classes has a valid range of IP addresses.
- Classes D and E are reserved for multicast and experimental purposes respectively.
- The order of bits in the first octet determine the classes of IP address.
- **IPv4 address is divided into two parts:**
  - **Network ID:**
    - It represents the number of networks.
  - **Host ID:**
    - It represents the number of hosts.



- **Class A** starts with 0 followed by 7 bits of network ID and 24 bits of host ID.
- **Class B** starts with 10 followed by 14 bits of network ID and 16 bits of host ID.
- **Class C** starts with 110 followed by 21 bits of network ID and 8 bits of host ID.
- **Class D** starts with 1110 followed by 28 bits. Class D is used only for multicast addressing by which a group of hosts form a multicast group and each group requires a multicast address.
- **Class E** starts with 1111 followed by 28 bits. Class E is reserved for network experiments only.

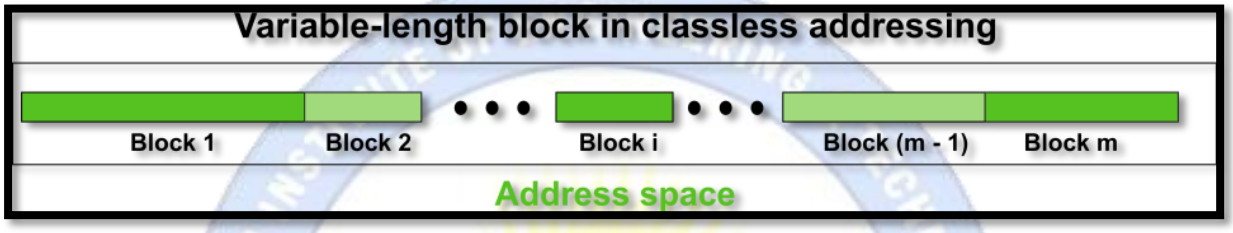
Class	Higher bits	NET ID bits	HOST ID bits	No.of networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 to 127.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 to 191.255.255.255
C	110	24	8	2^{21}	2^8	192.0.0.0 to 223.255.255.255
D	1110	Not Defined	Not Defined	Not Defined	Not Defined	224.0.0.0 to 239.255.255.255
E	1111	Not Defined	Not Defined	Not Defined	Not Defined	240.0.0.0 to 255.255.255.255



48. Explain Classless Addressing (CIDR).

Ans:

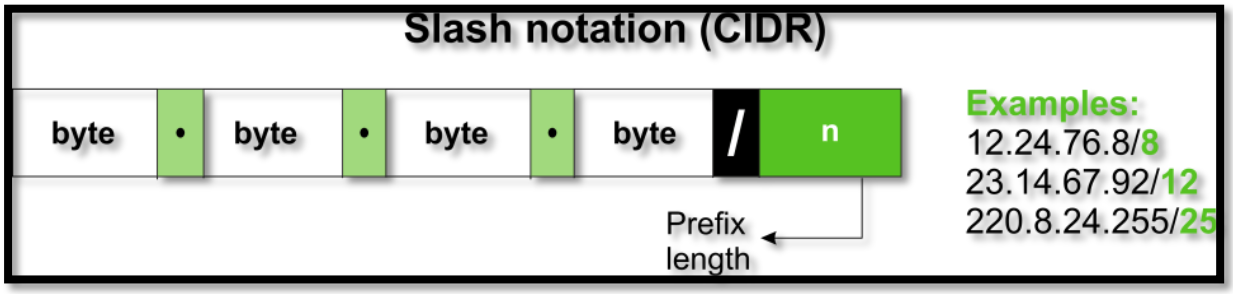
- A classless addressing system OR Classless interdomain routing (CIDR) is an improved IP addressing system.
- In a Classless addressing system, the block of IP addresses is assigned dynamically based on specific rules.
- It provides a **variable-length of blocks**, which have a **range of addresses according** to the **need of users.**



- **Classless Addressing Notation:**
  - Notation of a classless addressing system Or Classless interdomain routing (CIDR):

    p.q.r.s /n

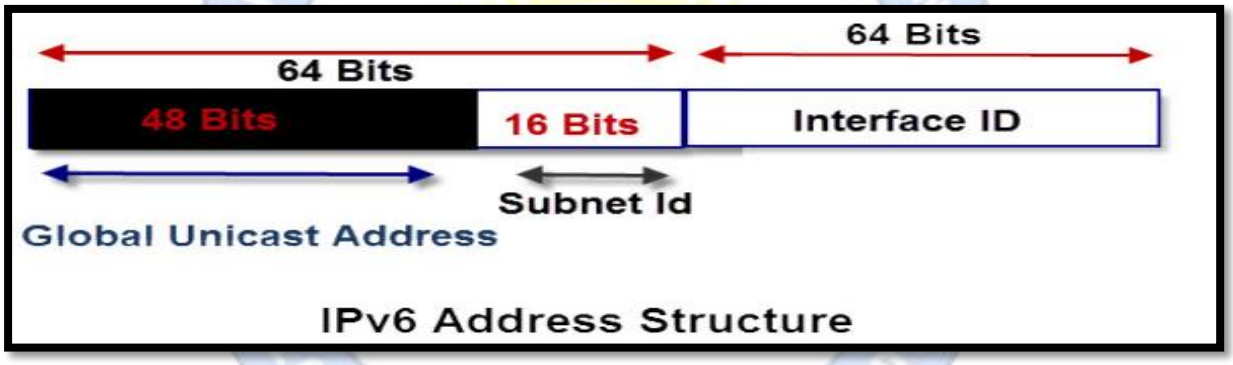
  - Where,
    - p.q.r.s represents the IP address,
    - n represents the mask bits.
- **Classless Addressing - Properties**
  - Addresses in a block must be in contiguous form.
  - The number of address in a block must be the power of 2 i.e. 2, 4, 8, 16,...
  - The first address must be evenly divisible by the number of addresses.
- **Classless Addressing - Representation**
  - In Classless addressing a block, IP address is given like 192.168.10.1/28 (after "/" number of the mask bit is given).

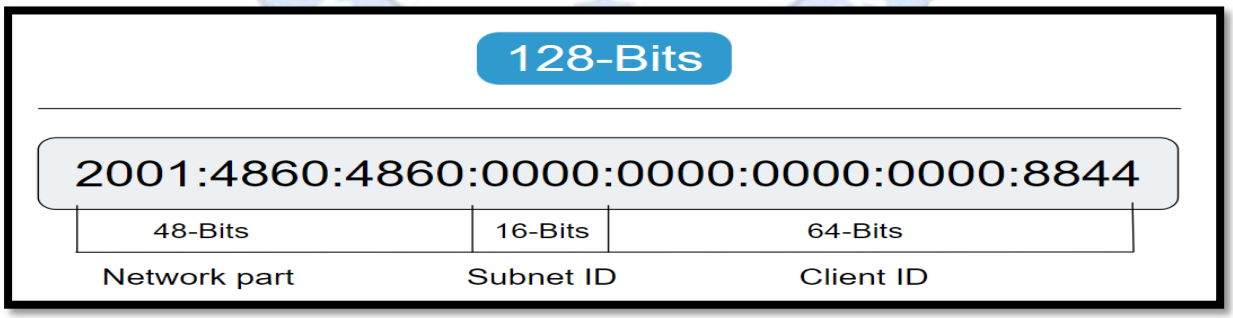


49. Explain Classify Binary and Hexadecimal Representation of IPv6 address.

Ans:

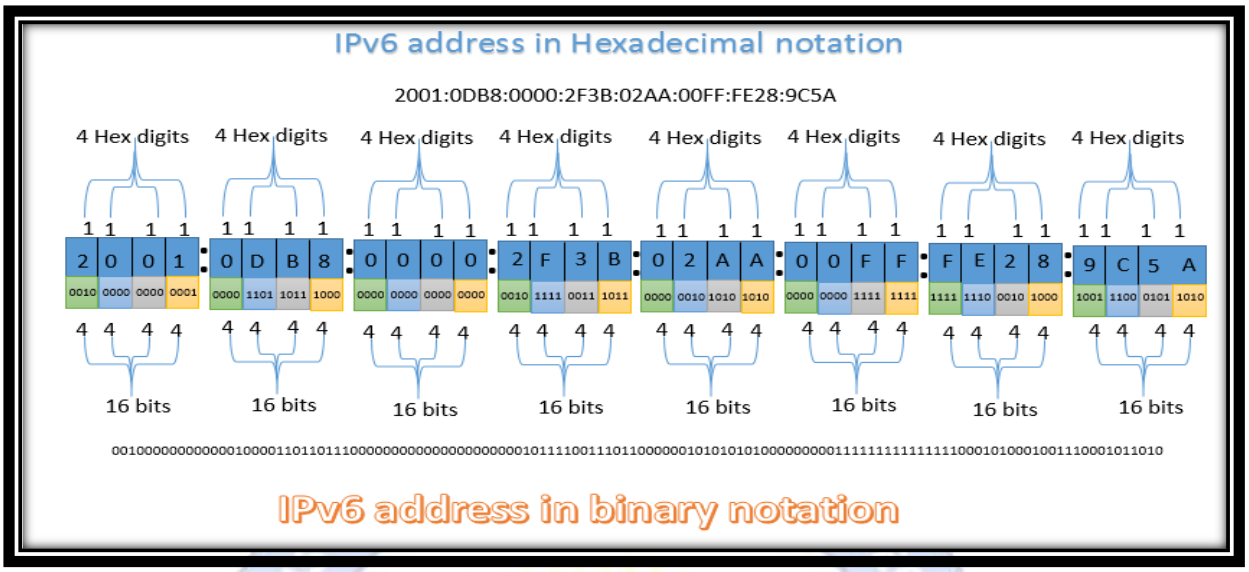
- **IPv6 addresses have three types:**
  - **Global Unicast Address:**
    - Scope Internet- routed on Internet
  - **Unique Local:**
    - Scope Internal Network or VPN internally routable, but Not routed on Internet
  - **Link Local:**
    - Scope network link- Not Routed internally or externally.





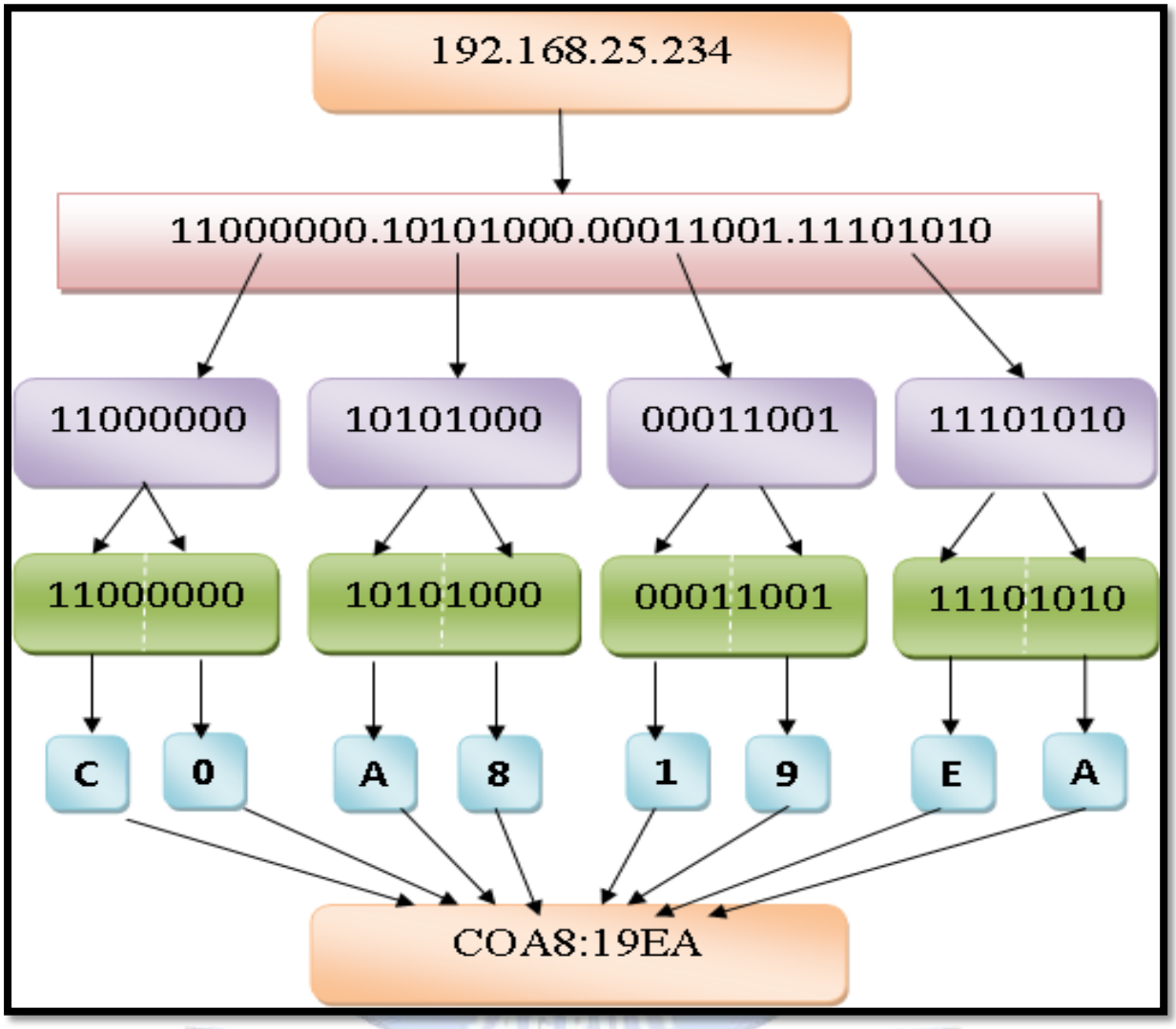
- **IPv6 address** is **128 bits** in length and is written as **eight groups of four hexadecimal digits.**
- Each group is separated from the others by **colons (:)** as shown in figure.
- Hexadecimal characters are **not case sensitive**, therefore an address can be written **either in uppercase or lowercase**, **both are equivalent**.

- **Example:**


IPv6 address in Hexadecimal notation
2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A
4 Hex digits
16 bits
IPv6 address in binary notation

50. Explain Convert the given IPv4 address to IPv6 address.

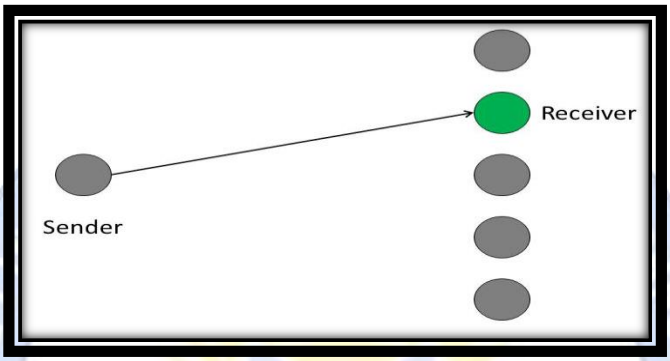
Ans:



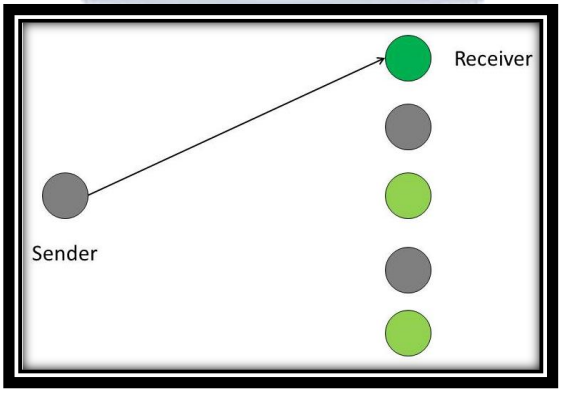
51. Write a short note on Network Transmission Types.

Ans:

- **Network Transmission Types:**
  - Unicasting
  - Any casting
  - Multicasting
  - Broadcasting
- **Unicasting:**



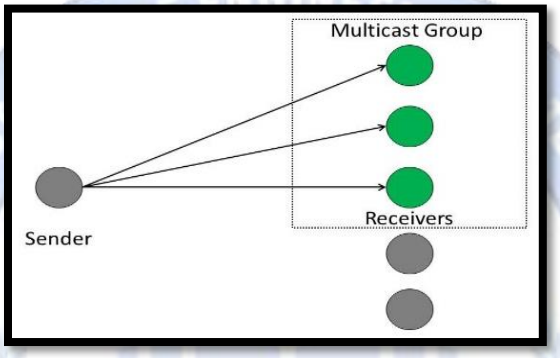
  - Unicasting is the most commonly used data transmission type on the internet.
  - In Unicasting, the data traffic flows from a single source node to a single destination node on the network.
  - It is a 'one-to-one' type of data transmission between the sender and receiver.
  - It can be best implemented in computer-to-computer or server-to-server or client-to-server kind of communications.
  - SMTP(Simple Mail Transfer Protocol) protocol can be used for unicasting an email on the internet.
  - Similarly, FTP(File Transfer Protocol) can be used for unicasting a particular file from one computer to another on the network.
  - Some other protocols like HTTP(HyperText Markup Language), Telnet, etc. can also be used for unicasting on the network.
- **Any-casting:**



  - Anycast is a one-to-nearest kind of transmission in which a single source sends a message to the nearest destination(among multiple possible destinations).

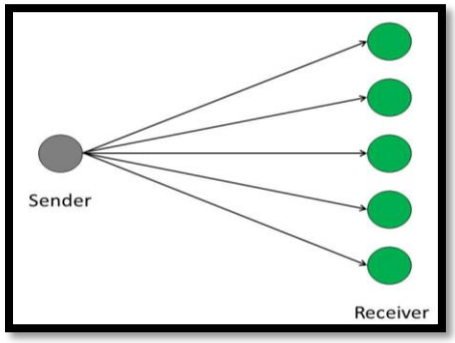
- It can only be implemented using IPv6 addressing.
- IPv4 addressing can not be used for anycasting.
- In Anycasting, a single IPv6 address is assigned to multiple devices in the network.
- Anycasting is mainly used by Routers.
- The Anycast address is an address that can be assigned to a group of devices on the network(mostly routers).
- In the above diagram, all the devices with green shade have the same anycast address.
- But the data is received by only one device, which is in dark green shade(because it was the first one to receive the message).

- **Multicasting:**



- Multicast is a kind of transmission type in which a single source communicates a message to a group of devices.
- It is a kind of one-to-multiple transmission.
- All the devices which are interested in receiving the messages will have to first join the multicast group.
- Multicasting is used in an IP Multicast group in the network.
- The IP multicast group consists of all the devices which are interested in receiving the multicast traffic.
- The source need not be a member of that group.
- Multicasting is always done using a single source.
- Also, a multicast address can never be the source address.
- Multicasting uses a class-D type of address(to connect multiple destination nodes for multicasting).

