Various guided media

Guided Media	Unguided Media
The signal energy propagates within the guided media.	The signal energy propagates through air.
Guided media is mainly suited for point-to-point communication.	Unguided media is mainly used for broadcasting purpose.
The signal propagates in guided media in the form of voltage or current	The signal propagates in unguided media in the form of electromagnetic waves.
Examples of guided media are - twisted pair cables - co-axial cable -optical fiber cable	Examples of unguided media are: - microwaves - infrared

Difference between guided and unguided media

Coaxial Cable	Twisted Pair	Fiber Optic
It uses electrical signal for transmission.	It uses electrical signal for transmission.	It uses optical signal over a glass fiber.
Less affect by EMI.	Affected by EMI.	Not affected by EMI.
Bandwidth is moderately high (350 MHz).	Bandwidth is low. (3 MHz)	Bandwidth is very high. (2 GHz)
Support moderately high data rates. (500 Mbps).	Support low data rates. (4 Mbps)	Data rates is very high. (2 Gbps)
Moderately costly.	Cheapest.	Costly.
Repeater spacing is 1-10 km	Repeater spacing 2-10 km.	Repeater spacing is 10-100 km.
It supports all radio frequencies.	Support all radio frequencies.	Frequency range is 902 MHz to 928 MHz.
Low attenuation.	High attenuation.	Very low attenuation.

Differentiate between broadcast, multicast and multiple unicast.

Feature	Multiple Unicast	Broadcast	Multicast
Transmission	Data is sent to multiple recipient	Data is sent to all recipients in a network	Data is sent to a group of recipients
Delivery	Guaranteed delivery	Not all devices may be interested in the data	Not all devices may be interested in the data
Network Traffic	Low	High	Moderate
Latency	Low	High	Moderate

Security	More secure	Less secure	Moderately secure
Destination	Multiple receiver	All receivers	Group of receivers
Examples	Email, file transfer	DHCP requests, ARP requests	Video streaming, online gaming

Out of various layers in TCP/IP model, name the layer used for: (i) Combination of bits into bytes and bytes into frames (ii) Hop to hop delivery (iii) Process to Process delivery (iv) End to end delivery (v) Segmentation and reassembly of data

(i) Data Link Layer
(ii) Network Layer
(iii) Transport Layer
(iv) Application Layer
(v) Transport Layer

How is repeater different from amplifier? How is hub related to repeater? Explain four network devices

Repeater	Amplifier
Repeater regenerates the signal, if the provided original signal is weak.	Amplifier increases the amplitude of the signal.
Repeater takes high input power and provides low output power.	Amplifier takes low input power and provides high output power.
Repeater is generally used in static(stationary) environment.	Amplifier is generally used in Mobile and Remote area network.
Repeater regenerates the signal so that the noise can be reduced or eliminated.	Amplifier increases the amplitude of the signal with the noise.
Repeater works on the physical layer of OSI model.	Generally Amplifier is used in wireless communication.

Hub is a multi-port repeater.

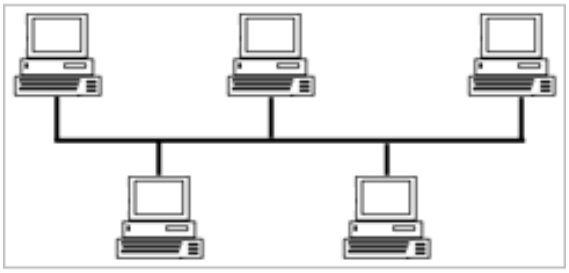
- **Hub** is a physical layer device that connects multiple devices on a network. It does not filter or forward data, but simply repeats any signal it receives on all of its ports. This means that all devices connected to a hub can see all the traffic on the network. Hubs are not very efficient, as they can cause collisions when multiple devices try to transmit data at the same time.

- **Repeater** is a physical layer device that amplifies and regenerates signals on a network. It does not filter or forward data, but simply makes the signals stronger so that they can travel further. Repeaters are used to extend the range of a network, or to connect two segments of a network that are using different media.
- **Bridge** is a data link layer device that connects two segments of a network that are using the same media. It filters and forwards data based on the MAC addresses of the devices on the network. Bridges can improve the performance of a network by isolating traffic between segments, and by preventing collisions.
- **Switch** is a data link layer device that connects multiple devices on a network. It filters and forwards data based on the MAC addresses of the devices on the network. Switches are more efficient than hubs, as they can forward data to the correct destination without broadcasting it to all devices on the network.

Name the four basic network topologies and cite an advantage of each type. Explain each topology with example.

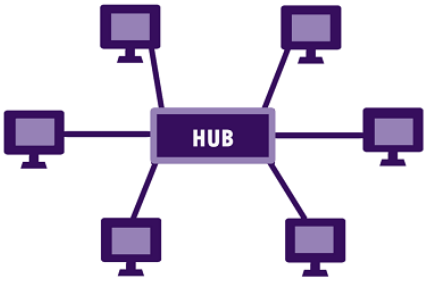
- **Bus topology:** A bus topology is a simple network topology in which all devices are connected to a single cable. For example, a bus topology could be used to connect a few computers in a small office.

  ✓ Advantage: Easy to set up and maintain.
  ✓ Disadvantage: Single point of failure.



- **Star topology:** A star topology is a network topology in which all devices are connected to a central hub or switch. For example, a star topology could be used to connect all of the computers in a corporate office.

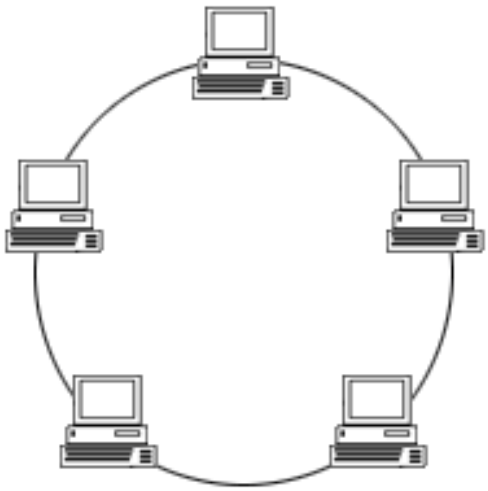
  ✓ Advantage: Easy to troubleshoot.
  ✓ Disadvantage: Centralized hub or switch is a single point of failure.



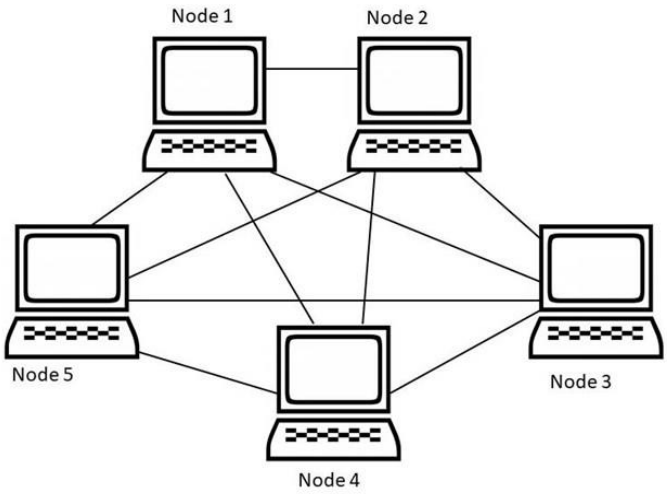
- **Ring topology:** A ring topology is a network topology in which all devices are connected in a loop. For example, a ring topology could be used to connect a few computers in a laboratory.

  ✓ Advantage: Fault-tolerant.

- ✓ Disadvantage: Difficult to troubleshoot.



- **Mesh topology:** A mesh topology is a network topology in which all devices are connected to each other. For example, a mesh topology could be used to connect all of the computers in a military base.
  - ✓ Advantage: Highly reliable.
  - ✓ Disadvantage: Expensive and difficult to manage.



Discuss the responsibilities of data link layer. Explain its design issues in detail.

Responsibilities of data link layer are:

- **Framing**
  Data-link layer takes packets from Network Layer and encapsulates them into frames. Then, it sends each frame bit-by-bit on the hardware. At receiver end, data link layer picks up signals from hardware and assembles them into frames.
- **Addressing**
  Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.
- **Synchronization**
  When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

- **Error Control**
  Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.
- **Flow Control**
  Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.
- **Multi-Access**
  When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism of accessing a shared media among multiple systems.

Design issues with data link layer are:

1. **Services provided to the network layer –**
   The data link layer act as a service interface to the network layer. The principle service is transferring data from network layer on sending machine to the network layer on destination machine. This transfer also takes place via DLL (Data link-layer).
2. **Frame synchronization –**
   The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine.
3. **Flow control –**
   Flow control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.
4. **Error control –**
   Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

Explain with the help of example why the window size is less than 2^m in Go back NARQ if frames are numbered from 0 to m-1.

- We choose m = 2, which means the size of the window can be 2^m - 1, or 3. We can now show why the size of the **send window must be less than 2^m**.

- If the size of the window is 3 (less than 2^2) and all three acknowledgments are lost, the frame 0 timer expires and all three frames are resent.

- The receiver is now expecting frame 3, not frame 0, so the duplicate frame is correctly discarded. On the other hand, if the size of the window is 4 (equal to 2^2) and all acknowledgments are lost, the sender will send a duplicate of frame O.

- However, this time the window of the receiver expects to receive frame 0, so it accepts frame 0, not as a duplicate, but as the first frame in the next cycle. **This is an error.**

Explain why the window size is less than or equal to 2^{m-1} in Selective Repeat ARQ if frames are numbered from 0 to m-1 with the help of example.

The window size is less than or equal to 2^{m-1} in Selective Repeat ARQ 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.

Give two reasons why networks might use an error correcting code instead of error detection and retransmission.

- **Reduced latency:** Error correcting codes can correct errors without the need to retransmit the data, which can reduce the latency of the communication. This is especially important in applications where latency is critical, such as real-time communication or streaming media.
- **Reduced bandwidth overhead:** Error detection and retransmission requires the sender to retransmit the data if an error is detected. This can increase the bandwidth overhead of the communication, especially if the error rate is high. Error correcting codes can reduce the bandwidth overhead by correcting errors without the need to retransmit the data.

Explain five key assumptions for formulating the dynamic channel allocation in LANs and MANs

1. **Independent traffic:** The traffic generated by each station is independent of the traffic generated by other stations. This means that the probability of a station generating a frame for transmission is not affected by the transmissions of other stations.
2. **Single channel:** All stations share a single channel for communication. This means that only one station can transmit at a time.
3. **Observable collision:** When two or more stations transmit at the same time, a collision occurs. All stations are able to detect collisions.
4. **Continuous or slotted time:** Time can be either continuous or slotted. In continuous time, frames can be transmitted at any time. In slotted time, frames can only be transmitted at the beginning of a slot.
5. **Carrier sensing:** Stations are able to sense if the channel is busy before transmitting. This means that stations will not transmit if the channel is already in use.

