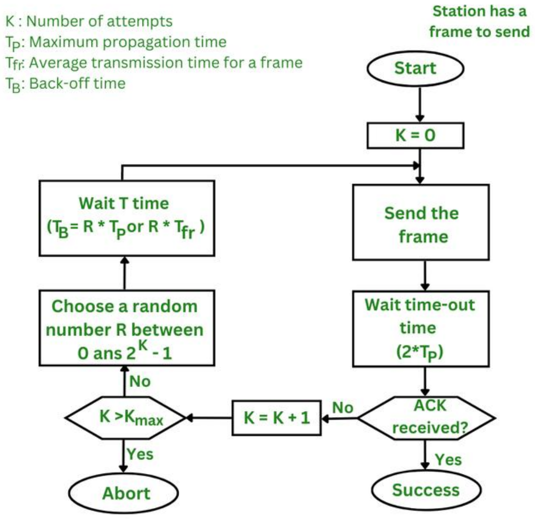
1) Explain Pure and Slotted ALOHA with figure.

Pure ALOHA :-

- Pure ALOHA refers to the original ALOHA protocol. The idea is that each station sends a frame whenever one is available. Because there is only one channel to share, there is a chance that frames from different stations will collide.
- The pure ALOHA protocol utilizes acknowledgments from the receiver to ensure successful transmission. When a user sends a frame, it expects confirmation from the receiver. If no acknowledgment is received within a designated time period, the sender assumes that the frame was not received and retransmits the frame.
- When two frames attempt to occupy the channel simultaneously, a collision occurs and both frames become garbled. If the first bit of a new frame overlaps with the last bit of a frame that is almost finished, both frames will be completely destroyed and will need to be retransmitted. If all users retransmit their frames at the same time after a time-out, the frames will collide again.
- To prevent this, the pure ALOHA protocol dictates that each user waits a random amount of time, known as the back-off time, before retransmitting the frame. This randomness helps to avoid further collisions.


K : Number of attempts
T_P: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Station has a frame to send
Start
K = 0
Wait T time (T_B = R * T_p or R * T_{fr})
Send the frame
Choose a random number R between 0 ans 2^K - 1
Wait time-out time (2*T_p)
No
K >K_{max}
K = K + 1
No
ACK received?
Yes
Yes
Abort
Success

- The time-out period is equal to the maximum possible round-trip propagation delay, which is twice the amount of time required to send a frame between the two most widely separated stations (2 x Top).

Throughput of Pure ALOHA

- The probability of successful transmission (S) can be derived from the probability that no other packets are sent during the vulnerable time period. This is given by:
- S = G × e-2G
- where:
- S is the throughput (the average number of successful packet transmissions per packet time).
- G is the average number of packets generated by the system in one packet time .
- **Maximum Throughput of Pure ALOHA**
- The **maximum throughput** occurs when G=0.5
- Smax=0.5 × e-1 ≈ 0.184

- This means the **maximum throughput of Pure ALOHA** is approximately 18.4%. In other words, only about 18.4% of the time is used for successful transmissions, and the rest is lost due to collisions.

Key Features of Pure ALOHA

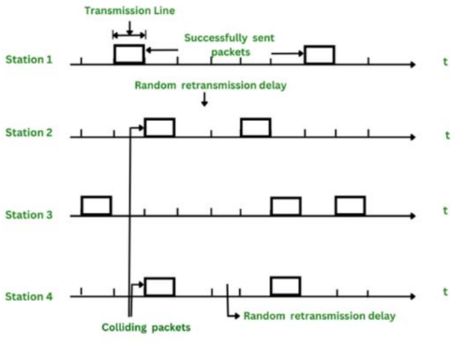
1) Random Access
2) Uncoordinated Transmission
3) Simple Implementation
4) Persistent Approach
5) Contention-Based

Slotted ALOHA

- Slotted ALOHA is an improved version of the pure ALOHA protocol that aims to make communication networks more efficient. In this version, the channel is divided into small, fixed-length time slots and users are only allowed to transmit data at the beginning of each time slot. This synchronization of transmissions reduces the chances of collisions between devices, increasing the overall efficiency of the network

How Does Slotted ALOHA work?

- The channel time is separated into time slots in slotted ALOHA, and stations are only authorized to transmit at particular times. These time slots correspond to the packet transmission time exactly. All users are then synchronized to these time slots so that whenever a user sends a packet, it must precisely match the next available channel slot. As a result, wasted time due to collisions can be reduced to one packet time or the susceptible period can be half.
- When a user wants to transmit a frame, it waits until the next time slot and then sends the frame. If the frame is received successfully, the receiver sends an acknowledgment. If the acknowledgment is not received within a time-out period, the sender assumes that the frame was not received and retransmits the frame in the next time slot.


Transmission Line
Successfully sent packets
Station 1
t
Random retransmission delay
Station 2
t
Station 3
t
Station 4
t
Random retransmission delay
Colliding packets

- Slotted ALOHA increases channel utilization by reducing the number of collisions. However, it also increases the delay for users, as they have to wait for the next time slot to transmit their frames. It's also worth noting that there is a variant of slotted ALOHA called "non-persistent slotted ALOHA" which is a variation of slotted ALOHA, in this variant the station that wants to send data, first listens to the channel before sending the data. If the channel is busy it waits for a certain time before trying again.

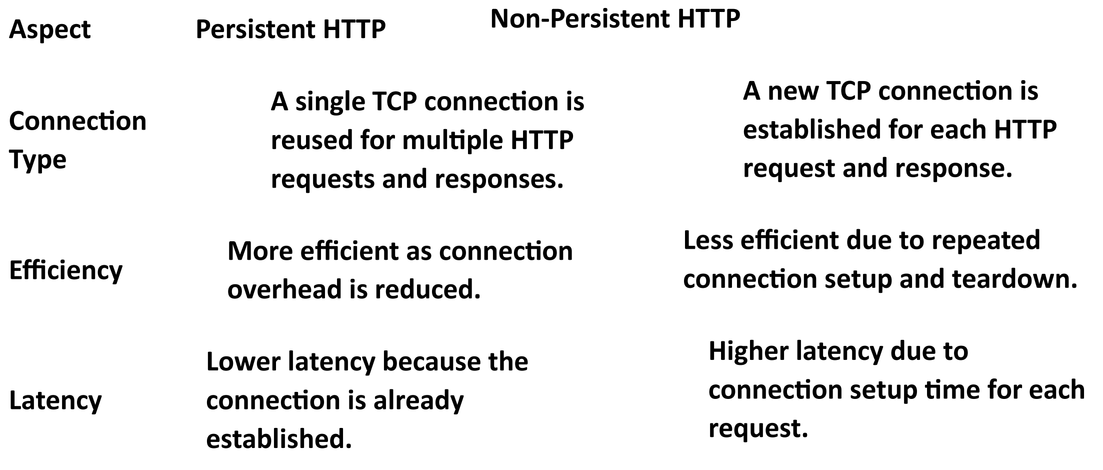
- The maximum throughput of a slotted ALOHA channel is given by the formula:
- Throughput (S) = G x e-G
- The maximum Throughput occurs at G = 1,
- i.e. S = 1/e = 0.368
- Where:
- G = the offered load (or the number of packets being transmitted per time slot). The offered load is a measure of the number of nodes attempting to transmit in a given time slot.

Assumption of Slotted ALOHA

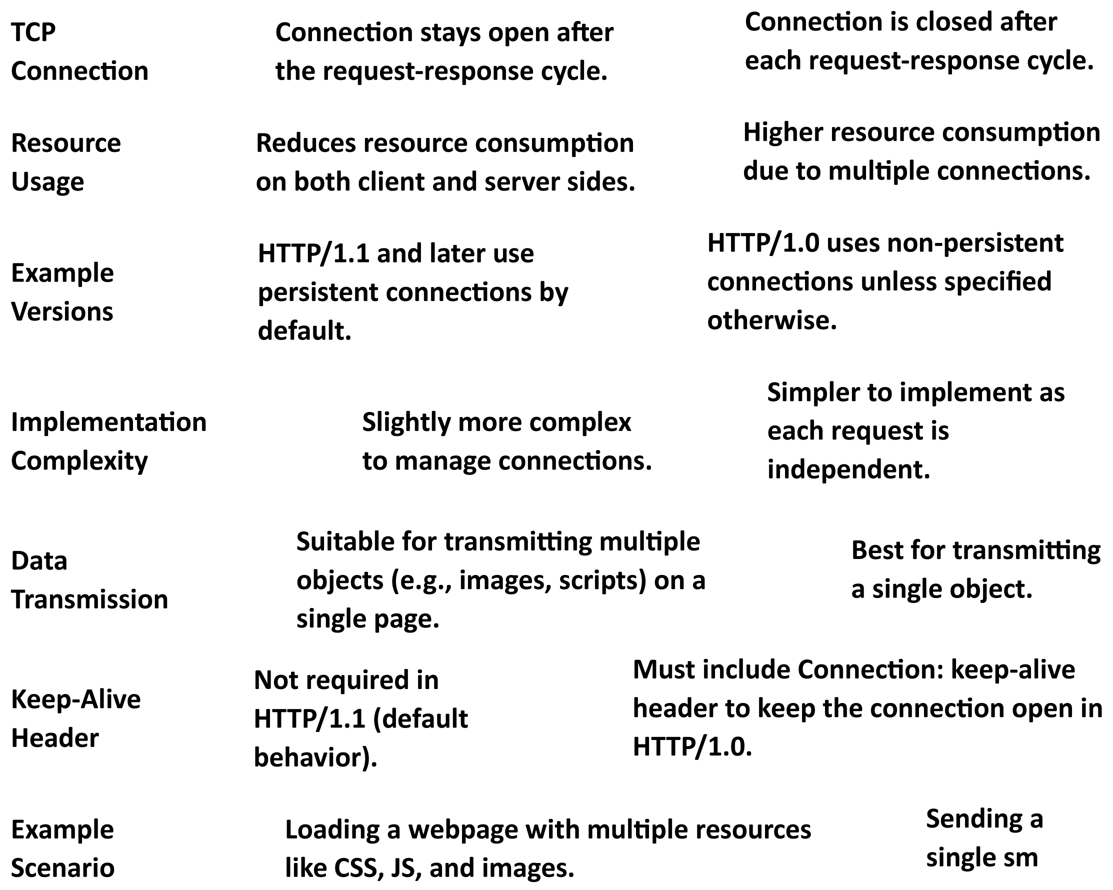
- All frames are of the same size.
- Time is divided into equal-sized slots, a slot equals the time to transmit one frame
- Nodes start to transmit frames only at beginning of slots.
- Nodes are synchronized.
- If two or more nodes transmit in a slot, all nodes detect collision before the slot ends.

Pure Aloha	**Slotted Aloha**
In this Aloha, any station can transmit the data at any time.	In this, any station can transmit the data at the beginning of any time slot.
In this, The time is continuous and not globally synchronized.	In this, The time is discrete and globally synchronized.
Vulnerable time for Pure Aloha = 2 x Tt	Vulnerable time for Slotted Aloha = Tt
In Pure Aloha, the Probability of successful transmission of the data packet = G x e-2G	In Slotted Aloha, the Probability of successful transmission of the data packet = G x e-G
In Pure Aloha, Maximum efficiency = 18.4%	In Slotted Aloha, Maximum efficiency = 36.8%
Pure Aloha doesn't reduce the number of collisions to half.	Slotted Aloha reduces the number of collisions to half and doubles the efficiency of Pure Aloha.

2) Compare Persistent and non-persistent HTTP.



Aspect	**Persistent HTTP**	**Non-Persistent HTTP**
Connection Type	**A single TCP connection is reused for multiple HTTP requests and responses.**	**A new TCP connection is established for each HTTP request and response.**
Efficiency	**More efficient as connection overhead is reduced.**	**Less efficient due to repeated connection setup and teardown.**
Latency	**Lower latency because the connection is already established.**	**Higher latency due to connection setup time for each request.**



TCP Connection	Connection stays open after the request-response cycle.	Connection is closed after each request-response cycle.
Resource Usage	Reduces resource consumption on both client and server sides.	Higher resource consumption due to multiple connections.
Example Versions	HTTP/1.1 and later use persistent connections by default.	HTTP/1.0 uses non-persistent connections unless specified otherwise.
Implementation Complexity	Slightly more complex to manage connections.	Simpler to implement as each request is independent.
Data Transmission	Suitable for transmitting multiple objects (e.g., images, scripts) on a single page.	Best for transmitting a single object.
Keep-Alive Header	Not required in HTTP/1.1 (default behavior).	Must include Connection: keep-alive header to keep the connection open in HTTP/1.0.
Example Scenario	Loading a webpage with multiple resources like CSS, JS, and images.	Sending a single sm

3) Explain TCP/IP Model in detail.

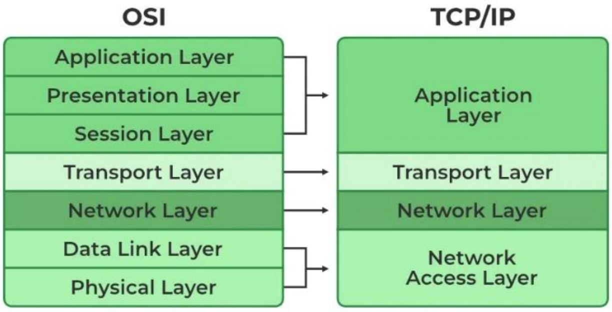
TCP/IP Model

- The TCP/IP model is a fundamental framework for computer networking. It stands for Transmission Control Protocol/Internet Protocol, which are the core protocols of the Internet. This model defines how data is transmitted over networks, ensuring reliable communication between devices. It consists of four layers: the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer. Each layer has specific functions that help manage different aspects of network communication, making it essential for understanding and working with modern networks.

- The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end. The TCP/IP model is used in the context of the real-world internet, where a wide range of physical media and network technologies are in use. Rather than specifying a particular Physical Layer, the TCP/IP model allows for flexibility in adapting to different physical implementations.

Layers of TCP/IP Model

- Application Layer
- Transport Layer(TCP/UDP)
- Network/Internet Layer(IP)
- Network Access Layer



1. Network Access Layer

- It is a group of applications requiring network communications. This layer is responsible for generating the data and requesting connections. It acts on behalf of the sender and the Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

- The packet's network protocol type, in this case, TCP/IP, is identified by network access layer. Error prevention and "framing" are also provided by this layer. Point-to-Point Protocol (PPP) framing and Ethernet IEEE 802.2 framing are two examples of data-link layer protocols.

2. Internet or Network Layer

- This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for the logical transmission of data over the entire network. The main protocols residing at this layer are as follows:

  - IP:IP stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.
  - ICMP:ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
  - ARP:ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.

3. Transport Layer

- The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error. End-to-end communication is referred to as such. Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).

- TCP: Applications can interact with one another using TCP as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission.
- UDP: The datagram delivery service is provided by UDP , the other transport layer protocol. Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP rather than TCP because it eliminates the processes of establishing and validating connections.

4. Application Layer

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The three main protocols present in this layer are:

- HTTP and HTTPS:HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions.
- SSH:SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
- NTP:NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

Advantages of TCP/IP Model

- **Interoperability** : The TCP/IP model allows different types of computers and networks to communicate with each other, promoting compatibility and cooperation among diverse systems.
- **Scalability** : TCP/IP is highly scalable, making it suitable for both small and large networks, from local area networks (LANs) to wide area networks (WANs) like the internet.
- **Standardization** : It is based on open standards and protocols, ensuring that different devices and software can work together without compatibility issues.
- **Flexibility** : The model supports various routing protocols, data types, and communication methods, making it adaptable to different networking needs.
- **Reliability** : TCP/IP includes error-checking and retransmission features that ensure reliable data transfer, even over long distances and through various network conditions.

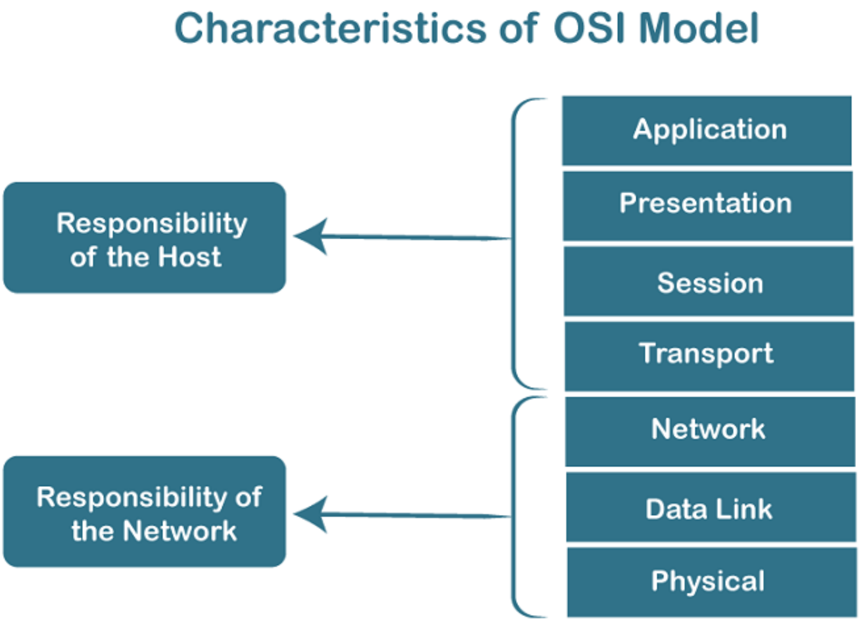
Disadvantages of TCP/IP Model

- **Complex Configuration** : Setting up and managing a TCP/IP network can be complex, especially for large networks with many devices. This complexity can lead to configuration errors.
- **Security Concerns** : TCP/IP was not originally designed with security in mind. While there are now many security protocols available (such as SSL/TLS), they have been added on top of the basic TCP/IP model, which can lead to vulnerabilities.
- **Inefficiency for Small Networks** : For very small networks, the overhead and complexity of the TCP/IP model may be unnecessary and inefficient compared to simpler networking protocols.
- **Limited by Address Space** : Although IPv6 addresses this issue, the older IPv4 system has a limited address space, which can lead to issues with address exhaustion in larger networks.
- **Data Overhead** : TCP, the transport protocol, includes a significant amount of overhead to ensure reliable transmission. This can reduce efficiency, especially for small data packets or in networks where speed is crucial.

4) Explain OSI model in detail.

OSI Model :-

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


Characteristics of OSI Model
Application
Presentation
Session
Transport
Network
Data Link
Physical
Responsibility of the Host
Responsibility of the Network

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

- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

7 Layers of OSI Model

- There are seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Physical layer

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

Functions of a Physical layer:

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

Data-Link Layer

- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
    - **Logical Link Control Layer**
        - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
        - It identifies the address of the network layer protocol from the header.
        - It also provides flow control.
    - **Media Access Control Layer**

  - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
  - It is used for transferring the packets over the network.

Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.
- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Network Layer

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

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

Transport Layer

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.

- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer

- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:-

- Dialog control: Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- Synchronization: Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer

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

Functions of Presentation layer:-

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application Layer

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

Functions of Application layer:-

- File transfer, access, and management (FTAM): An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- Mail services: An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

5) Define computer networks? Discuss various types of networks topologies in computer network. Also discuss various advantages and disadvantages of each Topology

Defination:-

- A computer network is a collection of computers or devices connected to share resources. Any device which can share or receive the data is called a Node. Through which the information or data propagate is known as channels, It can be guided or unguided.
- A computer network is a collection of interconnected devices that share resources and information. These devices can include computers, servers, printers, and other hardware. Networks allow for the efficient exchange of data, enabling various applications such as email, file sharing, and internet browsing.

What is Network Topology?

Network topology is the way devices are connected in a network. It defines how these components are connected and how data transfer between the network. Understanding the different types of network topologies can help in choosing the right design for a specific network.

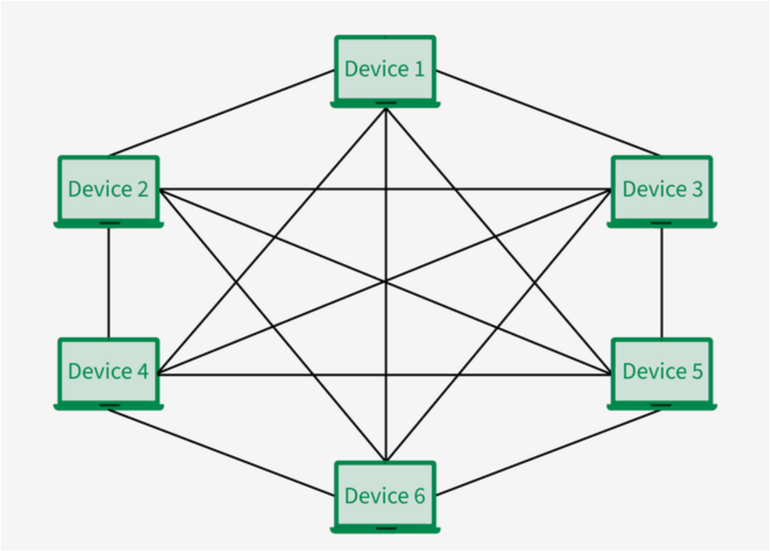
Types of Network Topology

Below mentioned are the types of Network Topology

- Mesh Topology
- Star Topology
- Bus Topology
- Ring Topology
- Hybrid Topology

Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. Every device is connected to another via dedicated channels. These channels are known as links. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N * (N-1).