- **Broadcasting:**

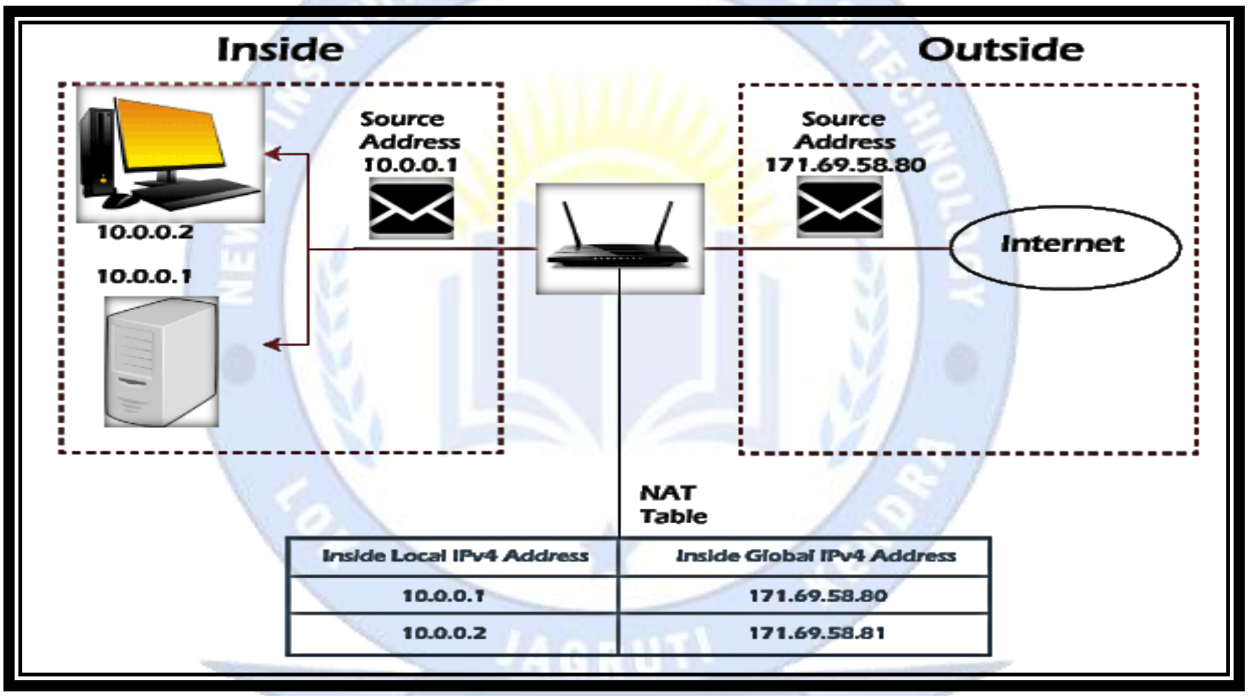


- Broadcasting is a transmission type in which the data traffic flows from a single source to all the devices on the network.
- It sends the information to every device at once.
- The same data is received by everyone, making it efficient for wide-spreading the message with all nodes.
- Broadcasting is an IPv4 specific data transmission type.
- In broadcasting, every node has a look at the sent data and information in the network.
- HTTP(HyperText Transfer Protocol) can be used for broadcasting.

52. Write a short note: NAT (Network Address Translation).

Ans:

- **NAT (Network Address Translation)** connects two networks and maps the private (inside local) addresses into public addresses (inside global).
- Inside local denotes that the best address belonged to an internal network and was not assigned by a **Network Information Centre** or **service power**.
- The inside global signifies that the address is a valid address assigned by the **NIC** or service provider, and one or more inside local addresses to the outside world.
- **NAT:**



- **NAT** is a method of converting a private IP address or a local address into a public IP address.
- NAT is a technique for reducing the rate at which available IP addresses are depleted by translating a local IP or private IP address into a global or public IP address.
- The NAT relation might be one-to-one or many-to-one.
- Furthermore, NAT can only configure one address in order to represent the entire network to the outside world.
- As a result, the translation process is transparent.
- NAT can be used to migrate and merge networks, share server loads, and create virtual servers, etc.

53. Explain Routing protocols: Distance vector routing, Link state routing and Path vector Routing.

OR

Q. Explain Distance vector routing (Bellman ford) Algorithm with Example.

Q. Explain Link state routing (Dijsktra) Algorithm with Example.

Q. Explain Path vector Routing Algorithm with Example.

Ans:

- A Router is a process of selecting path along which the data can be transferred from source to the destination.
- Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- Dynamic routing protocols use metric, cost, and hop count to identify the best path from the path available for the destination network.
- There are mainly 3 different classes of routing protocols:
    - **Distance vector routing**
    - **Link state routing**
    - **Path vector Routing.**

- **Distance Vector Routing:**
    - The Distance vector algorithm is:
        - Iterative
        - Asynchronous
        - Distributed
    - The Distance vector algorithm is a **dynamic algorithm**.
    - It is mainly used in **ARPANET, and RIP.**
    - Each router maintains a distance table known as **Vector**.
    - **Distributed:**
        - It is distributed in that each node receives information from one or more of its directly attached neighbors, performs calculation and then distributes the result back to its neighbors.
    - **Iterative:**
        - It is iterative in that its process continues until no more information is available to be exchanged between neighbors.
    - **Asynchronous:**
        - It does not require that all of its nodes operate in the lock step with each other.

- **Bellman Ford Basics:**
  - Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes.
  - **Information kept by DV router:**
    - Each router has an ID Associated with each link connected to a router
    - there is a link cost (static or dynamic).
    - Intermediate hops
  - **Distance Vector Table Initialization**
    - Distance to itself = 0
    - Distance to ALL other routers = infinity number.

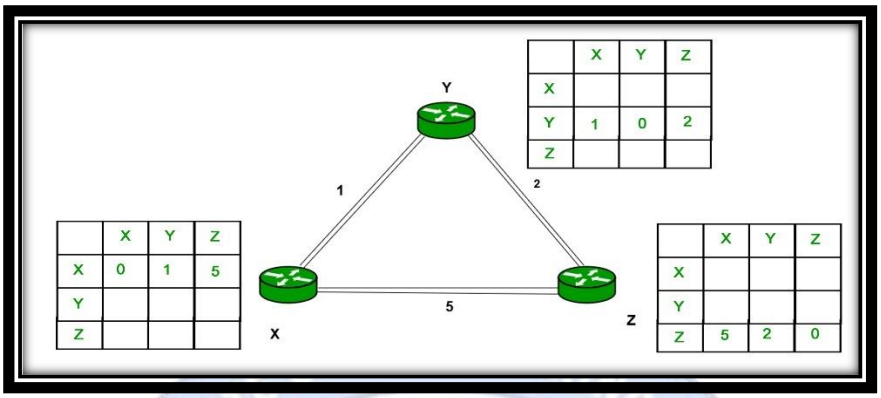
- **The Bellman-Ford algorithm is defined as :**

$$d_x(y) = \min_v \{c(x, v) + d_v(y)\}$$

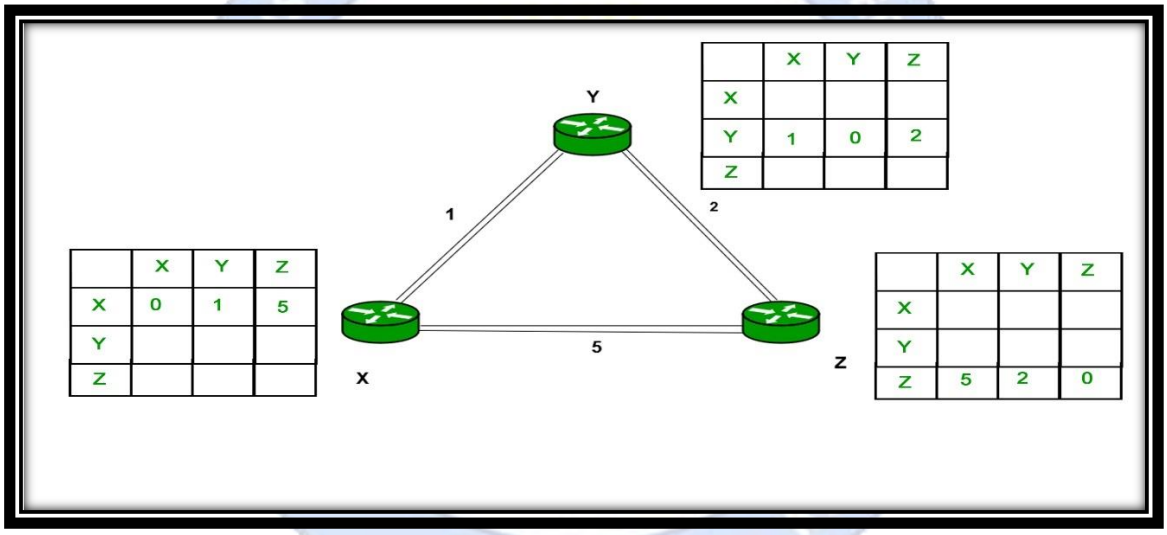
where, $dx(y)$ = The least distance from x to y
$c(x, v)$ = Node x's cost from each of its neighbour v
$dv(y)$ = Distance to each node from initial node
$minv$ = selecting shortest distance

- **Distance Vector Algorithm:**
  - A router transmits its distance vector to each of its neighbors in a routing packet.
  - Each router receives and saves the most recently received distance vector from each of its neighbors.
  - A router recalculates its distance vector when:
    - It receives a distance vector from a neighbor containing different information than before.
    - It discovers that a link to a neighbor has gone down.
  - The DV calculation is based on minimizing the cost to each destination

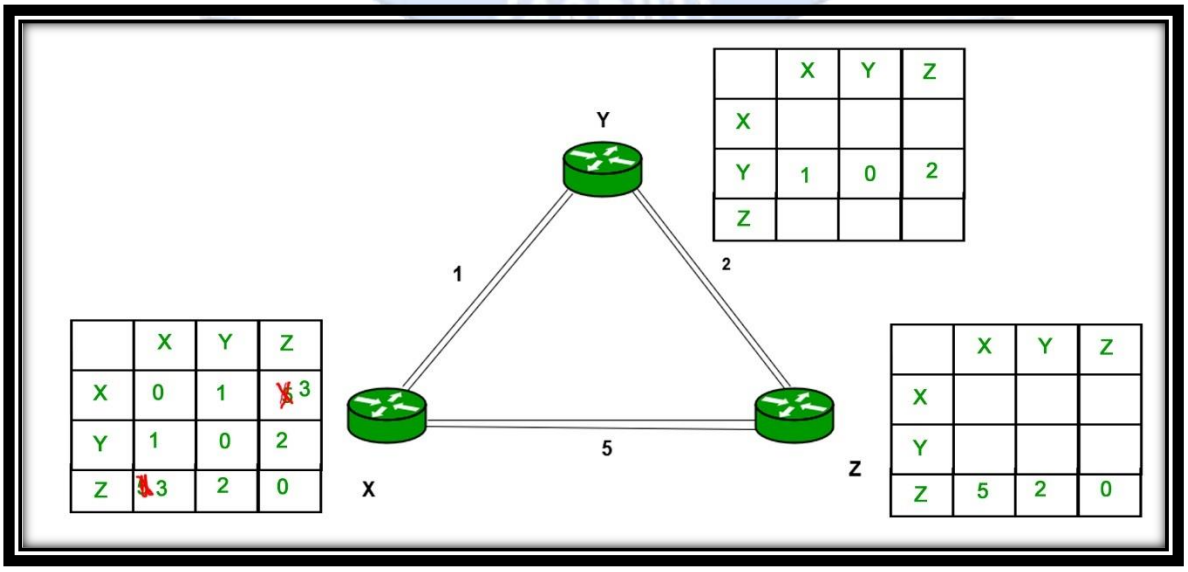
- **Example:** Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



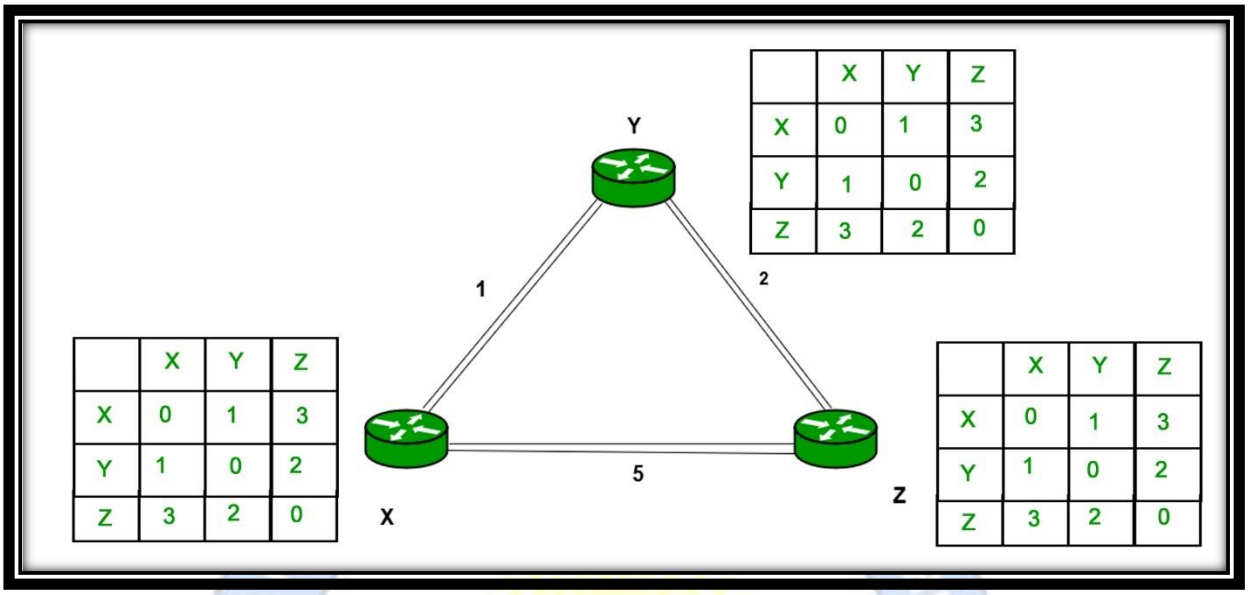
- **Consider router X**



- **Consider router Z**



- **Finally the routing table for all:**

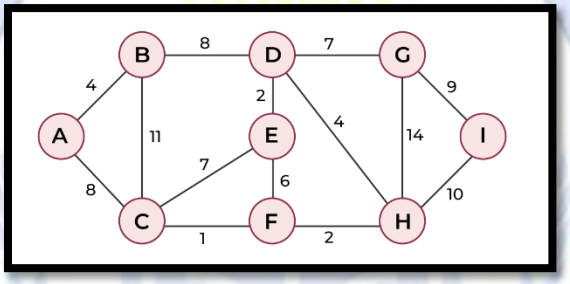


- **Link State Routing:**
  - Link State Routing (LSR) is a routing algorithm used in computer networks to determine the best path for data to travel from one node to another.
  - LSR is considered to be a more advanced and efficient method of routing compared to Distance Vector Routing (DVR) algorithm.
  - In LSR, each node in the network maintains a map or database, called a link state database (LSDB), that contains information about the state of all the links in the network.
  - This information includes the cost of each link, the status of each link (up or down), and the neighboring nodes that are connected to each link.
  - **Algorithm:**
    - **Dijsktra Algorithm**

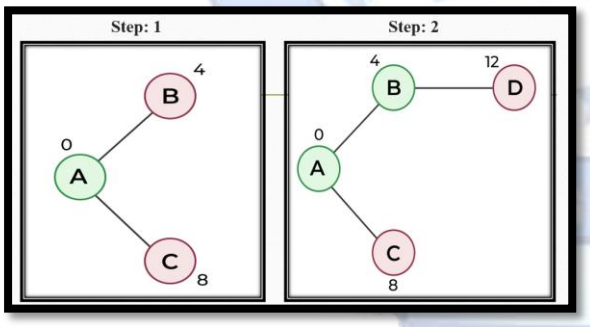
```
Initialization
N = {A}     // A is a root node.
for all nodes v
if v adjacent to A
then D(v) = c(A,v)
else D(v) = infinity
loop
find w not in N such that D(w) is a minimum.
Add w to N
Update D(v) for all v adjacent to w and not in N:
D(v) = min(D(v) , D(w) + c(w,v))
Until all nodes in N
```

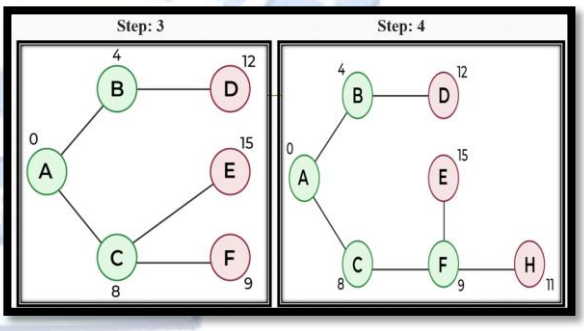
- **Let's describe some notations:**
  - **c(i , j):**
    - Link cost from node i to node j.
    - If i and j nodes are not directly linked, then c(i , j) = ∞.
  - **D(v):**
    - It defines the cost of the path from source code to destination v that has the least cost currently.
  - **P(v):**
    - It defines the previous node (neighbor of v) along with current least cost path from source to v.
  - **N:**
    - It is the total number of nodes available in the network.