Give an argument why the leaky bucket algorithm should allow just one packet per tick, independent of how large the packet is.

- **The leaky bucket algorithm is a rate limiter.** If the leaky bucket algorithm allowed more than one packet per tick, then it would not be able to effectively limit the rate of the sender.
- **Allowing more than one packet per tick would favor large packets over small packets.** This is because a large packet would be able to occupy the bucket for a longer period of time, allowing it to transmit more data before being blocked. This would give large packets an unfair advantage over small packets.

- **Allowing more than one packet per tick would make the algorithm more complex.** The algorithm would need to keep track of the size of each packet in order to ensure that only one packet was transmitted per tick. This would add unnecessary complexity to the algorithm.

What is the need of layered structure in OSIRM?

- **Modularity:** Each layer can be developed and maintained independently of the other layers. This makes it easier to add new features or fix bugs without affecting the rest of the system.
- **Abstraction:** The layers provide a layer of abstraction between the user and the underlying hardware. This makes it easier for users to interact with the system without having to worry about the details of how it works.
- **Scalability:** The layered structure makes it easy to scale the system by adding new layers or by increasing the capacity of the existing layers.
- **Security:** The layered structure can be used to improve the security of the system by isolating different components from each other.

Explain Back Off procedure.

The backoff procedure works as follows:

1. When a device wants to transmit data, it first listens to the network to see if it is clear. If the network is clear, the device can transmit its data.
2. If the network is not clear, the device waits for a random amount of time before trying again. The amount of time that the device waits is exponentially increasing, meaning that it will wait for a longer time each time it fails to transmit its data.
3. The device continues to wait for a random amount of time and retry transmitting its data until it is successful.

Advantages: simple to implement, effective in reducing collisions, fair to all devices on the network.

Disadvantages: increase the latency of the network, inefficient if there are a lot of collisions, vulnerable to denial-of-service attacks.

Define the terms latency and throughput.

- **Latency** is the time it takes for a packet to travel from one point to another in a network. It is measured in milliseconds (ms).
- **Throughput** is the amount of data that can be transferred in a given amount of time. It is measured in bits per second (bps) or bytes per second (Bps).

What are the drawbacks of stop and Wait ARQ?

- The data can be lost in between the transmission. So, in such a case, the sender waits for ACK and the receiver waits for the data frame for an infinite amount of time.
- The ACK from the receiver may get lost in the channel. So, the sender waits for ACK for an infinite amount of time.

- The window size of the sender and the receiver is only 1. So, only one frame can be sent at a time.
- As there is a timer concept, so the sender must wait for a long duration before retransmission. Hence, the stop and wait ARQ is a slow protocol.

Explain the design issues of Network layer.

Store and Forward Packet Switching

The node which has a packet to send, delivers it to the nearest router. The packet is stored in the router until it has fully arrived and its checksum is verified for error detection. Once, this is done, the packet is forwarded to the next router. Since, each router needs to store the entire packet before it can forward it to the next hop, the mechanism is called store − and − forward switching.

Services to Transport Layer

Network layer provides the services to the transport layer at the network layer/transport layer interface.

The network layer must fulfil following requirements.

1. The service should be independent of network topology.

2. The network addresses should be made available to the transport with a uniform numbering plan.

3. The transport layer should be shielded from the number, type and topology of the routers present.

Providing Connection Oriented Service

In connection − oriented services, a path or route called a **virtual circuit** is setup between the source and the destination nodes before the transmission starts. All the packets in the message are sent along this route. Each packet contains an identifier that denotes the virtual circuit to which it belongs to. When all the packets are transmitted, the virtual circuit is terminated and the connection is released. An example of connection − oriented service is MultiProtocol Label Switching (MPLS).

Providing Connectionless Service

In connectionless service, since each packet is transmitted independently, each packet contains its routing information and is termed as datagram. The network using datagrams for transmission is called datagram networks or datagram subnets. No prior setup of routes is needed before transmitting a message. Each datagram belong to the message follows its own individual route from the source to the destination. An example of connectionless service is Internet Protocol or IP.

Define Slotted Aloha.

In slotted Aloha, the shared channel is split into fixed time intervals called **slots**. As a result, if a station wants to send a frame to a shared channel, it can only do so at the start of the slot, and only one frame can be sent to each slot. Additionally, the station must wait until the beginning of the slot for the subsequent transmission if it is unable to transfer data at the beginning of the slot.

Differentiate between FDMA and FDM.

FDMA stands for **Frequency Division Multiple Access.** It is a channel access method that divides the available frequency spectrum into multiple channels, and each user is assigned a single channel. This allows multiple users to share the same physical medium, such as a cable or a radio frequency band, without interfering with each other.

FDM stands for **Frequency Division Multiplexing.** It is a multiplexing technique that combines multiple signals into a single signal by assigning each signal to a different frequency band. This allows multiple signals to be transmitted over the same physical medium without interfering with each other.

What are the advantages of Computer Network?

- **Resource sharing:** Computer networks allow users to share resources, such as printers, scanners, and software. This can save businesses money and improve productivity.
- **Communication:** Computer networks allow users to communicate with each other, regardless of their physical location. This can improve collaboration and productivity.
- **Information sharing:** Computer networks allow users to share information, such as files, documents, and databases. This can improve access to information and decision-making.
- **Remote access:** Computer networks allow users to access files, applications, and other resources remotely. This can improve flexibility and productivity.
- **Scalability:** Computer networks can be scaled to meet the needs of businesses of all sizes. This makes them a cost-effective solution for businesses that are growing.
- **Reliability:** Computer networks can be made highly reliable by using redundant components and fault-tolerant systems. This can help to ensure that businesses can continue to operate even if there is a failure in the network.

Explain the structure of OSIRM and compare it with TCP/IP model

OSI Layers

Layer	Description	Device	Protocol
Application	Provides network access for applications, flow control and error recovery	Gateway	SMTP
Presentation	Performs protocols conversion, encryption and data compression	Gateway and redirectors	TDI
Session	Allows two applications to communicate over a network by opening a session and synchronizing the involved computers.	Gateway	RPC
Transport	Repackages messages into smaller formats, provides error free delivers and error handling functions	Gateway	TCP
Network	Handles addressing, translates logical addresses and names to physical addresses, routing and traffic management.	Router and Brouter	IP
Data Link	Packages raw bits into frames and includes a cyclical redundancy check (CRC)	Switch, Bridge	LIC
Physical	Transmits data over physical medium	Multiplexer and Repeater	ISDN

TCP/IP Layers

Layer	Description	Protocol
Application	It is responsible for node-to-node communication and controls user-interface specifications.	SMTP
Transport	The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.	TCP
Internet	It sends packets from the source to destination, regardless of their route.	IP
Host to network	It specifies how much data should be sent, when, and where at what rate. This layer ensures that data units are supplied in a timely and error-free manner.	--------

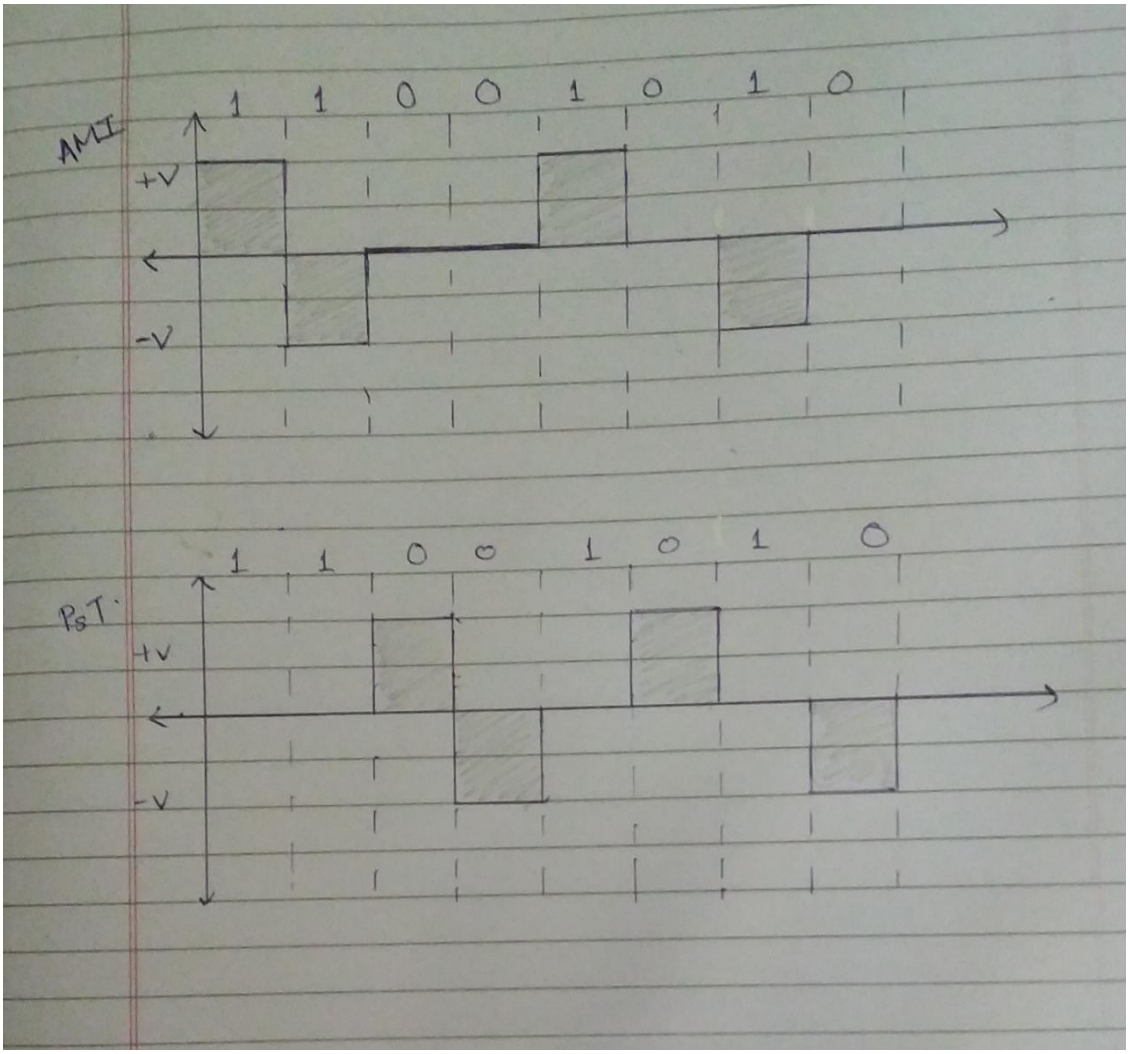
OSI Model	TCP/IP Model
OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
It has 7 layers.	It has 4 layers.
It is low in usage.	It is mostly used.
It is vertically approached.	It is horizontally approached.
Delivery of the package is guaranteed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

What are the benefits of using OPTICAL FIBRES?