Advantages of Mesh Topology

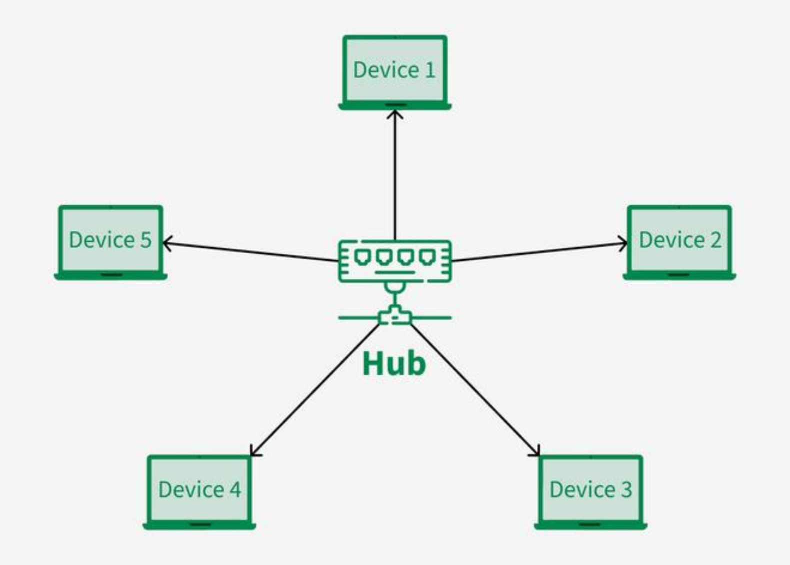
- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Disadvantages of Mesh Topology

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.



Advantages of Star Topology

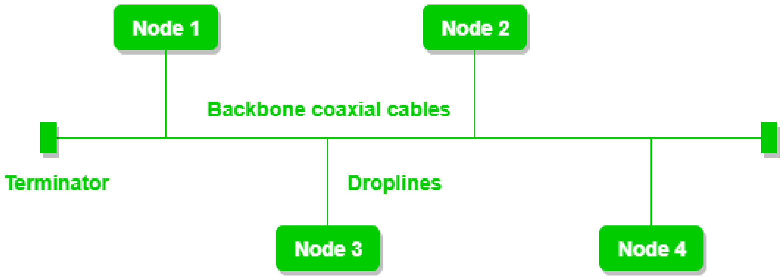
- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

Disadvantages of Star Topology

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.



Advantages of Bus Topology

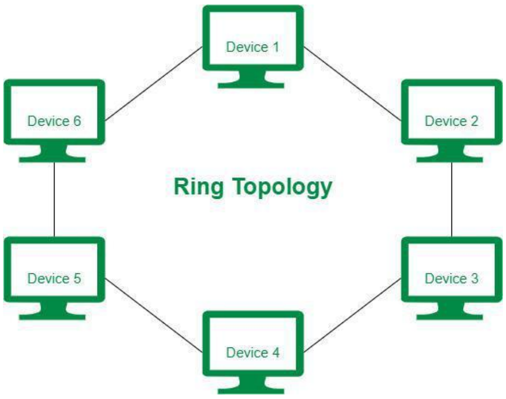
- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.

Disadvantages of Bus Topology

- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

Ring Topology

- In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
- The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



Advantages of Ring Topology

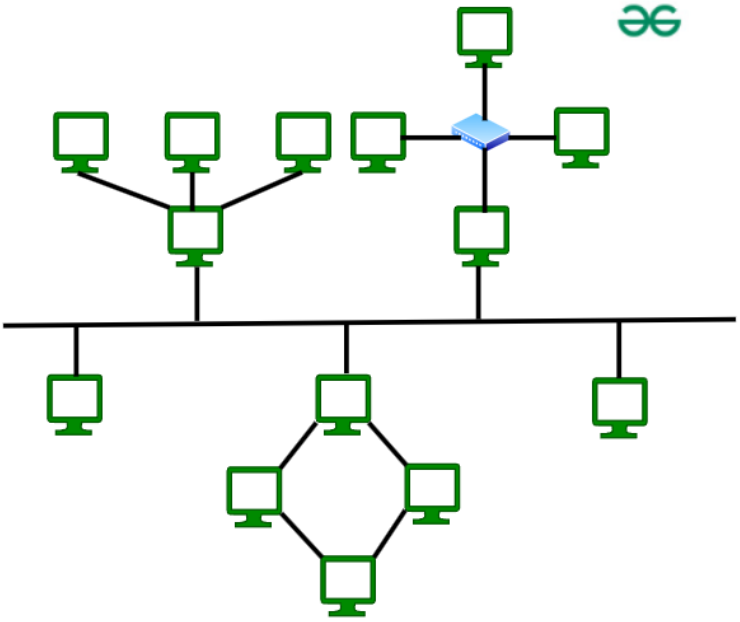
- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

Disadvantages of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

Hybrid Topology

Hybrid Topology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



Advantages of Hybrid Topology

- This topology is **very flexible** .
- The size of the network can be easily expanded by **adding new devices.**

Disadvantages of Hybrid Topology

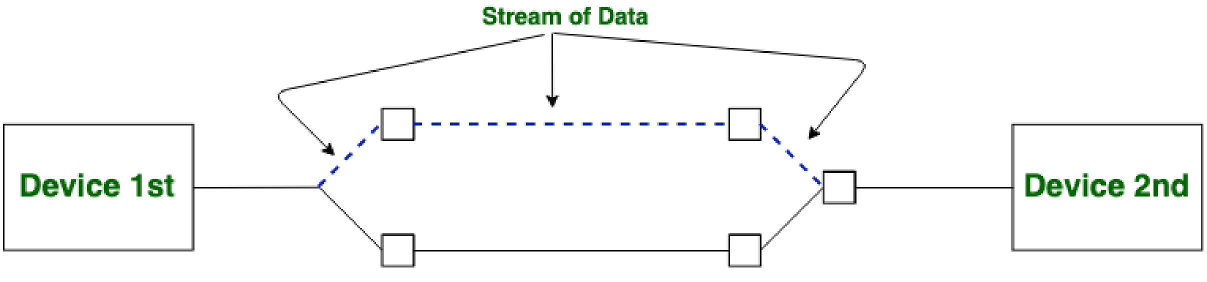
- It is challenging **to design the architecture** of the Hybrid Network.
- **Hubs** used in this topology are **very expensive.**
- The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices** .

6) Compare Connection less and connection-oriented service.

- Two basic forms of networking communication are connection-oriented and connection-less services. In order to provide dependable communication, connection-oriented services create a dedicated connection before transferring data. On the other hand, connection-less services prioritize speed and efficiency over reliability by transmitting data without establishing a connection. These types of services are offered by the network layer.

What is a Connection-Oriented Service?

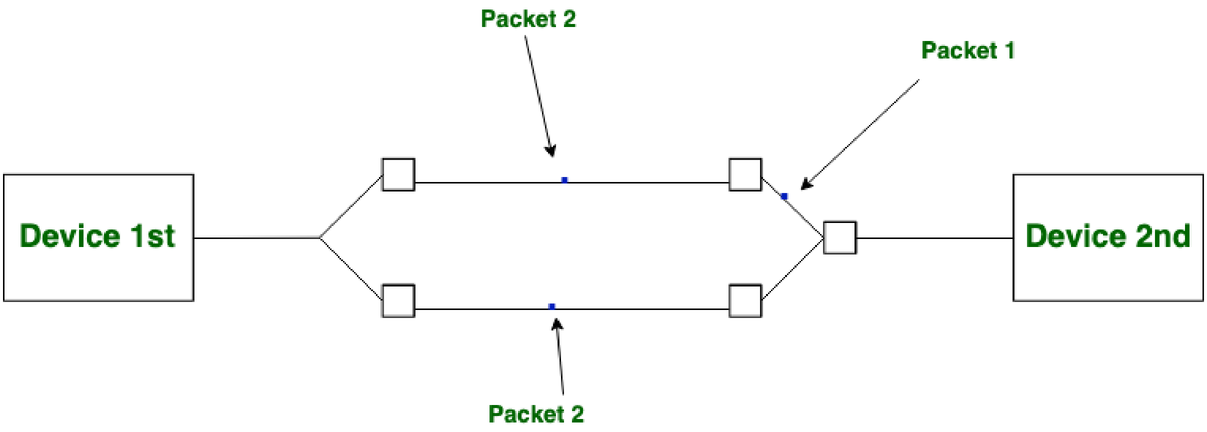
- Connection-oriented service is related to the telephone system. It includes connection establishment and connection termination. In a connection-oriented service, the Handshake method is used to establish the connection between sender and receiver. Before data transmission starts, connection-oriented services create a dedicated communication channel between the sender and the recipient. As the connection is kept open until all data is successfully transferred, this guarantees dependable data delivery. One example is TCP (Transmission Control Protocol), which ensures error-free and accurate data packet delivery.



CONNECTION-ORIENTED SERVICE

What is Connection-Less Service?

- Connection-less service is related to the postal system. It does not include any connection establishment and connection termination. Connection-less Service does not give a guarantee of reliability. In this, Packets do not follow the same path to reach their destination. Connection-less Services deliver individual data packets without first making a connection. Since each packet is sent separately, delivery, order, and mistake correction cannot be guaranteed. As a result, the service is quicker but less dependable. UDP (User Datagram Protocol) is one example, which is frequently used for streaming where dependability is not as important as speed.



CONNECTIONIESS SERVICE

Difference :-

Connection-oriented Service	Connection-less Service
Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
Connection-oriented Service is feasible.	Connection-less Service is not feasible.

In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give a guarantee of reliability.
In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.
Connection-oriented services require a bandwidth of a high range.	Connection-less Service requires a bandwidth of low range.
Ex: TCP (Transmission Control Protocol)	Ex: UDP (User Datagram Protocol)
Connection-oriented requires authentication.	Connection-less Service does not require authentication.

7) Explain the Protocols of Email Service.

Email Protocols

- Email protocols are a collection of protocols that are used to send and receive emails properly. The email protocols provide the ability for the client to transmit the mail to or from the intended mail server. Email protocols are a set of commands for sharing mails between two computers. Email protocols establish communication between the sender and receiver for the transmission of email. Email forwarding includes components like two computers sending and receiving emails and the mail server. There are three basic types of email protocols.

Types of Email Protocols:
Three basic types of email protocols involved for sending and receiving mails are:

- SMTP
- POP3
- IMAP

Simple Mail Transfer Protocol (SMTP)

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is an always-on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection through port 25. After successfully establishing a TCP connection the client process sends the mail instantly.

The SMTP model is of two types:

- End-to-End Method
- Store-and-Forward Method

- The end-to-end model is used to communicate between different organizations whereas the store and forward method is used within an organization. An SMTP client who wants to send the mail will contact the destination's host SMTP directly, to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP.
-

  The client SMTP is the one that initiates the session so let us call it the client-SMTP and the server SMTP is the one that responds to the session request so let us call it receiver-SMTP. The client-SMTP will start the session and the receiver SMTP will respond to the request.

Components of SMTP

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

How does SMTP Work?

- Communication between the sender and the receiver: The sender's user agent prepares the message and sends it to the MTA. The MTA's responsibility is to transfer the mail across the network to the receiver's MTA. To send mail, a system must have a client MTA, and to receive mail, a system must have a server MTA.
- Sending Emails: Mail is sent by a series of request and response messages between the client and the server. The message which is sent across consists of a header and a body. A null line is used to terminate the mail header and everything after the null line is considered the body of the message, which is a sequence of ASCII characters. The message body contains the actual information read by the receipt.
- Receiving Emails: The user agent on the server-side checks the mailboxes at a particular time of intervals. If any information is received, it informs the user about the mail. When the user tries to read the mail it displays a list of emails with a short description of each mail in the mailbox. By selecting any of the mail users can view its contents on the terminal.

Advantages of SMTP

- If necessary, the users can have a dedicated server.
- It allows for bulk mailing.
- Low cost and wide coverage area.
- Offer choices for email tracking.
- Reliable and prompt email delivery.

Disadvantages of SMTP

- SMTP's common port can be blocked by several firewalls.
- SMTP security is a bigger problem.
- Its simplicity restricts how useful it can be.
- Just 7-bit ASCII characters can be used.
- If a message is longer than a certain length, SMTP servers may reject the entire message.
- Delivering your message will typically involve additional back-and-forth processing between servers, which will delay sending and raise the likelihood that it won't be sent.

POP

- POP stands for Point of Presence (or Post Office Protocol). It refers to a connection point where many devices communicate and share a network. "Point of presence" describes the separation point between a service provider's public network and the customer's private network. We can say that it is a man-made separation point. It consists of high-speed telecommunications equipment and technologies that help bring people from all over the internet together. This protocol is used to retrieve messages from a mail server. The Message

Access Agent facilitates the transmission of the message from the receiving server to the host server. Both POP and POP3, they now become outdated and they are associated with email retrieval and now newer protocols like IMAP, offering more flexibility. In this article we will see POP protocol in detail.

Characteristics of POP

- Post Office Protocol is an open protocol, defined by Internet RFCs.
- It allows access to new mail from a spread of client platform types.
- POP can handle email access only while the emails are sent by SMTP.

Working of POP

Until the user logs in using an email client and downloads the message to their computer, all incoming messages are kept on the POP server. The message is removed from the server once it has been downloaded by the user.

Since SMTP is known to be the method used to move email messages from one server to another, POP essentially serves as a way to retrieve emails from servers using an email client; it does not offer a way to send messages.

A POP3 connection will be made on the server side whenever a user attempts to check all of their recent emails. To obtain the correct authentication, the user transmits the username and password to the server computer. Users can receive and keep all text-based emails on their local terminal (computer) after establishing a connection. They can subsequently delete any copies from the server and disconnect from the server. POP's work is also based on below five important pieces of equipment:

1. **Base stations –** A central point of reference to an access point and bandwidth management to ensure even distribution of the connection speed of the customer.
2. **Client equipment –** Customers use client equipment to connect to base stations.
3. **Network switches –** Used for proper distribution
4. **Routers –** Provides multiple paths for the data to be shared in the network
5. **Firewall –** Used for securing the network from threats (internal and external)

Advantages of POP

- The latest version of **Post Office Protocol (POP3)** is the most widely used protocol and is being supported by most email clients. It provides a convenient and standard way for users to access mailboxes and download messages. An important advantage of this is that the mail messages get delivered to the client's PC and they can be read with or without accessing the web.
- The creation of the latest messages is impossible without being logged onto the web.
- All messages get stored on the disc drive of your computer.
- Easy to use and configure.
- There isn't any maximum size on your mailbox, except as determined by the scale of your disc drive.

Disadvantages of POP

- Consumes large memory as all the messages are stored on the disc drive
- Opening attachments may be a fast process unless the attachment contains a virus.
- Since all attachments get downloaded on your computer, there's a danger of a virus attack if they're not
scanned by antivirus software.
- It is not easy to export a local mail folder to another physical machine or another mail client.

Internet Message Access Protocol (IMAP)

- The Internet Message Access Protocol (IMAP) serves as a cornerstone of cutting-edge email communication, facilitating seamless get admission to email messages. As a necessary element of the e-mail infrastructure, IMAP revolutionizes the manner customers interact with their digital correspondence. Unlike its predecessor, the Post Office Protocol (POP), IMAP gives a dynamic and synchronized approach to handling emails across multiple gadgets and structures.

Features of IMAP

- It is capable of managing multiple mailboxes and organizing them into various categories.
- Provides adding of message flags to keep track of which messages are being seen.
- It is capable of deciding whether to retrieve email from a mail server before downloading.
- It makes it easy to download media when multiple files are attached.

Working of IMAP

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.

- Email client Gmail establishes a connection with Gmail's SMTP server.
- By approving the sender's and recipient's email addresses, the SMTP server verifies (authenticates) that the email can be sent.
- The email is sent to the Outlook SMTP server by Gmail's SMTP server.
- The recipient's email address is authenticated by the Outlook SMTP server.
- IMAP or POP3 is used by the Outlook SMTP server to deliver the email to the Outlook email client.

Advantages

- It offers synchronization across all the maintained sessions by the user.
- It provides security over POP3 protocol as the email only exists on the IMAP server.
- Users have remote access to all the contents.
- It offers easy migration between the devices as it is synchronized by a centralized server.
- There is no need to physically allocate any storage to save contents.

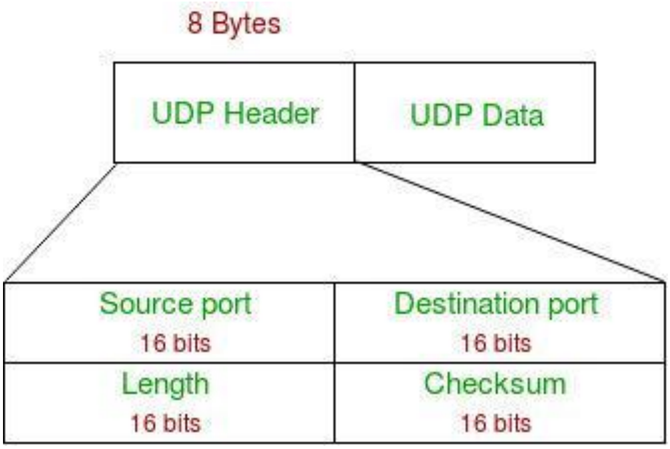
Disadvantages

- IMAP is complex to maintain.
- Emails of the user are only available when there is an internet connection.
- It is slower to load messages.
- Some emails don't support IMAP which makes it difficult to manage.

8) Draw and discuss each field of UDP Header.

UDP Header

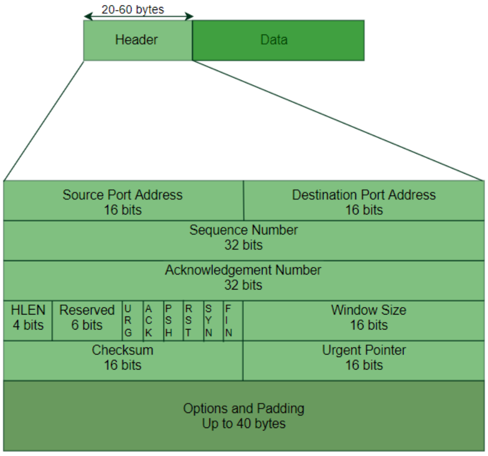
UDP header is an **8-byte** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contain all necessary header information and the remaining part consists of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.



- Source Port: Source Port is a 2 Byte long field used to identify the port number of the source.
- Destination Port: It is a 2 Byte long field, used to identify the port of the destined packet.
- Length: Length is the length of UDP including the header and the data. It is a 16-bits field.
- Checksum: Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

9) Draw and discuss each field of TCP Header.

TCP Segment structure –
A TCP segment consists of data bytes to be sent and a header that is added to the data by TCP as shown:



The header of a TCP segment can range from 20-60 bytes. 40 bytes are for options. If there are no options, a header is 20 bytes else it can be of upmost 60 bytes.
Header fields:

- **Source Port Address –**
  A 16-bit field that holds the port address of the application that is sending the data segment.

- **Destination Port Address –**
  A 16-bit field that holds the port address of the application in the host that is receiving the data segment.

- **Sequence Number –**
  A 32-bit field that holds the sequence number, i.e, the byte number of the first byte that is sent in that particular segment. It is used to reassemble the message at the receiving end of the segments that are received out of order.

- **Acknowledgement Number –**
  A 32-bit field that holds the acknowledgement number, i.e, the byte number that the receiver expects to receive next. It is an acknowledgement for the previous bytes being received successfully.

- **Header Length (HLEN) –**
  This is a 4-bit field that indicates the length of the TCP header by a number of 4-byte words in the header, i.e if the header is 20 bytes(min length of TCP header), then this field will hold 5 (because 5 x 4 = 20) and the maximum length: 60 bytes, then it'll hold the value 15(because 15 x 4 = 60). Hence, the value of this field is always between 5 and 15.

- **Control flags –**
  These are 6 1-bit control bits that control connection establishment, connection termination, connection abortion, flow control, mode of transfer etc. Their function is:
  - URG: Urgent pointer is valid
  - ACK: Acknowledgement number is valid(used in case of cumulative acknowledgement)
  - PSH: Request for push
  - RST: Reset the connection
  - SYN: Synchronize sequence numbers
  - FIN: Terminate the connection
- **Window size –**
  This field tells the window size of the sending TCP in bytes.

- **Checksum –**
  This field holds the checksum for error control. It is mandatory in TCP as opposed to UDP.

- **Urgent pointer –**
  This field (valid only if the URG control flag is set) is used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get the byte number of the last urgent byte.

10) Explain Go back N ARQ and Selective Repeat ARQ in detail. (Refer Gate Smashers YT Video and Written notes)

Sliding Window Protocol – Go Back N (GBN)

The **Sliding Window Protocol** is a method used in computer networks to manage the flow of data between two devices, ensuring that data is sent and received in the correct order. There are two types of sliding window protocol **Go-Back-N (GBN)**, and Selective Repeat (SR).
In **Go-Back-N**, the sender can send multiple data packets without waiting for an acknowledgement for each one. However, it can only send a certain number of packets (this is called the "window size"). If one packet is lost or not acknowledged, the sender must go back and resend that packet *and* all the packets that followed it, even if they were received correctly. For example, if packets 1, 2, 3, 4, and 5 are sent and packet 3 gets lost, the sender will have to resend packets 3, 4, and 5, even if 4 and 5 were received. In this article, we will discuss the Go-Back-N (GBN) protocol in detail.