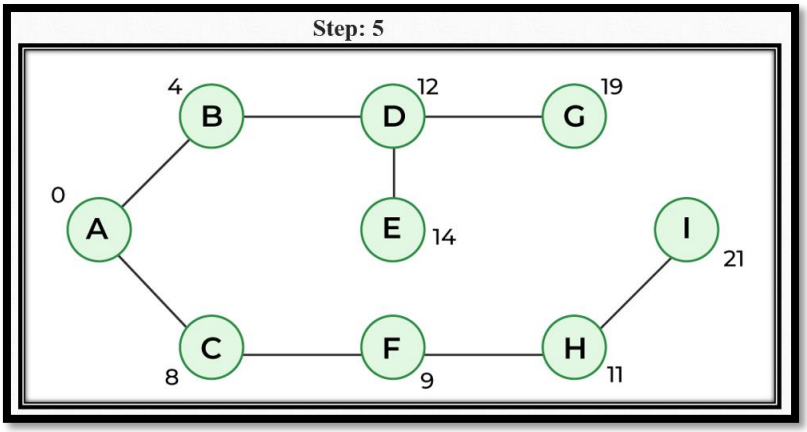
- **Example: Consider the below graph and src = 0.**



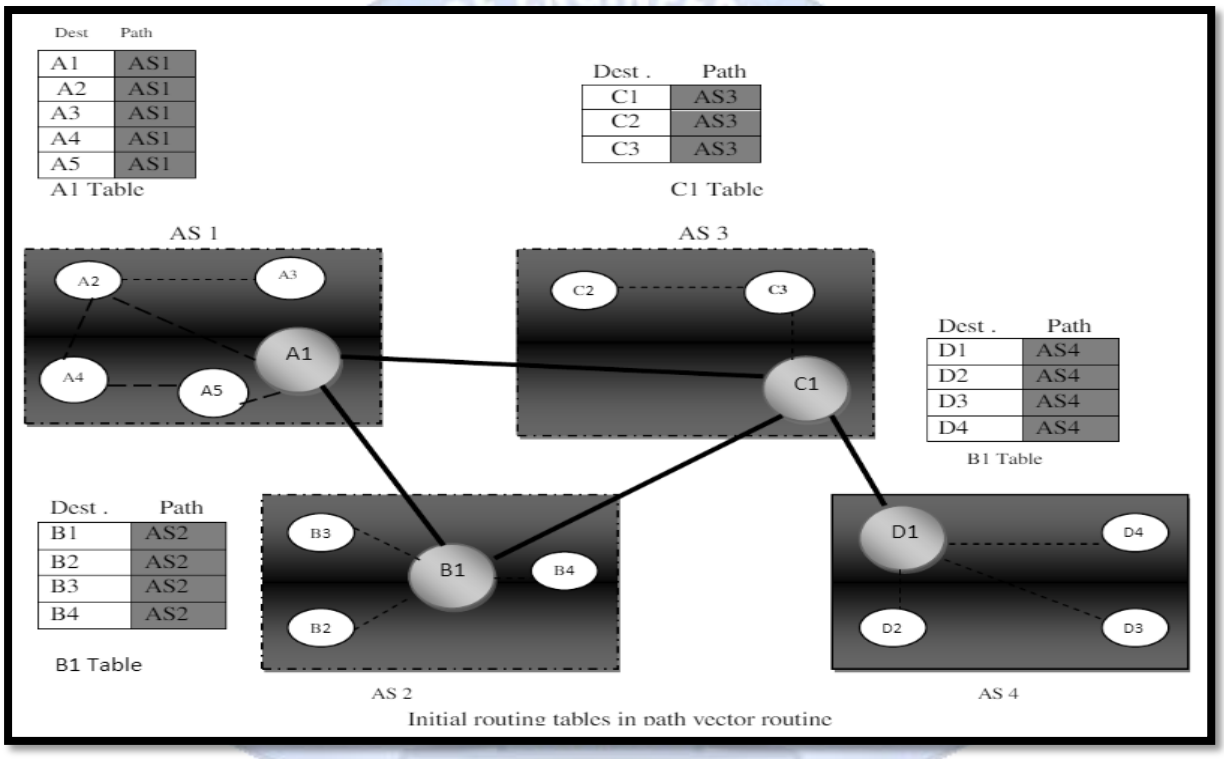
- **Solution:**







- **Path Vector Routing:**
  - Path Vector Routing is a routing algorithm in unicast routing protocol of network layer, and it is useful for interdomain routing.
  - The principle of path vector routing is similar to that of distance vector routing.
  - It assumes that there is one node in each autonomous system that acts on behalf of the entire autonomous system is called Speaker node.
  - The speaker node in an AS creates a routing cable and advertises to the speaker node in the neighboring ASs .
  - A speaker node advertises the path, not the metrics of the nodes, in its autonomous system or other autonomous systems



  - It is the initial table for each speaker node in a system made four ASs.
  - Here Node A1 is the speaker node for AS1, B1 for AS2, C1 for AS3 and D1 for AS4, Node A1 creates an initial table that shows A1 to A5 and these are located in AS1, it can be reached through it.
  - A speaker in an autonomous system shares its table with immediate neighbors ,here Node A1 share its table with nodes B1 and C1 , Node C1 share its table with nodes A1,B1 and D1 , Node B1 share its table with nodes A1 and C1 , Node D1 share its table with node C1
  - If router A1 receives a packet for nodes A3 , it knows that the path is in AS1,but if it receives a packet for D1,it knows that the packet should go from AS1,to AS2 and then to AS3 ,then the routing table shows that path completely on the other hand if the node D1 in AS4 receives a packet for node A2,it knows it should go through AS4,AS3,and AS1.

- **FUNCTIONS:**
  - **PREVENTION OF LOOP**
    - The creation of loop can be avoided in path vector routing .
    - A router receives a message it checks to see if its autonomous system is in the path list to the destination if it is looping is involved and the message is ignored
  - **POLICY ROUTING**
    - When a router receives a messages it can check the path, if one of the autonomous system listed in the path against its policy, it can ignore its path and destination it does not update its routing table with this path or it does not send the messages to its neighbors.
  - **OPTIMUM PATH**
    - A path to a destination that is the best for the organization that runs the autonomous system

54.Difference between:

a. **Virtual Circuit and Datagram Networks**
b. **IPv4 and IPv6**
c. **Classful Addressing and Classless Addressing**
d. **Distance Vector Routing and Link State Routing**
e. **Broadcast and Multicast**

Ans:

a. Virtual Circuit and Datagram Networks

Key	Virtual Circuits	Datagram Networks
Description	Virtual circuits are networks that provide only a connection service at the network layer.	Datagram networks are computer networks that provide only a connectionless service at the network layer.
Services	They are connection-oriented.	They are connectionless services.
Path	They use a fixed path for a particular session.	There is no fixed path for transmitting data.
Reliable	They are highly reliable.	They are comparatively less reliable.
Cost	costly	Less costly
Error Control	Provides reliable delivery of packets by detecting and retransmitting lost or corrupted packets.	Provides unreliable delivery of packets and does not guarantee delivery or correctness.
Example Protocol	ATM, Frame Relay	IP (Internet Protocol)

b. IPv4 and IPv6

BASIS OF COMPARISON	IPV4	IPV6
Full From	Internet Protocol Version four	Internet Protocol Version Six
Address Configuration	Supports Manual and DHCP configuration.	Supports Auto-configuration and renumbering
End-to-end connection integrity	Unachievable	Achievable
Security features	Security is dependent on application	IPSEC is inbuilt in the IPv6 protocol
Address length	32 bits (4 bytes)	128 bits (16 bytes)
Address Representation	In decimal	In hexadecimal
Packet flow identification	Not available	Available
Checksum Field	Available	Not available
Message Transmission Scheme	Broadcasting	Multicasting and Any casting
Encryption & Authentication	Not Provided	Provided

c. Classful Addressing and Classless Addressing

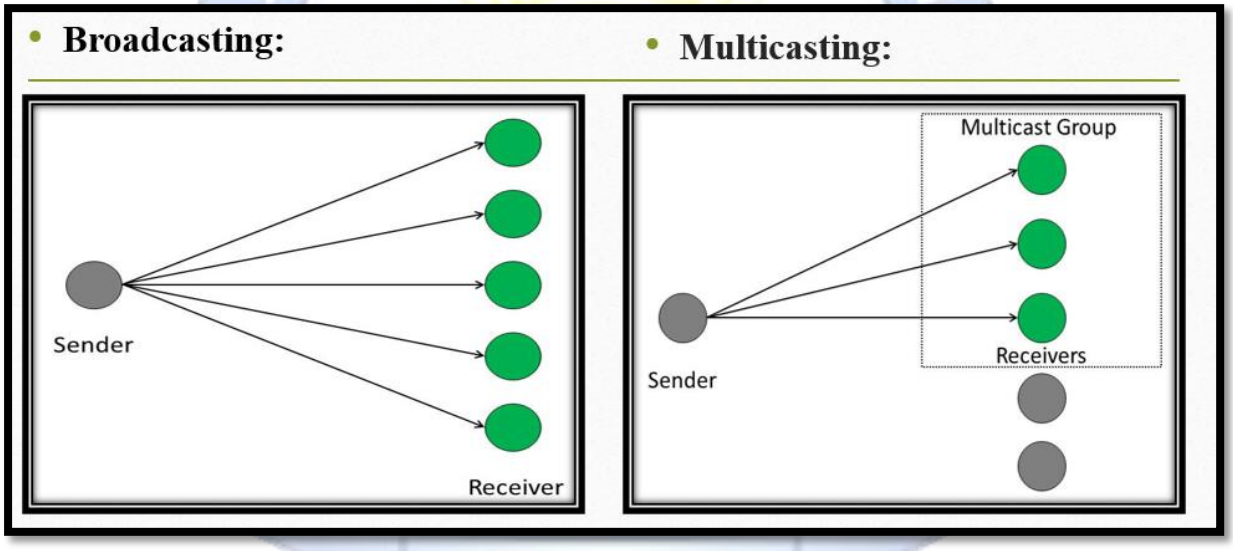
Parameter	Classful Addressing	Classless Addressing
Basics	In Classful addressing IP addresses are allocated according to the classes- A to E.	Classless addressing came to replace the classful addressing and to handle the issue of rapid exhaustion of IP addresses.
Practical	It is less practical.	It is more practical.
Network ID and Host ID	The changes in the Network ID and Host ID depend on the class.	There is no such restriction of class in classless addressing.
Variable Length Subnet Mask (VLSM).	Not Support	Support
Bandwidth	Requires More Bandwidth	Requires Less Bandwidth.
Classless Inter-Domain Routing (CIDR).	Not Support	Support
Troubleshooting and Problem detection	Detection are Easy	Detection Not Easy
Division of Address	• Network • Host • Subnet	• Host • Subnet

d. Distance Vector Routing and Link State Routing

BASIS FOR COMPARISON	DISTANCE VECTOR ROUTING	LINK STATE ROUTING
Algorithm	Bellman ford	Dijsktra
Network view	Topology information from the nearest point of view	Complete information on the network topology
Best path calculation	Based on the least number of hops	Based on the cost
Updates	Full routing table	Link state updates
Updates frequency	Periodic updates	Triggered updates
CPU and memory	Low utilisation	Intensive
Convergence time	Moderate	Fast
Updates	On broadcast	On multicast
Hierarchical structure	No	Yes
Intermediate Nodes	No	Yes

e. Broadcast and Multicast

BASIS FOR COMPARISON	BROADCAST	MULTICAST
Basic	The packet is transmitted to all the hosts connected to the network.	The packet is transmitted only to intended recipients in the network.
Transmission	One-to-all.	One-to-many.
Management	Broadcasting does not require any group management.	Multicasting requires group management to define the group of hosts/stations which will receive packets.
Bandwidth	Bandwidth is wasted.	Bandwidth is utilized efficiently.
Traffic	Unnecessarily huge amount traffic is generated in the network.	Traffic is under control.
Process	Slow.	Fast.

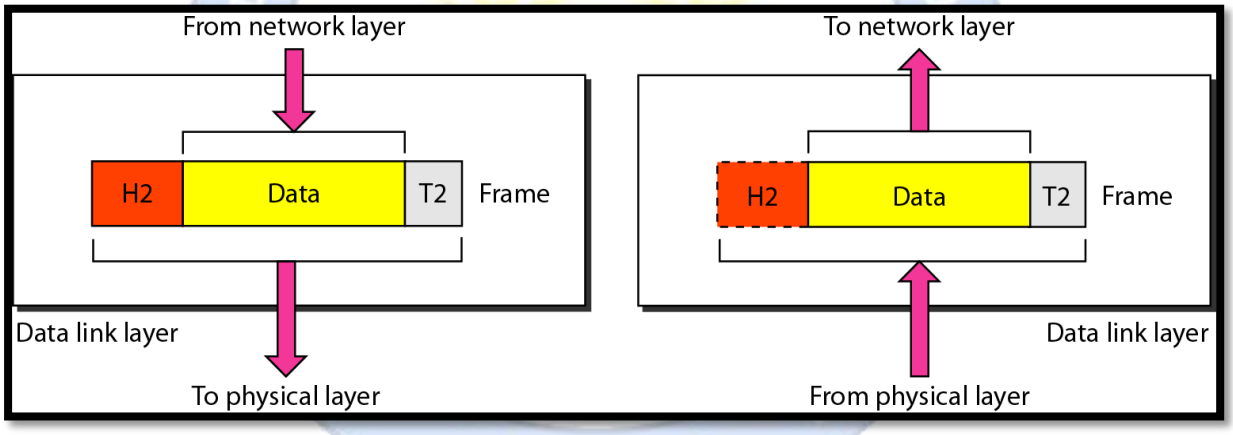


Unit - 5 The Link layer and Local Area Networks

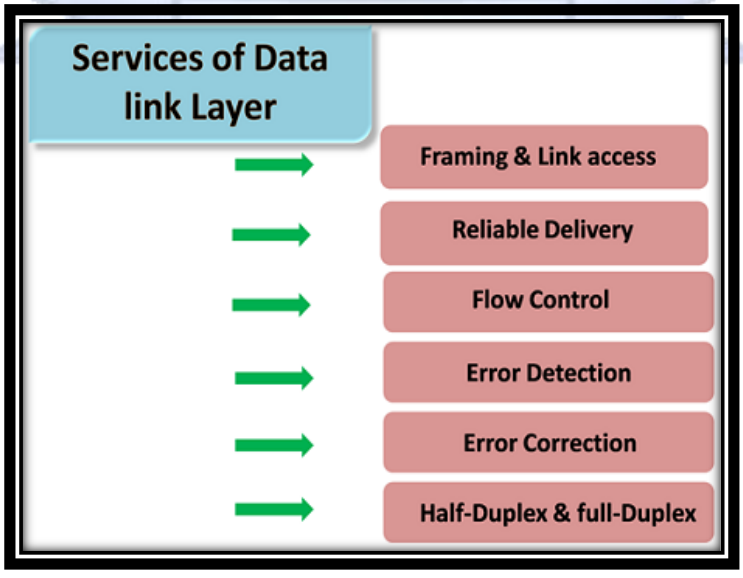
55. Explain Functions of Data Link Layer and List out Services of Data Link Layer.

Ans:

- **Data link layer:**
  - In the OSI model, the data link layer is a **4th layer from the top** and **2nd layer from the bottom**.
  - The **data link layer** is responsible for **moving frames** from one hop (node) to the next.
  - Groups of bits its called **Frame.**



- **Services of Data Link Layer:**



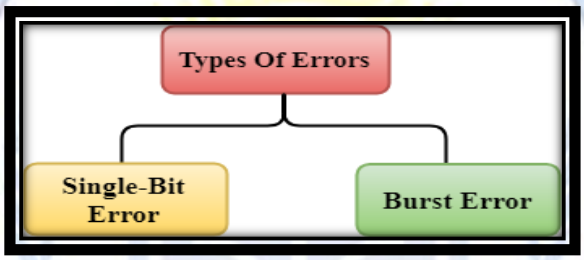
56. What is Error Detection? Explain Types of Errors.

OR

Q. Explain Single-Bit Error and Burst Error.

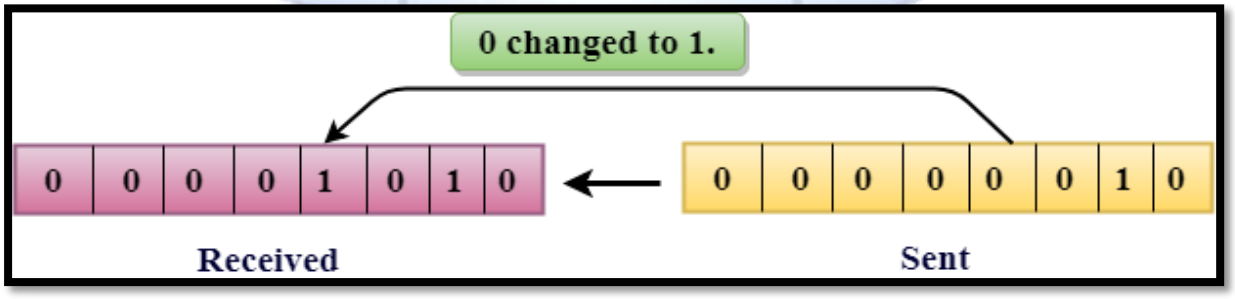
Ans:

- **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.

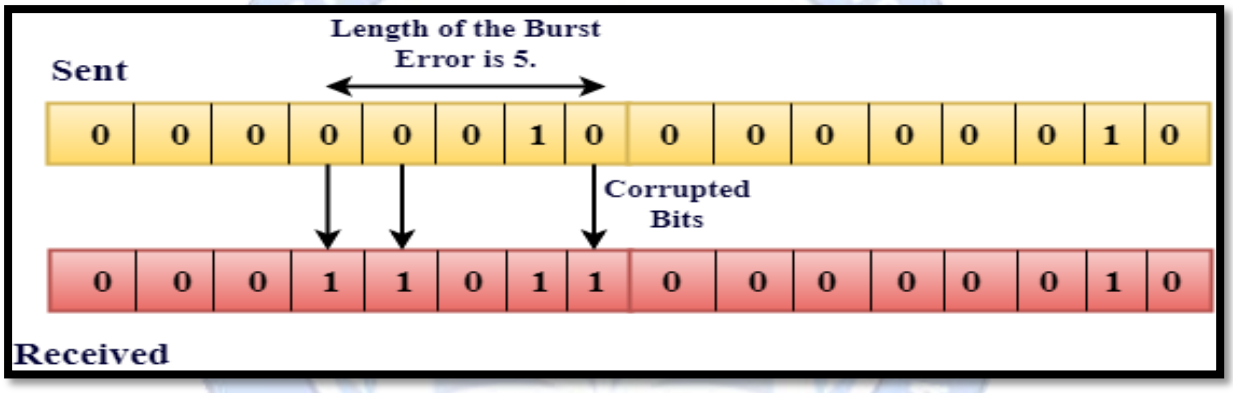


    - In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1.
    - **Single-Bit Error does not appear** more likely in **Serial Data Transmission**.

- **For example,** Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.
- **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.

o 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 occurr in Serial Data Transmission.
- The number of affected bits depends on the duration of the noise and data rate.