- **High bandwidth:** Optical fibers can carry much more data than copper cables. This is because they use light to transmit data, which is a much higher frequency than electricity.
- **Longer distances:** Optical fibers can transmit data over much longer distances than copper cables. This is because they are not as susceptible to attenuation, which is the loss of signal strength over distance.
- **Immunity to interference:** Optical fibers are immune to electromagnetic interference (EMI). This means that they are not affected by noise from other electronic devices.
- **Lightweight and flexible:** Optical fibers are much lighter and more flexible than copper cables. This makes them easier to install and to work with.
- **Security:** Optical fibers are more secure than copper cables. This is because they are difficult to tap into, and the data that is transmitted is encrypted.

Explain the concept of Pseudo ternary and AMI technique used for digital data transmission. Explain by considering 11001010 as the data bits.

- **Alternate Mark Inversion (AMI) –** A neutral zero voltage represents binary 0. Binary 1's is represented by alternating positive and negative voltages.
- **Pseudoternary –** Bit 1 is encoded as a zero voltage and the bit 0 is encoded as alternating positive and negative voltages i.e., opposite of AMI scheme.

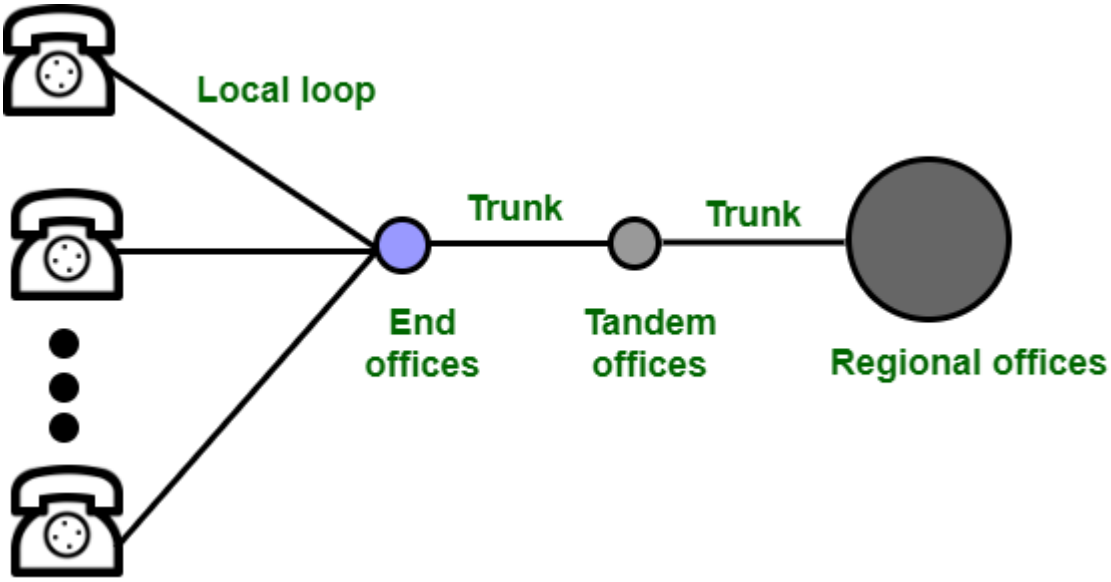


Write a short note on Telephone Systems

Telephone Network is used to provide voice communication. Telephone Network uses Circuit Switching.

Structure: There are three major components of the telephone network:

1. Local loops
2. Trunks
3. Switching Offices



Local Loops: Local Loops are the twisted pair cables that are used to connect a subscriber telephone to the nearest end office or local central office.

Trunks: It is a type of transmission medium used to handle the communication between offices. Through multiplexing, trunks can handle hundreds or thousands of connections. Mainly transmission is performed through optical fibers or satellite links.

Multiplexing: It is a method of combining more than one signal over a shared medium. The commonly used multiplexing techniques in trunks are time division multiplexing (TDM) and frequency division multiplexing (FDM). In TDM, the users are allowed the total available bandwidth on time sharing basis. In FDM, signals of different frequencies are combined for concurrent transmission.

Switching: As there is a permanent physical link between any two subscribers. To avoid this, the telephone company uses switches that are located in switching offices. A switch is able to connect various loops or trunks and allows a connection between different subscribes.

Explain the concept of Selective Repeat ARQ. Why the size of window is 2^{n-1}?

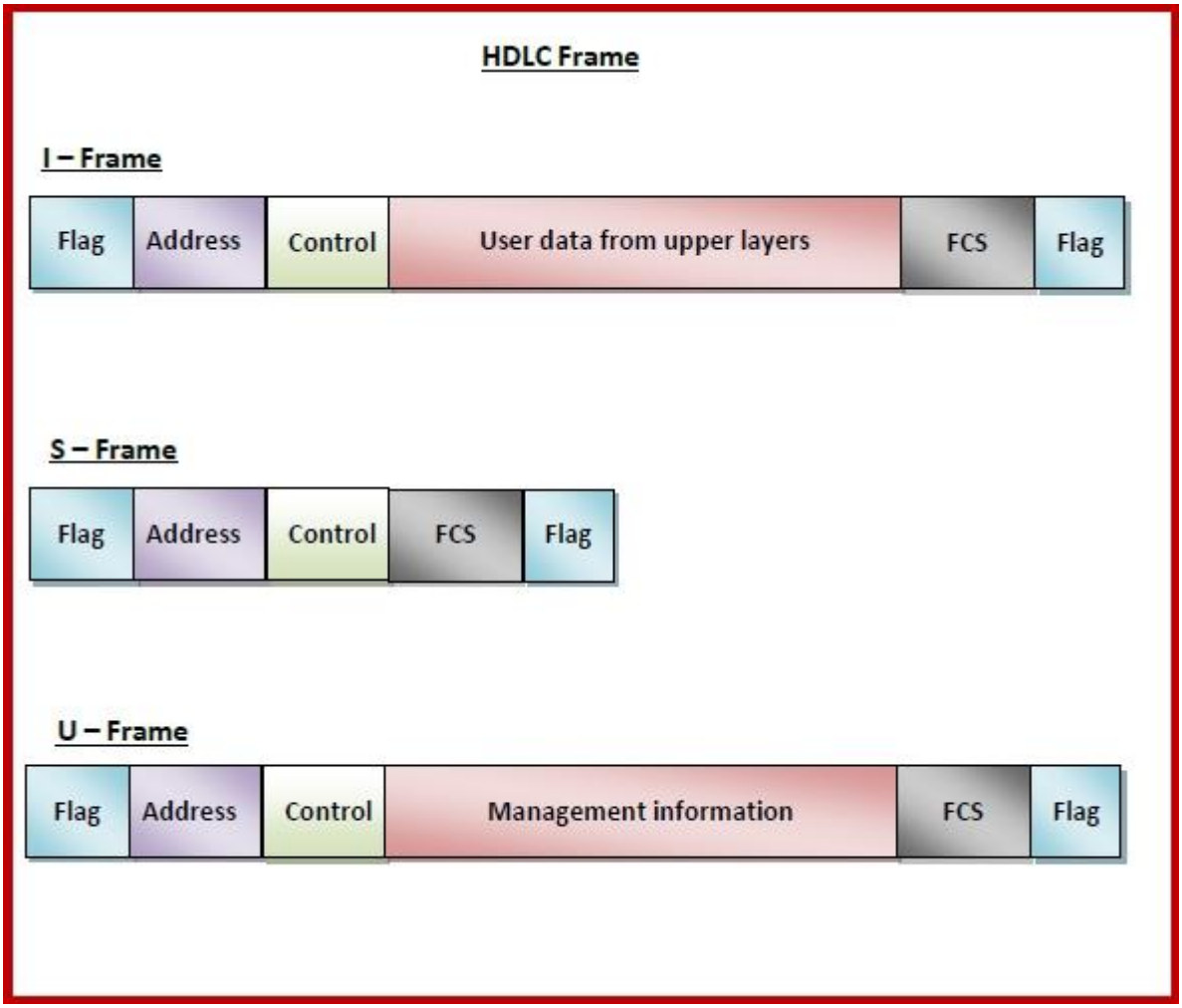
In the selective repeat ARQ, we only resend the data frames that are damaged or lost. If any frame is lost or damaged then the receiver sends a negative acknowledgment (NACK) to the sender and if the frame is correctly received, it sends back an acknowledgment (ACK). As we only resend the selected damaged frames so we name this technique the **Selective Repeat ARQ** technique. The ACK and the NACK have the sequence number of the frame that helps the sender to identify the lost frame.

The window size is less than or equal to 2^{n-1} in Selective Repeat ARQ 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.

Explain the frame formats of I, S and U frames of HDLC protocol

There are three types of HDLC frames −

- **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.



What do you mean by channel allocation problem?

Channel allocation problem is a problem in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. The goal is to maximize the number of users while minimizing interference between them.

Channel allocation problem can be solved by two schemes: Static Channel Allocation and Dynamic Channel Allocation.

Static Channel Allocation

In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user. For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.

This scheme is also referred as fixed channel allocation or fixed channel assignment.

In this allocation scheme, there is no interference between the users since each user is assigned a fixed channel. However, it is not suitable in case of a large number of users with variable bandwidth requirements.

Dynamic Channel Allocation

In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized.

This allocation scheme optimises bandwidth usage and results is faster transmissions.

Explain the technique used in Channelization (in Multiple Access Methods).

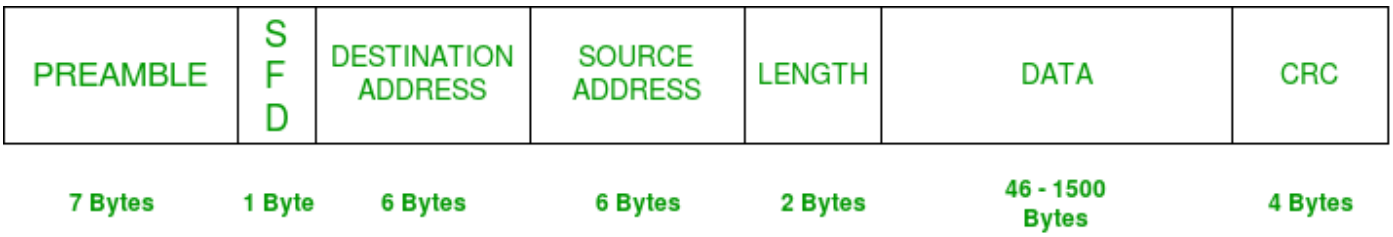
Channelization:
In this, the available bandwidth of the link is shared in time, frequency and code among multiple stations to access channel simultaneously.

- **Frequency Division Multiple Access (FDMA) –** The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.
- **Time Division Multiple Access (TDMA) –** In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However, there is an overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.
- **Code Division Multiple Access (CDMA) –** One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly, data from different stations can be transmitted simultaneously in different code languages.
- **Orthogonal Frequency Division Multiple Access (OFDMA) –** In OFDMA the available bandwidth is divided into small subcarriers in order to increase the overall performance. Now the data is transmitted through these small subcarriers. It is widely used in the 5G technology.