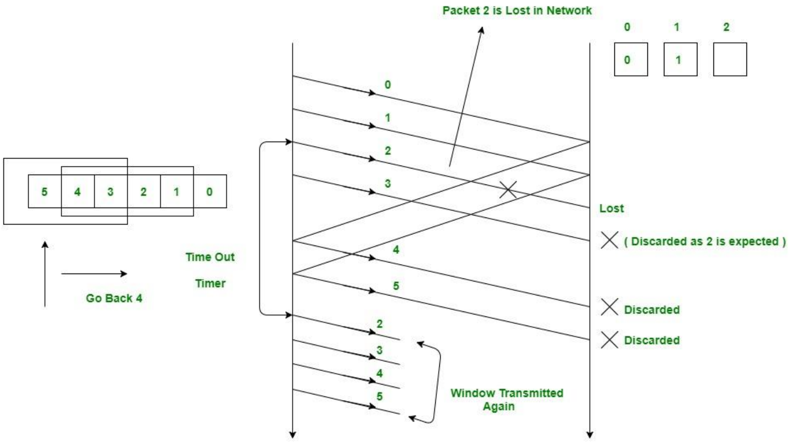
What is the Go Back N (GBN) Protocol?

The Go-Back-N (GBN) protocol is a sliding window protocol used in networking for reliable data transmission. It is part of the Automatic Repeat reQuest (ARQ) protocols, which ensure that data is correctly received and that any lost or corrupted packets are retransmitted.

main characteristic features of GBN

Working of GB-N Protocol

Now what exactly happens in GBN, we will explain with a help of example. Consider the diagram given below. We have sender window size of 4. Assume that we have lots of sequence numbers just for the sake of explanation. Now the sender has sent the packets 0, 1, 2 and 3. After acknowledging the packets 0 and 1, receiver is now expecting packet 2 and sender window has also slided to further transmit the packets 4 and 5. Now suppose the packet 2 is lost in the network, Receiver will discard all the packets which sender has transmitted after packet 2 as it is expecting sequence number of 2.
On the sender side for every packet send there is a time out timer which will expire for packet number 2. Now from the last transmitted packet 5 sender will go back to the packet number 2 in the current window and transmit all the packets till packet number 5. That's why it is called Go Back N. Go back means sender has to go back N places from the last transmitted packet in the unacknowledged window and not from the point where the packet is lost.



Relationship Between Window Size and Sequence Numbers

- The **window size** and **sequence numbers** in a sliding window protocol, like Go-Back-N or Selective Repeat, are closely related.
- The **window size** determines how many packets the sender can transmit without needing an acknowledgment. It's like a limit on how much data can be sent before the sender has to stop and wait for confirmation.
- **Sequence numbers** are used to label packets so the receiver knows their order and can detect any missing packets.
  The **window size** should be smaller than or equal to the range of available **sequence numbers**. If the window size is too large compared to the sequence number range, the receiver might get confused because the same sequence number could be reused before the first one is acknowledged. This would make it hard to know if a packet is new or a duplicate.

  Selective Repeat Protocol (SRP) : This protocol(SRP) is mostly identical to GBN protocol, except that buffers are used and the receiver, and the sender, each maintains a window of size. SRP works better when the link is very unreliable. Because in this case, retransmission tends to happen more frequently, selectively retransmitting frames is more efficient than retransmitting all of them. SRP also requires full-duplex link. backward acknowledgements are also in progress.
- Sender's Windows (Ws) = Receiver's Windows (Wr).
- Window size should be less than or equal to half the sequence number in SR protocol. This is to avoid packets being recognized incorrectly. If the size of the window is greater than half the sequence number space, then if an ACK is lost, the sender may send new packets that the receiver believes are retransmissions.
- Sender can transmit new packets as long as their number is with W of all unpacked packets.
- Sender retransmit un-ACKed packets after a timeout – Or upon a NAK if NAK is employed.
- Receiver ACKs all correct packets.
- Receiver stores correct packets until they can be delivered in order to the higher layer.
- In Selective Repeat ARQ, the size of the sender and receiver window must be at most one-half of 2^m.

11) Given a DUMP of a UDP header in hexadecimal format 0361101A104CY242. Find the following in decimal:- 1. Source port number? 2. Destination port number?

The given UDP header **0361101A104CY242** contains a non-hexadecimal character **Y**, which is invalid in standard UDP headers. However, assuming this is either a typographical error or the "Y" is replaced with a valid hexadecimal digit, let's focus on the valid part of the UDP header (0361101A104C) for analysis.

Structure of a UDP Header

A UDP header is 8 bytes (16 hexadecimal digits) long, containing:

1. **Source Port Number** (16 bits or 4 hex digits)
2. **Destination Port Number** (16 bits or 4 hex digits)
3. **Length** (16 bits or 4 hex digits)
4. **Checksum** (16 bits or 4 hex digits)

The header **0361101A104CY242** will be analyzed until the invalid character (Y) is encountered.

1. Source Port Number (First 4 Hex Digits)

- Hexadecimal: **0361**

- Convert to decimal: 036116=(0×163)+(3×162)+(6×161)+(1×160)=0+768+96+1=8650361_{16} = (0 \times 16^3) + (3 \times 16^2) + (6 \times 16^1) + (1 \times 16^0) = 0 + 768 + 96 + 1 = 865036116 =(0×163)+(3×162)+(6×161)+(1×160)=0+768+96+1=865
- **Source Port Number**: **865**

2. Destination Port Number (Next 4 Hex Digits)

- Hexadecimal: **101A**
- Convert to decimal: 101A16=(1×163)+(0×162)+(1×161)+(10×160)=4096+0+16+10=4122101A_{16} = (1 \times 16^3) + (0 \times 16^2) + (1 \times 16^1) + (10 \times 16^0) = 4096 + 0 + 16 + 10 = 4122101A16=(1×163)+(0×162)+(1×161)+(10×160)=4096+0+16+10=4122
- **Destination Port Number**: **4122**

12) What is traffic shaping? Explain it algorithm in details.

Traffic Shaping

Traffic shaping is a network traffic management technique used to control the flow of data in a network to ensure a consistent level of performance, reduce congestion, and maintain quality of service (QoS). It regulates the data rate transmitted over a network by delaying packets that exceed a predefined rate limit. This ensures that the network operates within its capacity, preventing issues like congestion, packet loss, and latency.

Key Objectives of Traffic Shaping

1. **Smooth Traffic Flow**: Avoiding traffic bursts that can overwhelm the network.
2. **Enforce QoS**: Ensuring specific traffic classes (e.g., video streams, VoIP) get priority.
3. **Optimize Bandwidth Utilization**: Preventing overloading of network resources.
4. **Compliance with SLA**: Ensuring adherence to Service Level Agreements by limiting or guaranteeing specific bandwidth allocations.

Common Traffic Shaping Algorithms

1. Token Bucket Algorithm

The **Token Bucket** algorithm controls the flow of traffic based on tokens added to a bucket at a fixed rate. Each token corresponds to a unit of data (e.g., 1 byte or 1 packet). Traffic can only be sent if sufficient tokens are available, and excess tokens may be stored up to a maximum limit (bucket capacity).

- **Mechanism**:
  1. Tokens are added to the bucket at a constant rate RRR (bytes per second).
  2. The bucket can hold a maximum of BBB tokens (bucket capacity).
  3. To send nnn bytes of data, nnn tokens are removed from the bucket.
  4. If the bucket does not have enough tokens, the data is delayed until enough tokens accumulate.
- **Advantages**:
  - Allows traffic bursts up to the bucket size while maintaining long-term rate control.
  - Suitable for applications requiring flexibility in traffic bursts.

2. Leaky Bucket Algorithm

The **Leaky Bucket** algorithm enforces a constant output data rate, regardless of incoming traffic. It acts like a bucket with a small hole at the bottom, where packets drip out at a steady rate. If incoming traffic exceeds the bucket's capacity, excess packets are discarded.

- **Mechanism**:
    1. Packets arrive and are queued in the bucket (buffer).
    2. Packets are transmitted from the bucket at a fixed rate RRR.
    3. If the bucket overflows due to high incoming traffic, packets are dropped.
- **Advantages**:
    - Ensures a steady output rate, ideal for network stability.
    - Prevents bursts of traffic from exceeding network capacity.

Implementation Steps

1. **Define Parameters**: Set the rate (R) and maximum capacity (B) for the algorithm.
2. **Monitor Incoming Traffic**: Check packet arrival rates against the defined limits.
3. **Queue Management**:
    - Token Bucket: Delay or buffer traffic until enough tokens are available.
    - Leaky Bucket: Drop excess traffic or buffer within the queue.
4. **Send Packets**: Transmit packets at a controlled rate based on algorithm rules.
5. **Feedback Mechanism**: Adjust parameters dynamically if network conditions change (optional).

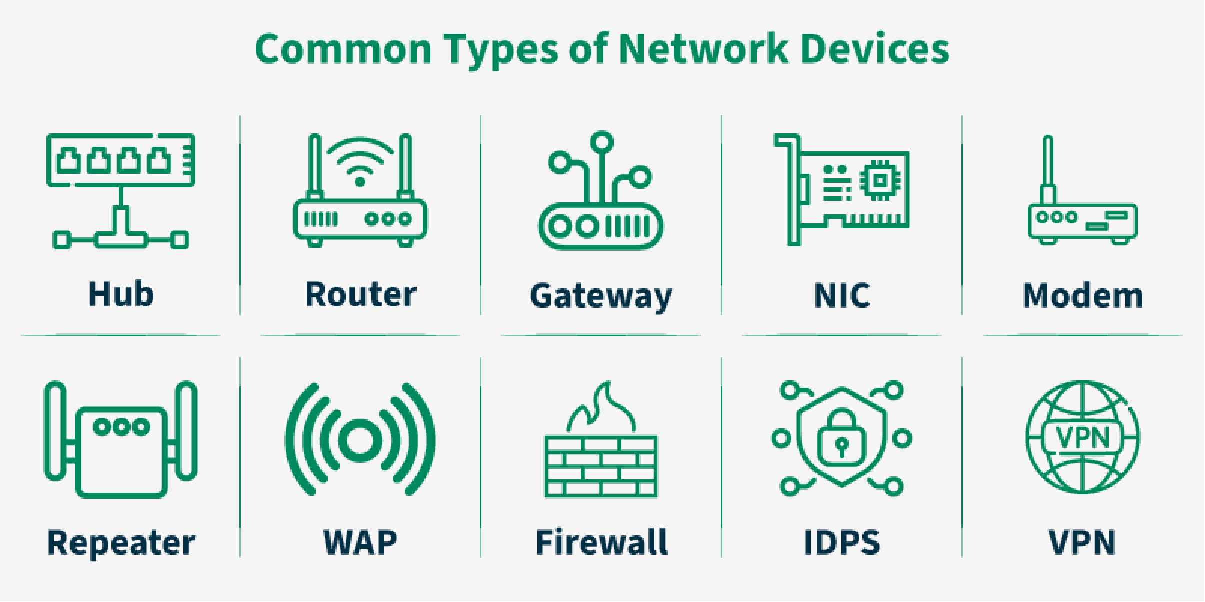
Applications

- **ISPs**: Limiting customer bandwidth to match subscription plans.
- **QoS Enforcement**: Prioritizing voice/video traffic over regular data.
- **Data Centers**: Balancing traffic across server clusters.
- **Cloud Services**: Allocating network resources based on SLA commitments.

13) Explain about the different types of connecting devices in computer networks?

Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter)

- Network devices are physical devices that allow hardware on a computer network to communicate and interact with each other. Network devices like hubs, repeaters, bridges, switches, routers, gateways, and brouters help manage and direct data flow in a network. They ensure efficient communication between connected devices by controlling data transfer, boosting signals, and linking different networks. Each device serves a specific role, from



simple data forwarding to complex routing between networks. In this article, we are going to discuss different types of network devices in detail.

Functions of Network Devices

- Network devices help to send and receive data between different devices.
- Network devices allow devices to connect to the network efficiently and securely.
- Network devices Improve network speed and manage data flow better.
- It protect the network by controlling access and preventing threats.
- Expand the network range and solve signal problems.

Common Types of Networking Devices and Their Uses

Network devices work as a mediator between two devices for transmission of data, and thus play a very important role in the functioning of a computer network. Below are some **common network devices used in modern networks:**

- Access Point
- Modems
- Firewalls
- Repeater
- Hub
- Bridge
- Switch
- Routers
- Gateway
- Brouter
- NIC

Access Point

An access point in networking is a device that allows wireless devices, like smartphones and laptops, to connect to a wired network. It creates a Wi-Fi network that lets wireless devices communicate with the internet or other devices on the network. Access points are used to extend the range of a network or provide Wi-Fi in areas that do not have it. They are commonly found in homes, offices, and public places to provide wireless internet access.

Router

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

Gateway

A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as 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 switches or routers.

Switch

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

Bridge

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It typically connects multiple network segments and each port is connected to different segment. The exact number of ports depends on the type of bridge and design, but it usually has at least two ports for basic functionality.

14) Write a note on HTTP. Also write its advantage and disadvantage

What is HyperText?

- The protocol used to transfer hypertext between two computers is known as HyperText Transfer Protocol. HTTP provides a standard between a web browser and a web server to establish communication. It is a set of rules for transferring data from one computer to another. Data such as text, images, and other multimedia files are shared on the World Wide Web. Whenever a web user opens their web browser, the user indirectly uses HTTP. It is an application protocol that is used for distributed, collaborative, hypermedia information systems.

Working of HTTP [HyperText Transfer Protocol]

- First of all, whenever we want to open any website we first open a web browser after that we will type the URL of that website (e.g., www.facebook.com). This URL is now sent to the Domain Name Server (DNS). Then DNS first checks records for this URL in their database, and then DNS will return the IP address to the web browser corresponding to this URL. Now the browser is able to send requests to the actual server.

- After the server sends data to the client, the connection will be closed. If we want something else from the server we should have to re-establish the connection between the client and the server.

What is an HTTP Request?

- HTTP request is simply termed as the information or data that is needed by Internet browsers for loading a website. This is simply known as HTTP Request.

- There is some common information that is generally present in all HTTP requests. These are mentioned below.

o HTTP Version
o URL
o HTTP Method
o HTTP Request Headers
o HTTP Body

HTTP Request Headers

HTTP Request Headers generally store information in the form of key-value and must be present in each HTTP Request. The use of this Request Header is to provide core information about the client's information, etc.

HTTP Request Body

HTTP Request Body simply contains the information that has to be transferred. HTTP Request has the information or data to be sent to these browsers.

HTTP Method

HTTP Methods are simply HTTP Verb. In spite of being present so many HTTP Methods, the most common HTTP Methods are HTTP GET and HTTP POST. These two are generally used in HTTP cases. In HTTP GET, the information is received in the form of a website.

What is HTTP Response?

HTTP Response is simply the answer to what a Server gets when the request is raised. There are various things contained in HTTP Response, some of them are listed below.

- HTTP Status Code
- HTTP Headers
- HTTP Body

HTTP Response Headers

HTTP Response headers are simply like an HTTP Request where it has that work to send some important files and data to the HTTP Response Body.

HTTP Response Body

HTTP Responses are the responses that are received successfully upon the request. Generally, it comes under the requests generated by the web. In most cases, the request is to transfer the HTML data into a webpage.

What is an HTTP Status Code?

HTTP Status Codes are the 3-digit codes that tell the message or simply tell us about the HTTP Request whether it has been completed or not.

Advantages of HTTP

- Memory usage and CPU usage are low because of fewer simultaneous connections.
- Since there are few TCP connections hence network congestion is less.
- Since handshaking is done at the initial connection stage, then latency is reduced because there is no further need for handshaking for subsequent requests.
- The error can be reported without closing the connection.
- HTTP allows HTTP pipe-lining of requests or responses.

Disadvantages of HTTP

- HTTP requires high power to establish communication and transfer data.
- HTTP is less secure because it does not use any encryption method like HTTPS and uses TLS to encrypt regular HTTP requests and responses.
- HTTP is not optimized for cellular phones and it is too gabby.
- HTTP does not offer a genuine exchange of data because it is less secure.
- The client does not close the connection until it receives complete data from the server; hence, the server needs to wait for data completion and cannot be available for other clients during this time

15) What are the applications of computer network?

Application of Computer Network

There are a variety of fields in computer networks that are used in industries. Some of them are as follows:

1. Internet and World Wide Web

In computer networks, we have a global internet, also known as the World Wide Web, that offers us various features like access to websites, online services and retrieval of information. With the help of the World Wide Web, we can browse, and we can do search, and access web pages and multimedia content.

2. Communication

With the help of computer networks, communication is also easy because we can do email, instant messaging, voice and video calls and video conferencing, which helps us to communicate with each other effectively. People can use these features in their businesses and organizations to stay connected with each other.

3. File Sharing and Data Transfer

Data transfer and file sharing are made possible by networks that connect different devices. This covers file sharing within a business setting, file sharing between personal devices, and downloading/uploading of content from the internet.

4. Online gaming

Multiplayer online games use computer networks to link players from all over the world, enabling online competitions and real-time gaming experiences.

5. Remote Access and Control

Networks enable users to access and control systems and devices from a distance. This is helpful when accessing home automation systems, managing servers, and providing remote IT support.

6. Social media

With the help of a computer network, we can use social media sites like Facebook, Twitter and Instagram to help people set up their profiles, and we can connect with others and share content on social media.

7. Cloud Computing

The provision of on-demand access to computing resources and services hosted in distant data centres relies on networks. Some example of cloud computing is software as a service (SaaS), platform as a service (PaaS) and infrastructure as service (IaaS).

8. Online Banking and E-Commerce

Online banking and e-commerce platforms, where customers conduct financial transactions and make online purchases, require secure computer networks.

9. Enterprise Networks

In Computer networks, we have some networks that are only used in businesses and organizations so they can store data and share files and resources like printers, scanners, etc.

10. Healthcare

With the help of computer networks in the health industry, we can share patient records and store the records in the form of data that is easy and secure compared to the file method. Networks are also necessary for telemedicine and remote patient monitoring.

11. Education

Schools use networks to access online courses, virtual classrooms, and other online learning materials. Campuses of colleges and universities frequently have extensive computer networks.

12. Transportation and Logistics

The transportation sector uses Computer Networks to manage and track shipments, plan the best routes, and coordinate logistics activities.

13. Internet of Things (IoT) and Smart Homes

Through the Internet of Things (IoT), smart homes use networks to connect to and manage a variety of devices, including thermostats, security cameras, and smart appliances.

14. Scientific Research

To share data, work together on projects, and access high-performance computing resources for data analysis and scientific simulations, researchers use networks.

15. Government and Defense

With the help of computer networks, we can communicate, share data, and advance national defence. Government agencies and the military rely on secure networks.

These are just a few instances of the many areas of our lives where computer networks are used. Computer networks are fundamental to facilitating communication, teamwork, and the effective exchange of knowledge and resources globally.

16) Differentiate OSI and TCP/IP model.

Parameters	**OSI Model**	**TCP/IP Model**
Full Form	OSI stands for Open Systems Interconnection	TCP/IP stands for Transmission Control Protocol/Internet Protocol
Layers	It has 7 layers	It has 4 layers
Usage	It is low in usage	It is mostly used
Approach	It is vertically approached	It is horizontally approached
Delivery	Delivery of the package is guaranteed in OSI Model	Delivery of the package is not guaranteed in TCP/IP Model
Replacement	Replacement of tools and changes can easily be done in this model	Replacing the tools is not easy as it is in OSI Model

Reliability	It is less reliable than TCP/IP Model	It is more reliable than OSI Model
Protocol Example	Not tied to specific protocols, but examples include HTTP (Application), SSL/TLS (Presentation), TCP (Transport), IP (Network), Ethernet (Data Link)	HTTP, FTP, TCP, UDP, IP, Ethernet
Error Handling	Built into Data Link and Transport layers	Built into protocols like TCP
Connection Orientation	Both connection-oriented (TCP) and connectionless (UDP) protocols are covered at the Transport layer	TCP (connection-oriented), UDP (connectionless)

17) Explain the components of DNS.

The **Domain Name System (DNS)** is a hierarchical and decentralized naming system used to resolve human-readable domain names (e.g., www.example.com) into machine-readable IP addresses (e.g., 192.0.2.1). The key components of DNS are as follows:

1. Domain Names

- A hierarchical structure consisting of:
  - **Root Domain**: Represented as a dot (.) at the top of the DNS hierarchy.
  - **Top-Level Domain (TLD)**: Includes domains like .com, .org, .net, and country-specific domains like .uk or .in.
  - **Second-Level Domain (SLD)**: The name registered under the TLD, e.g., example in example.com.
  - **Subdomains**: Further divisions within a domain, e.g., blog.example.com.

---

2. DNS Resolver (Client-Side)

- Also known as a **recursive resolver**, this is responsible for:
  - Receiving queries from user devices.
  - Interacting with other DNS components (like root servers, TLD servers, and authoritative servers) to resolve domain names to IP addresses.

---

3. DNS Servers

DNS servers work in a distributed manner to store and resolve domain names:

a) Root Name Servers

- The top-level DNS servers that know the authoritative servers for all TLDs.
- Example: If the query is for example.com, the root server directs it to the .com TLD server.

b) Top-Level Domain (TLD) Servers

- Responsible for storing information about second-level domains registered under a specific TLD.
- Example: The .com TLD server knows the authoritative server for example.com.

c) Authoritative Name Servers

- The final source of truth for domain records, storing actual mappings of domain names to IP addresses.
- Example: The authoritative server for example.com will provide the IP address for the domain.

---

4. DNS Records

- **A Record**: Maps a domain to an IPv4 address.
- **AAAA Record**: Maps a domain to an IPv6 address.
- **CNAME Record**: Maps an alias domain to a canonical domain name.
- **MX Record**: Specifies mail servers for email services.
- **NS Record**: Points to authoritative name servers for a domain.
- **TXT Record**: Holds arbitrary text for verification or other purposes.

---

5. Caching

- DNS responses are cached by recursive resolvers and user devices to reduce lookup times and improve performance.
- Example: If a resolver already knows the IP address for example.com, it will provide the cached result without querying DNS servers again.

---

6. Zone Files

- A database file maintained by authoritative servers containing DNS records for a specific domain or subdomain.
- Divides the DNS namespace into manageable segments.