57. What is Error Detection? Explain Error Detecting Techniques.

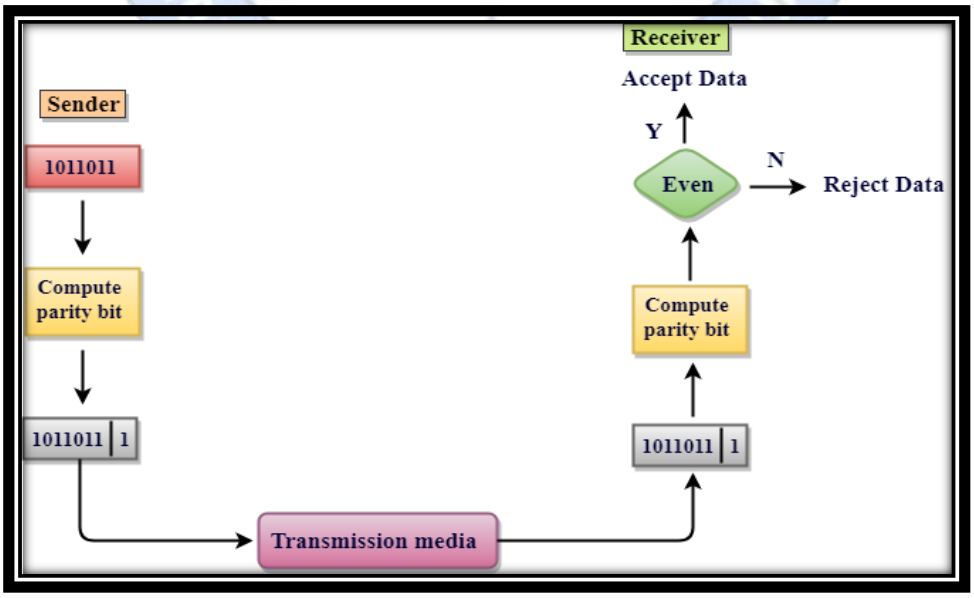
OR

Q. Explain Single parity check and Two-dimensional parity check.

Q. Explain Checksum and Cyclic redundancy check (CRC) with example.

- **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.
- **Error Detecting Techniques:**
  - The most popular Error Detecting Techniques are:
    1. Single parity check
    2. Two-dimensional parity check
    3. Checksum
    4. Cyclic redundancy check

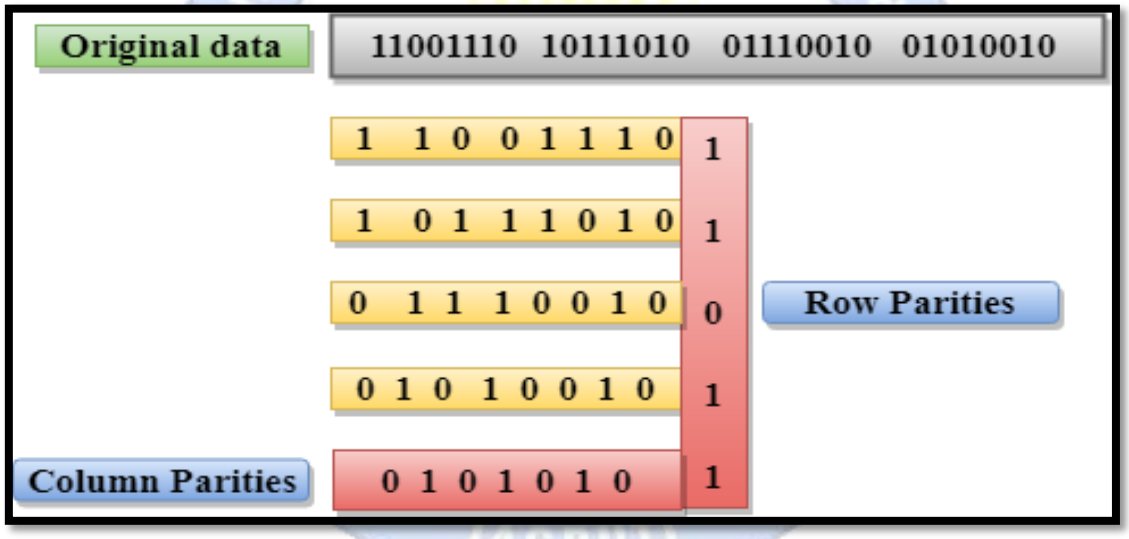
- **Single Parity Check:**
  - Single Parity checking is the simple mechanism and inexpensive to detect the errors.



  - 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.

- **Two-Dimensional Parity Check:**



- Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.
- Parity check bits are computed for each row, which is equivalent to the single-parity check.
- In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.
- At the receiving end, the parity bits are compared with the parity bits computed from the received data.
- **Drawbacks Of 2D Parity Check**
  - If two bits in one data unit are corrupted and two bits exactly the same position in another data unit are also corrupted, then 2D Parity checker will not be able to detect the error.
  - This technique cannot be used to detect the 4-bit errors or more in some cases.

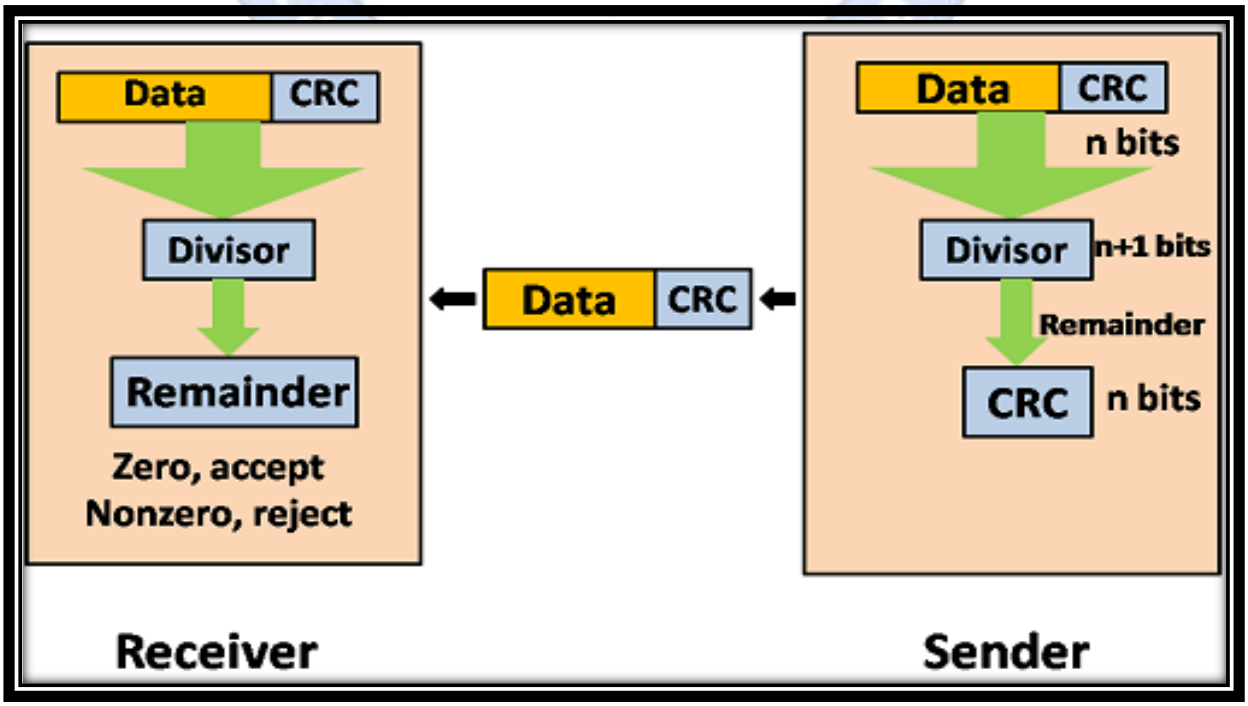
- **Checksum:**
  - A Checksum is an error detection technique based on the concept of redundancy.
  - It is divided into two parts:
    - Checksum Generator
    - Checksum Checker
  - **Checksum Generator :**
    - A Checksum is generated at the sending side.
    - Checksum generator subdivides the 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.

The Sender follows the given steps:
• The block unit is divided into k sections, and each of n bits.
• All the k sections are added together by using one's complement to get the sum.
• The sum is complemented and it becomes the checksum field.
• The original data and checksum field are sent across the network.

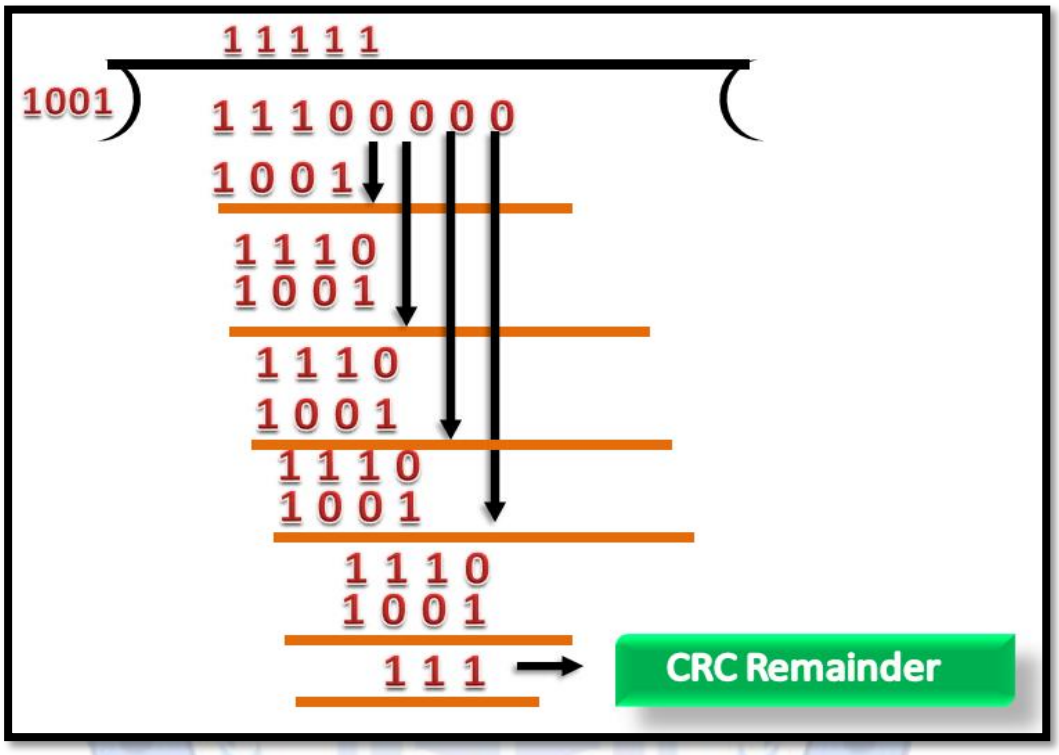
  - **Checksum Checker:**
    - A Checksum is verified at the receiving side.
    - The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented.
    - If the complement of the sum is zero, then the data is accepted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

The Receiver follows the given steps:
• The block unit is divided into k sections and each of n bits.
• All the k sections are added together by using one's complement algorithm to get the sum.
• The sum is complemented.
• If the result of the sum is zero, then the data is accepted otherwise the data is discarded.

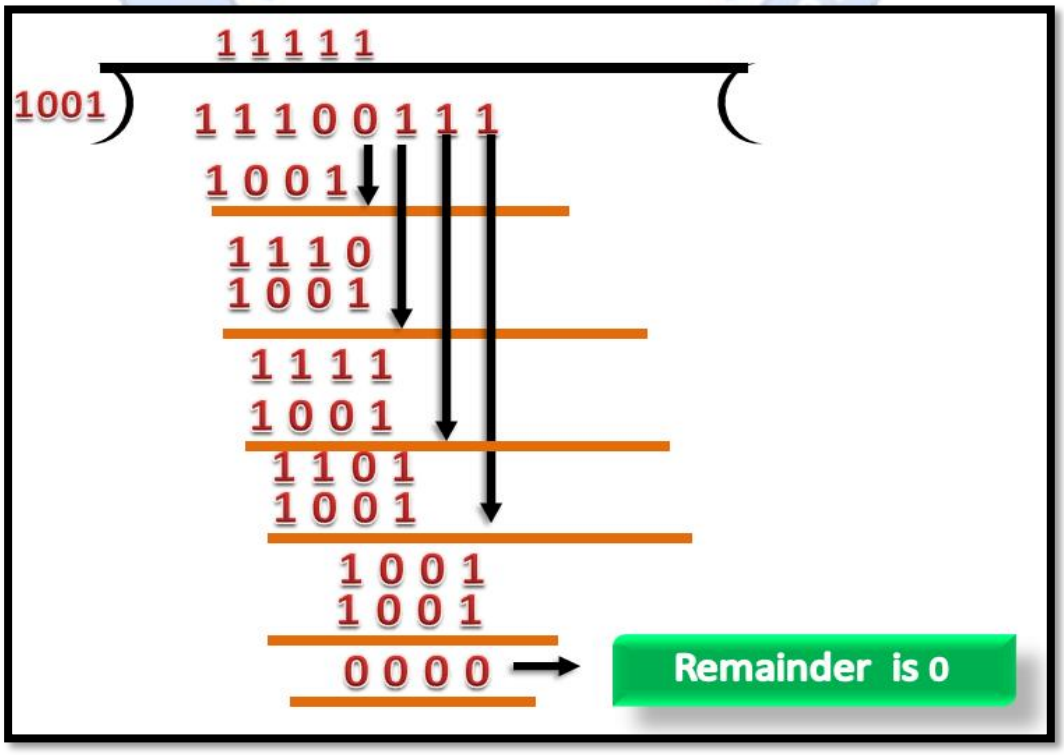
- **Cyclic Redundancy Check (CRC):**
  - CRC is a redundancy error technique used to determine the error.
  - **Following are the steps used in CRC for error detection:**
    - In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined 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.
    - The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.
- If the resultant of this division is zero which means that it has no error, and the data is accepted.
- If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.



- **Example: Suppose the original data is 11100 and divisor is 1001.**
  - **CRC Generator:**



  - **CRC Checker:**



58. Write a short note: Hamming Code.

Ans:

- Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.
- **Error Correction can be handled in two ways:**
  1. Backward error correction
  2. Forward error correction
  - **Backward error correction:**
    - Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
  - **Forward error correction:**
    - In this case, the receiver uses the error-correcting code which automatically corrects the errors.
    - A single additional bit can detect the error, but cannot correct it.
- **Hamming Code:**
  - **Parity Bits:**
    - The bit which is appended to the original data of binary bits so that the total number of 1s is even or odd.
  - **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:**
  1. An information of 'd' bits are added to the redundant bits 'r' to form d+r.
  2. The location of each of the (d+r) digits is assigned a decimal value.
  3. The 'r' bits are placed in the positions $1,2,.....2^{k-1}$.
  4. At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determines the position of an error.

- **Hamming code through an example:**
  - Suppose the original data is 1010 which is to be sent.

Total number of data bits 'd' = 4

Number of redundant bits r : $2^r >= d+r+1$

$2^r >= 4+r+1$

Therefore, the value of r is 3 that satisfies the above relation.

Total number of bits = d+r = 4+3 = 7;

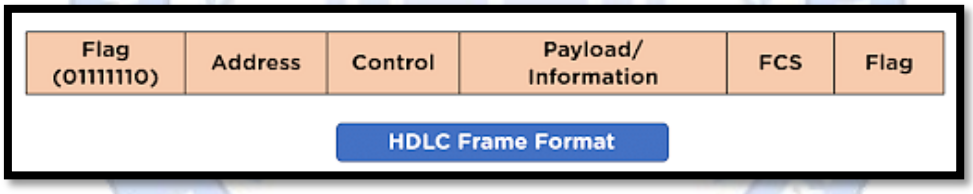
59. Write a short note: High-Level Data Link Control (HDLC).

OR

Q. Draw and Explain HDLC frame format.

Ans:

- **HDLC Frames:**
  - **High-Level Data Link Control (HDLC)** basically provides reliable delivery of data frames over a network or communication link.
  - HDLC provides **various operations** such as **framing, data transparency, error detection, and correction, and even flow control**.
  - The High-Level Data Link Control (HDLC) is **part of the data link layer protocol in the OSI Model.**
  - HDLC is applied for **point-to-point and multipoint link structures** based on the bit-oriented data format.
  - The data unit for sharing information in HDLC is known as frames.
  - HDLC frame consists of multiple frame fields, which may vary according to the type of frame used, and are as follows:



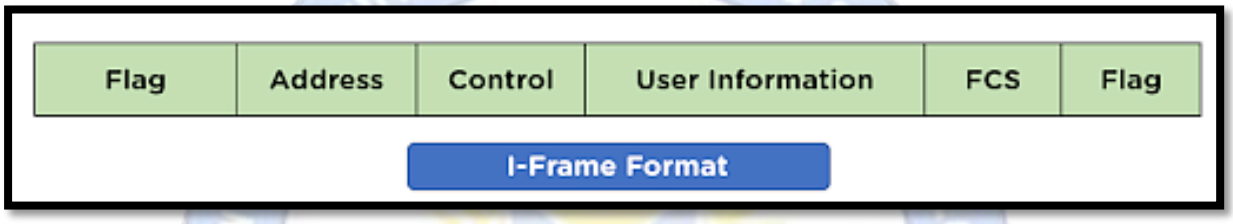
  - **Flag Field:**
    - In HDLC, each frame starts and ends with the flag field in the configuration and is defined by an 8-bit octet sequence 01111110 in the flag field.
  - **Address Field:**
    - It encapsulates the receiver's address in the field.
    - For example, if the frame is sent from the primary station, it contains the secondary station's address and vice versa.
  - **Control Field:**
    - This field contains the flow and error control information in byte format.
  - **Payload/Information Field:**
    - It carries information from the network layer, and the data size may vary depending on the network.
  - **FCS Field:**
    - This field stands for Frame Check Sequence and acts as an error detection field in the HDLC protocol, which includes a 16-bit CRC check bit.

60. Explain HDLC frames types.

Ans:

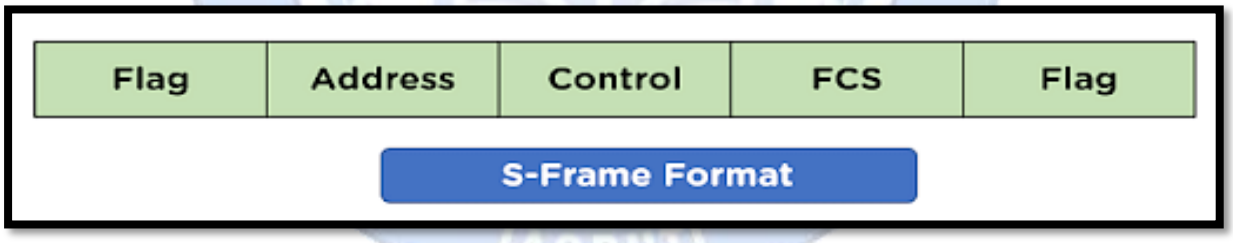
- **HDLC Frames Types:**
  - HDLC frames can be of the following **three types**, depending on the control field value of the frame:
    - I-Frame
    - S-Frame
    - U-Frame

  - **I-Frame:**



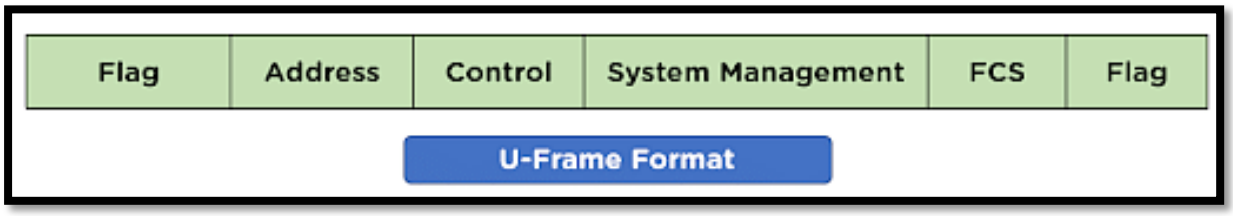
    - The information frame or I-frame is applied to encapsulate the user information from the upper layer in the model and then transmit it in the network channel and contains 0 in the control field.