Explain the frame format of IEEE 802.3 MAC sublayer

- **Preamble**: It is the starting field that provides alert and timing pulse for transmission. In case of classic Ethernet it is an 8 byte field and in case of IEEE 802.3 it is of 7 bytes.
- **Start of Frame Delimiter**: It is a 1 byte field in a IEEE 802.3 frame that contains an alternating pattern of ones and zeros ending with two ones.
- **Destination Address**: It is a 6 byte field containing physical address of destination stations.
- **Source Address**: It is a 6 byte field containing the physical address of the sending station.
- **Length**: It a 7 bytes field that stores the number of bytes in the data field.

- **Data**: This is a variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- **Padding**: This is added to the data to bring its length to the minimum requirement of 46 bytes.
- **CRC**: CRC stands for cyclic redundancy check. It contains the error detection information.



IEEE 802.3 ETHERNET Frame Format

Write short notes on the following:

(a) Distance Vector Routing

Distance Vector Routing Algorithm –

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
   - It receives a distance vector from a neighbor containing different information than before.
   - It discovers that a link to a neighbor has gone down.

(b) Forwarding Techniques

Forwarding means to place the packet in its route to its destination.

a. Next-Hop Method

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

b. Network-Specific Method

Here, instead of having an entry for every destination host connected to the same physical network (host-specific method), we have only one entry that defines the address of the destination network itself.

c. Default Method

Host A is connected to a network with two routers. Router R1 routes the packets to hosts connected to network N2. However, for the rest of the Internet, router R2 is used. So instead of listing all networks in the entire Internet, host A can just have one entry called the default

(c) How to create a routing table?

Routing table consists of the following entries:

1. **Network ID:**
   The network ID or destination corresponding to the route.
2. **Subnet Mask:**
   The mask that is used to match a destination IP address to the network ID.
3. **Next Hop:**
   The IP address to which the packet is forwarded
4. **Outgoing Interface:**
   Outgoing interface the packet should go out to reach the destination network.
5. **Metric:**
   A common use of the metric is to indicate the *minimum number of hops* (routers crossed) to the network ID.

Give difference between following:

(a) Classification of classes in Binary notation and Dotted Decimal notation

Feature	Binary Notation	Dotted Decimal Notation
Representation	32 bits in binary form	Four decimal numbers separated by periods
Readability	More suitable for computer-based calculations	Easier for humans to read and remember
Usage	Used in network programming, subnetting, and other technical operations	Used for general IP address representation
Efficiency	More efficient	Less efficient
Human-Readability	Less human-readable	More human-readable

(b) Functions of transport layer and data link layer

Function	Function of Transport Layer	Function of Data Link Layer
End-to-end delivery	Provides reliable data delivery between two hosts.	Provides reliable data transfer between two nodes on the same network.

Flow control	Controls the flow of data between the two hosts.	Controls the flow of data between the two nodes.
Error detection and correction	Detects and corrects errors in the data.	Detects errors in the data, but does not correct them.
Segmentation and reassembly	Breaks the data into smaller units called segments, and then reassembles the segments at the receiver.	Breaks the data into smaller units called frames, and then reassembles the frames at the receiver.
Addressing	Provides a way to uniquely identify the two hosts that are communicating.	Provides a way to uniquely identify the two nodes that are communicating.

(c)Overlay networks and frame relay networks.

Feature	Overlay Network	Frame Relay Network
Purpose	Create a virtual network on top of an existing physical network	Provide a reliable and efficient way to transmit data between two points
Architecture	Software-based	Hardware-based
Performance	Can provide better performance for applications that require low latency or high bandwidth	Typically provides lower performance than overlay networks
Security	Can provide better security by creating isolated virtual networks	Typically provides lower security than overlay networks
Cost	Can be more expensive than frame relay networks	Typically less expensive than overlay networks

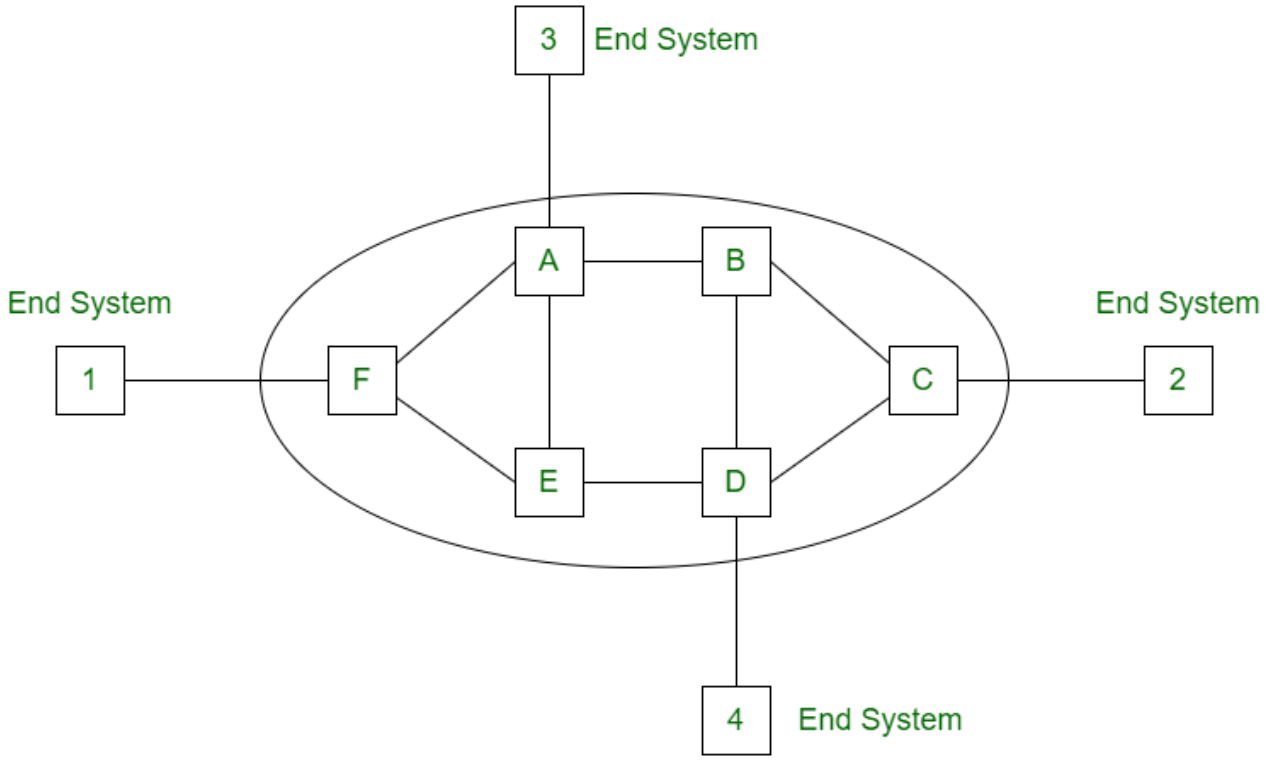
d)Star and Mesh Topologies

Feature	Star Topology	Mesh Topology
Connection	Devices are connected to a central hub or switch.	Devices are connected to each other.
Fault tolerance	Fault tolerant, as the failure of one device will not affect the rest of the network.	More fault tolerant than star topology, as there are multiple paths for data to travel between any two devices.
Scalability	Easy to scale, as new devices can be added by connecting them to the hub or switch.	More difficult to scale, as new connections must be made between all devices in the network.
Cost	More expensive, as each device must be connected to the hub or switch.	Less expensive, as devices do not need to be connected to a central hub or switch.

Compare coaxial cable, FOX, microwave and Infra-'Red with respect to frequency range and application.

Medium	Frequency Range	Application
Coaxial cable	50 MHz to 1 GHz	Cable television, computer networking, and high-definition television
FOX	2 GHz to 10 GHz	Microwave ovens, satellite television, and point-to-point communications
Microwave	300 MHz to 300 GHz	Cellular networks, radar, and satellite communications
Infrared	300 GHz to 400 THz	Remote controls, night vision, and medical imaging

Draw labelled diagram of virtual circuit network and describe working.



Working of Virtual Circuit:

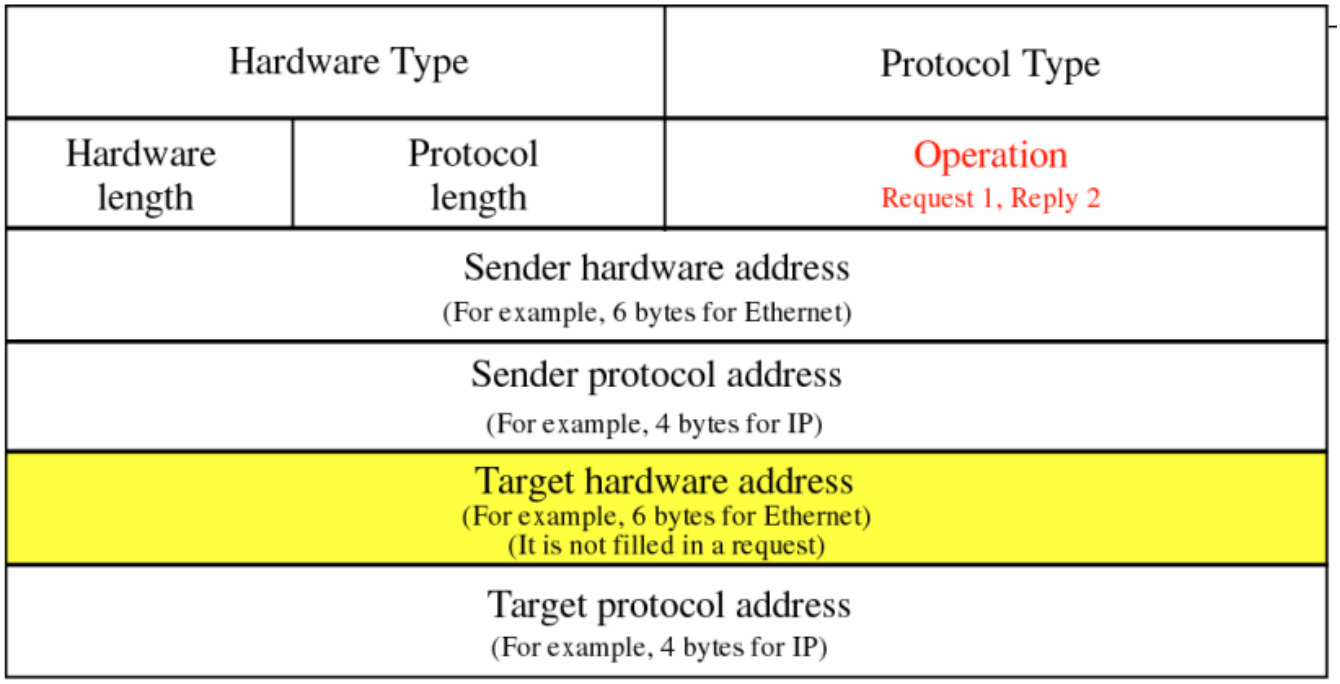
- In the first step a medium is set up between the two end nodes.
- Resources are reserved for the transmission of packets.
- Then a signal is sent to sender to tell the medium is set up and transmission can be started.
- It ensures the transmission of all packets.
- A global header is used in the first packet of the connection.
- Whenever data is to be transmitted a new connection is set up.

