What is the difference between connectionless and connection oriented communication?

Feature	Connection-oriented	Connectionless
Connection establishment	Yes	No
Packet acknowledgement	Yes	No
Reliability	High	Low
Speed	Slow	Fast
Applications	File transfer, email	Web browsing, streaming media

Explain bit stuffing process.

Bit stuffing is a process of inserting non-information bits into a data stream to break up the data sequence and help in synchronization.

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?

- Subnetting is the process of dividing a large network into smaller networks, or subnets.
- Subnetting can be used to improve network performance, security, and flexibility.
- Benefits of subnetting include:
    - 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.

Explain the token early release. in What are Transmission impairments?

Token early release (TER) is a technique used in token ring networks to improve performance. In a token ring network, a token is passed around the ring, and only the node that has the token can transmit data.

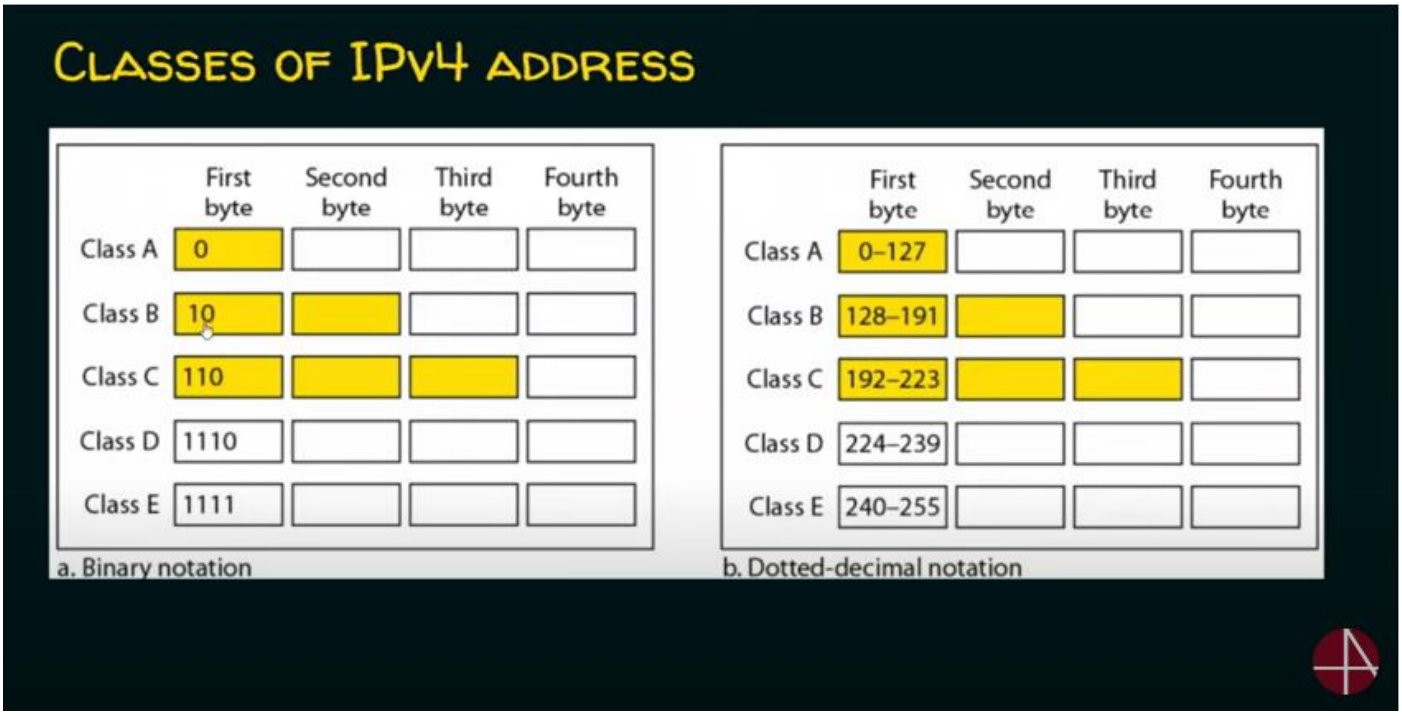
With TER, a node can release the token early if it knows that there is no other node that needs to transmit data. This can improve performance because it allows nodes to transmit data more quickly.

Transmission impairments are any factors that can degrade the quality of a signal as it is transmitted over a network. These factors can include noise, attenuation, and distortion.

Noise is any unwanted signal that is added to the desired signal. Attenuation is the loss of signal strength as it travels over a network. Distortion is the alteration of the signal waveform as it travels over a network.

Which class does the following IP address belong to?

(i) 157.143.252.207 (ii) 93.31.1.245



(i) The first octet of IP address 157.143.252.207 is 157, which is in the range of 128 to 191. Therefore, IP address 157.143.252.207 is a **class B** IP address.

(ii) The first octet of IP address 93.31.1.245 is 93, which is in the range of 0 to 127. Therefore, IP address 93.31.1.245 is a **class A** IP address.

Assume a Go-Back-N protocol is used with a window size of 4 and that the ACK for packet 2 gets lost. Show the events until packet 2 is acknowledged at the sender side.