  - **S-Frame:**



    - The supervisory frame or S-frames are used for error and data flow control and do not contain the information field in the frame format.
    - The control field is 1 and 0 for the first two bits.

  - **U-Frame:**



  - The un-numbered frame or U-frames are used for system management and exchanging control information between the connected network devices.

61. Write a short note: Multiple Access Protocols.

OR

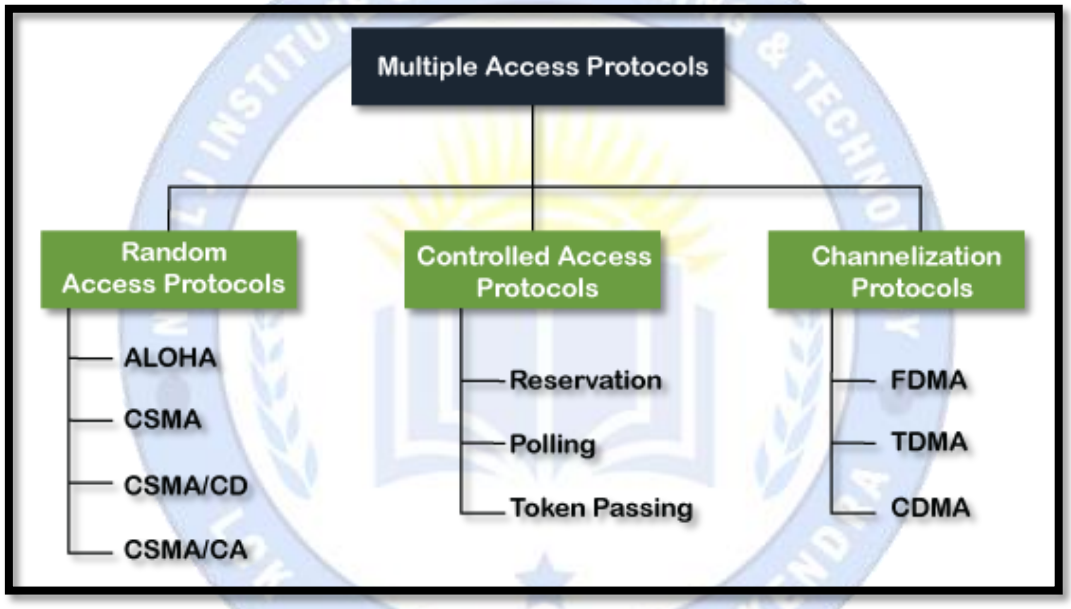
Q. What is Aloha Protocol? Explain Types of Aloha Protocols.

Q. Explain Channelization Protocols (FDMA, TDMA and CDMA).

Q. Write a short note: CSMA (Carrier Sense Multiple Access).

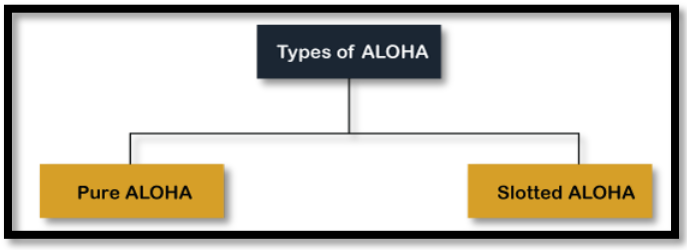
Q. Write a short note: CSMA/CD and CSMA/CA.

Ans:

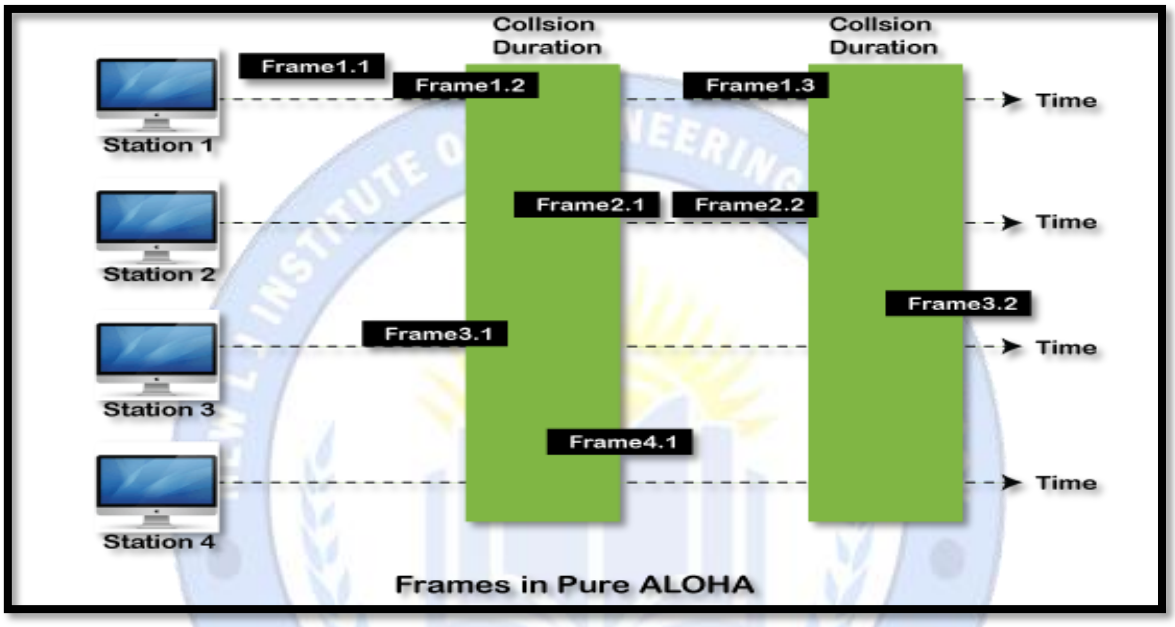


- **ALOHA :**
  - **ALO** means **"Share".**
  - **HA** means **"Essence of life"**
- It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data.
- Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.
- **Aloha Rules**
  - Any station can transmit data to a channel at any time.
  - It does not require any carrier sensing.
  - Collision and data frames may be lost during the transmission of data through multiple stations.
  - Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
  - It requires retransmission of data after some random amount of time.

- **Types of ALOHA:**



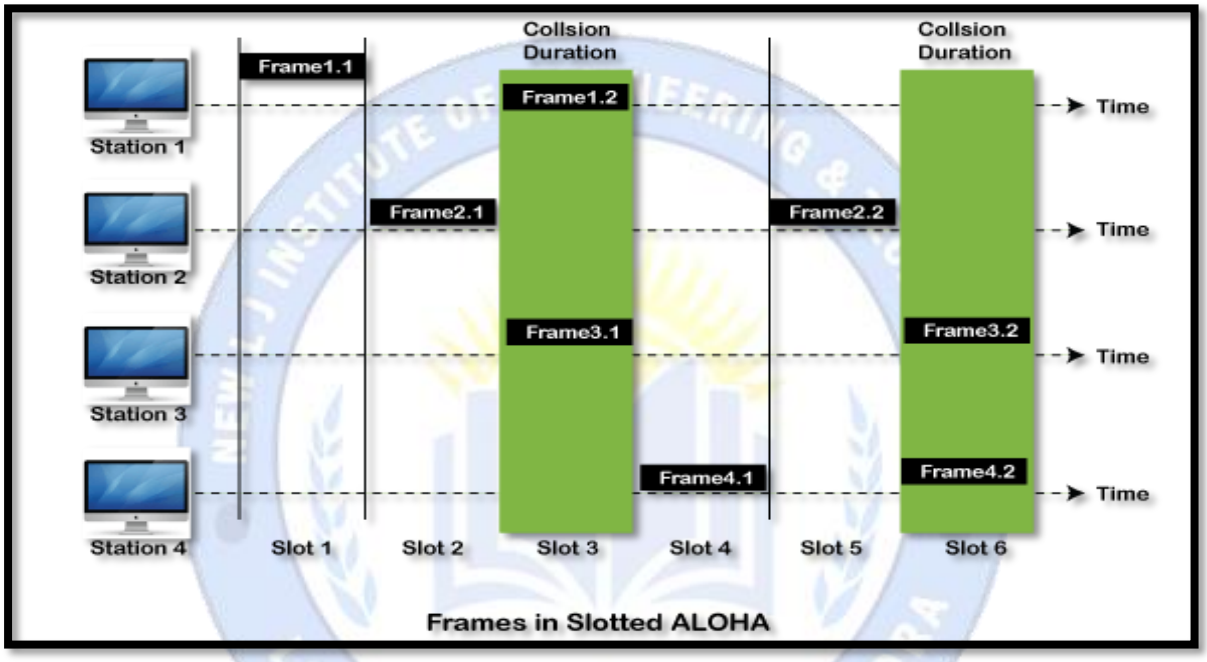
- **Pure Aloha:**



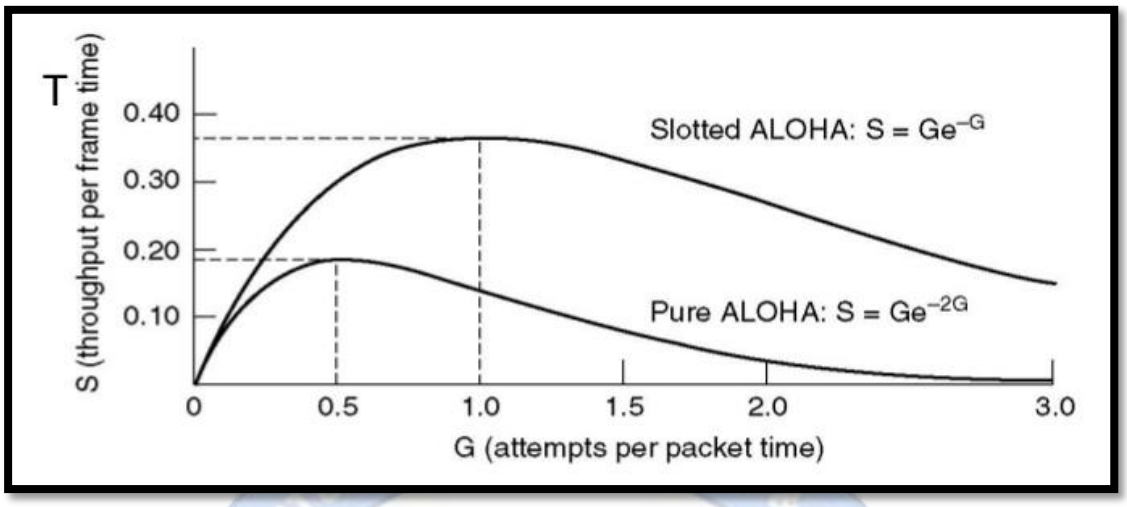
  - Whenever data is available for sending over a channel at stations, we use Pure Aloha.
  - In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost.
  - When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment.
  - If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.
    - The total vulnerable time of pure Aloha is 2 * Tfr.
    - Maximum throughput occurs when G = 1/ 2 that is 18.4%.
    - Successful transmission of data frame is S = G * e ^ - 2 G.
  - As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time.
  - Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end.

- At the same time, other frames are lost or destroyed.
- Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage.
- If the new frame's first bit enters the channel before finishing the last bit of the second frame.
- Both frames are completely finished, and both stations must retransmit the data frame.

- **Slotted Aloha:**

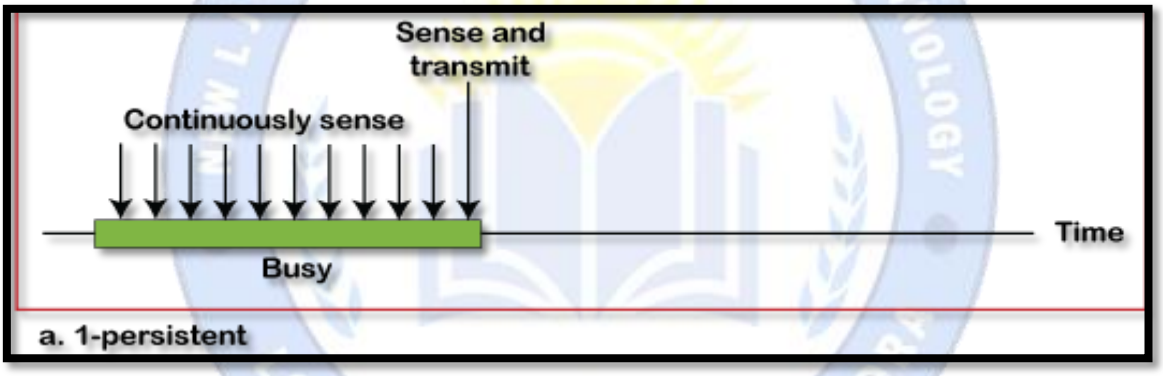


- The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting.
- In slotted Aloha, the shared channel is divided into a fixed time interval called slots.
- So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot.
- And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time.
- However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.
    - Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
    - The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
    - The total vulnerable time required in slotted Aloha is Tfr.

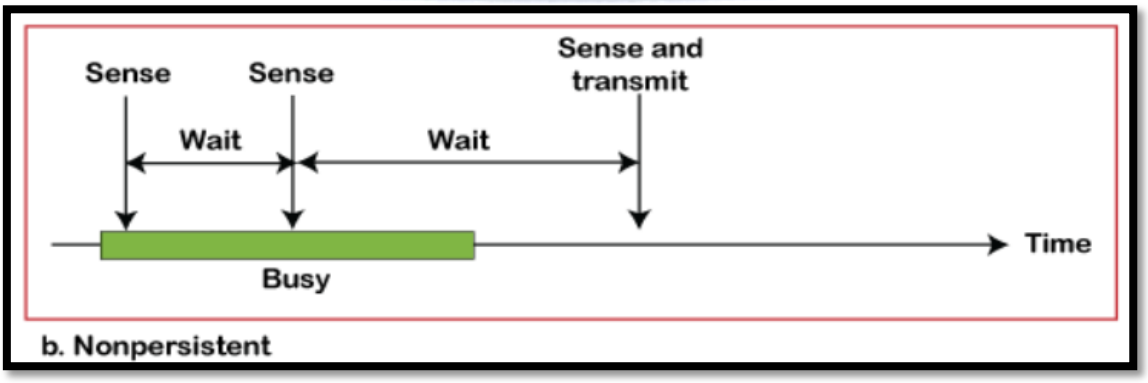

T
S (throughput per frame time)
0.40
0.30
0.20
0.10
Slotted ALOHA: S = Ge^–G
Pure ALOHA: S = Ge^–2G
0
0.5
1.0
1.5
2.0
3.0
G (attempts per packet time)

- **CSMA:**
  - It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data.
  - It means that if the channel is idle, the station can send data to the channel.
  - Otherwise, it must wait until the channel becomes idle.
  - Hence, it reduces the chances of a collision on a transmission medium.

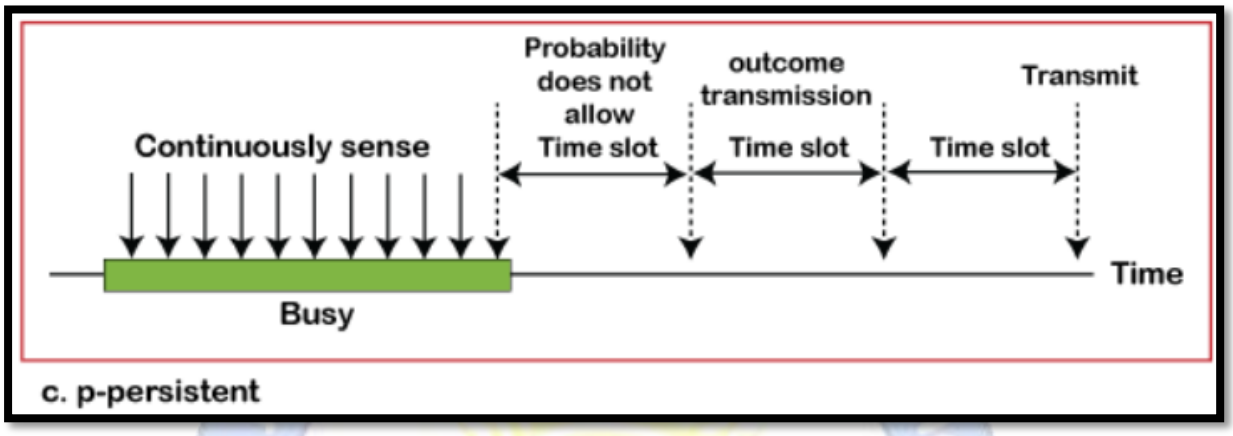
  - **CSMA Access Modes**
    - **1-Persistent:**
      - In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data.
      - Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.



    - **Non-Persistent:**
      - It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data.
      - Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.



- **P-Persistent:**
  - It is the combination of 1-Persistent and Non-persistent modes.
  - The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a P probability.
  - If the data is not transmitted, it waits for a (q = 1-p probability) random time and resumes the frame with the next time slot.



- **CSMA/CD:**
  - **CS:** It stands for **Carrier Sensing**. It implies that before sending data, a station first senses the carrier. If the carrier is found free, then the station transmits data else it refrains.
  - **MA:** Stands for **Multiple Access** i.e. if there's a channel, then there are many stations that are trying to access it.
  - **CD:** Stands for **Collision Detection**. It also guides to proceed in case of packet data collision.