Differentiate between repeater, amplifier, bridge, router, hub, switch and gateway. Clearly identify the position of each of the element in OSI layer protocol.

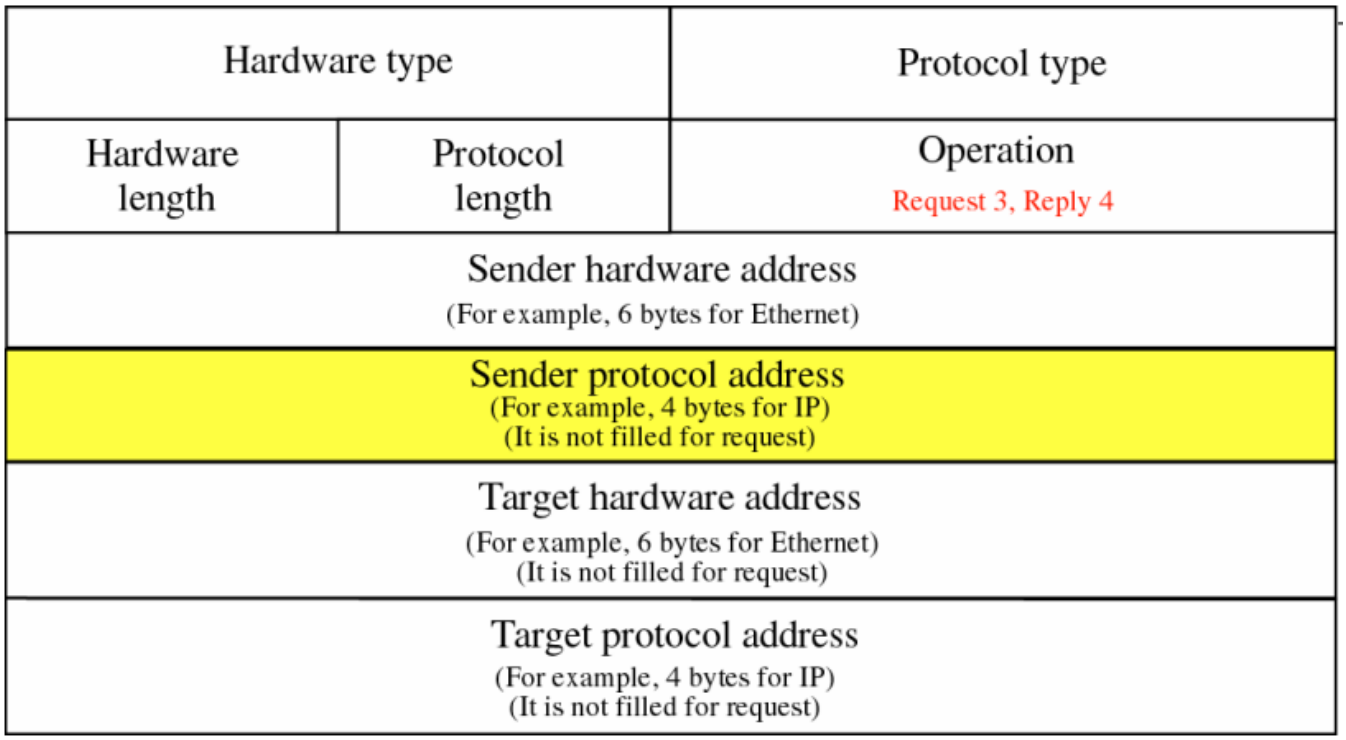
Device	Description	OSI Layer
Repeater	A device that amplifies and regenerates signals, extending the range of a network.	Physical layer
Amplifier	A device that increases the power of a signal, improving its quality.	Physical layer

Bridge	A device that connects two networks that use the same protocol.	Data link layer
Router	A device that connects two networks that use different protocols.	Network layer
Hub	A device that connects multiple devices on the same network.	Physical layer
Switch	A device that connects multiple devices on the same network, filtering and forwarding traffic based on MAC addresses.	Data link layer
Gateway	A device that connects two networks that use different protocols and technologies.	Application layer

Draw ARP and RARP header and explain its working with example. Is the size of the ARP packet is fixed? Explain.



ARP Header



RARP Header

Working of ARP with example:

1. Host A wants to send a packet to Host B.
2. Host A does not know the MAC address of Host B, so it sends an ARP request packet to the local network.
3. The ARP request packet contains Host A's IP address and hardware address.
4. Host B receives the ARP request packet and responds with an ARP reply packet.
5. The ARP reply packet contains Host B's IP address and hardware address.
6. Host A now knows the MAC address of Host B, so it can send the packet to Host B.

Working of RARP with example

- A device boots up and does not know its own IP address.
- The device broadcasts a RARP request packet containing its MAC address.
- A RARP server that is listening on the network receives the request packet.
- The RARP server looks up the MAC address in its database and finds the corresponding IP address.
- The RARP server sends a RARP reply packet containing the IP address to the device.
- The device now knows its own IP address.

The size of an ARP packet is fixed at 28 bytes.

- The ARP header is a standard format that is used by all devices on an Ethernet network.

- The size of the fields in the ARP header is fixed, so the size of the ARP packet is also fixed.
- This allows for efficient communication between devices on an Ethernet network and ensures that all devices are using the same format for ARP packets.

Differentiate between Connection less and connection oriented operations

Connection-oriented Service	Connection-less Service
It is related to the telephone system.	It is related to the postal system.
It is necessary. Feasible.	It is not necessary. Not feasible.
Congestion is absent	Congestion is present
Reliable Packets follow the same route.	Not reliable Packets do not follow the same route.
High bandwidth needed	Low bandwidth needed
Ex: TCP (Transmission Control Protocol)	Ex: UDP (User Datagram Protocol)

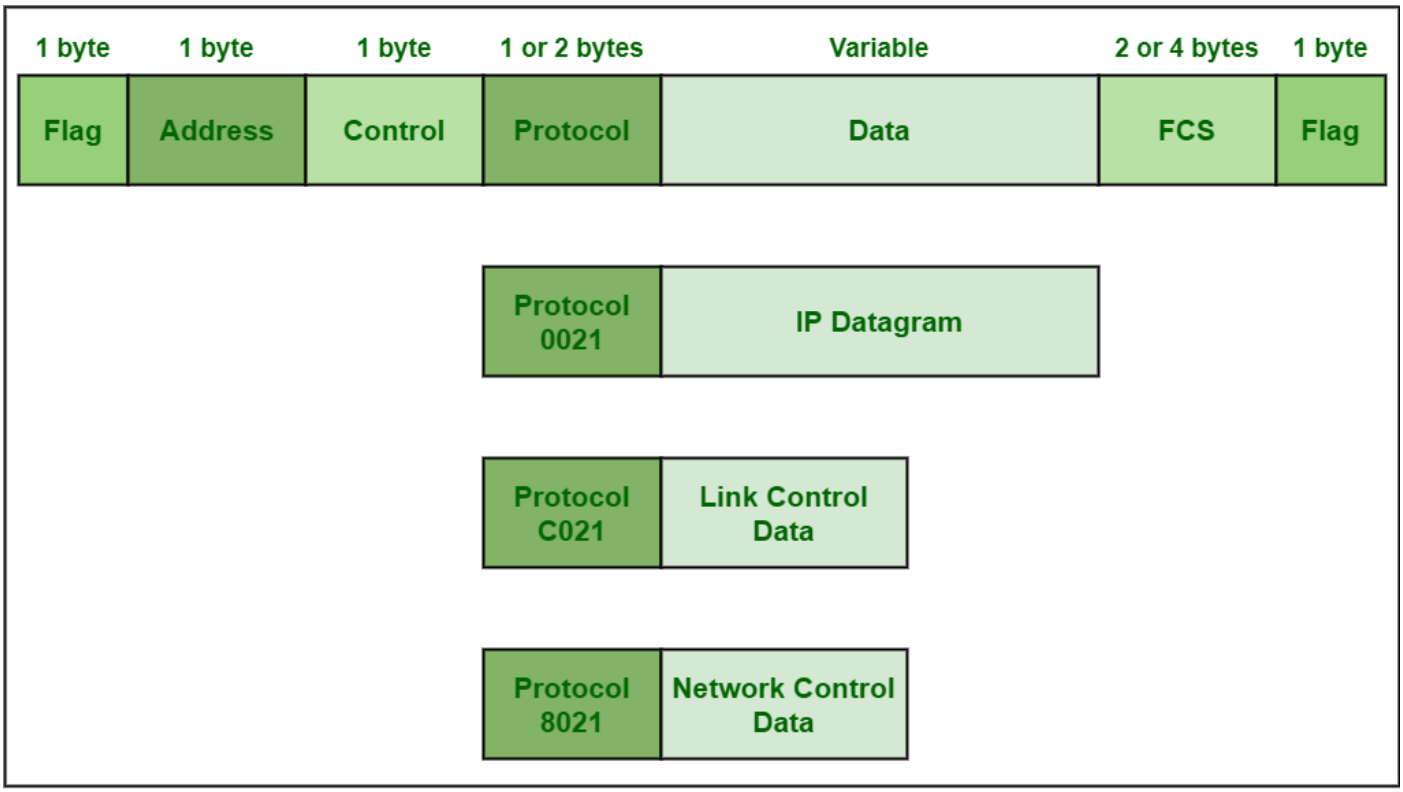
Differentiate between Link-State routing and Distance-Vector routing.

Distance Vector Routing	Link State Routing
Less Bandwidth needed	More Bandwidth needed
Based on local knowledge Uses Bellman Ford Algorithm.	Based on global knowledge Uses Dijkstra algorithm.
Traffic is less. Converges slowly Count of infinity problem.	Traffic is more. Converges fastly. No count of infinity problem.

Persistent looping problem	No persistent loops, only transient loops.
Practical implementation is RIP	Practical implementation is ISIS.