---

7. Reverse DNS (rDNS)

- Performs the reverse operation of DNS by resolving an IP address back to its domain name.
- Uses **PTR Records**.

---

8. TTL (Time-To-Live)

- A setting that determines how long DNS information is cached before it must be refreshed.
- Helps balance speed and accuracy in DNS resolution.

Together, these components ensure that users can access websites and services by translating domain names into IP addresses seamlessly.

18) Explain Delay in detail.

Delays in Computer Network

The delays, here, means the time for which the processing of a particular packet takes place. We have the following types of delays in computer networks:

1. **Transmission Delay:**
   The time taken to transmit a packet from the host to the transmission medium is called Transmission delay. For example, if bandwidth is 1 bps (every second 1 bit can be transmitted onto the transmission medium) and data size is 20 bits then what is the transmission delay? If in one second, 1 bit can be transmitted. To transmit 20 bits, 20 seconds would be required.

This delay depends upon the following factors:

- If there are multiple active sessions, the delay will become significant.
- Increasing bandwidth decreases transmission delay.
- MAC protocol largely influences the delay if the link is shared among multiple devices.
- Sending and receiving a packet involves a context switch in the operating system, which takes a finite time.

2. **Propagation delay:**
   After the packet is transmitted to the transmission medium, it has to go through the medium to reach the destination. Hence the time taken by the last bit of the packet to reach the destination is called propagation delay.

Factors affecting propagation delay:

1. **Distance –** It takes more time to reach the destination if the distance of the medium is longer.
2. **Velocity –** If the velocity(speed) of the medium is higher, the packet will be received faster.

3. Queueing delay:

Let the packet is received by the destination, the packet will not be processed by the destination immediately. It has to wait in a queue in something called a buffer. So the amount of time it waits in queue before being processed is called queueing delay.

In general, we can't calculate queueing delay because we don't have any formula for that.

This delay depends upon the following factors:

- If the size of the queue is large, the queuing delay will be huge. If the queue is empty there will be less or no delay.
- If more packets are arriving in a short or no time interval, queuing delay will be large.
- The less the number of servers/links, the greater is the queuing delay.

4. Processing delay:

Now the packet will be taken for the processing which is called processing delay.

Time is taken to process the data packet by the processor that is the time required by intermediate routers to decide where to forward the packet, update TTL, perform header checksum calculations.

It also doesn't have any formula since it depends upon the speed of the processor and the speed of the processor varies from computer to computer.

Note: Both queueing delay and processing delay doesn't have any formula because they depend on the speed of the processor

This delay depends upon the following factors:

- It depends on the speed of the processor.

19) Explain Connection less and connection-oriented service.

Connection-less Service

- A Connectionless Service is technique that is used in data communications to send or transfer data or message at Layer 4 i.e., Transport Layer of Open System Interconnection model. This service does not require session connection among sender or source and receiver or destination. Sender starts transferring or sending data or messages to destination.

- In other words, we can say that connectionless service simply means that node can transfer or send data packets or messages to its receiver even without session connection to receiver. Message is sent or transferred without prior arrangement. This usually works due to error handling protocols that allow and give permission for correction of errors just like requesting retransmission.

- In this service, network sends each packet of data to sender one at a time, independently of other packets. But network does not have any state information to determine or identify whether packet is part of stream of other packets. Even the network doesn't have any knowledge and information about amount of traffic that will be transferred by user. In this, each of data packets has source or destination address and is routed independently from source to destination.

- Therefore, data packets or messages might follow different paths to reach destination. Data packets are also called datagrams. It is also similar to that of postal services, as it also carries full address of destination where message is to send. Data is also sent in one direction from source to destination without checking that destination is still present there or not or if receiver or destination is prepared to accept message.

Connectionless Protocols :
These protocols simply allow data to be transferred without any link among processes. Some Of data packets may also be lost during transmission. Some of protocols for connectionless services are given below:

Internet Protocol (IP) –
This protocol is connectionless. In this protocol, all packets in IP network are routed independently. They might not go through same route.

User Datagram Protocol (UDP) –
This protocol does not establish any connection before transferring data. It just sends data that's why UDP is known as connectionless.

Internet Control Message Protocol (ICMP) –
ICMP is called connectionless simply because it does not need any hosts to handshake before establishing any connection.

Internetwork Packet Exchange (IPX) –
IPX is called connectionless as it doesn't need any consistent connection that is required to be maintained while data packets or messages are being transferred from one system to another.

Types of Connectionless Services :-

Service	**Example**
Unreliable Datagram	Electronic Junk Mail, etc.
Acknowledged Datagram	Registered mail, text messages along with delivery report, etc.
Request Reply	Queries from remote databases, etc.

Advantages :

- It is very fast and also allows for multicast and broadcast operations in which similar data are transferred to various recipients in a single transmission.
- The effect of any error occurred can be reduced by implementing error-correcting within an application protocol.
- This service is very easy and simple and is also low overhead.
- At the network layer, host software is very much simpler.
- No authentication is required in this service.
- Some of the application doesn't even require sequential delivery of packets or data. Examples include packet voice, etc.

Disadvantages :

- This service is less reliable as compared to connection-oriented service.
- It does not guarantee that there will be no loss, or error occurrence, misdelivery, duplication, or out-of-sequence delivery of the packet.
- They are more prone towards network congestions.

Connection-Oriented Service

Connection-Oriented Service is basically a technique that is typically used to transport and send data at session layer. The data streams or packets are transferred or delivered to receiver in a similar order in which they have seen transferred by sender. It is actually a data transfer method among two devices or computers in a different network, that is designed and developed after telephone system. Whenever a network implements this service, it sends or transfers data or message from sender or source to receiver or destination in correct order and manner.

This connection service is generally provided by protocols of both network layer (signifies different path for various data packets that belongs to same message) as well as transport layer (use to exhibits independence among packets rather than different paths that various packets belong to same message will follow).

Operations :

There is a sequence of operations that are needed to b followed by users. These operations are given below :

1. **Establishing Connection –**
   It generally requires a session connection to be established just before any data is transported or sent with a direct physical connection among sessions.
2. **Transferring Data or Message –**
   When this session connection is established, then we transfer or send message or data.
3. **Releasing the Connection –**
   After sending or transferring data, we release connection.

Different Ways :

There are two ways in which connection-oriented services can be done. These ways are given below :

1. **Circuit-Switched Connection –**
   Circuit-switching networks or connections are generally known as connection-oriented networks. In this connection, a dedicated route is being established among sender and receiver, and whole data or message is sent through it. A dedicated physical route or a path or a circuit is established among all communication nodes, and after that, data stream or message is sent or transferred.
2. **Virtual Circuit-Switched Connection –**
   Virtual Circuit-Switched Connection or Virtual Circuit Switching is also known as Connection-Oriented Switching. In this connection, a preplanned route or path is established before data or messages are transferred or sent. The message Is transferred over this network is such a way that it seems to user that there is a dedicated route or path from source or sender to destination or receiver.

Types of Connection-Oriented Service :

Service	**Example**
Reliable Message Stream	Sequence of pages, etc.
Reliable Byte Stream	Song Download, etc.
Unreliable Connection	VoIP (Voice Over Internet Protocol)

Advantages :

- It kindly support for quality of service is an easy way.
- This connection is more reliable than connectionless service.
- Long and large messages can be divided into various smaller messages so that it can fit inside packets.
- Problems or issues that are related to duplicate data packets are made less severe.

Disadvantages :

□ In this connection, cost is fixed no matter how traffic is.

□ It is necessary to have resource allocation before communication.

□ If any route or path failures or network congestions arise, there is no alternative way available to continue communication.

20) The periodic signal is decomposed into five sine waves with frequencies of 100, 300, 400, 600, and 700 Hz. Calculate the bandwidth and draw the spectrum. Assume all components have a maximum amplitude of 10 V.

21) The following code words are mapped with respective data words. How many bits of errors can be corrected with the below mentioned Hamming code?

Data Block	Codeword
00	00000
01	00111
10	11001
11	11110

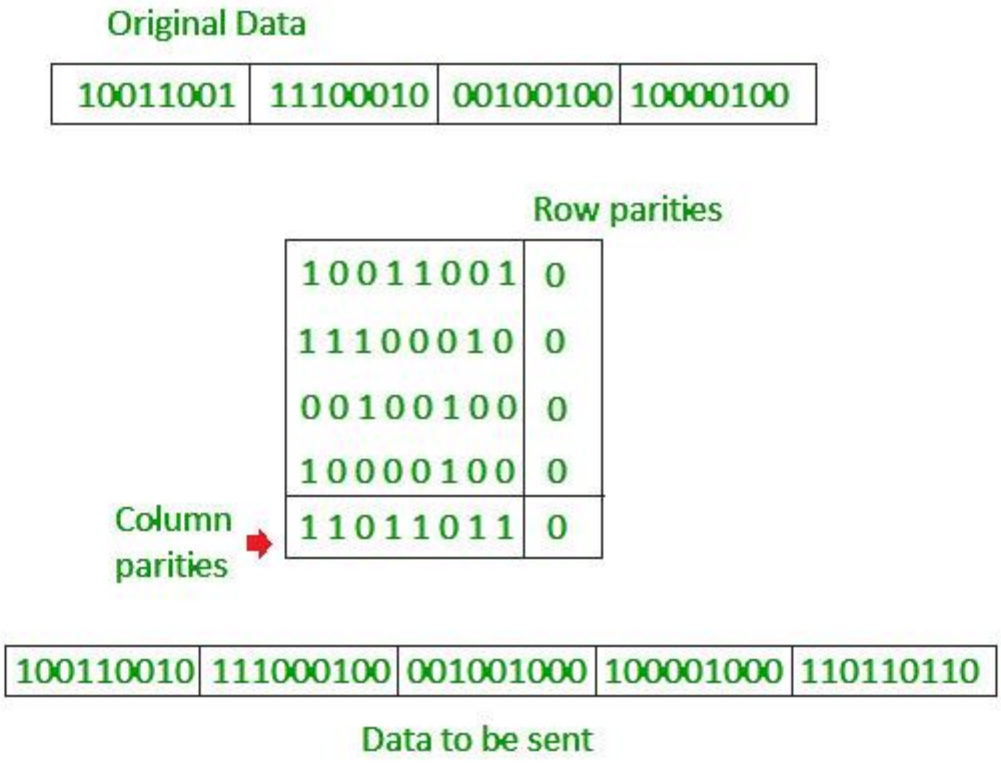
Receiver receives 10110. Which data work receiver will understand?

22) Apply bit stuffing and destuffing on below given frame.
01111110(Flag) 10111111111111001010111110 **01111110** (Flag)

23) Explain two-dimension parity check code. How many numbers of bit error can be detected using two-dimension parity check code?

Two-Dimensional Parity Check

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



Advantages of Two-Dimensional Parity Check

- Two-Dimensional Parity Check can detect and correct all single bit error.
- Two-Dimensional Parity Check can detect two or three bit error that occur any where in the matrix.

Disadvantages of Two-Dimensional Parity Check

- Two-Dimensional Parity Check can not correct two or three bit error. It can only detect two or three bit error.
- If we have a error in the parity bit then this scheme will not work.

24) Explain framing by character count using an example.

Framing by Character Count

Framing by character count is a method of data link layer framing in which the frame length is explicitly specified as a count of characters (bytes) included in the frame. The character count field at the beginning of the frame helps the receiver determine where the frame ends.

Process

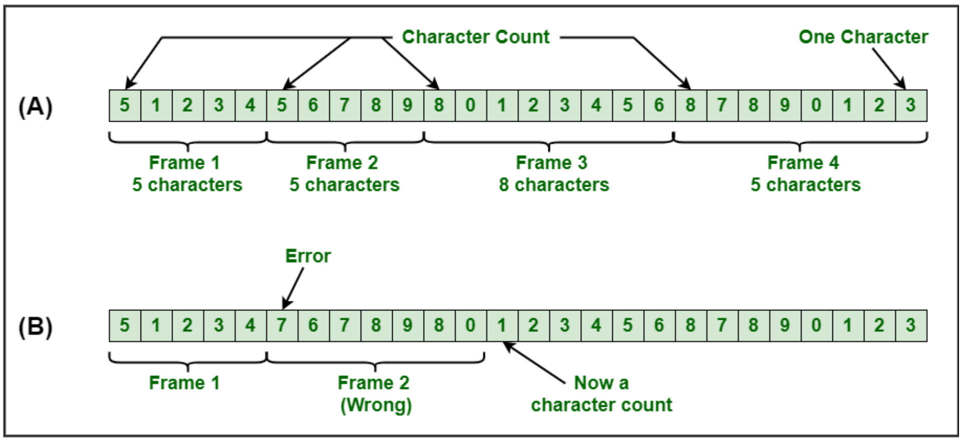
1. The frame begins with a **character count field** that specifies the number of characters in the frame, including the count field itself.
2. The receiver reads the character count field to determine how many bytes to read to form a complete frame.
3. After receiving the specified number of bytes, the receiver processes the frame.

Advantages

1. **Simple to Implement**: Easy for the receiver to identify the frame length.
2. **Efficient**: No need for additional synchronization bits or markers.

Challenges

1. **Corruption Risk**: If the count field is corrupted during transmission, the receiver may misinterpret the frame length, leading to errors in framing.
2. **Lack of Error Detection**: Framing by character count doesn't inherently include error detection; a separate mechanism (e.g., checksum) is needed.



A Character Stream

(A) Without Errors
(B) With one Error

25) Why does a header is included in a packet? Is it always necessary to include a header? Justify your answer.

A **header** is included in a packet to provide essential metadata and control information that allows the packet to be correctly routed, processed, and understood by the receiving system. The header typically contains:

1. **Source and destination addresses**: To ensure that the packet reaches the correct destination.
2. **Packet sequencing**: To enable reassembly of fragmented data.
3. **Protocol information**: To identify the protocol being used (e.g., TCP, UDP).
4. **Error-checking data**: To help verify that the packet has not been corrupted during transmission.
5. **Time-to-live (TTL)**: To prevent packets from circulating endlessly in the network.
6. **Other control information**: Such as flags or priority levels.

Is it always necessary to include a header?

In most network communication scenarios, **yes**, a header is essential because it ensures that the data reaches its intended recipient correctly and is processed without errors. Without the header, the network devices (such as routers and switches) would not know where to send the packet or how to handle it.

However, there are some cases where headers might be minimal or not needed, such as in very simple communication protocols or low-level hardware communication (e.g., certain internal system bus protocols). But for most internet or wide-area network communications, headers are always included to ensure reliable and accurate delivery.

Justification:

1. **Routing and addressing**: Without a header, the packet would not have the necessary information to be routed across different network segments.
2. **Error detection and correction**: The header can include checksums or other mechanisms to detect errors in the data.

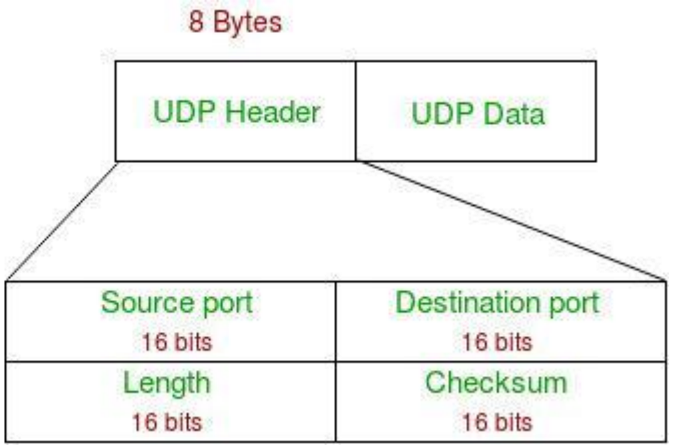
3. **Protocol compatibility**: Different protocols (like IP, TCP) require headers to understand the type of data being transmitted.
   Therefore, in the majority of networking contexts, including headers is necessary for the packet's proper functioning.

26) Explain connectionless transport protocol UDP with popular internet application.

User Datagram Protocol (UDP)

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

UDP Header
UDP header is an **8-byte** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contain all necessary header information and the remaining part consists of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.



UDP Header

- **Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
- **Destination Port:** It is a 2 Byte long field, used to identify the port of the destined packet.
- **Length:** Length is the length of UDP including the header and the data. It is a 16-bits field.
- **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

Applications of UDP

- Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
- It is a suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.

Advantages of UDP

- **Speed:** UDP is faster than TCP because it does not have the overhead of establishing a connection and ensuring reliable data delivery.
- Lower latency: Since there is no connection establishment, there is lower latency and faster response time.
- **Simplicity:** UDP has a simpler protocol design than TCP, making it easier to implement and manage.
- **Broadcast support:** UDP supports broadcasting to multiple recipients, making it useful for applications such as video streaming and online gaming.
- **Smaller packet size:** UDP uses smaller packet sizes than TCP, which can reduce network congestion and improve overall network performance.
- User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

Disadvantages of UDP

- **No reliability:** UDP does not guarantee delivery of packets or order of delivery, which can lead to missing or duplicate data.
- **No congestion control:** UDP does not have congestion control, which means that it can send packets at a rate that can cause network congestion.
- **Vulnerable to attacks:** UDP is vulnerable to denial-of-service attacks , where an attacker can flood a network with UDP packets, overwhelming the network and causing it to crash.
- **Limited use cases:** UDP is not suitable for applications that require reliable data delivery, such as email or file transfers, and is better suited for applications that can tolerate some data loss, such as video streaming or online gaming.

27) What is Data Communication? What are the components required for data communication?

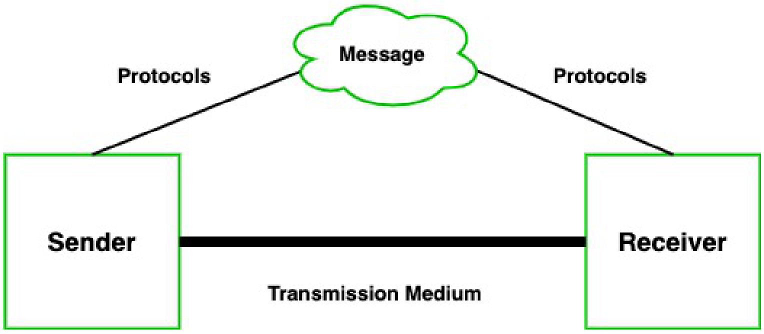
Data Communication

Transferring data over a transmission medium between two or more devices, systems, or places is known as data communication. Nowadays, computing and telecommunications depend heavily on this data transmission, which makes a variety of applications conceivable, including email, video chatting, the Internet, and many more things.
In this article, we will learn about Data communication, Definition, Components, Types, and Channels.

Components of Data Communication

A communication system is made up of the following components:

1. **Message:** A message is a piece of information that is to be transmitted from one person to another. It could be a text file, an audio file, a video file, etc.
2. **Sender:** It is simply a device that sends data messages. It can be a computer, mobile, telephone, laptop, video camera, or workstation, etc.
3. **Receiver:** It is a device that receives messages. It can be a computer, telephone mobile, workstation, etc.
4. **Transmission Medium / Communication Channels:** Communication channels are the medium that connect two or more workstations. Workstations can be connected by either wired media or wireless media.
5. **Set of rules (Protocol):** When someone sends the data (The sender), it should be understandable to the receiver also otherwise it is meaningless. For example, Sonali sends a message to Chetan. If Sonali writes in Hindi and Chetan cannot understand Hindi, it is a meaningless conversation.



28) What is transmission media? Write a brief of all of them

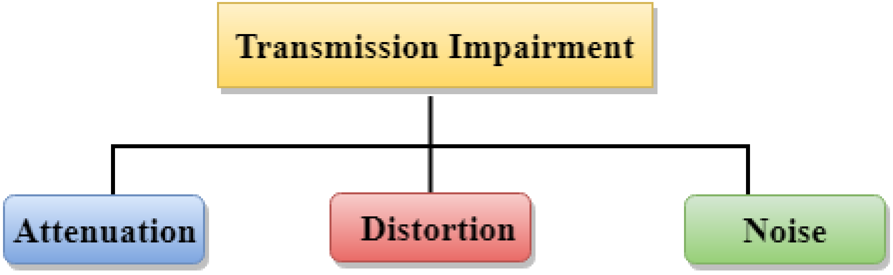
What is Transmission media?

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre based network, the bits in the form of light pulses.
- In **OSI**(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
- The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

Some factors need to be considered for designing the transmission media:

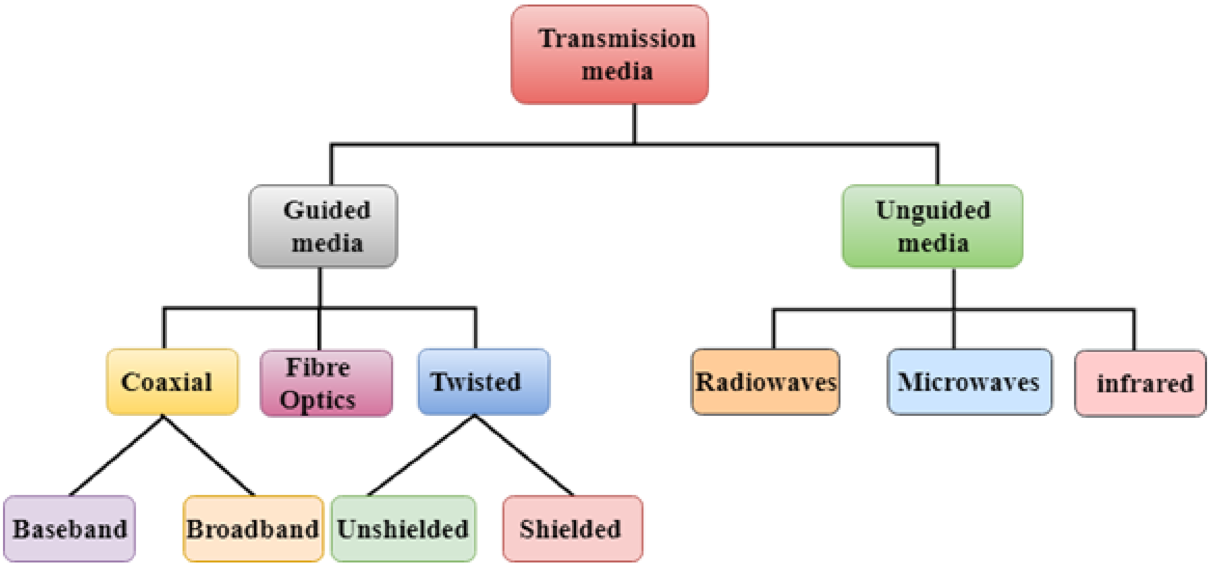
- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

Causes Of Transmission Impairment:



- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

  Classification Of Transmission Media:



29) What is the difference between a user agent (UA) and a mail transfer agent? (MTA)?