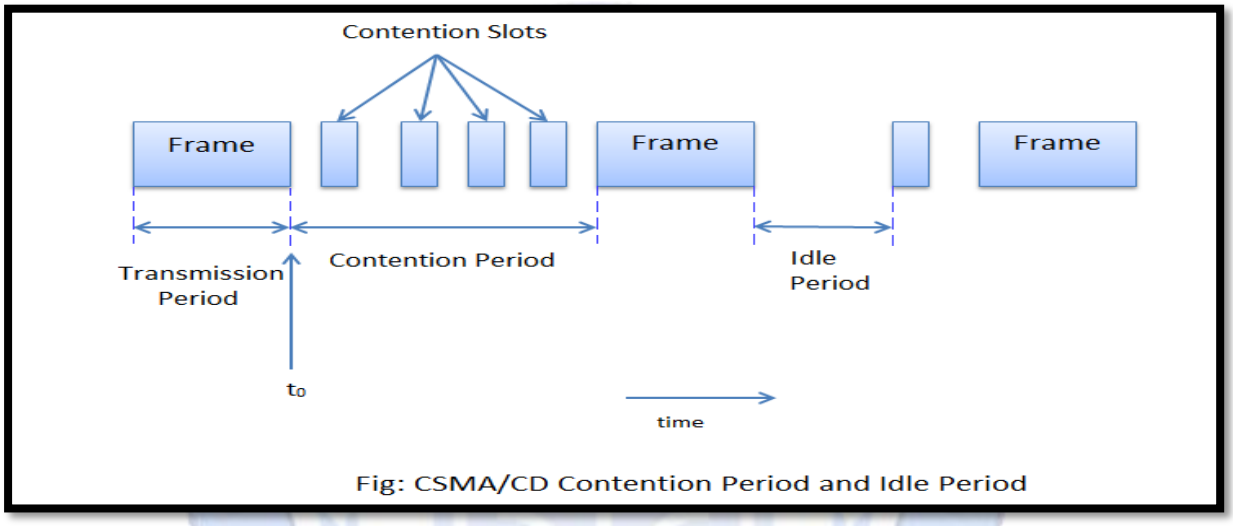
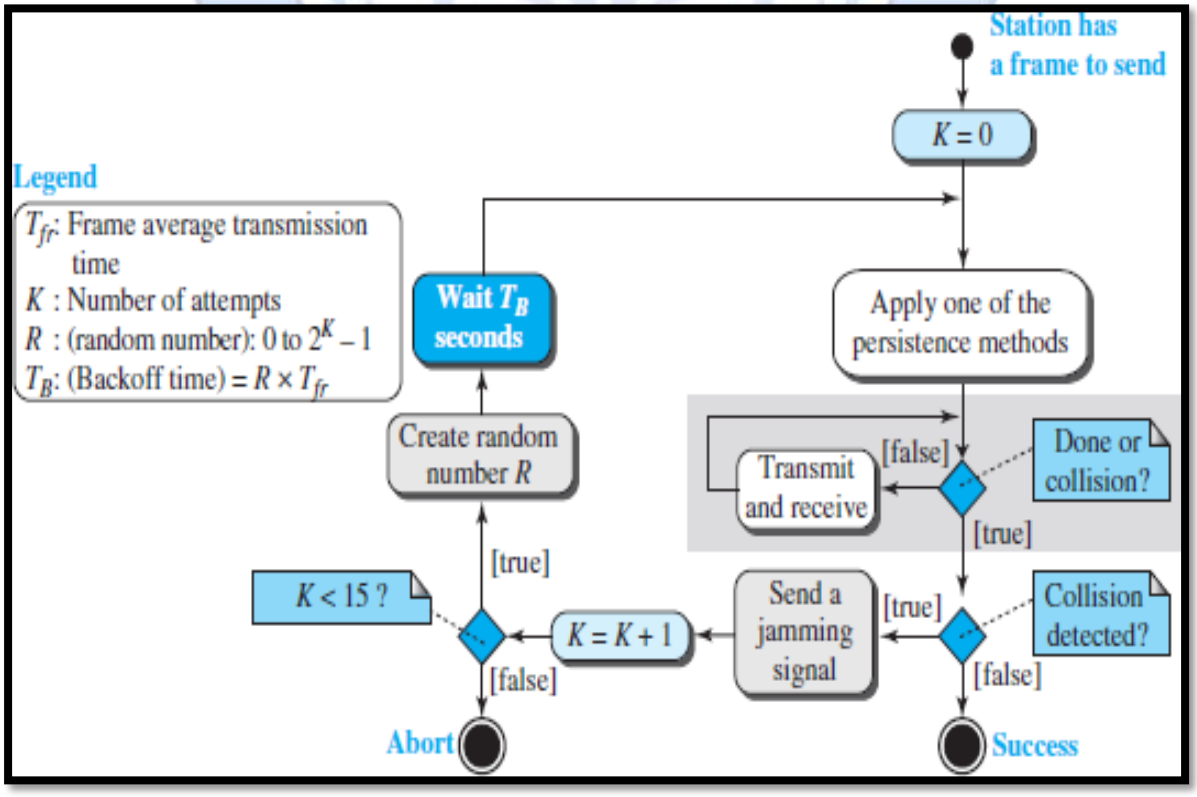
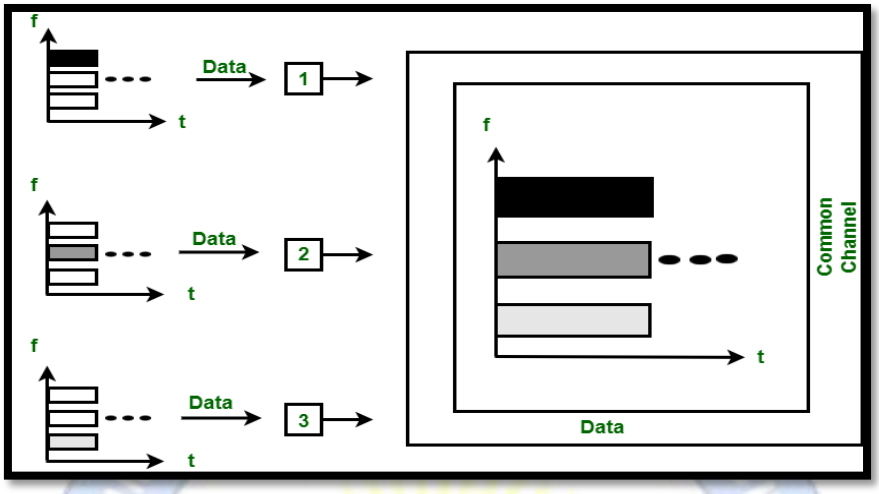


Fig: CSMA/CD Contention Period and Idle Period



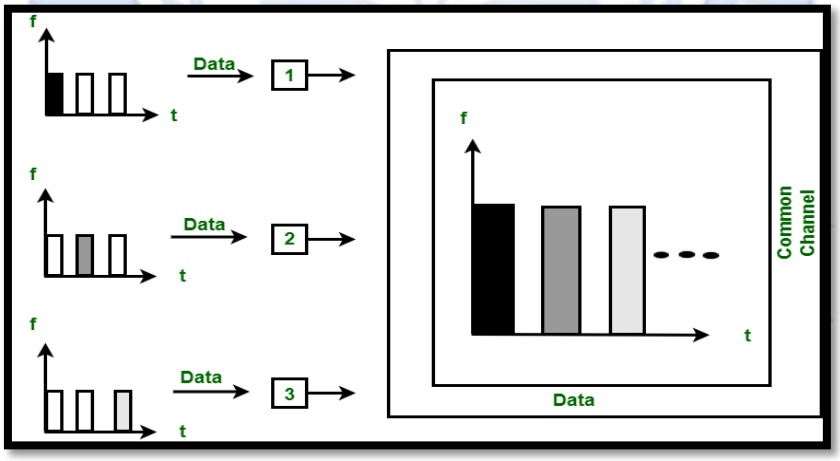
- The **Carrier Sense Multiple Access/ Collision Detection** protocol is used to detect a collision in the media access control (**MAC**) layer.
- Once the collision was detected, the CSMA CD immediately stopped the transmission by sending the signal so that the sender does not waste all the time to send the data packet.
- Suppose a collision is detected from each station while broadcasting the packets.
- In that case, the CSMA CD immediately sends a jam signal to stop transmission and waits for a random time context before transmitting another data packet.
- If the channel is found free, it immediately sends the data and returns it.
- **Advantages of CSMA CD:**
  - It is used for collision detection on a shared channel within a very short time.
  - CSMA CD is better than CSMA for collision detection.
  - CSMA CD is used to avoid any form of waste transmission.
  - When necessary, it is used to use or share the same amount of bandwidth at each station.
  - It has lower CSMA CD overhead as compared to the CSMA CA.

- **FDMA, TDMA and CDMA.**
- **FDMA:**



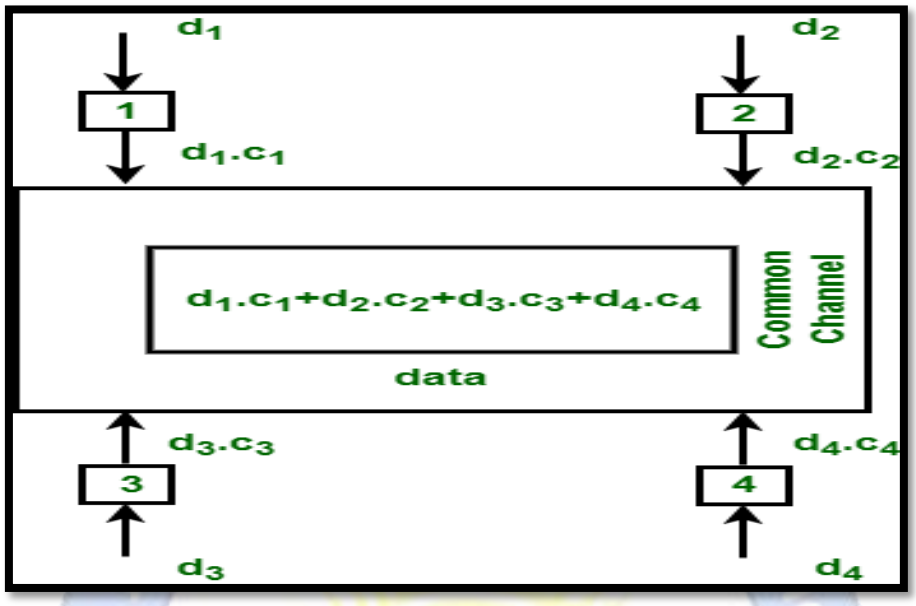
  - It is a frequency division multiple access (FDMA) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel.
  - Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.

- **TDMA**



  - Time Division Multiple Access (**TDMA**) is a channel access method.
  - It allows the same frequency bandwidth to be shared across multiple stations.
  - And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames.
  - The same **frequency** bandwidth into the shared channel by dividing the signal into various time slots to transmit it.
  - However, TDMA has an overhead of synchronization that specifies each station's time slot by adding synchronization bits to each slot.

- **CDMA**

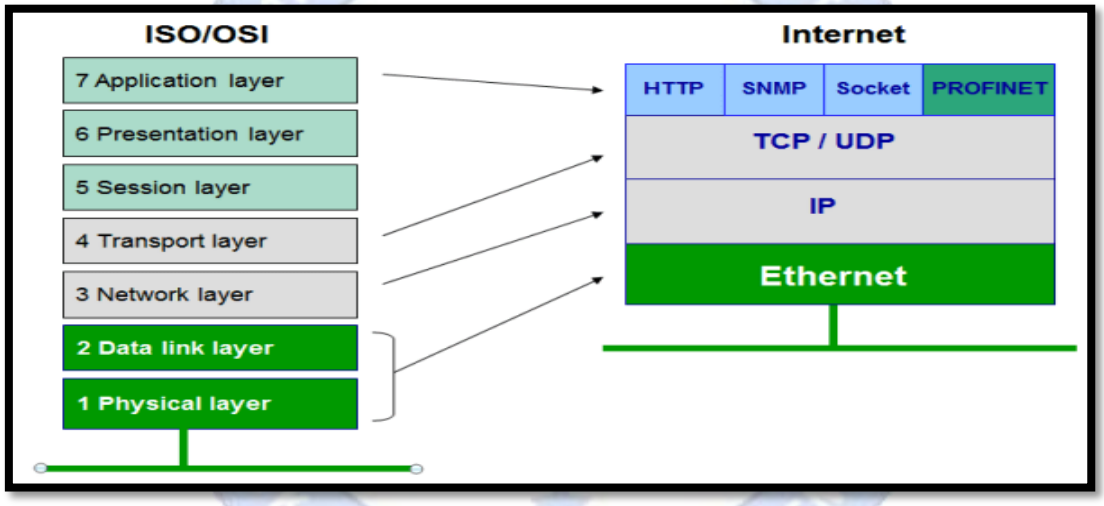


- The code division multiple access (CDMA) is a channel access method.
- In CDMA, all stations can simultaneously send the data over the same channel.
- It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times.
- It does not require the division of bandwidth on a shared channel based on time slots.
- If multiple stations send data to a channel simultaneously, their data frames are separated by a unique code sequence.
- Each station has a different unique code for transmitting the data over a shared channel.

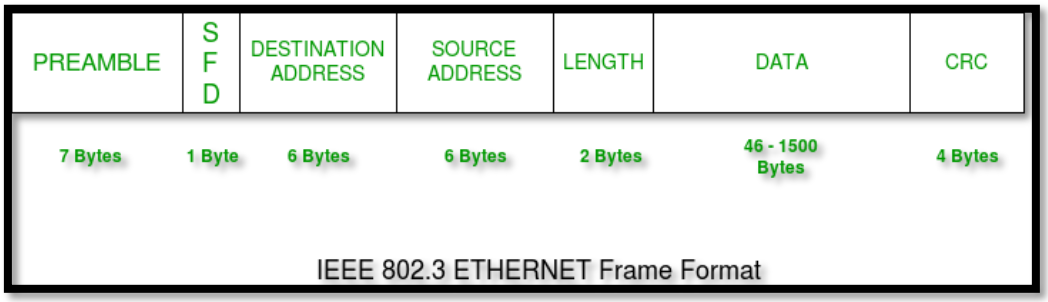
62. Explain Ethernet (IEEE standards 802.3).

Ans:

- **Ethernet** is the most widely used LAN technology, which is defined under IEEE **standards 802.3.**
- The reason behind its wide usability is Ethernet is easy to understand, implement, maintain, and allows low-cost network implementation.
- Also, Ethernet offers flexibility in terms of topologies that are allowed.
- Ethernet generally uses Bus Topology.
- Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer.



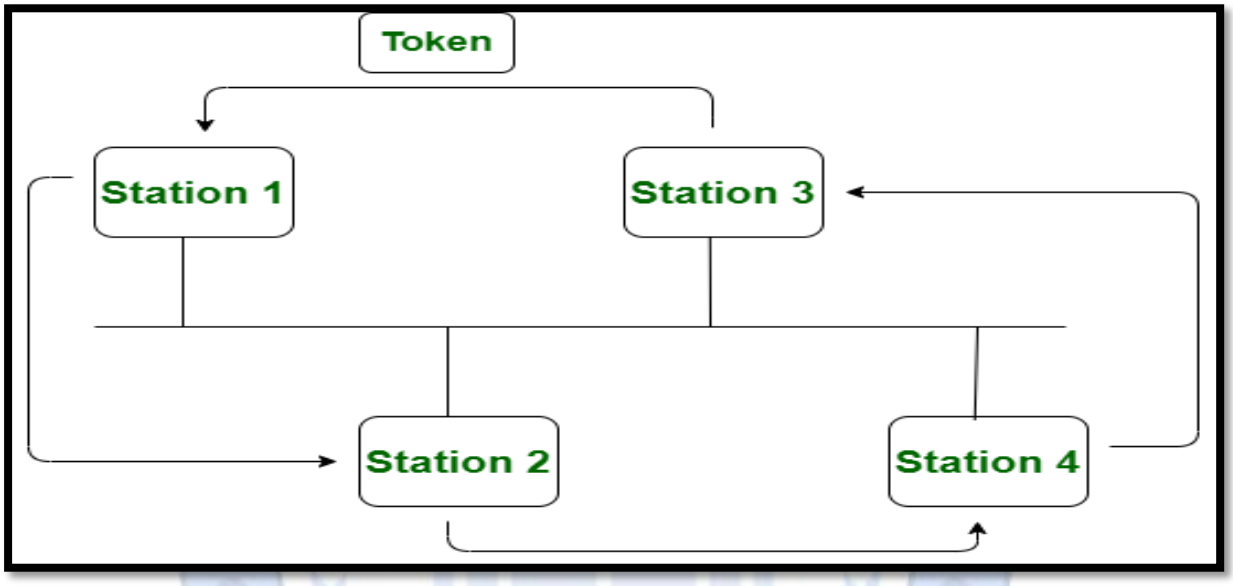
- For Ethernet, the protocol data unit is Frame since we mainly deal with DLL.
- In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.
- Manchester Encoding Technique is used in Ethernet.
- Since we are talking about IEEE 802.3 standard Ethernet, therefore, 0 is expressed by a high-to-low transition, a 1 by the low-to-high transition.
- In both Manchester Encoding and Differential Manchester, the Encoding Baud rate is double of bit rate.
- **Ethernet Frame Format:**



63. Explain Token bus (IEEE standards 802.4) and Token ring (IEEE standards 802.5).

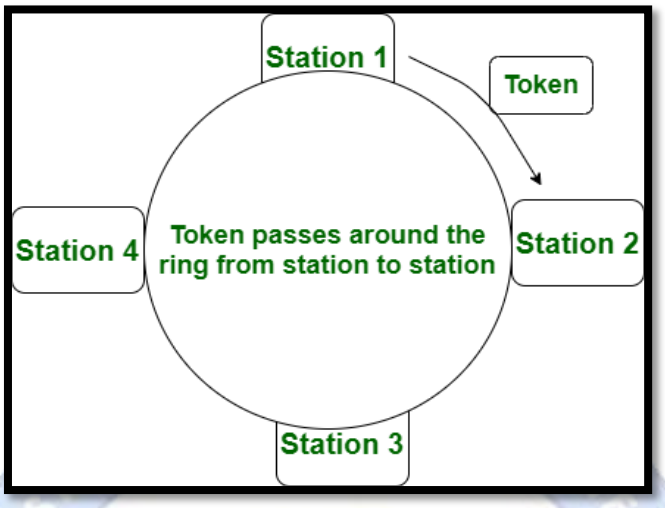
Ans:

- **Token bus (IEEE standards 802.4):**



- **Token Bus (IEEE 802.4)** is a popular standard for token passing LANs.
- In a token bus LAN, the physical media is a bus or a tree, and a logical ring is created using a coaxial cable.
- The token is passed from one user to another in a sequence (clockwise or anticlockwise).
- Each station knows the address of the station to its "left" and "right" as per the sequence in the logical ring.
- A station can only transmit data when it has the token.
- The working of a token bus is somewhat similar to Token Ring.
- The Token Bus (IEEE 802.4) is a standard for deploying token rings in LANs over a virtual ring.
- The physical medium uses coaxial cables and has a bus or tree architecture.
- The nodes/stations form a virtual ring, and the token is transmitted from one node to the next in a sequence along the virtual ring.
- Each node knows the address of the station before it and the station after it. When a station has the token, it can only broadcast data.
- **The token bus works in a similar way as the Token Ring.**

- **Token ring (IEEE 802.5):**

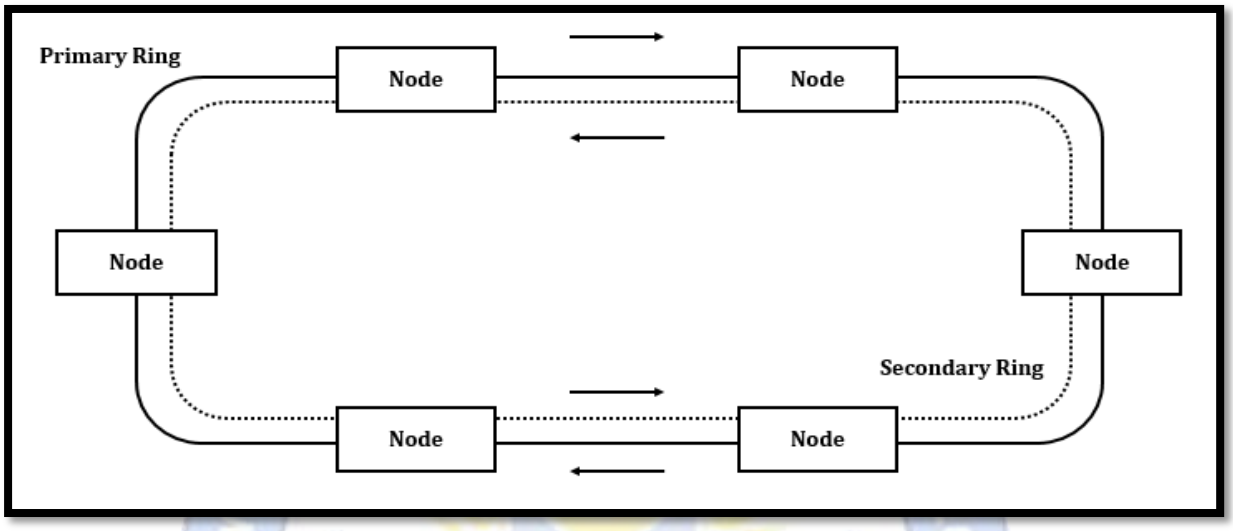


- Token ring (IEEE 802.5) is a communication protocol in a local area network (LAN) where all stations are connected in a ring topology and pass one or more tokens for channel acquisition.
- A token is a special frame of 3 bytes that circulates along the ring of stations.
- A station can send data frames only if it holds a token.
- The tokens are released on successful receipt of the data frame.
- If a station has a frame to transmit when it receives a token, it sends the frame and then passes the token to the next station; otherwise it simply passes the token to the next station.
- Passing the token means receiving the token from the preceding station and transmitting to the successor station.
- The data flow is unidirectional in the direction of the token passing.
- In order that tokens are not circulated infinitely, they are removed from the network once their purpose is completed.