Explain following in brief and discuss their frame format and control field

(a) PPP



PPP Frame Format

1. **Flag field –** It always begins and ends with standard HDLC flag
2. **Address field –** Address field is basically broadcast address.
3. **Control field –** This field basically uses format of U-frame
4. **Protocol field –** This field basically identifies network protocol of the datagram
5. **Data field –** It usually contains the upper layer datagram
6. **FCS field –** This field usually contains checksum simply for identification of errors

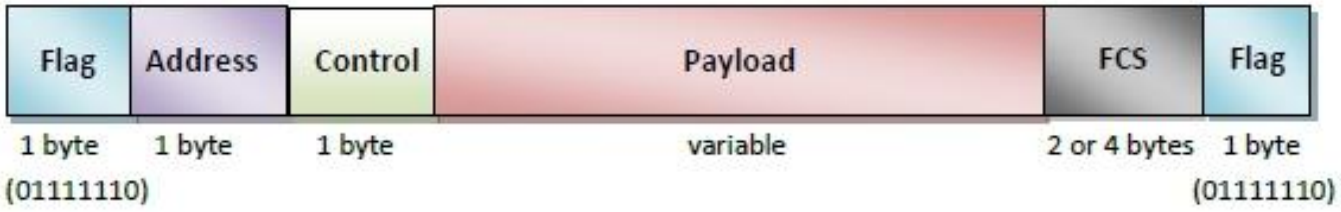
(b) HDLC

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)

HDLC Frame



Why sub-netting and super-netting is needed while designing the network and assigning the internet addresses?

Need of Subnetting

1. It helps in organizing the network in an efficient way
2. It reduces traffic and maintain order and efficiency.
3. It helps in improving network performance.
4. It is used in increasing network security.

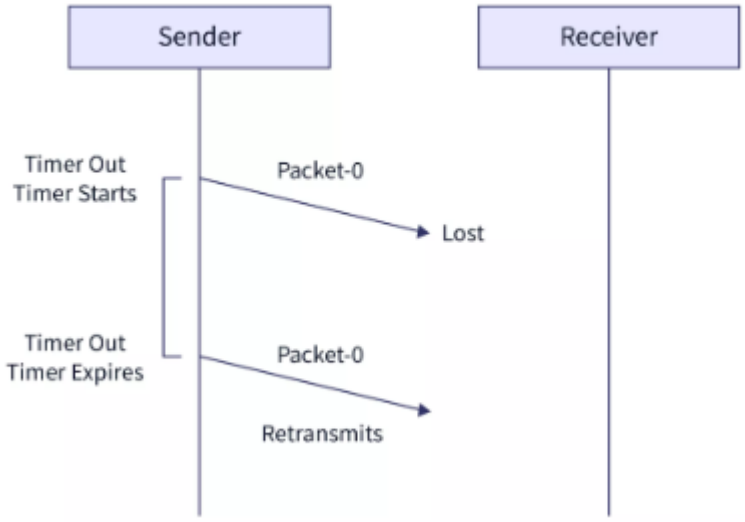
Need of Supernetting

1. It controls and reduces network traffic
2. It helps to solve the problem of lacking IP addresses
3. It minimizes the routing table

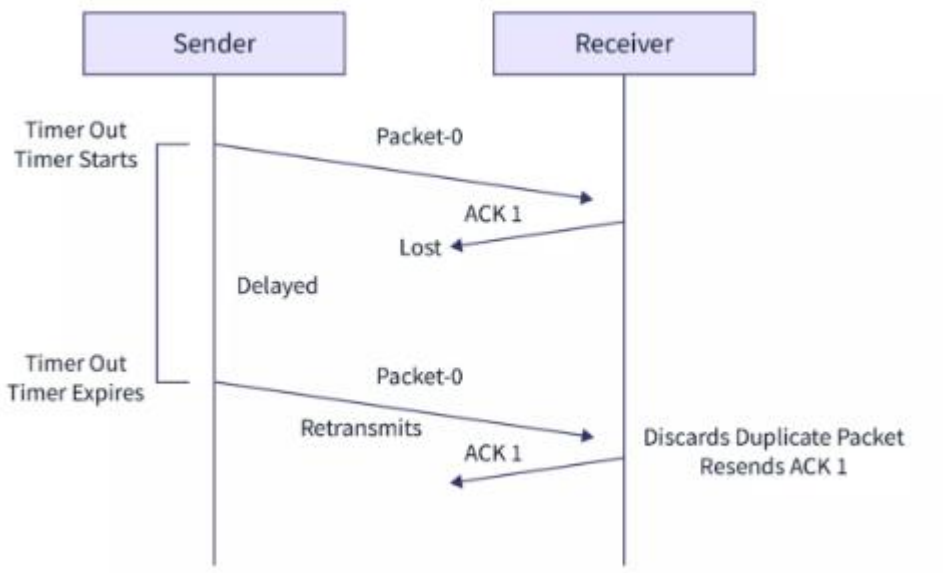
Discuss the principle of Stop and Wait flow control algorithm. Draw time line diagram and explain how the loss of data frame and loss of acknowledge frame is handled. Also discuss the effect of delay bandwidth product on link utilization.

Principle of Stop and Wait Flow Control Algorithm: Initially, the sender sends one frame as the window size is 1. The receiver on the other end receives the frame and sends the ACK for the correctly received frame. The sender waits for the ACK until the timer expires. If the sender does not receive the ACK within the timer limit, it re-transmits the frame for which the ACK has not been received.

Problem of Lost Data Packet When the sender sends the data packet and the receiver does not receive the data packet, it means that the data is lost in between the transmission. So, to overcome this type of problem, the sender uses a timer. When the sender sends the data packet, it starts a timer. If the timer goes off before receiving the acknowledgment from the receiver, the sender retransmits the same data packet.



Problem of Lost Acknowledgement When the sender sends the data packet and the receiver receives the data packet but the acknowledgment from the receiver is not received. It means that the acknowledgment is lost in between the transmission. So, to overcome this type of problem, the sender uses sequence numbering. When the sender sends the data packet, it attaches a certain sequence number which helps the receiver identify the data packet. If the timer goes off before receiving the acknowledgment from the receiver, the sender retransmits the same data packet. But in this case, the receiver already has the data packet, so it discards the data and sends it back an acknowledgment. This tells the sender that the certain data packet is now received correctly.



Bandwidth delay product is calculated as the product of the link capacity of the channel and the round – trip delay time of transmission. The unit of bandwidth delay product is bits or bytes.

If the BDP is smaller than the window size of the transport protocol, then the link will be underutilized. On the other hand, if the BDP is larger than the window size of the transport protocol, then the link will be overutilized.

What is CSMA/CD? How does it work? Distinguish between 1- persistent and non-persistent CSMA.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer.

The algorithm of CSMA/CD is:

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits until the channel becomes idle.
- If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
- If a collision is detected, the station starts the collision resolution algorithm.
- The station resets the retransmission counters and completes frame transmission.

Basis	1-persistent CSMA	Non-persistent CSMA
Carrier Sense	When channel is idle it will send with probability 1.	When channel is idle it will send frame.
Waiting	It will continuously sense channel for transmission of frames.	It will wait for random amount of time to check carrier.
Chance of Collision	In this method, there are highest number of collisions observed.	In this method, chance of collision are less than in 1-persistent.
Utilization	It's utilization is above ALOHA because frames are sent only when channel is found in idle state.	It's utilization is above 1-persistent because in this all stations constantly check for channel at same time.
Delay Low Load	It is small because frames are sent only in idle state.	It is longer than 1-persistent as it only checks randomly when channel is busy.
Delay High Load	It is high due to collision.	It is longer than 1-persistent because stations check randomly when channel is busy.

Briefly explain the different types of packet switching techniques with suitable networks. Write each of its advantages and disadvantages.

There are two approaches to Packet Switching:

Datagram Packet switching:

- It is a packet switching technology in which packet (datagram), is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.

- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Advantages of Datagram Switching:
Highly scalable, Flexible, Simple routing, Lower latency

Disadvantages of Datagram Switching:
High error rates, Increased network congestion

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Advantages of Virtual Circuit Switching:

Guaranteed delivery, Lower error rates, Efficient use of bandwidth

Disadvantages of Virtual Circuit Switching:

Limited scalability, Increased setup time, Fixed data rates

What is the significance of twisting in twisted pair cable?

- **Reduces EMI:** It helps to reduce EMI by cancelling out the EMI that is induced in each wire.
- **Improves signal quality:** The twisting also helps to improve signal quality by reducing crosstalk.
- **Increases bandwidth:** The twisting also helps to increase bandwidth by reducing attenuation.

What field in the IP datagram header is used to avoid forwarding datagram's endlessly through routing loop? How is that header used to accomplish that?

Time to Live(TTL) field in the IP datagram header is used to avoid forwarding datagrams endlessly through routing loops.

- The TTL field is an 8-bit unsigned integer that specifies the number of hops that a datagram can make before it is discarded.
- When a datagram is forwarded by a router, the router decrements the TTL field by one.
- If the TTL field reaches zero, the router discards the datagram.
- This prevents datagrams from being forwarded endlessly through routing loops.

What is subnet masking? Discuss.

Subnet masking is a technique used to divide a network into smaller networks, or subnets. This is done by using a subnet mask, which is a 32-bit number that tells routers how to interpret an IP address.

For example, an IP address of 192.168.1.100 has a subnet mask of 255.255.255.0

What is the difference between packet switching and circuit switching?

Circuit Switching	Packet Switching
A circuit needs to be established for data transmission	Each packet goes through the dynamic route.
A uniform path is followed throughout the session.	No uniform path is followed throughout the session.
It is ideal for voice communication	It is ideal for data transmission
Connection is necessary	Connection is not necessary
Data to be transmitted is processed at the source itself.	Data is processed at source and at each switching station.

What is early token release?

Early Token Release:

- Token is released as soon as the data is transmitted.
- Multiple packets are present in the ring.
- Less reliable than Delayed Token Release.
- Collision is possible as multiple packets are present in the ring.

How is the minimum size of the Ethernet frame determined? How is it related to slot time?

- The minimum size of the Ethernet frame is 64 bytes.
- This is because the CSMA/CD protocol requires that a frame be at least 64 bytes long in order to ensure that the sender of the frame has enough time to detect a collision if one occurs.
- The slot time is the amount of time it takes for a frame to propagate across the network.
- The minimum size of the Ethernet frame is related to the slot time because the sender of a frame must wait for at least the slot time before transmitting another frame.
- This is to ensure that any collisions that occur will have enough time to propagate back to the sender.

Compare the data rates for Standard Ethernet, Fast Ethernet, Gigabit Ethernet, and Ten-Gigabit Ethernet.

Ethernet Type	Data Rate
Standard Ethernet	10 Mbps
Fast Ethernet	100 Mbps

Gigabit Ethernet	1 Gbps
Ten-Gigabit Ethernet	10 Gbps

Define slow start.

1. A sender begins transmissions to a receiver by slowly probing the network with a packet that contains its initial congestion window (cwnd).
2. The client receives the packet and replies with its maximum buffer size, also known as the receiver's advertised window (rwnd).
3. If the sender receives an acknowledgement from the client, it then doubles the amount of packets to send to the client.
4. Step 3 is repeated until the sender no longer receives acknowledgment from the receiver which means either congestion is detected, or the client's window limit has been reached.

Explain the three types of transmission impairment?