A **User Agent (UA)** and a **Mail Transfer Agent (MTA)** are both involved in the process of handling email, but they serve different roles in the email delivery system.

1. User Agent (UA):

- **Definition**: A User Agent is a software application that allows users to create, send, receive, and manage email messages. It is typically an email client such as Microsoft Outlook, Mozilla Thunderbird, or a web-based client like Gmail or Yahoo Mail.
- **Role**: The UA is responsible for interacting with the end-user. It provides an interface for composing, reading, organizing, and managing email messages.
  - **Sending**: When you compose an email, the UA formats it and sends it to the MTA for delivery.
  - **Receiving**: The UA retrieves messages from an MTA or a Mail Delivery Agent (MDA) using protocols like POP3 or IMAP.
  - **Protocols**: The UA uses protocols such as SMTP (Simple Mail Transfer Protocol) to send emails and IMAP or POP3 to retrieve them.

2. Mail Transfer Agent (MTA):

- **Definition**: A Mail Transfer Agent is a software application that handles the routing and transfer of email messages between email servers. Examples include Postfix, Sendmail, and Microsoft Exchange Server.
- **Role**: The MTA is responsible for the transmission of emails between mail servers, ensuring that messages are properly routed from the sender's server to the recipient's server.
  - **Sending**: When an email is sent, the MTA takes the message from the UA, determines the recipient's domain, and routes it to the correct mail server.

- **Routing**: The MTA uses DNS to find the recipient's mail server and ensures that the message is forwarded correctly.
- **Protocols**: The MTA uses SMTP to send emails to other MTAs or email servers.

30) What are the Functions of the Application Layer? And Design Issue With Application Layer?

Functions of the Application Layer:

The **Application Layer** is the topmost layer in the OSI (Open Systems Interconnection) model and the TCP/IP model, and it is responsible for providing network services directly to the user or application. Its primary functions include:

1. **End-User Services**:
   - This layer interacts with the end-user and provides the interface for applications to access network services, such as email, file transfer, and web browsing.
   - Examples: Web browsers (HTTP), email clients (SMTP, IMAP), and FTP clients.
2. **Data Representation**:
   - It ensures that the data is in a usable format for the application. This can include data encryption, compression, or translation between different data formats.
   - Examples: ASCII to EBCDIC conversion, multimedia formats like JPEG or PNG.
3. **Application Protocols**:
   - Defines rules for communication between applications on different hosts. These protocols ensure that communication happens correctly and reliably between client and server.
   - Examples: HTTP, FTP, SMTP, POP3, IMAP, DNS, etc.
4. **Session Management**:
   - It handles session establishment, maintenance, and termination between applications on different devices.
   - Examples: Establishing a session for data transfer (e.g., file transfer protocols).
5. **Error Handling**:
   - Provides mechanisms to handle errors related to data transfer at the application level. This may include retries, acknowledgments, or generating specific error messages.
   - Example: Error responses in HTTP like 404 (not found), 500 (internal server error).
6. **Resource Allocation**:
   - It can also be responsible for managing and allocating resources like bandwidth and memory for network applications.
   - Example: Bandwidth management in video streaming services.

Design Issues with the Application Layer:

The **Application Layer** is key to ensuring smooth communication, but it also faces several design challenges, including:

1. **Protocol Design**:
   - Creating efficient and interoperable protocols that work across different platforms and devices can be complex. Each application needs a robust, scalable, and secure protocol to ensure smooth communication.
   - Example: HTTP (Hypertext Transfer Protocol) evolving to HTTPS for secure communication.
2. **Interoperability**:
   - Ensuring that different software applications and hardware platforms can communicate with each other can be difficult. Different applications may need to use the same protocol, but they may be built on different operating systems or technologies.
   - Example: Ensuring that an email client works across various operating systems.

3. **Security**:
   - The Application Layer must address security concerns such as data confidentiality, integrity, and authentication. Securing data at this layer is critical, especially with increasing threats like hacking, phishing, and malware.
   - Example: Using TLS/SSL encryption in web browsers to secure data.
4. **Scalability**:
   - As the number of users and devices grows, applications at the Application Layer must scale efficiently to handle increased traffic and data volume without sacrificing performance.
   - Example: Ensuring a web server can handle millions of users simultaneously.
5. **Data Integrity**:
   - Ensuring that the data being sent and received remains uncorrupted and intact is a challenge, especially in environments with high traffic or unreliable networks.
   - Example: Using checksums, hashes, and error-correcting codes to verify data integrity.
6. **Latency and Performance**:
   - Applications at this layer often require real-time communication, making minimizing latency and maximizing performance essential.
   - Example: Video streaming and online gaming applications must ensure low latency for smooth user experience.
7. **Resource Consumption**:
   - Applications must balance the consumption of system resources such as bandwidth, CPU, and memory. Excessive resource consumption can lead to slowdowns or crashes, especially with resource-intensive applications like video conferencing or file sharing.
   - Example: Optimizing the bandwidth for video conferencing applications to reduce latency and avoid packet loss.

31) What is FTP? Write at least three FTP commands with their responses.

File Transfer Protocol (FTP)

File transfer protocol (FTP) is an Internet tool provided by TCP/IP. The first feature of FTP is developed by Abhay Bhushan in 1971. It helps to transfer files from one computer to another by providing access to directories or folders on remote computers and allows software, data, text file to be transferred between different kinds of computers. The end-user in the connection is known as localhost and the server which provides data is known as the remote host.

The goals of FTP are:

- It encourages the direct use of remote computers.
- It shields users from system variations (operating system, directory structures, file structures, etc.)
- It promotes sharing of files and other types of data.

FTP Clients

FTP works on a client-server model. The FTP client is a program that runs on the user's computer to enable the user to talk to and get files from remote computers. It is a set of commands that establishes the connection between two hosts, helps to transfer the files, and then closes the connection. Some of the commands are: *get filename(retrieve the file from server), mget filename(retrieve multiple files from* the *server), ls(lists files available in the current directory of the server).* There are also built-in FTP programs, which makes it easier to transfer files and it does not require remembering the commands.

Type of FTP Connections

FTP connections are of two types:

Active FTP connection: In an Active FTP connection, the client establishes the command channel and the server establishes the data channel. When the client requests the data over the connection the server initiates the transfer of the data to the client. It is not the default connection because it may cause problems if there is a firewall in between the client and the server.

Passive FTP connection: In a Passive FTP connection, the client establishes both the data channel as well as the command channel. When the client requests the data over the connection, the server sends a random port number to the client, as soon as the client receives this port number it establishes the data channel. It is the default connection, as it works better even if the client is protected by the firewall.

Anonymous FTP

Some sites can enable anonymous FTP whose files are available for public access. So, the user can access those files without any username or password. Instead, the username is set to anonymous and the password to the guest by default. Here, the access of the user is very limited. For example, the user can copy the files but not allowed to navigate through directories.

Detail steps of FTP

- FTP client contacts FTP server at port 21 specifying TCP as transport protocol.
- Client obtain authorization over control connection.
- Client browse remote directory by sending commands over control connection.
- When server receives a command for a file transfer, the server open a TCP data connection to client.
- after transferring one file, server closes connection.
- server opens a second TCP data connection to transfer another file.
- FTP server maintains state i.e. current directory, earlier authentication.

FTP Commands

Sr. no.	Command	Meaning
1.	cd	Changes the working directory on the remote host
2.	close	Closes the FTP connection
3.	quit	Quits FTP
4.	pwd	displays the current working Directory on the remote host
5.	dir or ls	Provides a Directory Listing of the current working directory
6.	help	Displays a list of all client FTP commands
7.	remotehelp	Displays a list of all server FTP commands

Sr. no.	Command	Meaning
8.	type	Allows the user to specify the file type
9.	struct	specifies the files structure

Applications of FTP

The following are the applications of FTP:

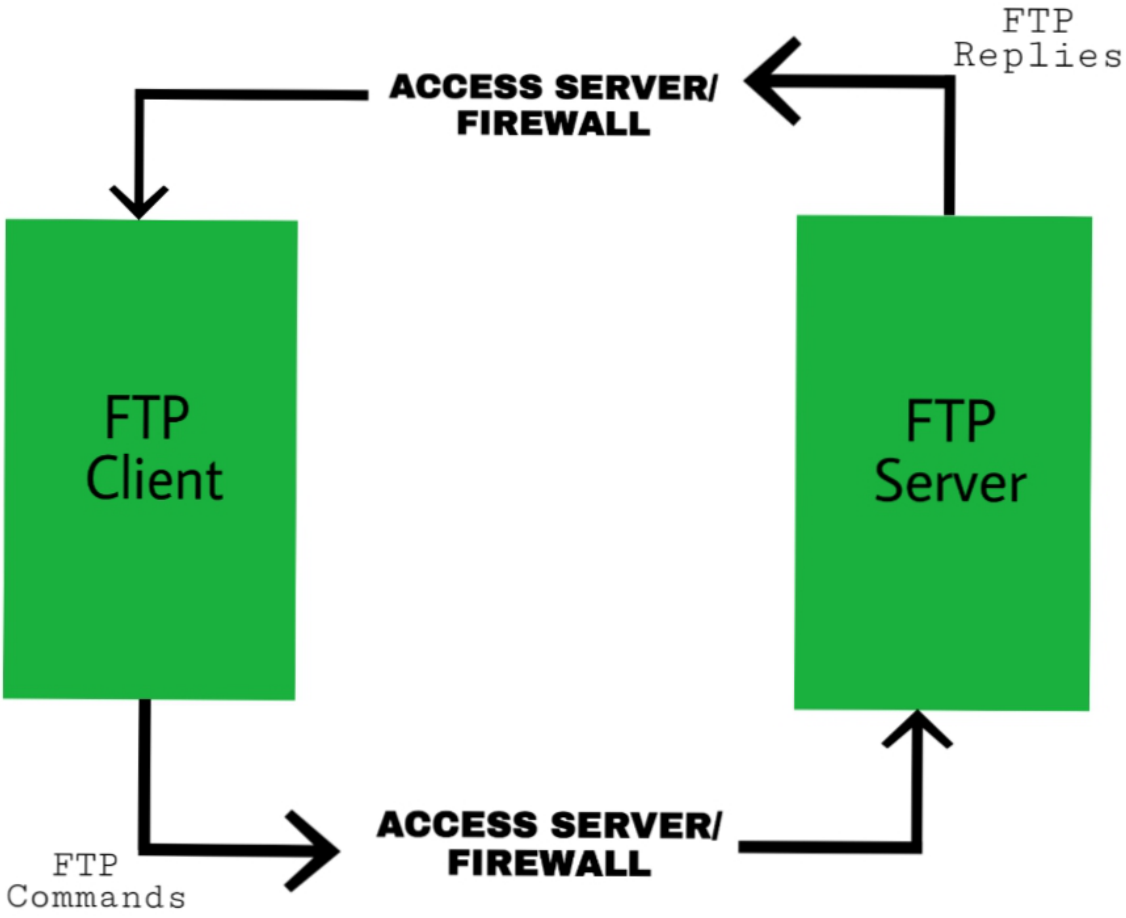
- FTP connection is used by different big business organizations for transferring files in between them, like sharing files to other employees working at different locations or different branches of the organization.
- FTP connection is used by IT companies to provide backup files at disaster recovery sites.
- Financial services use FTP connections to securely transfer financial documents to the respective company, organization, or government.
- Employees use FTP connections to share any data with their co-workers.

Advantages

- **Multiple transfers:** FTP helps to transfer multiple large files in between the systems.
- **Efficiency:** FTP helps to organize files in an efficient manner and transfer them efficiently over the network.
- **Security:** FTP provides access to any user only through user ID and password. Moreover, the server can create multiple levels of access.
- **Continuous transfer:** If the transfer of the file is interrupted by any means, then the user can resume the file transfer whenever the connection is established.
- **Simple:** FTP is very simple to implement and use, thus it is a widely used connection.
- **Speed:** It is the fastest way to transfer files from one computer to another.

Disadvantages

- **Less security:** FTP does not provide an encryption facility when transferring files. Moreover, the username and passwords are in plain text and not a combination of symbols, digits, and alphabets, which makes it easier to be attacked by hackers.
- **Old technology:** FTP is one of the oldest protocols and thus it uses multiple TCP/IP connections to transfer files. These connections are hindered by firewalls.
- **Virus:** The FTP connection is difficult to be scanned for viruses, which again increases the risk of vulnerability.
- **Limited:** The FTP provides very limited user permission and mobile device access.
- **Memory and programming:** FTP requires more memory and programming efforts, as it is very difficult to find errors without the commands.



32) Discuss the DNS services in detail. Also briefly explain iterated and recursive query.

DNS (Domain Name System) Services

DNS (Domain Name System) is a hierarchical and decentralized naming system used to resolve domain names (like www.example.com) into IP addresses (like 192.168.1.1) required for routing information on the internet. DNS allows users to access websites using human-readable domain names rather than IP addresses, which are harder to remember.

Primary Functions of DNS:

1. **Name Resolution**:
   - DNS resolves domain names to IP addresses, which is crucial for routing requests over the internet. For example, when a user types "www.example.com" into a browser, DNS resolves it to an IP address that the browser uses to connect to the web server.
2. **Name Registration**:
   - DNS allows domain owners to register domain names with domain registrars, making them publicly accessible across the internet.
3. **Mapping Services**:

    - It provides a system for mapping domain names to various types of resources, such as IP addresses, mail servers, and more. This involves the creation of DNS records like:
        - **A Records**: Maps domain names to IPv4 addresses.
        - **AAAA Records**: Maps domain names to IPv6 addresses.
        - **MX Records**: Specifies mail exchange servers for handling email for a domain.
        - **CNAME Records**: Aliases one domain name to another.
        - **NS Records**: Identifies the authoritative DNS servers for a domain.
4. **Caching**:
    - DNS servers cache previously queried records to speed up subsequent requests, reducing the time it takes to resolve domain names and decreasing the load on authoritative DNS servers.
5. **Distributed Database**:
    - The DNS system is hierarchical and distributed across many servers around the world. This ensures that no single server is responsible for all DNS queries, improving reliability and scalability.
6. **Load Balancing**:
    - DNS can be used for load balancing by resolving a domain name to different IP addresses depending on server availability or load.

Types of DNS Queries

There are two main types of DNS queries: **Iterated Queries** and **Recursive Queries**.

1. Iterative Query:

- **Definition**: In an iterative query, the DNS resolver (client) asks a DNS server for information about a domain name. If the server does not have the answer, it responds with the address of another server that is more likely to have the requested information. The client then sends the query to the next server, and this process repeats until the answer is found.
- **Process**: The client queries one server at a time, and each server provides a referral to the next server in the DNS hierarchy.
- **Example**:
    1. A client queries the local DNS server for "www.example.com".
    2. The DNS server does not have the answer, so it refers the client to a root DNS server.
    3. The client then queries the root server, which refers it to a Top-Level Domain (TLD) server (e.g., ".com").
    4. The client queries the TLD server, which refers it to an authoritative DNS server for "example.com".
    5. The client finally queries the authoritative DNS server for "www.example.com" and gets the IP address.
- **Advantages**:
    - Less load on DNS servers since they don’t need to perform the entire query resolution process.
    - Faster for the client as it can move to the next server if the current one cannot resolve the query.
- **Disadvantages**:
    - Requires multiple requests and responses, which could increase query latency.

2. Recursive Query:

- **Definition**: In a recursive query, the client asks the DNS server to resolve the domain name completely. The DNS server will take on the responsibility of querying other DNS servers on behalf of the client, following the DNS hierarchy until it finds the final answer. Once the DNS server has resolved the query, it returns the result to the client.

- **Process**: The client sends a single request to a DNS server, and the server will continue querying other DNS servers (if necessary) until it finds the final answer.
- **Example**:
  1. The client queries the local DNS server for "www.example.com".
  2. The local server queries the root DNS server, then the TLD server, and finally the authoritative DNS server for "example.com".
  3. The authoritative server returns the IP address of "www.example.com" to the local DNS server.
  4. The local DNS server then returns the final IP address to the client.
- **Advantages**:
  - The client does not need to perform multiple queries.
  - The process is more straightforward for the client since the DNS server takes full responsibility.
- **Disadvantages**:
  - Places more load on the DNS server since it performs all the steps of the query resolution.
  - Can lead to higher latency if the DNS server needs to make multiple queries to other servers.

33) Analyze error detection and correction capabilities of (23,11) code in which hamming distance varies in the range of 8 to 20.

34) Why Cyclic Redundancy check is called so? Step wise explain the procedure of CRC Encoder for generating codeword for the data words of (7,4) code.

35) What are the two part of Data link layer ? what are the roles of each ? Classify various medium access protocol.

Two Parts of the Data Link Layer

The **Data Link Layer** (Layer 2) in the OSI model is responsible for transferring data between two directly connected nodes and ensuring that the data is transferred reliably over a physical link. The two main sub-layers of the Data Link Layer are:

1. Logical Link Control (LLC)

- **Role**: The LLC sub-layer provides interface and control between the network layer (Layer 3) and the Media Access Control (MAC) sub-layer. It ensures error checking, flow control, and multiplexing.
  - **Error Detection**: LLC checks for errors that might occur during data transmission by using techniques such as Cyclic Redundancy Check (CRC).
  - **Flow Control**: It helps prevent data overflow and ensures that the sender doesn't overwhelm the receiver.
  - **Multiplexing**: It allows multiple Layer 3 protocols to use the same link by distinguishing between them with different protocol identifiers.

2. Media Access Control (MAC)

- **Role**: The MAC sub-layer is responsible for managing access to the physical medium (the transmission channel) and ensuring that data frames are transmitted properly across the link. It handles the following:
  - **Frame Delimiting**: It defines the structure and format of frames.
  - **Access Control**: It determines how devices on the same network access the shared medium. It ensures that multiple devices don't collide when trying to send data at the same time.
  - **Addressing**: The MAC sub-layer uses **MAC addresses** (hardware addresses) to identify devices on a local network.

Medium Access Protocols

Medium Access Control (MAC) protocols are methods that manage access to the shared transmission medium in the data link layer. These protocols ensure that multiple devices can use the same physical medium without causing interference or collisions. MAC protocols are classified based on how the access to the shared medium is controlled. Some of the commonly classified MAC protocols include:

1. Channel Partitioning Protocols

These protocols divide the available bandwidth into smaller, separate channels and assign each device a specific channel to use.

- **Time Division Multiple Access (TDMA)**:
  - Time is divided into slots, and each device is assigned a specific time slot in which it can transmit.
  - Example: Cellular networks (2G, 3G).
- **Frequency Division Multiple Access (FDMA)**:
  - The frequency spectrum is divided into smaller frequency bands, and each device is assigned a different frequency band for transmission.
  - Example: Analog cellular systems.
- **Code Division Multiple Access (CDMA)**:
  - Each device is assigned a unique code that is used to distinguish its signal from others. All devices transmit simultaneously, but the signals are separated by their codes.
  - Example: 3G mobile networks.

2. Random Access Protocols

These protocols allow devices to transmit whenever they have data to send. If two devices transmit at the same time (collision), they must retransmit after a random delay.

- **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**:
  - Devices listen to the channel (carrier sense) before transmitting. If the channel is clear, the device sends its data. If two devices transmit at the same time, a collision occurs, and both devices must retransmit after waiting a random period.
  - Example: Ethernet (in older versions).
- **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**:
  - Similar to CSMA/CD, but instead of detecting collisions after they occur, CSMA/CA tries to avoid collisions by using techniques like waiting for a clear channel before transmitting.
  - Example: Wi-Fi (IEEE 802.11).

3. Polling Protocols

In polling protocols, one device (typically called the **master**) controls access to the medium and polls other devices (the **slaves**) to check if they have data to transmit.

- **Polling Protocol**:
  - The master device asks each device in turn if it has data to send. Only the device that is polled is allowed to transmit.
  - Example: Some serial communication systems and token ring networks.
- **Token Passing**:
  - A token is passed around a network in a sequential manner, and only the device holding the token can transmit.
  - Example: Token Ring networks, FDDI (Fiber Distributed Data Interface).

36) Draw the flow chart of CSMA-CD and CSMA-CA. Explain each step in details.

37) Explain Stop and wait Error control and Flow control Mechanism in TCP.

Stop-and-Wait Error Control and Flow Control Mechanism in TCP

TCP (Transmission Control Protocol) is a reliable, connection-oriented protocol that ensures reliable data transmission between two endpoints. It uses several mechanisms to ensure that data is transferred correctly and efficiently. **Stop-and-Wait** is one such error control and flow control mechanism used in TCP.