64. Write a short note: FDDI and DQDB (IEEE standards 802.6).

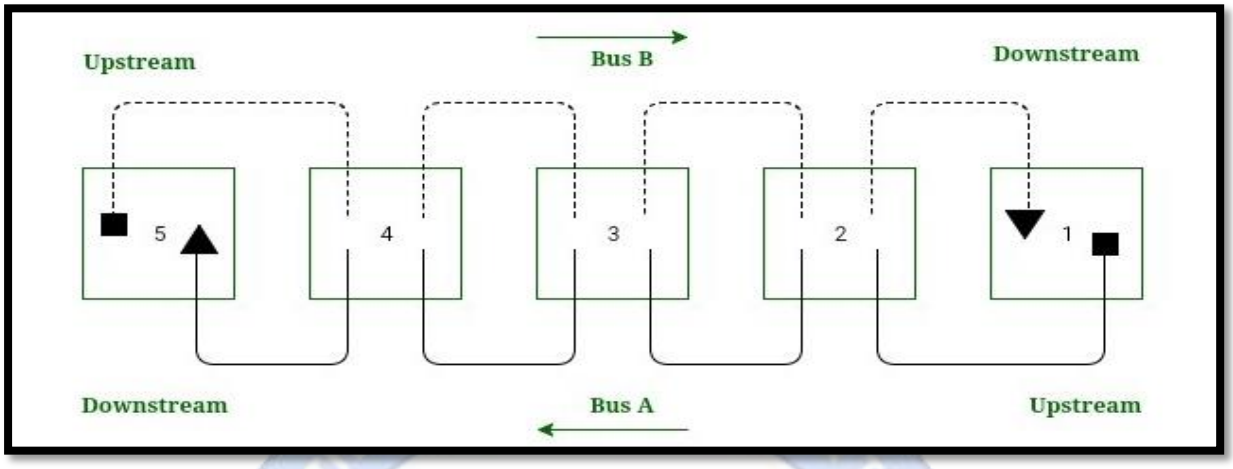
Ans:

- **FDDI.**



- FDDI stands for **Fiber Distributed Data Interface**.
- FDDI is a set of ANSI and ISO standards for data transmission on fiber optic lines in a local area network.
- In addition to being large geographically, an FDDI local area network can support thousands of users.
- FDDI is frequently used on the backbone for a wide area network (WAN).
- The FDDI protocol is based on the token ring protocol.
- An FDDI network contains two token rings, one for possible backup in case the primary ring fails.
- Any station wants to transmit information holds the token and then transmits the information.
- When it finish it release the token in the ring.
- The time a station holds the token is called as Synchronous Allocation Time (SAT).
- SAT time is variable for each station.
- The allocation of this time to each station is achieved by Station Management (SMT).
- The function of SMT are Ring Control, Ring Initialization, Station Insertion and Station Removal.
- **FDDI Characteristics:**
  1. FDDI provides 100 Mbps of data throughput.
  2. FDDI includes two interfaces.
  3. It is used to connect the equipment to the ring over long distances.
  4. FDDI is a LAN with Station Management.
  5. Allows all stations to have equal amount of time to transmit data.

- **IEEE 802.6(DQDB):**

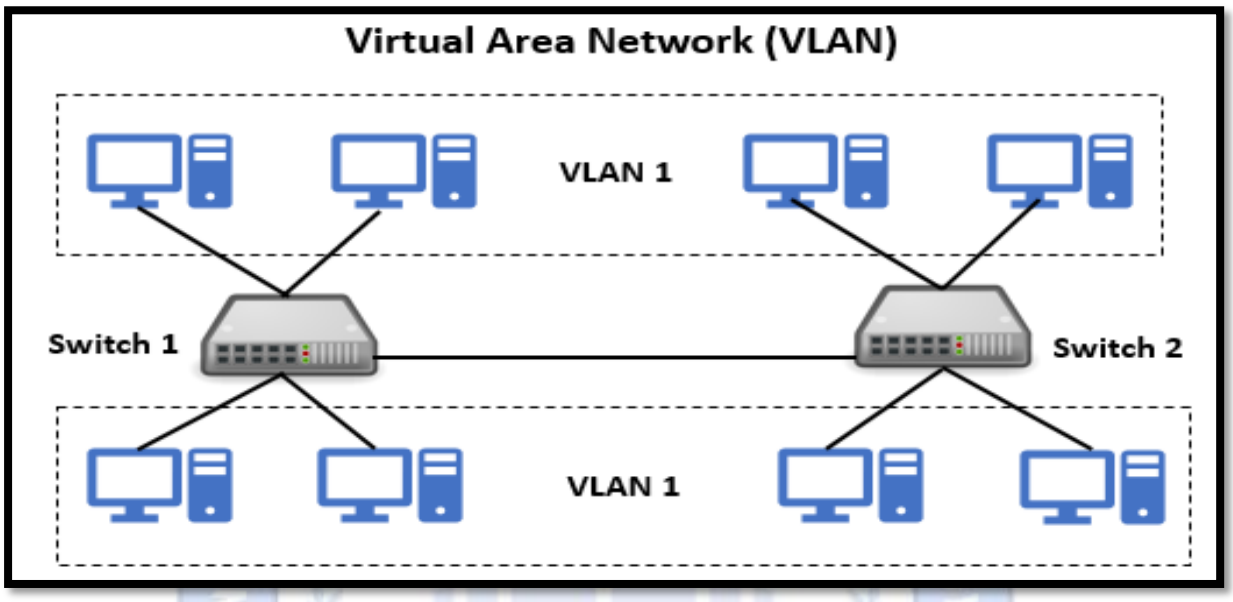


- IEEE 802.6 standard i.e. DQDB(Distributed Queue Dual Bus) is a MAN(Metropolitan Area Network) protocol.
- It can be defined as a high speed shared medium access control protocol that is used over a bus network.
- It has two unidirectional buses, for controlling purposes, where the bus can carry data, video, and voice over a network with bandwidth being allocated as per time slots.
- The advantage of using the paired bus is that it is used to tackles failure configuration.
- It can be extended up to 30 miles at 34-55 Mbps.
- **Directional Traffic:**
  - Each bus support traffic in only one direction and are opposite to one another.
  - The start of the bus being represented as a *square* and the end of the bus being represented as a *triangle* (Fig.).
  - Bus A traffic moves from right to left (i.e. from station 1 to 5) whereas the bus B traffic moves from left to right (i.e. from station 5 to 1).
- **Upstream and Downstream:**
  - The relationship of stations of the DQDB network depends on the directional flow of traffic of the buses.
  - Considering bus A in Fig., which has station 1 & 2 marked as upstream w.r.t station 3 and station 4 & 5 are downstream w.r.t station 3.
  - Here in bus A, station 1 is head of the bus as there is no upstream station and station 5 has no downstream station and it is regarded as to end of bus A.
- **Applications of IEEE 802.6 (DQDB)**
  - Video Conferencing
  - Real-Time Applications
  - Data Transfer

65. Write a short note: VLAN (Virtual Local Area Network).

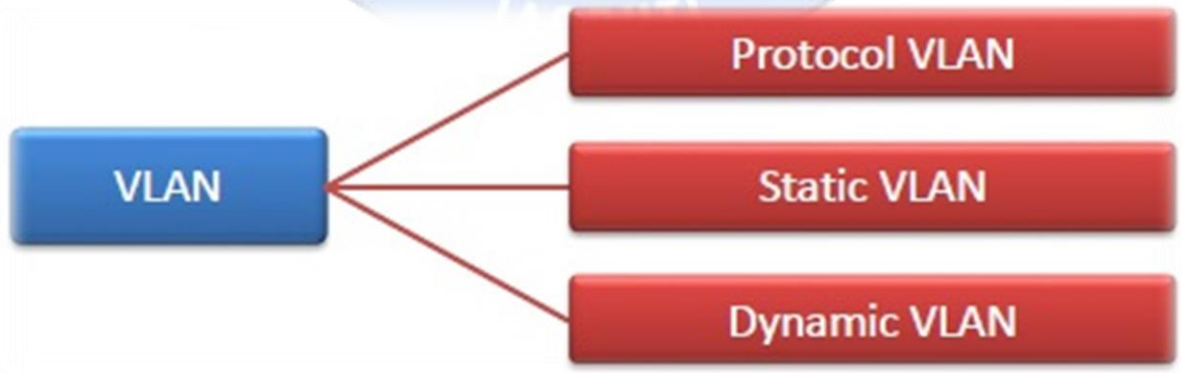
Ans:

- VLAN stands for **Virtual Local Area Network**.



- A virtual local area network (VLAN) is a virtualized connection that connects multiple devices and network nodes from different LANs into one logical network.
- VLAN is a logical system grouping in the same area of the broadcast.
- VLANs are configured on switches by putting interfaces in one and many interfaces on another broadcast domain.

- **Types of VLANs:**



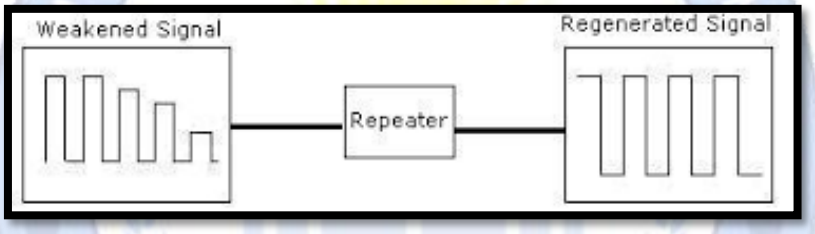
- **Protocol VLAN:**
  - Here, the traffic is handled based on the protocol used.
  - A switch or bridge segregates, forwards or discards frames the come to it based upon the traffics protocol.

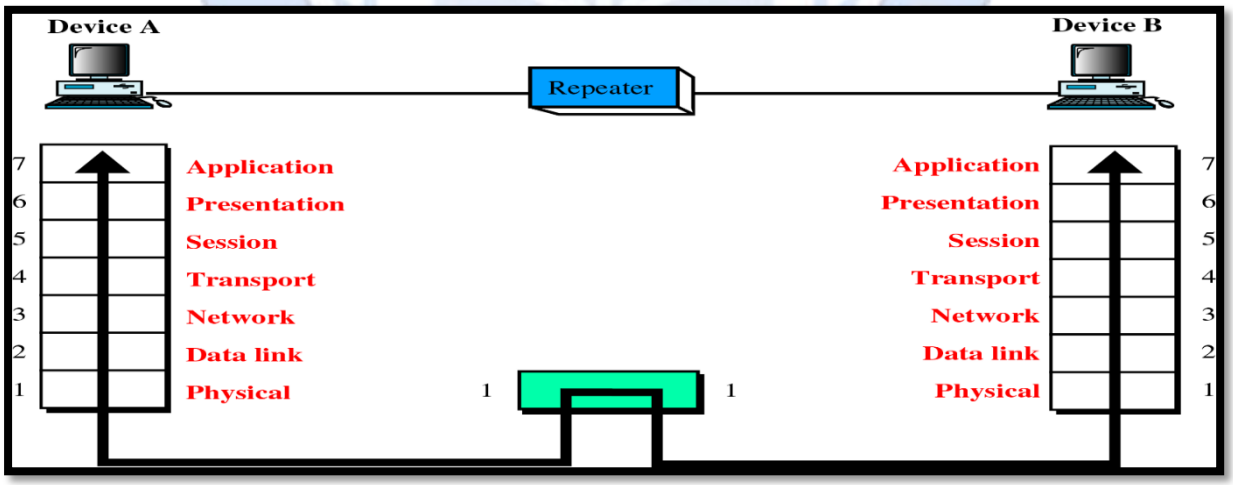
- **Port-based VLAN:**
  - This is also called static VLAN.
  - Here, the network administrator assigns the ports on the switch / bridge to form a virtual network.
- **Dynamic VLAN:**
  - The network administrator simply defines network membership according to device characteristics.

66. Explain Different types of Networking Connecting Devices (Repeater, Hub, Switch, Bridge, Router and Gateways).

Ans:

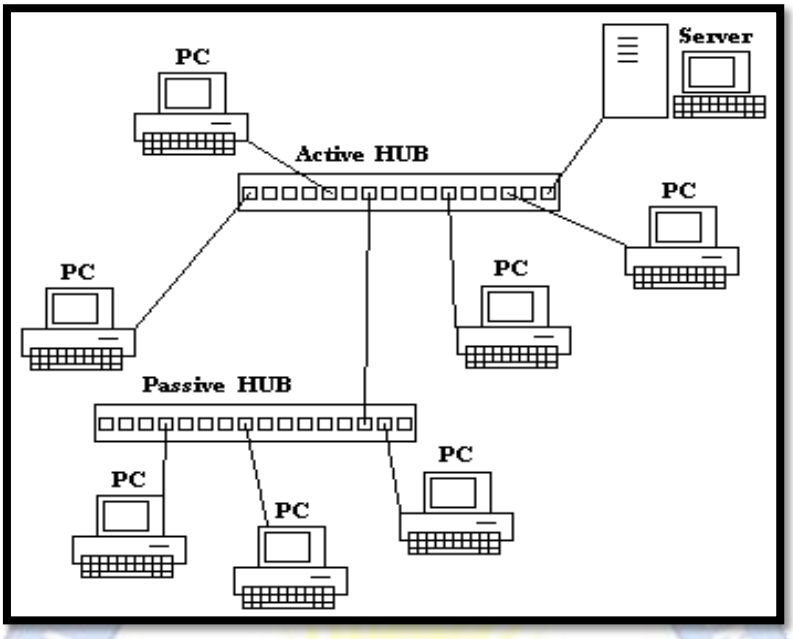
- Different types of Networking Connecting Devices are:
  - Repeater
  - Hub
  - Switch
  - Bridge
  - Router
  - Gateways
- **Repeater**:



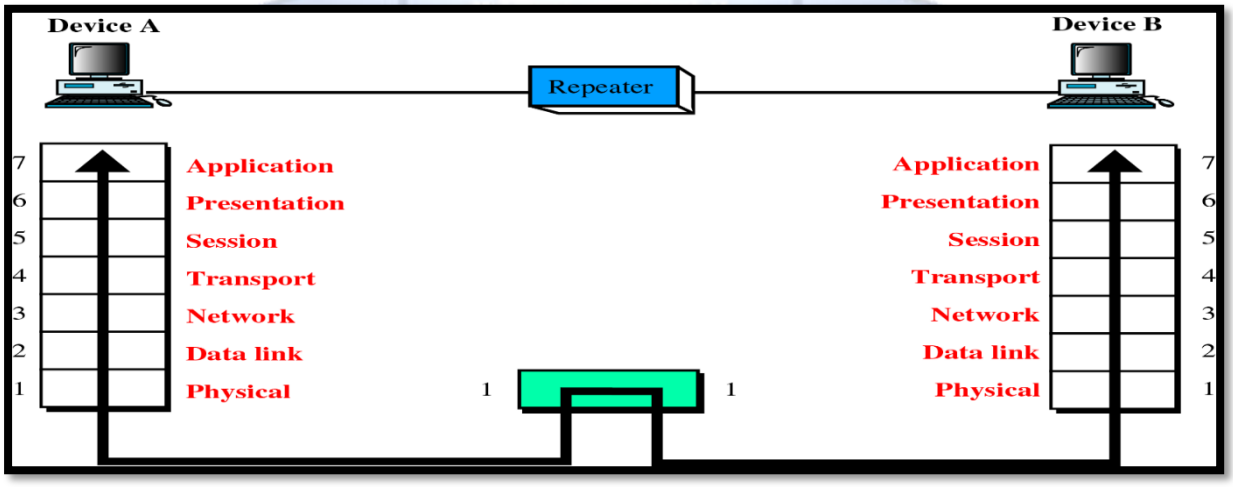


  - A repeater operates at the physical layer.
  - Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
  - An important point to be noted about repeaters is that they do not amplify the signal.
  - When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.
  - It is a 2-port device.