- **Attenuation:** Attenuation is the loss of signal strength as it travels through a medium. It is caused by a variety of factors, such as the length of the medium and the type of medium.
- **Delay:** Delay is the time it takes for a signal to travel from one point to another. It is caused by the speed of the medium and the distance the signal has to travel.
- **Distortion:** Distortion is the change in the shape of a signal as it travels through a medium. It is caused by a variety of factors, such as the frequency of the signal and the type of medium.

Explain any two methods used for data transmission using unguided media.

- **Radio:** Radio waves are a form of electromagnetic waves that can be used to transmit data over long distances. Radio waves are commonly used for radio broadcasting, television broadcasting, and cellular networks.
- **Microwave:** Microwaves are a form of electromagnetic waves that can be used to transmit data over short distances. Microwaves are commonly used for point-to-point communication, such as between two buildings or between a satellite and a ground station.

Explain the addressing mechanism of IEEE 802.11 standard.

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Explain in detail the problems associated with IEEE 802.11 standard.

- **Security:** The IEEE 802.11 standard does not provide strong security. This makes it vulnerable to a variety of attacks, such as eavesdropping, man-in-the-middle attacks, and denial-of-service attacks.
- **Interference:** The IEEE 802.11 standard uses the 2.4 GHz and 5 GHz frequency bands. These bands are also used by other devices, such as microwaves and cordless phones. This can cause interference.
- **Range:** The range of a wireless network is limited by the power of the transmitter and the environment.
- **Performance:** The performance is affected by: the number of users on the network, the distance between the devices, and the amount of interference.
- **Complexity:** The IEEE 802.11 standard is complex, which can make it difficult to configure and troubleshoot.

Compare and Contrast CSMA/CD with CSMA/CA.

CSMA/CD	CSMA/CA
CSMA / CD is effective after a collision.	CSMA / CA is effective before a collision.
CSMA / CD is used in wired networks.	CSMA / CA is used in wireless networks.
It only reduces the recovery time.	It minimizes the possibility of collision.
CSMA / CD is used in 802.3 standard.	While CSMA / CA is used in 802.11 standard.
It is more efficient than simple CSMA	It is similar to simple CSMA
It detects the collision on a shared channel.	It avoids collision on a shared channel.

Explain the loop problem associated with bridges.

Transparent bridges work fine as long as there are no redundant bridges in the system. If a bridge fails, another bridge takes over until the failed one is repaired or replaced. Redundancy can create loops in the system, which is very undesirable.

When a loop occurs, data packets can be sent around the loop indefinitely. This can cause a number of problems, including: packet loss, performance degradation, instability

What are the differences between classful addressing and classless addressing in IPv4?

Classful Addressing	Classless Addressing
IP addresses are allocated according to the classes- A to E.	It handles the issue of rapid exhaustion of IP addresses.
It is less practical.	It is more practical.
It does not support VLSM	It supports VLSM
It requires more bandwidth.	It requires less bandwidth
It does not support CIDR	It supports CIDR
Regular or periodic updates	Triggered Updates
Troubleshooting is easy • Network • Host • Subnet	Troubleshooting is tough • Host • Subnet

Explain the principles of congestion control in TCP.

1. Open-Loop Congestion Control

In open-loop congestion control, policies are applied to prevent congestion before it happens.

(a) Retransmission Policy: The retransmission policy must be designed to optimize efficiency and prevent congestion.

(b) Window Policy: The Selective Repeat window is better than the Go-Back-N window for congestion control.

(c) Acknowledgement Policy: If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.

(d) Discarding Policy: A good discarding policy by the routers may prevent congestion.

(e) Admission Policy: An admission policy can also prevent congestion in virtual circuit networks

2. Closed-Loop Congestion Control

Closed-loop congestion control mechanisms can reduce congestion after it happens.

(a) Back Pressure: When a router is congested, it can inform the previous upstream router to reduce the rate of outgoing packets. The action can be recursive all the way to the router before the source. This mechanism is called backpressure.

(b) Choke Point: A Choke point is a packet sent by a router to the source to inform it of congestion.

(c) Implicit Signalling: The source can detect an implicit signal and slow down its sending rate.

(d) Explicit Signalling: Explicit signalling can occur in either the forward or the backward direction.

Explain bit stuffing process.

The bit stuffing process works as follows:

1. The data stream is scanned for sequences of consecutive bits of the same value.
2. If a sequence of five or more consecutive 1 bits is found, a 0 bit is stuffed into the stream after the fifth 1 bit.
3. The process is repeated until the entire data stream has been scanned.

What is the need of subnetting?

- Improved network performance by reducing broadcast traffic
- Improved security by isolating different parts of the network
- Increased flexibility in how you design your network

What is the difference between hub topology and star topology?

Feature	Hub topology	Star topology
Connectivity	All devices are connected to a central hub.	Each device is connected to a central switch.
Broadcast traffic	All devices on the network can see all broadcast traffic.	Only the device that is addressed in a broadcast packet can see the packet.
Fault tolerance	If the hub fails, the entire network fails.	If the switch fails, only the devices that were connected to the switch will be affected.
Cost	Hubs are less expensive than switches.	Switches are more expensive than hubs.
Complexity	Hub topologies are easier to configure than star topologies.	Star topologies are more complex to configure than hub topologies.

What does Shannon capacity have to do with communications?

The Shannon capacity theorem defines the maximum amount of information, or data capacity, which can be sent over any channel.

$$\text{Shannon Capacity} = \text{bandwidth} * \log_2(1 + \text{SNR}) \text{ bits/sec}$$

It can be used to design communication protocols that are able to achieve the maximum data rate and to ensure that data is transmitted without errors.

Discuss various ATM layers and their functions.

- **Physical Layer −** This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium.
- **ATM Layer −**This layer is comparable to data link layer of OSI model. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.
- **ATM Adaptation Layer (AAL) −**This layer corresponds to network layer of OSI model. It accepts the data and converts them into fixed sized segments.
- **ATM endpoints −** It contains ATM network interface adaptor
- **ATM switch −**It transmits cells through the ATM networks.

Compare and contrast G-Back-N ARQ protocol with Selective repeat ARQ.

Feature	Go-Back-N ARQ	Selective Repeat ARQ
Window size	Fixed	Variable
Retransmission	All frames after the corrupted frame	Only the corrupted frame
Bandwidth efficiency	Low	High
Complexity	Low	High
Error detection	Cumulative ACK	Individual ACK

In Hamming code, for a data of m bits how do you compute the number of redundant bits r' needed?

$r = 2^p - m - 1$

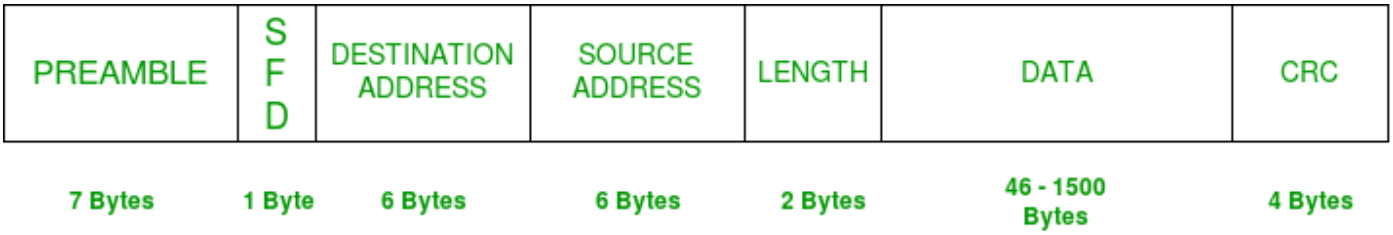
where p is the number of parity bits & m is the number of data bits

Explain in detail the working principles of IEEE 802.3 standard.

The IEEE 802.3 standard uses a carrier sense multiple access with collision detection (CSMA/CD) access method to control access to the shared medium. CSMA/CD is a contention-based protocol, which means that devices on the network share the medium and must compete for access to the medium.

When a device wants to transmit data, it first listens to the medium to see if it is busy. If the medium is not busy, the device transmits its data frame. If the medium is busy, the device waits until the medium is free before transmitting its data frame.

If two devices transmit data frames at the same time, a collision occurs. When a collision occurs, the devices detect the collision and then back off for a random amount of time before retransmitting their data frames.



IEEE 802.3 ETHERNET Frame Format

Discuss briefly about the high speed networks.

- **Fast Ethernet:** Fast Ethernet is a standard that offers a data rate of 100 Mbps. It is backward compatible with standard Ethernet, which means that it can be used on the same network as standard Ethernet devices.
- **Gigabit Ethernet:** Gigabit Ethernet is a standard that offers a data rate of 1 Gbps. It is much faster than Fast Ethernet and is often used for applications that require high bandwidth.
- **10 Gigabit Ethernet:** 10 Gigabit Ethernet is a standard that offers a data rate of 10 Gbps. It is even faster than Gigabit Ethernet and is used for applications that require the highest bandwidth, such as data center networking and high-performance computing.

Explain the working of Carrier Sense Multiple Access protocol.

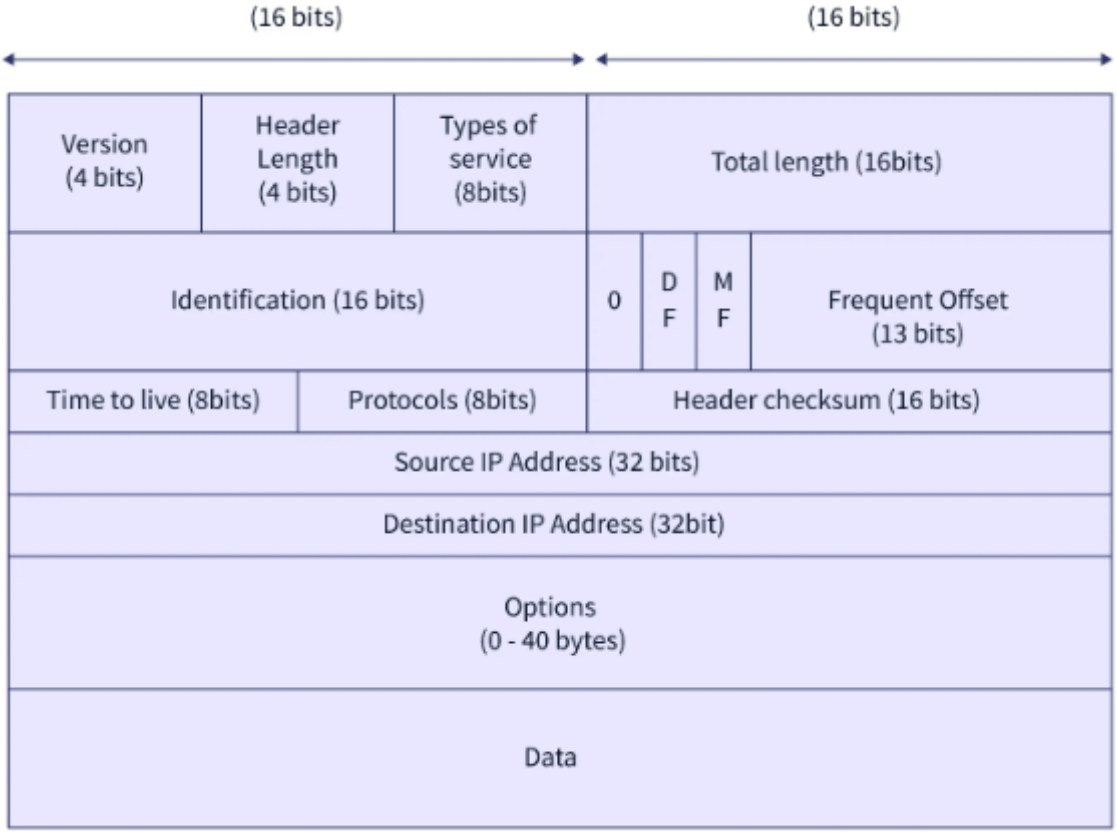
Carrier Sense Multiple Access (CSMA) is a medium access control (MAC) protocol that allows multiple nodes to share a single communication channel.