Stop-and-Wait Error Control in TCP

Stop-and-Wait is a simple error control mechanism used to ensure reliable communication in data transmission. The key concept is that after sending a packet, the sender stops and waits for an acknowledgment (ACK) from the receiver before sending the next packet. If the sender does not receive an acknowledgment within a certain time frame, it retransmits the packet.

How Stop-and-Wait Error Control Works:

1. **Sender sends a packet**: The sender sends a data segment (packet) to the receiver.
2. **Receiver acknowledges**: The receiver processes the data and sends an acknowledgment (ACK) back to the sender.
3. **Sender waits**: The sender waits for the acknowledgment. If the acknowledgment is received within a timeout period, the sender sends the next packet.
4. **Timeout and retransmission**: If the sender does not receive the acknowledgment within a timeout period, it assumes the packet was lost or corrupted and retransmits the same packet.

Advantages:

- Simple and easy to implement.
- Ensures reliable data delivery by waiting for an acknowledgment before sending the next packet.

Disadvantages:

- Inefficient for high-speed networks: Stop-and-Wait leads to idle periods, especially if the network latency is high, because the sender has to wait for the ACK before sending the next packet.
- Low throughput: The sender has to wait for an ACK after every packet, which limits the overall throughput of the connection.

Flow Control Mechanism in TCP

Flow control is a mechanism to ensure that the sender does not overwhelm the receiver by sending too much data too quickly. It ensures that the sender adjusts its sending rate based on the receiver's capacity, preventing buffer overflow at the receiver’s end.

TCP uses **Sliding Window Protocol** for flow control. This mechanism allows the sender to send multiple packets before waiting for an acknowledgment, improving the efficiency of the connection.

How Flow Control Works in TCP:

1. **Receiver's Window Size**: The receiver advertises a **window size** in the TCP header that indicates how much data it is able to receive without overflowing its buffer. This is called the **advertised window**.
2. **Sliding Window**: The sender can send data up to the size of the receiver’s window. As the receiver acknowledges the received data, the window "slides" forward, allowing the sender to send more data.
3. **Dynamic Adjustment**: The receiver can adjust the window size to indicate its current available buffer space. If the receiver’s buffer becomes full, it reduces the window size, slowing down the sender's transmission rate. If the buffer has space, it increases the window size, allowing the sender to transmit more data.

Flow Control Process:

1. **Initial Communication**: The sender starts sending packets, and the receiver’s window size defines how much data can be sent before receiving an acknowledgment.
2. **Sliding Window Mechanism**: As the sender transmits data, the receiver acknowledges the packets, and the window size moves forward, allowing more data to be sent.

3. **Adjustments Based on Network Conditions**: The receiver can notify the sender to slow down (if buffer space is limited) or speed up (if buffer space is available).
Advantages:

- **Prevents Buffer Overflow**: Ensures that the sender doesn't overwhelm the receiver with too much data.
- **Dynamic Adjustment**: The window size can be adjusted in real-time based on the receiver's available buffer capacity, allowing for optimal data flow.
Disadvantages:
- **Complexity**: More complex than simple flow control mechanisms.
- **Potential for Latency**: The sliding window protocol requires the sender to manage the window size and data flow, which may introduce delays if not managed properly.

38) Match correct answers: 1. Encapsulation a. Telephone Communication 2. Datagram packet switching b. LAN Connection 3. Twisted Pair Cable c. Adding a header 4. Domain Name System d. Satellite communication 5. Circuit Switching e. TV Channel Connection 6. Microwave f. Internet 7. Virtual Circuit Switching g. Host Aliasing & Mail Aliasing 8. Co – Axial Cable h. ATM

00 • **Encapsulation** - Adding a header
01 • **Datagram packet switching** - Internet
02 • **Twisted Pair Cable** - LAN Connection
03 • **Domain Name System** - Host Aliasing & Mail Aliasing
04 • **Circuit Switching** - Telephone Communication
05 • **Microwave** - Satellite communication
06 • **Virtual Circuit Switching** - ATM
07 • **Co-axial Cable** - TV Channel Connection

39) Compare SMTP, POP3 and IMAP.

Comparison Table

Feature	**SMTP**	**POP3**	**IMAP**
Purpose	Sending emails	Retrieving emails	Retrieving and managing emails
Direction	Outbound (sending emails)	Inbound (retrieving emails)	Inbound (retrieving emails)
Port	25, 587 (secure)	110 (unencrypted), 995 (secure)	143 (unencrypted), 993 (secure)
Connection Type	Push (email sent to server)	Pull (email downloaded to client)	Push (email synchronized with server)
State	Stateless (no session maintained)	State: emails removed from server	Stateful (emails stay on server)
Email Storage	No storage (just sends emails)	Emails are stored locally	Emails stay on server

Feature	SMTP	POP3	IMAP
Multi-Device Support	No	No	Yes
Security	STARTTLS, SSL/TLS for encryption	SSL/TLS for encryption	SSL/TLS for encryption
Authentication	Required for sending emails	Required for retrieving emails	Required for retrieving emails
Advantages	Reliable email sending	Simple, offline email retrieval	Multi-device synchronization, server-side storage
Disadvantages	Cannot retrieve emails	Cannot synchronize across devices	Requires constant server connection

40) Which layers in the Internet protocol stack does a router process? Which layers does a . link-layer switch process? Which layers does a host process?

Here's a breakdown of which layers are processed by a **router**, a **link-layer switch**, and a **host** in the **Internet protocol stack**:

1. Router

A **router** processes the following layers:

- **Network Layer (Layer 3)**: Routers operate primarily at the **Network Layer**. They are responsible for routing packets between different networks by using logical addressing (typically IP addresses). Routers examine the **IP address** of incoming packets and forward them to the appropriate destination network.
- **Data Link Layer (Layer 2)**: Routers also interact with the **Data Link Layer** for the actual transmission of packets over physical links. However, their main function is to forward packets based on the IP address, not directly handling the physical transmission.

Router Processes:

- **Layer 3 (Network Layer)**: Routes based on IP addresses.
- **Layer 2 (Data Link Layer)**: Handles the framing of data for transmission between devices within the same local network.

2. Link-layer Switch

A **link-layer switch** (often just called a **switch**) processes the following layers:

- **Data Link Layer (Layer 2)**: Switches operate primarily at the **Data Link Layer**. They forward frames based on the **MAC (Media Access Control) addresses** of devices within the same local network (or LAN). Switches maintain a MAC address table to keep track of where each device is located on the network.
- **Physical Layer (Layer 1)**: Switches also interact with the **Physical Layer** to transmit bits over physical connections (e.g., cables, fiber optics).

Link-layer Switch Processes:

- **Layer 2 (Data Link Layer)**: Forwards frames based on MAC addresses.
- **Layer 1 (Physical Layer)**: Transmits raw bits over physical connections.

3. Host

A **host** (such as a computer or server) processes the following layers:

- **Application Layer (Layer 7)**: Hosts run applications (such as web browsers, email clients, etc.) that interact with users or other systems. The host processes and generates data that is ultimately transmitted across the network.
- **Transport Layer (Layer 4)**: Hosts process **TCP** (Transmission Control Protocol) or **UDP** (User Datagram Protocol) to ensure reliable or unreliable data transmission (e.g., flow control, error detection, etc.).
- **Network Layer (Layer 3)**: Hosts process **IP** (Internet Protocol) to handle routing of packets between different networks. They also assign themselves an IP address for communication.
- **Data Link Layer (Layer 2)**: Hosts process the **Ethernet protocol** or similar data link protocols to interact with the physical network and transmit frames over a local network.
- **Physical Layer (Layer 1)**: Hosts also manage the actual physical connection to the network (e.g., using network interface cards (NICs) to transmit bits over Ethernet or Wi-Fi).
  Host Processes:
- **Layer 7 (Application Layer)**: Executes applications and protocols like HTTP, FTP, etc.
- **Layer 4 (Transport Layer)**: Manages data flow via TCP or UDP.
- **Layer 3 (Network Layer)**: Handles IP addressing and routing.
- **Layer 2 (Data Link Layer)**: Handles data transmission and MAC addressing.
- **Layer 1 (Physical Layer)**: Transmits raw bits on the physical medium.
  Summary of Layers Processed:

Device	**Layers Processed**
Router	**Layer 3 (Network Layer)** and **Layer 2 (Data Link Layer)**
Link-layer Switch	**Layer 2 (Data Link Layer)** and **Layer 1 (Physical Layer)**
Host	**Layer 7 (Application Layer)**, **Layer 4 (Transport Layer)**, **Layer 3 (Network Layer)**, **Layer 2 (Data Link Layer)**, **Layer 1 (Physical Layer)**

In summary:

- **Routers** mainly operate at **Layer 3 (Network Layer)** but also interact with **Layer 2 (Data Link Layer)**.
- **Switches** operate at **Layer 2 (Data Link Layer)** and interact with **Layer 1 (Physical Layer)**.
- **Hosts** process all layers from **Layer 1** to **Layer 7** depending on the type of communication being made.

41) How ARP works :-

ARP Protocol

- ARP stands for “Address Resolution Protocol”. It is a network protocol used to determine the MAC address (hardware address) from any IP address.

- In other words, ARP is used to mapping the IP Address into MAC Address. When one device wants to communicate with another device in a LAN (local area network) network, the ARP protocol is used.

- This protocol is used when a device wants to communicate with another device over a local area network or ethernet.

- ARP is a network layer protocol. This is a very important protocol in the TCP/IP protocol suite. Although it was developed in the early 80s, it was defined in RFC 826 in 1982. ARP is implemented with important technologies like IPv4, X.25, frame relay, and ATM.

- ARP protocol finds the MAC address based on IP address. IP address is used to communicate with any device at the application layer. But to communicate with a device at the data link layer or to send data to it, a MAC address is required.

- When data is sent to a local host, the data travels between networks via IP address. But to reach that host in LAN, it needs the MAC address of that host. In this situation the address resolution protocol plays an important role.

Important ARP Terms

- **ARP Cache :-** After receiving the MAC address, ARP passes it to the sender where it is stored in a table for future reference. And this is called ARP Cache which is later used to obtain the MAC address.
- **ARP Cache Timeout :-** This is the time in which the MAC address can remain in the ARP Cache.
- **ARP request :-** Broadcasting a packet over the network to verify whether we have arrived at the destination MAC address.
- **ARP response/reply :-** It is a MAC address response that the sender receives from the receiver which helps in further communication of data.

Types of ARP

There are four types of ARP protocol they are as follows:-

1. Proxy ARP
2. Gratuitous ARP
3. Reverse ARP
4. Inverse ARP

1. Proxy ARP

This is a technique through which proxy ARP in a network can answer ARP queries of IP addresses that are not in that network. That is, if we understand it in simple language, the Proxy server can also respond to queries of IP-address of other networks.

Through this we can fool the other person because instead of the MAC address of the destination device, the MAC address of the proxy server is used and the other person does not even know.

2. Gratuitous ARP

This is an arp request of a host, which we use to check duplicate ip-address. And we can also use it to update the arp table of other devices. That is, through this we can check whether the host is using its original IP-address, or is using a duplicate IP-address.

This is a very important ARP. Which proves to be very helpful in protecting us from the wrong person, and by using it we can check the ip-address.

3. Reverse ARP

This is also a networking protocol, which we can use through client computer. That is, it is used to obtain information about one's own network from the computer network. That is, if understood in simple language, it is a TCP/IP protocol which we use to obtain information about the IP address of the computer server.

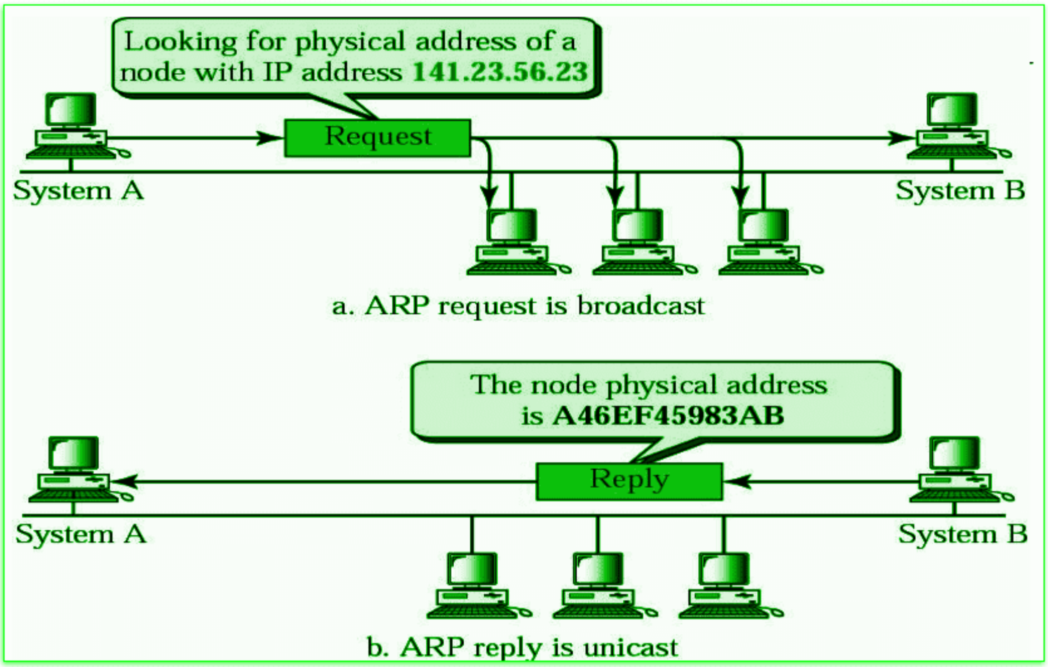
That is, to know the IP address of our computer server, we use Reverse ARP, which works under a networking protocol.

4. Inverse ARP (InARP)

Inverse ARP, it is the opposite of ARP, that is, we use it to know the IP address of our device through MAC Address, that is, it is such a networking technology, through this we convert MAC Address into IP address. Can translate. It is mainly used in ATM machines.

How ARP Protocol Works?

Below is a Working flow diagram of ARP Protocol


Looking for physical address of a node with IP address 141.23.56.23
Request
System A
System B
a. ARP request is broadcast
The node physical address is A46EF45983AB
Reply
System A
System B
b. ARP reply is unicast

ARP Protocol

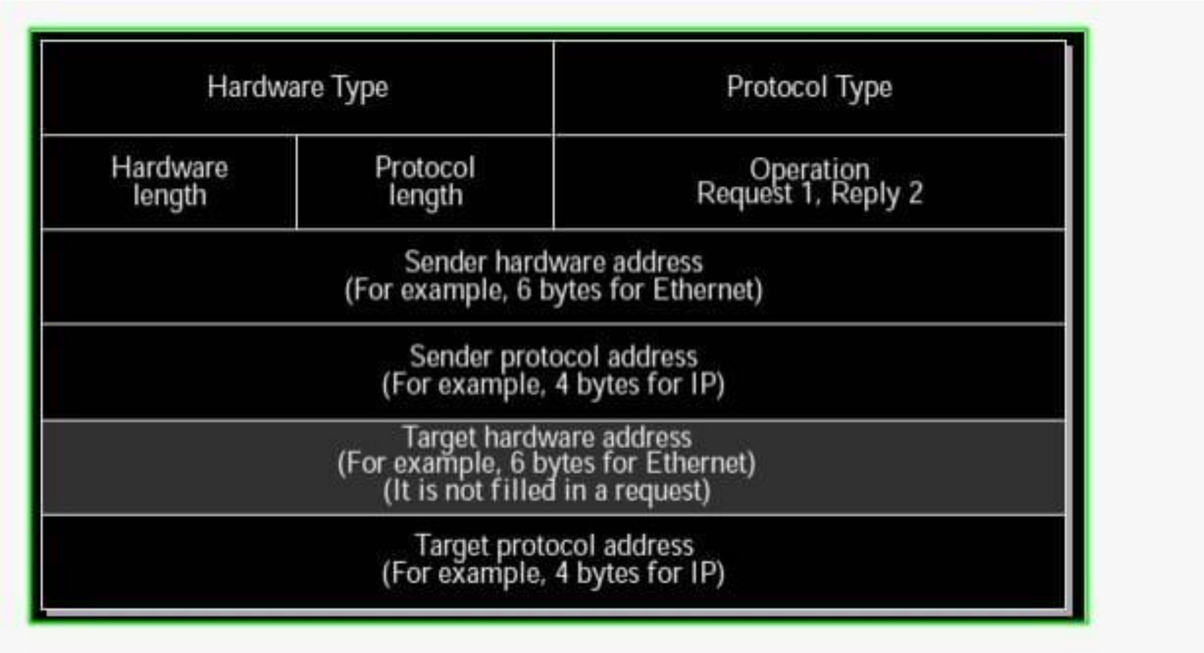
Below is the working of address resolution protocol is being explained in some steps :-

- When a sender wants to communicate with a receiver, the sender first checks its ARP cache. Sender checks whether the receiver's MAC address is already present in the ARP cache or not?
- If the receiver's MAC address is already present in the ARP cache, the sender will communicate with the receiver using that MAC address.
- If the MAC address of the receiver device is not already present in the ARP cache, then in such a situation an ARP request message is prepared by the sender device.This message contains the MAC address of the sender, IP address of the sender and IP address of the receiver. The field containing the MAC address of the receiver is left blank because it is being searched.
- Sender device broadcasts this ARP request message in the LAN. Because this is a broadcast message, every device connected to the LAN receives this message.
- All devices match the receiver IP address of this request message with their own IP address. Devices whose IP address does not match drop this request message.
- The device whose IP address matches the receiver IP address of this request message receives this message and prepares an ARP reply message. This is a unicast message which is sent only to the sender.

- In ARP reply message, the sender's IP address and MAC address are used to send the reply message. Besides, in this message the receiver also sends its IP address and MAC address.
- As soon as the sender device receives this ARP reply message, it updates its ARP cache with the new information (Receiver's MAC address). Now the MAC address of the receiver is present in the ARP cache of the sender. The sender can send and receive data without any problem.

Message Format of ARP Protocol

Messages are sent to find the MAC address through ARP(address resolution protocol). These messages are broadcast to all the devices in the LAN. The format of this message is being shown in the diagram below :



Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled in a request)		
Target protocol address (For example, 4 bytes for IP)		

Message format of ARP

All the fields given in ARP message format are being explained in detail below:-

- **Hardware Type:** The size of this field is 2 bytes. This field defines what type of Hardware is used to transmit the message. The most common Hardware type is Ethernet. The value of Ethernet is 1.
- **Protocol Type:** This field tells which protocol has been used to transmit the message. substantially the value of this field is 2048 which indicates IPv4.
- **Hardware Address Length:** It shows the length of the tackle address in bytes. The size of Ethernet MAC address is 6 bytes.
- **Protocol Address Length:** It shows the size of the IP address in bytes. The size of IP address is 4 bytes.
- **OP law:** This field tells the type of message. If the value of this field is 1 also it's a request message and if the value of this field is 2 also it's a reply message.
- **Sender Hardware Address:** This field contains the MAC address of the device transferring the message.
- **Sender Protocol Address:** This field contains the IP address of the device transferring the message.
- **Target Hardware Address:** This field is empty in the request message. This field contains the MAC address of the entering device.
- **Target Protocol Address:** This field contains the IP address of the entering device.

Advantages of ARP Protocol

There are many Advantages of ARP protocol but below we have told you about some important advantages.

- By using this protocol we can easily find out the MAC Address of the device.
- There is no need to configure the end nodes at all to extract the MAC address through this protocol.
- Through this protocol we can easily translate IP address into MAC Address.
- There are four main types of this protocol. Which we can use in different ways, and they prove to be very helpful.

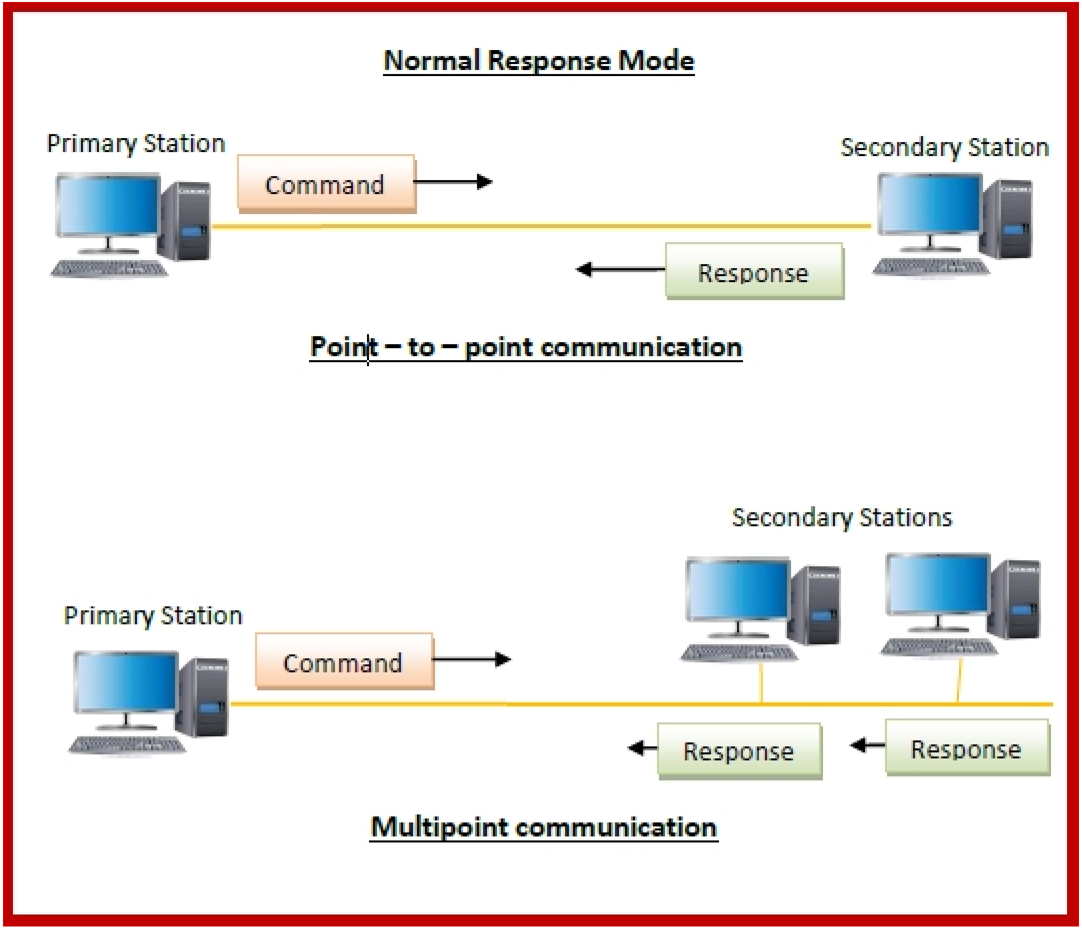
42) Consider sending a packet from a source host to a destination host over a fixed route. List the delay components in the end-to-end delay.
43) What advantage does a circuit-switched network have over a packet-switched network?
44) What are the five layers in the Internet protocol stack? What are the principal responsibilities of each of these layers?
45) Explain HDLC Protocol.