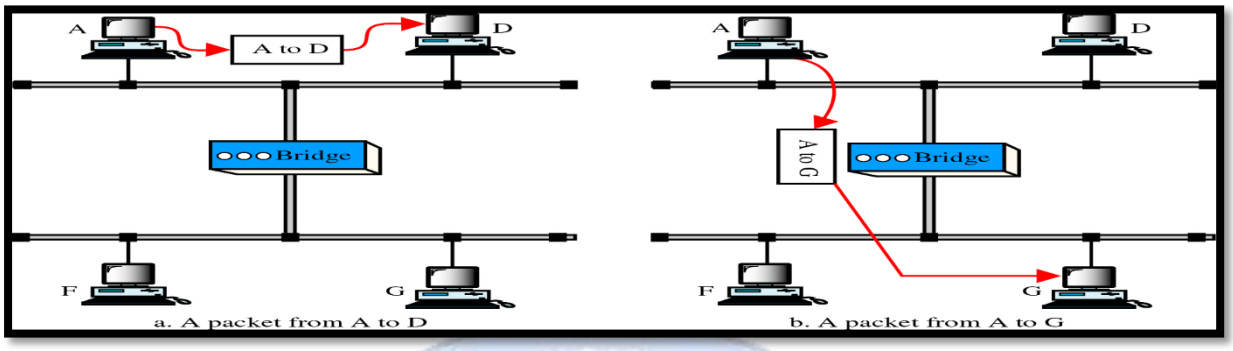
- **Hub:**

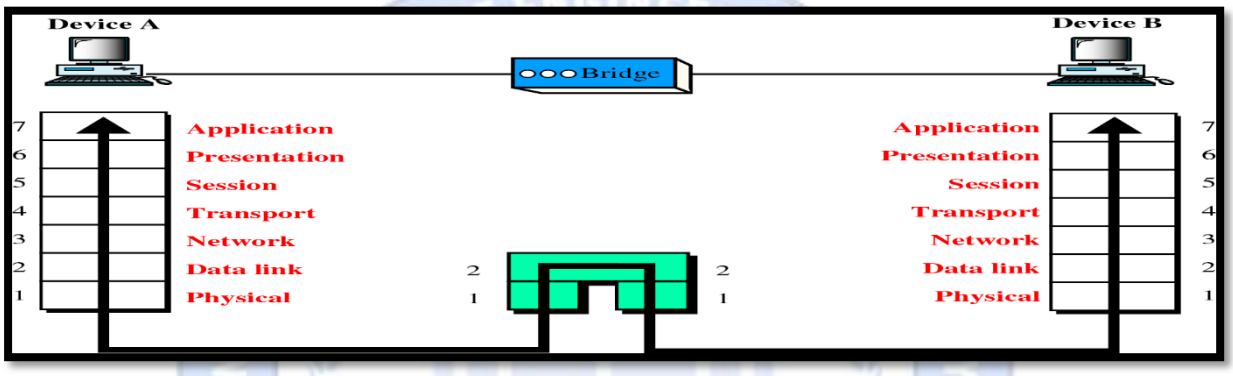


  - A hub is basically a multiport repeater.
  - A hub **works at** the **physical layer (layer 1)** of the OSI model.
  - A hub connects multiple wires coming from different branches.
  - **Types of Hub**
    - **Active Hub :-**
      - These are the hubs which have their own power supply and can clean , boost and relay the signal along the network.
      - These are used to extend maximum distance between nodes.
    - **Passive Hub :-**
      - These are the hubs which collect wiring from nodes and power supply from active hub.

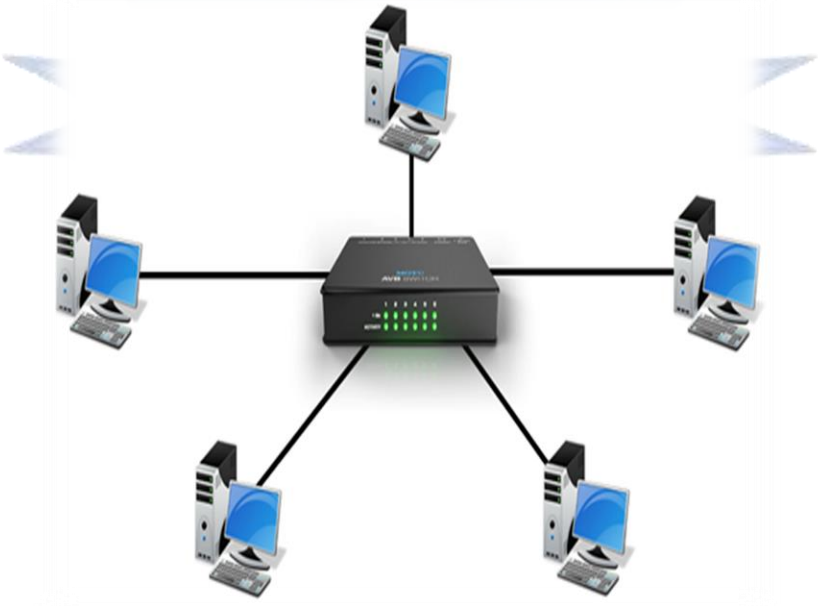


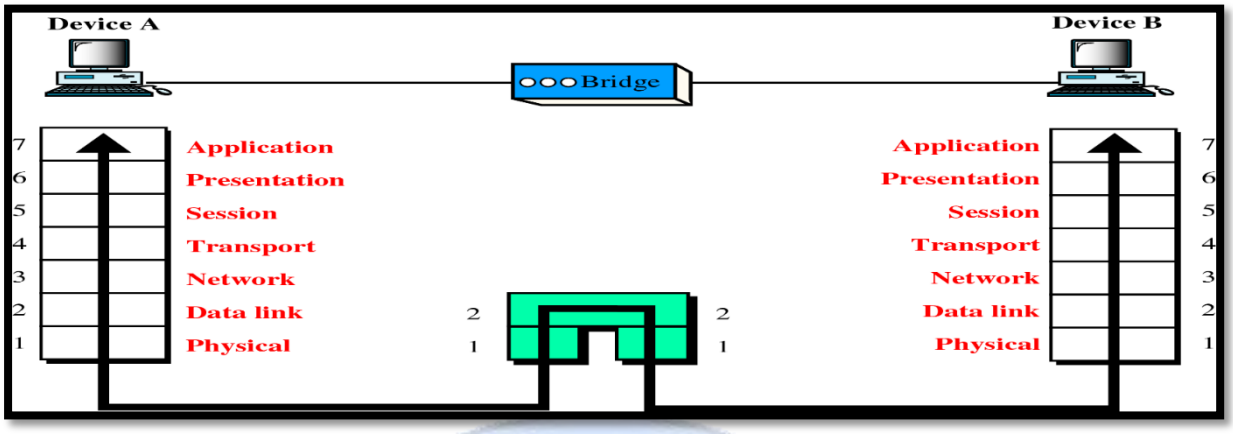
- **Bridge:**





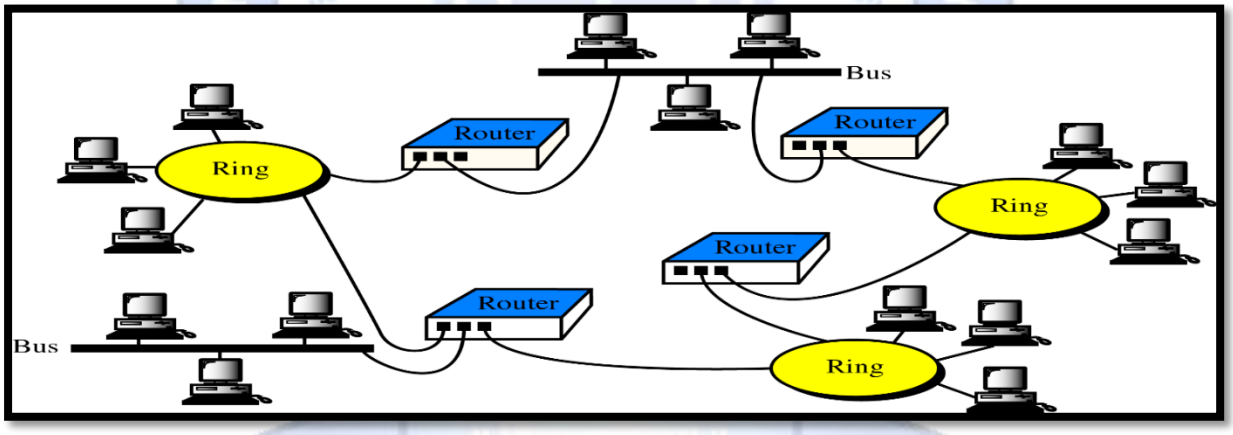
  - A bridge operates at **data link layer**.
  - A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination.
  - It is also used for interconnecting two LANs working on the same protocol.
  - It has a single input and single output port, thus making it a **2-port device**.
- **Switch**:

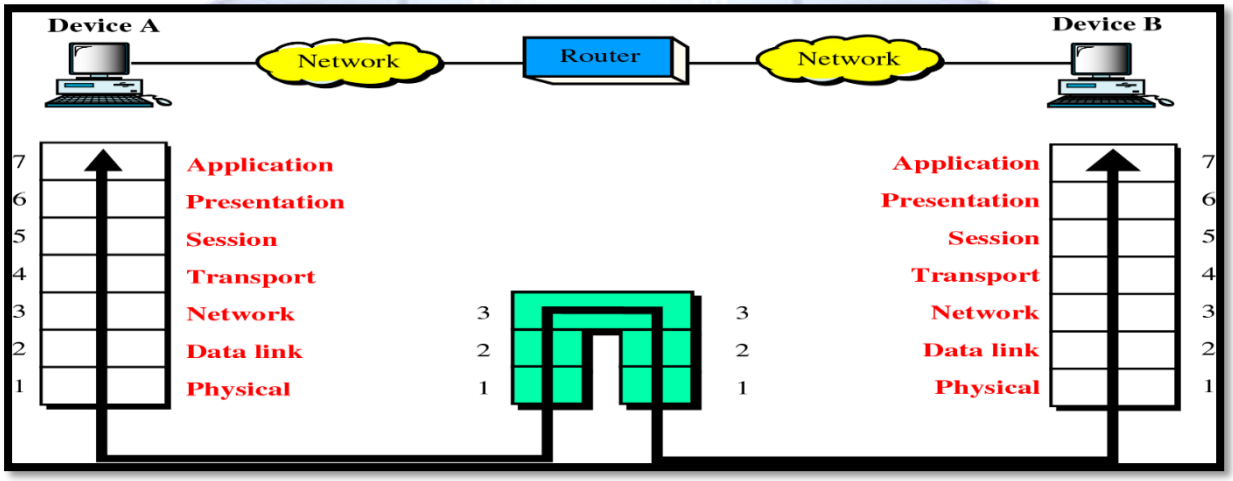




- Switch is **data link** layer device.
- A switch is a multi-port bridge with a buffer and a design that can boost its efficiency (large number of ports imply less traffic) and performance.
- Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.
- In other words, switch divides collision domain of hosts, but broadcast domain remains same.

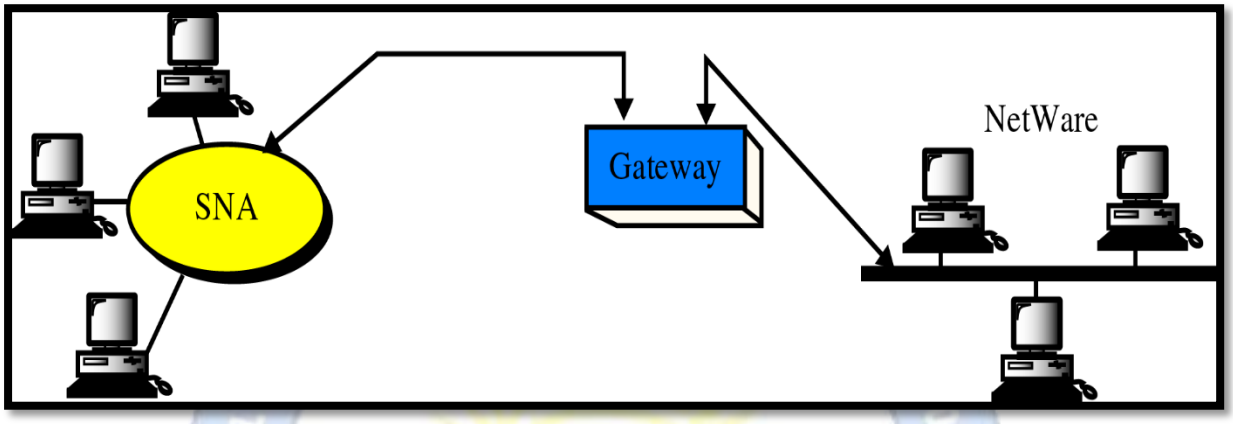
- **Routers:**

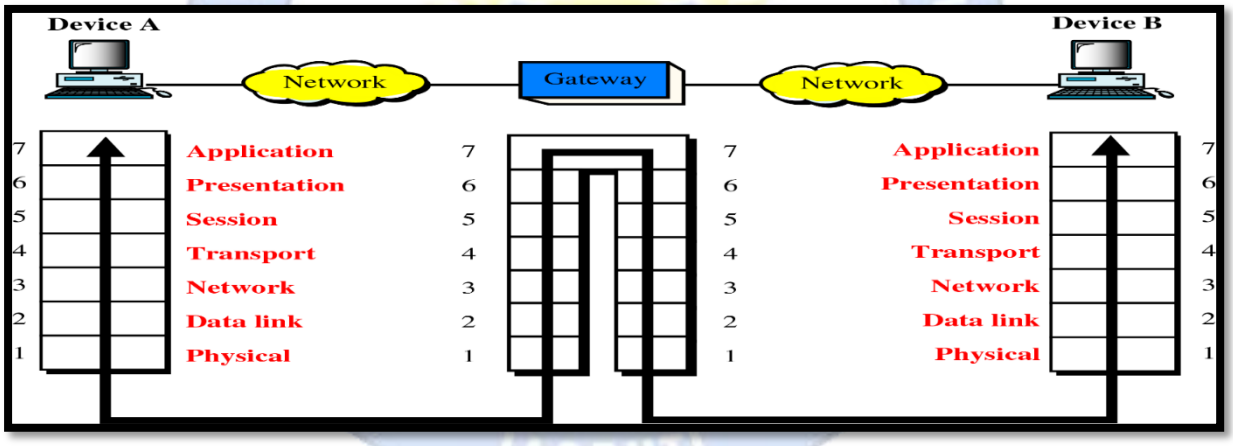




- Router is mainly a Network Layer device.
- A router is a device like a switch that routes data packets based on their IP addresses.
- Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.
- Router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

- **Gateway:**





- Gateway is mainly used All seven Layer in OSI Model.
- A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models.
- They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

67. Difference Between:

a. **Pure ALOHA and Slotted ALOHA**

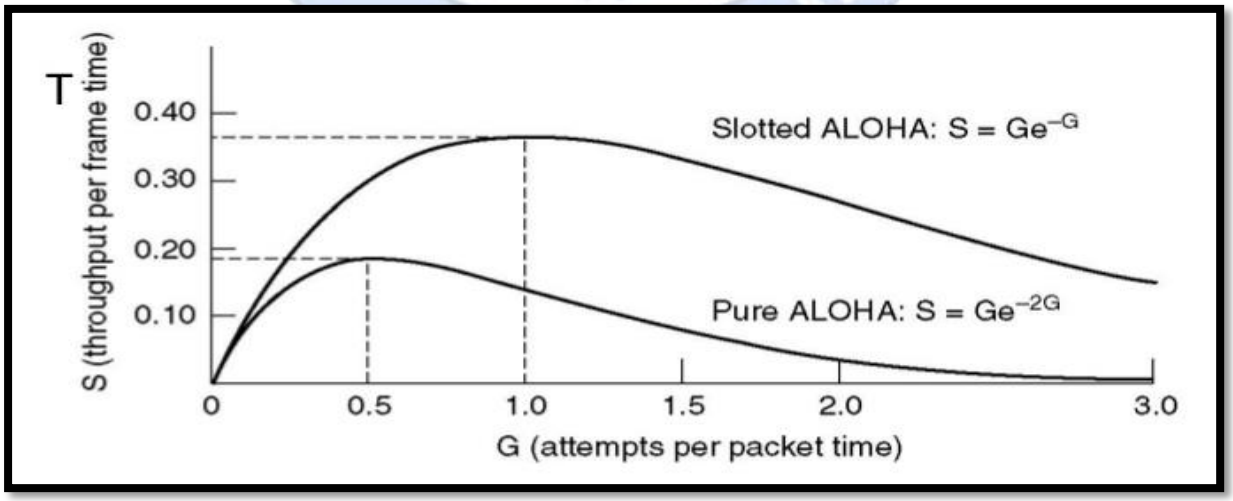
b. **FDMA, TDMA, and CDMA**

c. **Token Bus and the Token Ring**

Ans:

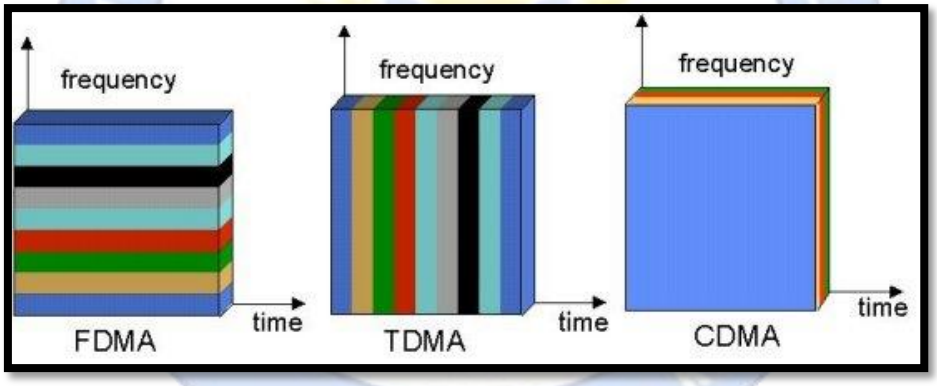
a. Pure ALOHA and Slotted ALOHA

BASIS FOR COMPARISON	PURE ALOHA	SLOTTED ALOHA
Frame Transmission	The user can transmit the data frame whenever the station has the data to be transmitted.	The user has to wait till the next time slot start, to transmit the data frame.
Time	In Pure ALOHA the time is continuous.	In Slotted ALOHA the time is discrete.
Successful Transmission	The probability of successful transmission of the data frame is: S= G* e^-2G	The probability of successful transmission of the data frame is: S= G*e^-G
Synchronization	The time is not globally synchronized.	The time here is globally synchronized.
Maximum Efficiency	Maximum efficiency = 18.4%.	Maximum efficiency = 36.8%.
Number of collisions	Does not reduce the number of collisions.	Slotted Aloha reduces the number of collisions to half, thus doubles the efficiency.



b. FDMA, TDMA, and CDMA

Parameters	FDMA	TDMA	CDMA
Full Form	Frequency Division Multiple Access.	Time Division Multiple Access.	Code Division Multiple Access.
Flexibility	It has a little flexible.	It has moderate flexibility.	It has high flexibility.
Rate of Data	It has a low data rate.	It has a medium data rate.	It has a high data rate.
Synchronization	It doesn't need any synchronization.	It requires synchronization.	It also doesn't require any synchronization.
Codeword	It doesn't require a codeword.	It also doesn't require a codeword.	It needs a codeword.
Mode of data transfer	Mode of data transfer is continuous signal.	Mode of data transfer is signal in bursts.	Mode of data transfer is digital signal.
Cost	It has a high cost.	It has a low cost.	Its installation cost is high, but operational cost is low.



c. Token Bus and the Token Ring

Parameters	Token Bus	Token Ring
IEEE standard	IEEE 802.4 standard	IEEE 802.5 standard
Bandwidth	Better	Does Not Provide Better
Networks are Reliable	No	Yes
Topology is Used	Bus topology is used.	Star topology is used.
Cable is Used	Coaxial Cable	Twisted Pair and Fiber Optic
Network is Designed	Large Industries.	Offices.

- **Teaching and Examination Scheme:**

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE (E)	PA (M)	ESE (V)	PA (I)	
4	0	2	5	70	30	30	20	150

Unit No.	Unit Title	% Weightage
1	Introduction to computer networks and Internet	15
2	Application Layer	17
3	Transport Layer	25
4	Network Layer	25
5	The Link layer and Local Area Networks	18