Steps involved in the working of CSMA protocol are:

1. A node listens to the channel to see if it is busy.

2. If the channel is busy, the node waits until it becomes idle.
3. If the channel is idle, the node transmits its data.
4. If a collision occurs, the nodes involved in the collision backoff for a random amount of time before trying to transmit again.

Discuss the following w.r.t IPv4: - (a) Datagram format



IPv4 Header

- **Version (VER):** It is a 4-bit field that defines the version of the IPv4 protocol
- **Header Length (HLEN):** It is a 4-bit field containing the IP header's length.
- **Type of Service:** It is an 8-bit field. This field is used for Quality of Service.
- **Total Length:** It is a 16-bit field that contains the total length of the IP Packet
- **Identification:** It is a 16-bit field used to identify the fragments of an original IP datagram.
- **DF Bit:** DF bit stands for Do Not Fragment bit. It is a 1-bit field, and its value maybe 0 or 1.
- **MF Bit:** MF bit stands for More Fragments bit. It is a 1-bit field, and its value may be 0 or 1.
- **Fragment Offset:** It is a 13-bit field. It tells the exact position of the fragmented datagram.
- **Time To Live (TTL):** TTL is an 8-bit field. It prevents the datagram from looping over the network by reducing the number of hops a packet can take before reaching its destination.
- **Protocol:** It is an 8-bit field. It identifies which protocol this IP datagram belongs to.
- **Header Checksum:** It is a 16-bit field containing the entire header's checksum value.
- **Source IP Address:** It is a 32-bit field and contains the IP address of the datagram's sender.
- **Destination IP Address:** It is a 32-bit field and contains the IP address of the datagram's receiver
- **Options:** It is optional and can range in size from 0 bytes to 40 bytes.

(b) Fields related to fragmentation and reassembly of an IPv4 datagram.

- **Identification:** It is a 16-bit field used to identify the fragments of an original IP datagram.
- **DF Bit:** DF bit stands for Do Not Fragment bit. It is a 1-bit field, and its value maybe 0 or 1.
- **MF Bit:** MF bit stands for More Fragments bit. It is a 1-bit field, and its value may be 0 or 1.
- **Fragment Offset:** It is a 13-bit field. It tells the exact position of the fragmented datagram.

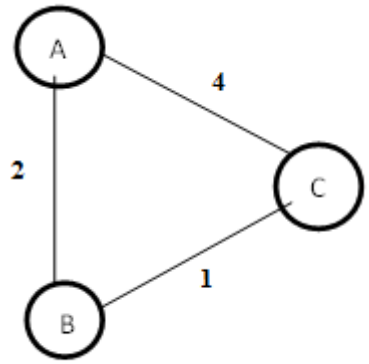
Explain the working of distance vector routing protocol with an example.

DVR Protocol Working

- In DVR, each router maintains a routing table. It contains only one entry for each router. It contains two parts − a preferred outgoing line to use for that destination and an estimate of time (delay). Tables are updated by exchanging the information with the neighbor's nodes.
- Each router knows the delay in reaching its neighbors (Ex − send echo request).
- Routers periodically exchange routing tables with each of their neighbors.
- It compares the delay in its local table with the delay in the neighbor's table and the cost of reaching that neighbor.
- If the path via the neighbor has a lower cost, then the router updates its local table to forward packets to the neighbor.

Example − Distance Vector Router Protocol

In the network shown below, there are three routers, A, B, and C, with the following weights − AB =2, BC =3 and CA =5.



Step 1 − In this DVR network, each router shares its routing table with every neighbor. For example, A will share its routing table with neighbors B and C and neighbors B and C will share their routing table with A.

Form A	A	B	C
A	0	2	3

B			
C			
Form B	A	B	C
A			
B	2	0	1
C			
Form C	A	B	C
A			
B			
C	3	1	0

Step 2 − If the path via a neighbor has a lower cost, then the router updates its local table to forward packets to the neighbor. In this table, the router updates the lower cost for A and C by updating the new weight from 4 to 3 in router A and from 4 to 3 in router C.

Form A	A	B	C
A	0	2	3
B			
C			
Form B	A	B	C
A			
B	2	0	1
C			
Form C	A	B	C
A			

B			
C	3	1	0

Step 3 − The final updated routing table with lower cost distance vector routing protocol for all routers A, B, and C is given below −

Router A

Form A	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0

Router B

Form B	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0

Router C

Form C	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0

Define TDM, FDM and WDM.

- Time-division multiplexing (TDM) is a digital multiplexing technique that allows multiple signals to be transmitted over a single channel by dividing the channel into time slots.
- Frequency-division multiplexing (FDM) is an analog multiplexing technique that allows multiple signals to be transmitted over a single channel by dividing the channel into frequency bands.
- Wavelength-division multiplexing (WDM) is an optical multiplexing technique that allows multiple signals to be transmitted over a single optical fiber by dividing the fiber into wavelength channels..

What is tunnelling?

Tunneling is used when source and destination networks of the same type are to be connected through a network of different types. Tunneling uses a layered protocol model such as those of the OSI or TCP/IP protocol suite.

What is the minimum and maximum frame size of IEEE 802.3 frame?

The IEEE 802.3 standard defines a minimum frame size of **64 bytes** and a maximum frame size of **1518 bytes.**

Discuss Hubs and Switches

Feature	Hub	Switch
Layer	Physical	Data link
Operation	Repeats signals	Reads destination address and forwards packets
Performance	Lower	Higher
Congestion	Can cause congestion	Can help to prevent congestion
Cost	Lower	Higher

Differentiate between Data and Signal.

Feature	Data	Signal
Definition	Data is a collection of values in any form.	A signal is a waveform that represents data.
Type	Discrete or continuous	Analog or digital
Representation	Bits, bytes, or characters	Voltage, current, or light
Purpose	To represent information	To transmit information

Explain sliding window protocols.

Sliding window protocol has two types:

1. Go-Back-N ARQ
2. Selective Repeat ARQ

Feature	Go-Back-N ARQ	Selective Repeat ARQ
Window size	Fixed	Variable
Retransmission	All frames after the corrupted frame	Only the corrupted frame
Bandwidth efficiency	Low	High
Complexity	Low	High
Error detection	Cumulative ACK	Individual ACK
Searching	Not needed	Needed
Sorting	Not needed	Needed

What is error correction and error detection? Discuss various error correction techniques.

Error Detection

Simple Parity Check

- 1 is added as a parity bit to the data block if the data block has an **odd number of 1's**.
- 0 is added as a parity bit to the data block if the data block has an **even number of 1's**.

Two-Dimensional Parity Check: For every **row and column**, parity check bits are calculated by a simple method of parity check.

Checksum: It is an error detection which detects the error by dividing the data into the segments of equal size and then **use 1's complement** to find the sum of the segments and then sum is transmitted with the data to the receiver and same process is done by the receiver and at the receiver side, all **zeros** in the sum indicates the correctness of the data.

Cyclic Redundancy Check

- A bit sequence commonly known as cyclic redundancy check is added to the end of the bits in CRC. This is done so that the resulting data unit will be divisible by the second binary number that is predetermined.
- The receiving data units on the receiver's side need to be divided by the same number. These data units are accepted and found to be correct only on the condition of the remainder of this division is zero.

Error Correction

- **Backward error correction:** Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
- **Forward error correction:** In this case, the receiver uses the error-correcting code which automatically corrects the errors.

Algorithm of Hamming code:

1. Add the information in **'d'** bits to the redundant bits **'r'** to make data as **d+r**.
2. A decimal value will be assigned by the position of each **(d+r)** digit.
3. In positions **1,2…2k**, the **'r'** bits will be placed.
4. The parity bits are again calculated on the receiver's end. The position of an error defines the parity bit's decimal value.

What are functions of MAC layer of IEEE 802.11

- **Distributed Coordination Function (DCF)** −
  - It is a mandatory function used in CSMA/CA.
  - It is used in distributed contention-based channel access.
  - It is deployed in both Infrastructure BSS (basic service set) as well as Independent BSS.
- **Point Coordination Function (PCF)** −
  - It is an optional function used by 802.11 MAC Sublayer.
  - It is used in centralized contention-free channel access.
  - It is deployed in Infrastructure BSS only.

Explain fragmentation

Fragmentation is done by the network layer when the maximum size of datagram is greater than maximum size of data that can be held in a frame. It is technique in which gateways break up or divide larger packets into smaller ones called fragments. Each

fragment is then sent as a separate internal packet. Each fragment has its separate header and trailer.

Transparent fragmentation is a process where the fragments are reassembled by the routers on the network.

Non-transparent fragmentation is a process where the fragments are reassembled by the receiver of the datagram.

Discuss the need of internet protocol

- **To route data packets:** IP is responsible for routing data packets between different networks. This is done by using IP addresses.
- **To address data packets:** IP is also responsible for addressing data packets. This is done by adding a header to each data packet that contains the source and destination IP addresses. The source IP address identifies the device that sent the data packet, and the destination IP address identifies the device that should receive the data packet.
- **To ensure reliable delivery:** IP also provides mechanisms to ensure reliable delivery of data packets. This is done by error detection and correction.
- **To provide a common addressing scheme:** IP provides a common addressing scheme for all devices on the Internet. This makes it possible for devices from different networks to communicate with each other.

Explain adaptive and non-adaptive algorithm with one example each

Adaptive Routing algorithm	Non-Adaptive Routing algorithm
It involves routers for exchanging and updating router table data.	It involves a network administrator for the manual entry of the routing paths into the router.
It creates a routing table based on network conditions.	It creates a static table
Used by dynamic routing.	Used by static routing.
Routing decisions are made based on network traffic and topology.	Routing decisions are not made based on network traffic and topology.
Complex	Simple
More used	Less Used
Example: Distance Vector Routing, Link State Routing	Example: Shortest Path Routing, Flooding, Flow based Routing