High-level Data Link Control (HDLC) is a group of communication protocols of the **data link layer** for transmitting data between network points or nodes. Since it is a **data link protocol**, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

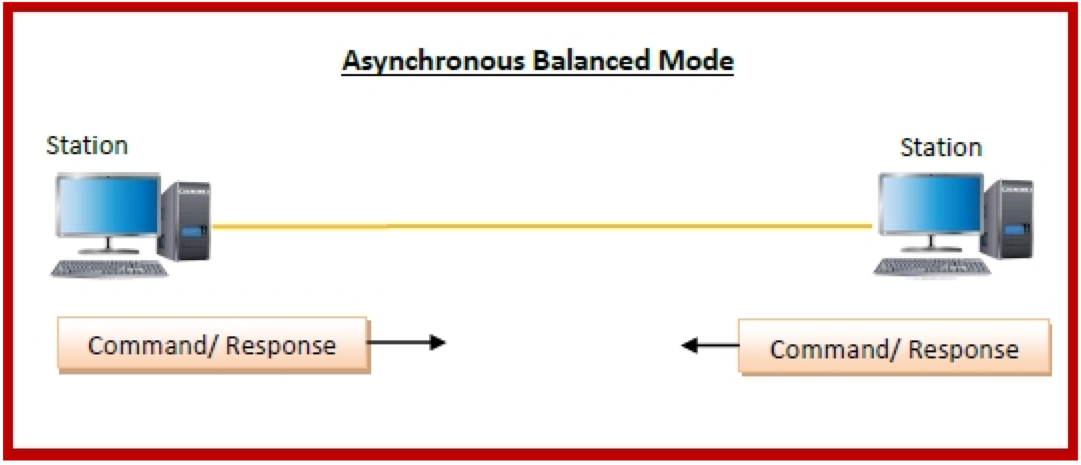
Transfer Modes

HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

- **Normal Response Mode (NRM)** − Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.



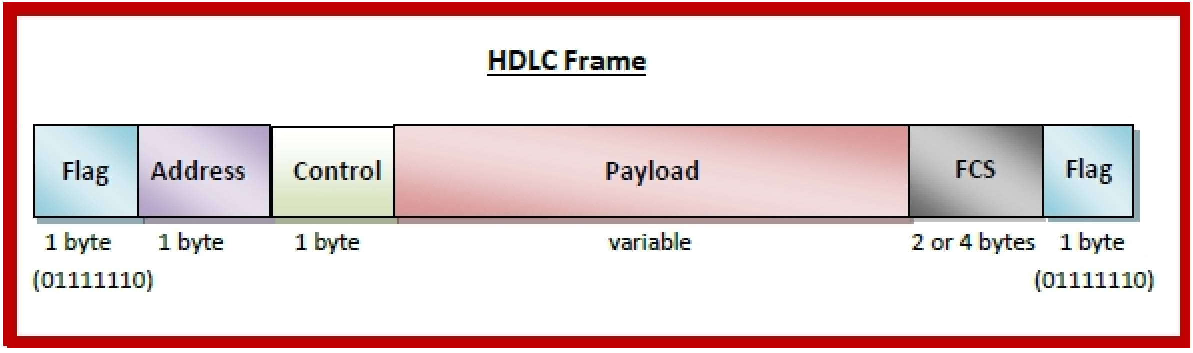
- **Asynchronous Balanced Mode (ABM)** − Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.



HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are −

- **Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control** − It is 1 or 2 bytes containing flow and error control information.
- **Payload** − This carries the data from the network layer. Its length may vary from one network to another.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)

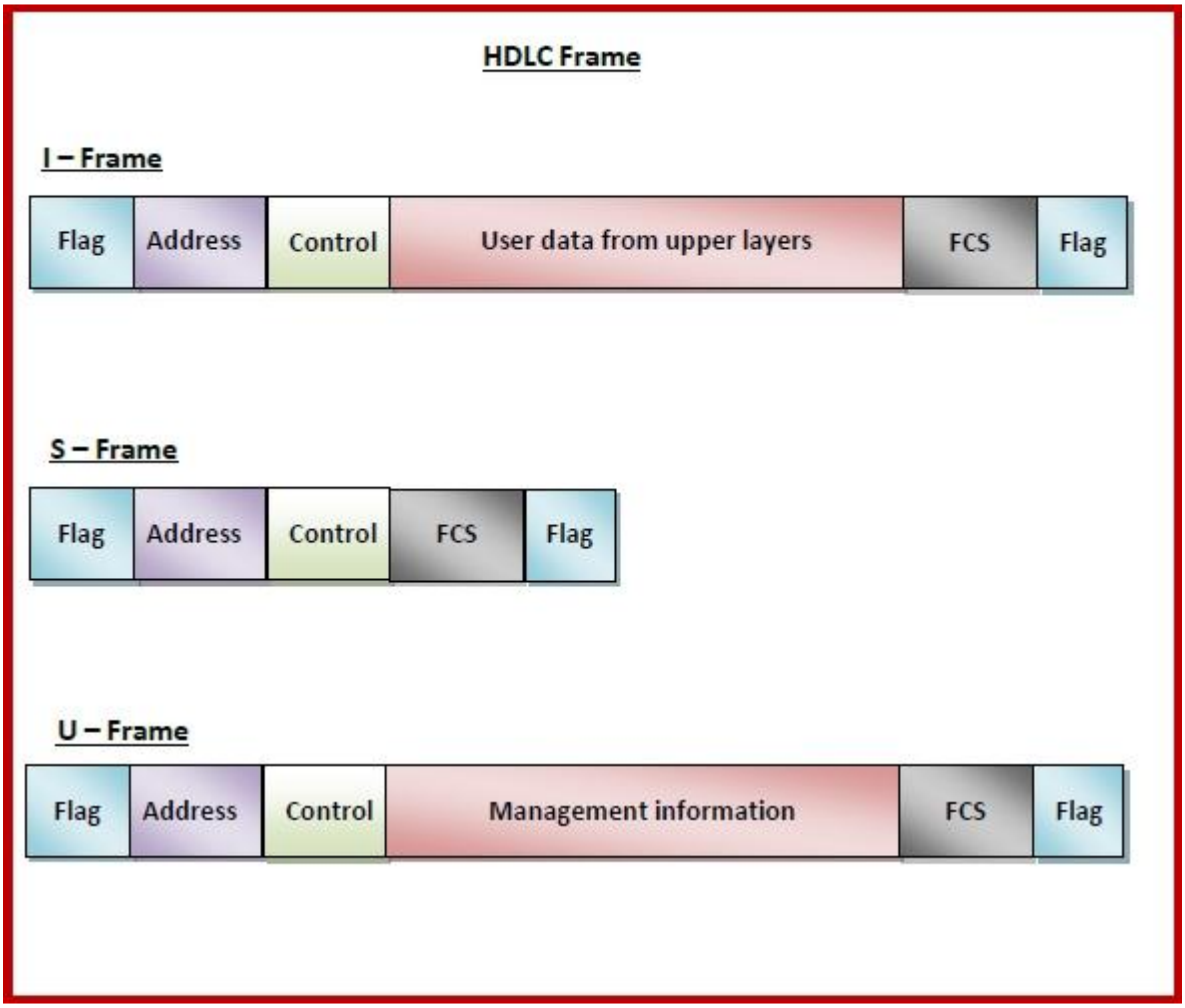


Types of HDLC Frames

There are three types of HDLC frames. The type of frame is determined by the control field of the frame −

- **I-frame** − I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.

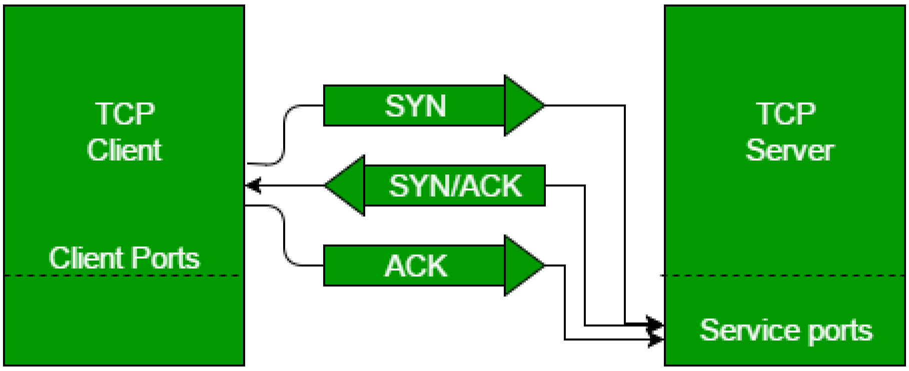
- **S-frame** − S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.
- **U-frame** − U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11.



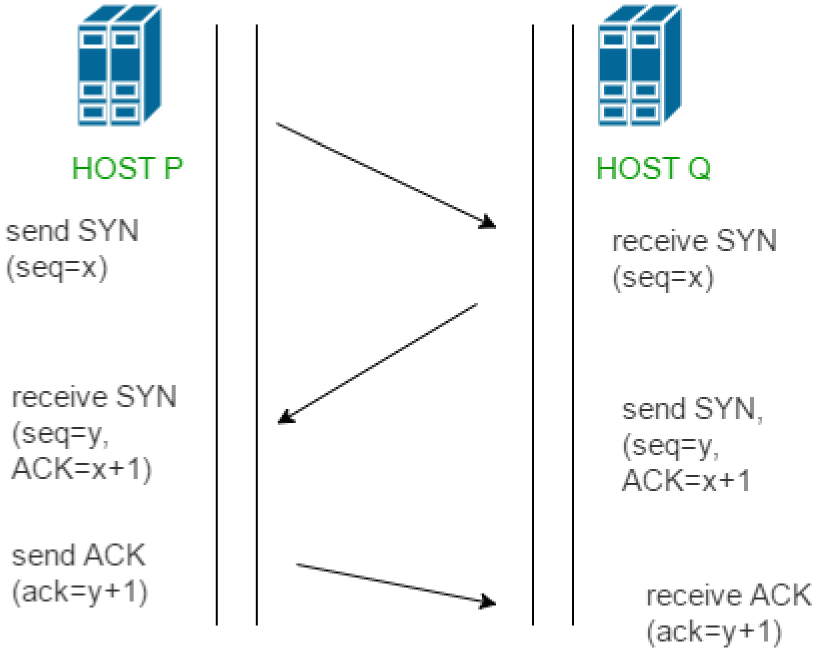
46) Explain Sliding window protocol with sequence number logic and figures
47) Differentiate congestion control and flow Control.
48) Explain the process of connection establishment and connection release process.(it is in TCP).

TCP 3-way Handshake Process

The process of communication between devices over the internet happens according to the current **TCP/IP** suite model(stripped-out version of OSI reference model). The Application layer is a top pile of a stack of TCP/IP models from where network-referenced applications like web browsers on the client side establish a connection with the server. From the application layer, the information is transferred to the transport layer where our topic comes into the picture. The two important protocols of this layer are – TCP, and **UDP(User Datagram Protocol)** out of which TCP is prevalent(since it provides reliability for the connection established). However, you can find an application of UDP in querying the DNS server to get the binary equivalent of the Domain Name used for the website.



TCP provides reliable communication with something called **Positive Acknowledgement with Re-transmission(PAR)** . The Protocol Data Unit(PDU) of the transport layer is called a segment. Now a device using PAR resend the data unit until it receives an acknowledgement. If the data unit received at the receiver's end is damaged(It checks the data with checksum functionality of the transport layer that is used for Error Detection), the receiver discards the segment. So the sender has to resend the data unit for which positive acknowledgement is not received. You can realize from the above mechanism that three segments are exchanged between sender(client) and receiver(server) for a reliable TCP connection to get established. Let us delve into how this mechanism works



- **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

CP is a connection-oriented protocol and every connection-oriented protocol needs to establish a connection in order to reserve resources at both the communicating ends.

Connection Establishment –

TCP connection establishment involves a three-way handshake to ensure reliable communication between devices. Understanding each step of this handshake process is critical for networking professionals. For a deeper dive into how TCP connections are established and managed, the **GATE CS and IT – 2025 course** provides practical insights and detailed explanations, making it easier to grasp the intricacies of TCP and other networking protocols

1. Sender starts the process with the following:

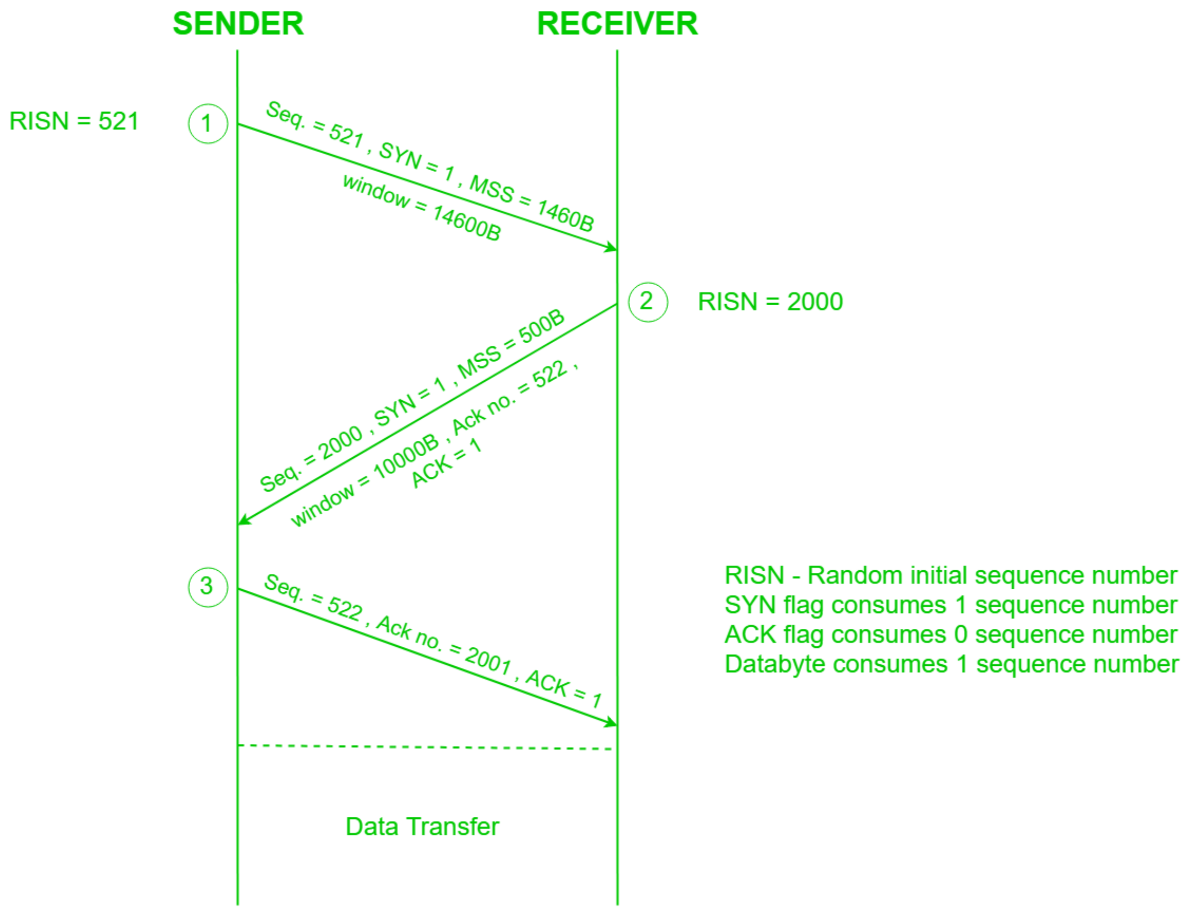
- **Sequence number (Seq=521):** contains the random initial sequence number generated at the sender side.
- **Syn flag (Syn=1):** request the receiver to synchronize its sequence number with the above-provided sequence number.
- **Maximum segment size (MSS=1460 B):** sender tells its maximum segment size, so that receiver sends datagram which won't require any fragmentation. MSS field is present inside **Option** field in TCP header.
- **Window size (window=14600 B):** sender tells about his buffer capacity in which he has to store messages from the receiver.

2. TCP is a full-duplex protocol so both sender and receiver require a window for receiving messages from one another.

- **Sequence number (Seq=2000):** contains the random initial sequence number generated at the receiver side.
- **Syn flag (Syn=1):** request the sender to synchronize its sequence number with the above-provided sequence number.
- **Maximum segment size (MSS=500 B):** receiver tells its maximum segment size, so that sender sends datagram which won't require any fragmentation. MSS field is present inside **Option** field in TCP header.
  Since MSS receiver < MSS sender , both parties agree for minimum MSS i.e., 500 B to avoid fragmentation of packets at both ends.
  Therefore, receiver can send maximum of 14600/500 = 29 packets.
  This is the receiver's sending window size.
- **Window size (window=10000 B):** receiver tells about his buffer capacity in which he has to store messages from the sender.
  Therefore, sender can send a maximum of 10000/500 = 20 packets.
  This is the sender's sending window size.
- **Acknowledgement Number (Ack no.=522):** Since sequence number 521 is received by the receiver so, it makes a request for the next sequence number with Ack no.=522 which is the next packet expected by the receiver since Syn flag consumes 1 sequence no.
- **ACK flag (ACk=1):** tells that the acknowledgement number field contains the next sequence expected by the receiver.

3. Sender makes the final reply for connection establishment in the following way:

- **Sequence number (Seq=522):** since sequence number = 521 in 1 st step and SYN flag consumes one sequence number hence, the next sequence number will be 522.
- **Acknowledgement Number (Ack no.=2001):** since the sender is acknowledging SYN=1 packet from the receiver with sequence number 2000 so, the next sequence number expected is 2001.
- **ACK flag (ACK=1):** tells that the acknowledgement number field contains the next sequence expected by the sender.


SENDER
RECEIVER
RISN = 521
1
Seq. = 521 , SYN = 1 , MSS = 1460B
window = 14600B
2
RISN = 2000
Seq. = 2000 , SYN = 1 , MSS = 500B
window = 10000B , Ack no. = 522 ,
ACK = 1
3
Seq. = 522 , Ack no. = 2001 , ACK = 1
RISN - Random initial sequence number
SYN flag consumes 1 sequence number
ACK flag consumes 0 sequence number
Databyte consumes 1 sequence number
Data Transfer

Since the connection establishment phase of TCP makes use of 3 packets, it is also known as 3-way Handshaking**(SYN, SYN + ACK, ACK).**

TCP Connection Termination

In TCP 3-way Handshake Process we studied that how connections are established between client and server in Transmission Control Protocol (TCP) using SYN bit segments. In this article, we will study how TCP close connection between Client and Server. Here we will also need to send bit segments to a server which FIN bit is set to 1. TCP supports two types of connection releases like most connection-oriented transport protocols:

1. **Graceful connection release –**
   In the Graceful connection release, the connection is open until both parties have closed their sides of the connection.
2. **Abrupt connection release –**
   In an Abrupt connection release, either one TCP entity is forced to close the connection or one user closes both directions of data transfer.
   Abrupt connection release :
   An abrupt connection release is carried out when an RST segment is sent. An RST segment can be sent for the below reasons:

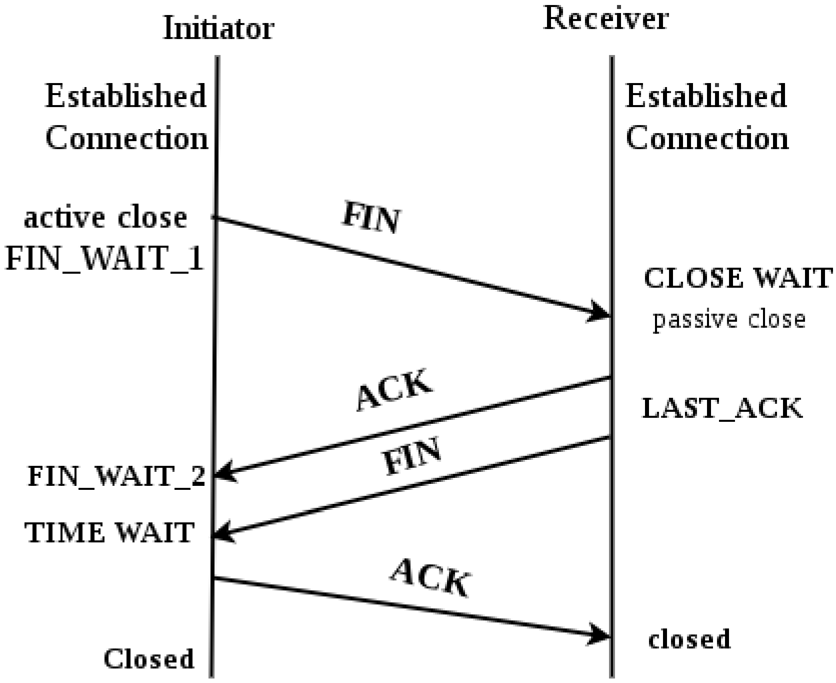
1. **When a non-SYN segment was received for a non-existing TCP connection.**
2. **In an open connection, some TCP implementations send an RST segment when a segment with an invalid header is received. This will prevent attacks by closing the corresponding connection.**

3. **When some implementations need to close an existing TCP connection, they send an RST segment. They will close an existing TCP connection for the following reasons:**
   - **Lack of resources to support the connection**
   - **The remote host is now unreachable and has stopped responding.**

   When a TCP entity sends an RST segment, it should contain 00 if it does not belong to any existing connection else it should contain the current value of the sequence number for the connection and the acknowledgment number should be set to the next expected in- sequence number on this connection.

   Graceful Connection Release :

   The common way of terminating a TCP connection is by using the TCP header's FIN flag. This mechanism allows each host to release its own side of the connection individually.



How mechanism works In TCP :

1. **Step 1 (FIN From Client) –**
   Suppose that the client application decides it wants to close the connection. (Note that the server could also choose to close the connection). This causes the client to send a TCP segment with the FIN bit set to 1 to the server and to enter the FIN_WAIT_1 state. While in the FIN_WAIT_1 state, the client waits for a TCP segment from the server with an acknowledgment (ACK).
2. **Step 2 (ACK From Server) –**
   When the Server received the FIN bit segment from Sender (Client), Server Immediately sends acknowledgement (ACK) segment to the Sender (Client).
3. **Step 3 (Client waiting) –**
   While in the FIN_WAIT_1 state, the client waits for a TCP segment from the server with an acknowledgment. When it receives this segment, the client enters the FIN_WAIT_2 state. While in the FIN_WAIT_2 state, the client waits for another segment from the server with the FIN bit set to 1.
4. **Step 4 (FIN from Server) –**
   The server sends the FIN bit segment to the Sender(Client) after some time when the Server sends the ACK segment (because of some closing process in the Server).
5. **Step 5 (ACK from Client) –**
   When the Client receives the FIN bit segment from the Server, the client acknowledges

the server's segment and enters the TIME_WAIT state. The TIME_WAIT state lets the client resend the final acknowledgment in case the ACK is lost. The time spent by clients in the TIME_WAIT state depends on their implementation, but their typical values are 30 seconds, 1 minute, and 2 minutes. After the wait, the connection formally closes and all resources on the client-side (including port numbers and buffer data) are released.
TCP connection termination involves a four-way handshake to gracefully end the connection between two devices. Understanding each step—FIN, ACK, and how timers work—is critical for networking professionals and students alike. Since exam scenarios often require in-depth knowledge of protocols like TCP, studying additional material that covers both theoretical and practical aspects can be very helpful. For example, this GATE CS and IT – 2025 course goes beyond the basics and dives into real-world applications, ensuring you're well-prepared for both exams and practical implementations.
In the below Figures illustrate the series of states visited by the server-side and also the Client-side, assuming the client begins connection tear-down. In these two state-transition figures, we have only shown how a TCP connection is normally established and shut down.
TCP states visited by ClientSide –

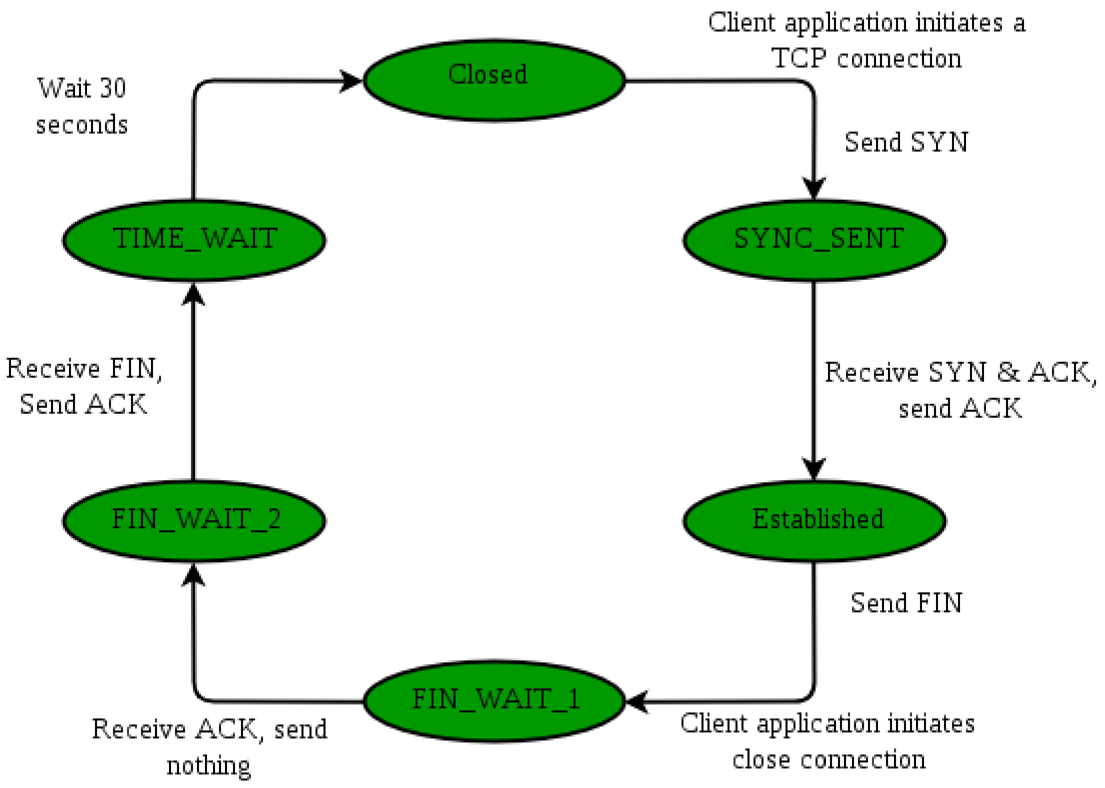

Client application initiates a TCP connection
Closed
Wait 30 seconds
Send SYN
TIME_WAIT
SYNC_SENT
Receive FIN, Send ACK
Receive SYN & ACK, send ACK
FIN_WAIT_2
Established
Send FIN
FIN_WAIT_1
Receive ACK, send nothing
Client application initiates close connection

Fig : TCP states visited by a client TCP

TCP states visited by ServerSide –

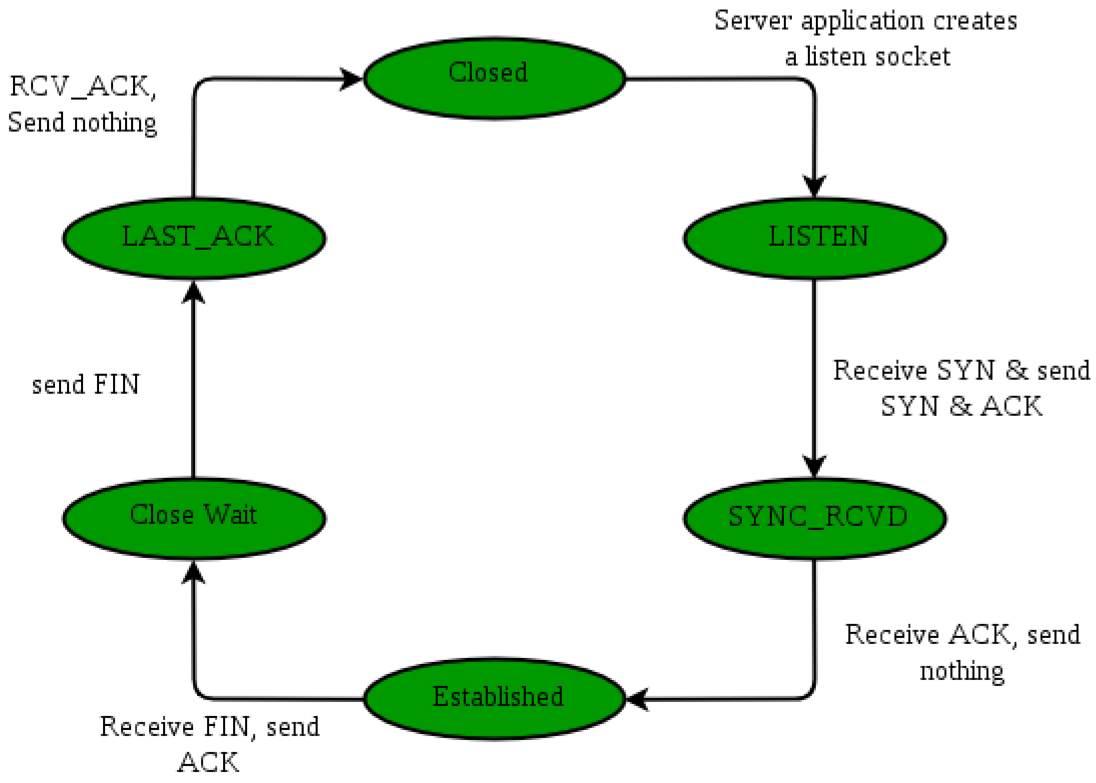


Fig : TCP states visited by a client TCP

Here we have not described what happens in certain scenarios like when both sides of a connection want to initiate or shut down at the same time. If you are interested in learning more about this and other advanced issues concerning TCP, you are encouraged to see Stevens'comprehensive book.

49) Explain the concept of multiplexing and demultiplexing in transport layer.
50) Draw IPV4 header format and explain the functionality of each field of IPV4 header.
51) Explain Routing Information Protocol with appropriate diagram.
52) Discuss Link state routing protocol with proper diagram.
53) Discuss Distance Vector Routing protocol with proper diagram.
54) Discuss the concept of EIGRP with example.

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco-proprietary Hybrid routing protocol that contains features of distance-vector and link-state routing protocols. It is a network layer protocol that works on protocol number 88.
Some of its features are:

1. **Rapid convergence** – EIGRP uses a DUAL algorithm to support rapid convergence. If a route to a network goes down then another route(feasible successor) can be used. If there is no route present to that network in the topology table also then a query message is multicast to find out the alternative route to that network.

2. **Reduced bandwidth usage** – EIGRP doesn't send periodic updates like other distance vector routing protocol does. Distance Vector Routing protocol like RIP sends full routing table over a period of time, therefore, consumes the available bandwidth needlessly but EIGRP uses partial updates if there is any change in the topology occurs i.e updates are triggered only if any event occurs therefore consuming the bandwidth when needed. Also, EIGRP updates are

propagated to the routers only who require it.

3. **Support all LAN and WAN data link protocols and topologies –** EIGRP supports multi-access networks like FDDI, token ring, etc, and all WAN topologies like leased line, point-to-point links. EIGRP doesn't require any additional configuration across layer 2 protocols like frame relay.

4. **Supports auto-summary –** In EIGRP, auto-summarization is enabled by default. Auto summarization is a feature that allows Routing Protocols to summarize their routes to their classful networks automatically i.e routers will receive summarised routes automatically. EIGRP. e.g-1.1.1.1 /24 will be automatically summarised to the classful 1.1.1.1/8

5. **Supports unequal cost load balancing –** Unequal cost load balancing is possible in EIGRP by changing the value of variance. By default, variance is 1, therefore, supports equal-cost load balancing but if we want to use unequal cost load balancing then we can change the value of variance according to the amount of traffic we want to divide across different paths. Feasible distance is multiplied in such a way that it becomes greater than the value of the feasible distance of successor.

6. **Communication via Reliable Transfer Protocol (RTP) –** EIGRP depends upon proprietary protocol RTP to manage the communication between EIGRP speaking routers. EIGRP uses 224.0.0.10 as its a multicast address. For each multicast it sends, the router prepares and maintains a list of routers (speaking EIGRP). If no acknowledgement of multicast is received then the same data is transmitted through 16 unicast messages. If no acknowledgement is received even after 16 unicast attempts then it is declared dead. This process is known as reliable multicast.

7. **Best path selection using DUAL –** EIGRP uses Diffusing Update Algorithm (DUAL) to find out the best path available to a network. EIGRP speaking routers maintain a topology table in which all the routes to the network are maintained. If the best path (successor) goes down, then the second best path (feasible successor) is used from the topology table. If there is no path available in the topology table then it sends a query message to resolve the query.
It maintains 3 different tables mainly:
(a) Neighbor table: It contains information about the routers with which neighbourship has been formed. It contains the SRTT, RTP. It also contains the queue count value for the hello messages that are not being acknowledged.
(b) Topology table: It contains all the routes available to a network (both feasible successor and successor).
(c) Routing table: It contains all the routes which are being used to make current routing decisions. The routes in this table are considered as successor (best path) routes.

8. **Traffic control –** Suppose if one of the interfaces of the router is connected to ISP then we don't want that interface to be part of the EIGRP process. For this scenario, EIGRP provides a feature in which we can flag the interface as passive i.e not to take part in the EIGRP process.

9. Support Variable Length Subnet Mask (VLSM).
10. Support for both IPv4 and IPv6.

55) Distinguish between IPV4 address and IPV6 address.
56) Make a list of IP address class with its range. What are the default subnet mask of class A, B & C. Draw and explain network id and host id in class A, B & C.

57) Calculate the checksum of given frame: Frame1 - 11001100, Frame2 - 10101010, Frame3 - 11110000, Frame4 – 11000011. Justify your answer whether data accepted or rejected at receiver side?

58) Write a shot note on virtual local area network.

59) Discuss the concept of variable size framing in terms of character oriented and Bit oriented with example.

60) A bit stream is transmitted 1101101 using the CRC method. The generator polynomial is X4+X2+1. What is the actual bit stream transmitted?

61) Write short note on random access collision sense protocol for collision detection and collision avoidance.

62) Solve the following example using Cyclic redundancy check Data=1101101 Divisor =10101

63) Describe LAN,WAN, MAN with example.

64) The following is a dump of a UDP header in hexadecimal format. CB84000D001C001C ⎤ What is the source port number? ⎤ What is the destination port number? ⎤ What is the total length of the user datagram? ⎤ What is the length of the data?

65) Classify connection establishment and connection termination in TCP.

66) The following is a dump of a UDP header in hexadecimal format. 0421000B002AE217 ⎤ What is the source port number? ⎤ What is the destination port number? ⎤ What is the total length of the user datagram? ⎤ What is the length of the data?

67) Classify open loop and close loop principal of congestion control.

68) Explain IPV6 header with its fields.

69) Explain Distance vector routing with example.

70) Compare circuit switching and Packet switching.

71) Justify the statement, “HTTP server is stateless”.

72) What is socket? Explain TCP socket in detail.

73) Explain types of error with example.

74) Write short notes on circuit switching and packet switching

75) If a file consisting of 100,000 characters takes 40 seconds to send, then the data rate is

____

76) What is congestion? Discuss the approaches to congestion control

77) Explain why is UDP used for multimedia applications instead of TCP

78) Explain Segmentation in TCP

79) Explain Three-Ways-Handshaking in TCP

80) Explain Congestion control protocol in TCP

81) What is the Count To Infinity Problem

82) Please suggest the solution to Count to Infinity Problem

83) What is DHCP and how does it works

84) What is ARP and RARP? Explain the usage of both

85) What is a MAC Address

86) State and explain any 4 Flags from IPv4 Header

87) What is Fragmentation. Explain how scaling factor can be used to store large fragment number into small field size

88) Explain Time to Live field in IPv4

89) What is Header Checksum. Explain with an Example

90) Explain the DORA process in DHCP.

91) Write the difference between TCP and UDP.

92) Compare IPV4 and IPV6.

93) Give the classification of Unicast routing protocol. Explain the protocol which is used to communicate between two autonomous system.

94) Discuss the concept of EIGRP with example.

95) List classes of IP address with range. Write the default subnet mask class A, B & C. Explain host id and network id in class A, B & C with diagram.

96) A bit stream is transmitted 1101101 using the CRC method. The generator polynomial is X4+X2+1. What is the actual bit stream transmitted?

97) Discuss the concept of VLAN. Explain different types of VLAN.

98) Write short note on CSMA/CD and CSMA/CA.

99) Calculate the checksum of given frame: Frame1 - 11001100, Frame2 - 10101010, Frame3 - 11110000, Frame4 – 11000011. Justify your answer whether data accepted or rejected at receiver side?

100) Discuss Byte stuffing and Bit Stuffing with example.

101) Differentiate LAN & WAN.

102) Solve the following example using Cyclic redundancy check Data=1101101 Divisor=10101

103) Define LAN, WAN and MAN in detail.

104) Write a note on DORA Process.

105) Explain stop and wait for ARQ.

106) If a periodic signal is decomposed into four sine waves with frequencies of 200, 300, 700, and 800 Hz, what is its bandwidth? Draw the spectrum, assuming all components have a maximum amplitude of 5 V.

107) Explain bit-oriented Data link layer protocol in detail.

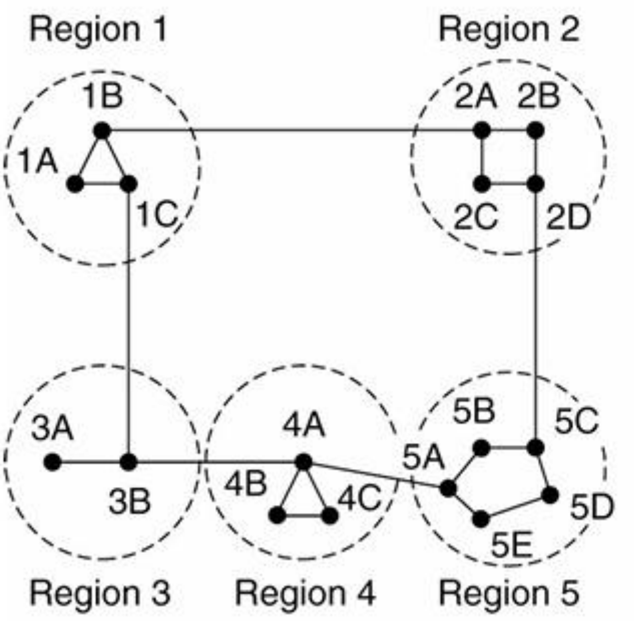
108) Sketch and explain CRC code.

109) Sketch and explain Selective Repeat ARQ protocol. Calculate the receiver window size for Selective Repeat ARQ if m=2.

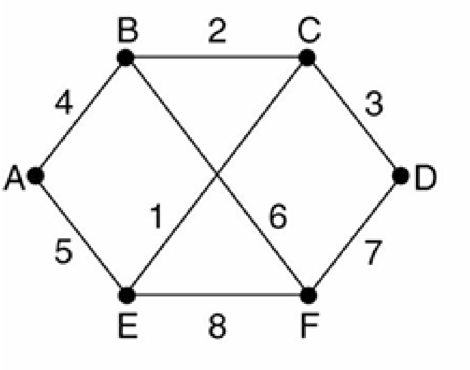
110) Compare Pure ALOHA with Slotted ALOHA protocol.

111) Sketch and explain CSMA protocol.

112) Explain the Hierarchical routing algorithm. Draw the Hierarchical routing table for Node 1A for the below given subnet.



113) Explain Link state routing algorithm. Create link state packets for all the nodes of the below given subnet.



114) Compare Public IP address with Private IP address with example.

115) Sketch and explain Token bucket algorithm.

116) Sketch and explain leaky bucket algorithm.

117) What is congestion? Why congestion occurs?

118) Sketch and explain the process of Hop-by-Hop choke packet.

119) What is Jitter? Compare High jitter with Low jitter with its graphs.

120) Define congestion prevention policies at Transport layer.

121) Compare flow control protocols for the noiseless channel. Support your answer with design figure, pseudo code, flow diagram and analysis.

122) (i) What do you mean by Piggybacking? Demonstrate with design figure of piggybacking in Go-Back-N ARQ. [4] (ii) Demonstrate different scenarios with the help of flow diagram for the cases of frame lost, acknowledgement lost, duplication of frame. [4]

123) Classify multiple access protocols. Analyze any one protocol in detail.

124) Draw and explain throughput Vs offered load for pure ALOHA, slotted ALOHA, 1-persistnet, non-persistent, 0.5 persistent methods for Carrier sense multiple access.

125) What is spanning tree arrangement and why it is required?

126) Compare CSMA-CD and CSMA-CA.

127) What do you mean by Hamming distance? How minimum Hamming distance is useful to detect capabilities of error detection and correction. Demonstrate with suitable example.

128) What is the difference between systematic and non-systematic code word. Derive code word using (7,4) CRC systematic and non-systematic method for the give data words, 1101, 1000, 0011, 1111.What do you mean by syndrome? What is the role of syndrome to identify error in the received code word? Explain the steps of CRC decoding.

129) What is the difference between static and dynamic routing algorithms? Demonstrate shortest path routing with figure for each stage of metric calculation.

130) Write a brief note on DHCP.

131) What is the problem in flooding and how it can be resolved?

132) Why distance vector routing is falls under dynamic algorithm. Demonstrate calculation of route considering some network and distance vector.

133) Where RARP and BOOTP techniques are used in the networking? Compare both.

134) What is the difference between connection oriented and connection less packet routing service? Explain with the help of subnet and routing table.

135) Illustrate HTTP and WWW in web.

136) Explain the structure of e-mail.

137) What are the different port numbers ? How they are differing to each other ? what is the role of each in transport layer?