1. The sender sends packets 1, 2, 3, and 4.
2. The receiver receives packets 1 and 3, and sends an acknowledgement for packet 1.
3. The sender receives the acknowledgement for packet 1.
4. The sender times out waiting for an acknowledgement for packet 2.
5. The sender resends packets 2, 3, and 4.
6. The receiver receives packets 2, 3, and 4, and sends an acknowledgement for packet 2.
7. The sender receives the acknowledgement for packet 2.

Explain the various layers present in OSI model and their functions.

1. **Physical layer:** This layer is responsible for the physical transmission of data over the network. It defines the electrical and mechanical specifications for how data is transmitted over the physical medium, such as copper wire or fiber optic cable.

2. **Data link layer:** This layer is responsible for error detection and correction. It ensures that data is transmitted without errors by adding error-checking bits to the data and by detecting and correcting errors that occur during transmission.
3. **Network layer:** This layer is responsible for routing data between different networks. It determines the best path for data to travel from source to destination and encapsulates data into packets that can be routed over different networks.
4. **Transport layer:** This layer is responsible for ensuring that data is delivered reliably. It breaks data up into smaller units called segments and provides mechanisms for ensuring that segments are delivered in the correct order and without errors.
5. **Session layer:** This layer is responsible for managing the communication between two applications. It establishes and terminates connections between applications and provides mechanisms for managing the flow of data between applications.
6. **Presentation layer:** This layer is responsible for formatting data so that it can be understood by the application. It translates data between different formats and ensures that data is presented in a way that is understandable by the application.
7. **Application layer:** This layer is the highest layer in the OSI model. It provides services to the application, such as file transfer, email, and web browsing.

What does Shannon capacity have to do with communications?

- Shannon capacity is a theoretical limit on the maximum rate of error-free data that can be transmitted over a communication channel.
- It is defined as the maximum amount of information that can be transmitted over a channel per unit time in the presence of noise.
- The Shannon capacity of a channel depends on the bandwidth of the channel and the noise level.
- Shannon capacity is an important concept in communications because it provides a theoretical limit on the maximum data rate that can be supported by a given channel.
- This limit 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.

Explain all the main components of Telephone system.

- **Telephone instrument:** This is the device that you use to make and receive calls. It includes a handset, a keypad, and a speaker.
- **Local loop:** This is the physical connection between the telephone instrument and the telephone exchange. It is typically made up of twisted-pair copper wire.
- **Telephone exchange:** This is the central point in the telephone system where calls are routed. It is responsible for connecting calls between different telephone instruments.
- **Trunks:** These are the high-capacity links that connect telephone exchanges together. They are typically made up of fiber optic cables.
- **Signalling system:** This is the system that controls the routing of calls through the telephone system. It is responsible for ensuring that calls are routed to the correct destination.
- **Control system:** This is the system that manages the operation of the telephone system. It is responsible for tasks such as billing, customer service, and network security.

Explain all types of frames format in HDLC protocol

The HDLC protocol (High-Level Data Link Control) defines three types of frames:

- **Information frames (I-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.
- **Supervisory frames (S-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.
- **Unnumbered frames (U-frames)** are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first bit of control field of U-frame is 1.

The frame format for each type of frame is the same. It consists of the following fields:

- **Flag:** This is a 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address:** This field identifies the destination of the frame. It can be one byte or several bytes long.
- **Control:** This field contains control information that is used to manage the flow of data and to detect and correct errors.
- **Information:** This field contains the user data that is being transmitted.
- **FCS:** This is a 16-bit field that contains a checksum that is used to detect errors in the frame.

Discuss various types of transmission media, highlighting their merits and demerits.

- **Twisted-pair cable:** Inexpensive, easy to install, resistant to noise, but limited bandwidth and cannot be used for long distances.
- **Coaxial cable:** More expensive than twisted-pair cable, but has higher bandwidth, can be used for longer distances, and more resistant to noise.
- **Fiber optic cable:** Fastest type of transmission media, very resistant to noise, can be used for long distances, but more expensive and difficult to install.
- **Wireless:** Convenient and easy to use, but more susceptible to interference and not as secure as other types of transmission media.

Discuss various ATM layers and their functions.

The ATM (Asynchronous Transfer Mode) protocol has five layers:

- **Physical layer:** Transmits data over the physical medium.
- **ATM layer:** Segment and reassemble data into cells, route cells through the network, and manage virtual circuits.
- **ATM Adaptation Layer (AAL):** Adapt data from the upper layers to the ATM layer.
- **User Network Interface (UNI) layer:** Interact between ATM devices and the user network.

- **Control plane:** Establish and maintain connections between ATM devices.

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 defines the physical layer and data link layer of wired Ethernet networks.
- It uses a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method to control access to the physical medium.
- The IEEE 802.3 standard is a widely used standard for wired Ethernet networks. It is a reliable and efficient standard that can be used to transmit data over a variety of physical media.

The IEEE 802.3 standard also defines the format of Ethernet frames. An Ethernet frame consists of the following fields:

- **Preamble:** The preamble is a 7-byte field that is used to synchronize the sender and receiver.
- **Start of Frame Delimiter (SFD):** The SFD is a 1-byte field that marks the beginning of the frame.
- **Destination Address:** The Destination Address is a 6-byte field that identifies the destination device.

- **Source Address:** The Source Address is a 6-byte field that identifies the source device.
- **Length:** The Length field is a 2-byte field that specifies the length of the data field.
- **Data:** The Data field is a variable-length field that contains the data to be transmitted.
- **Frame Check Sequence (FCS):** The FCS is a 4-byte field that is used to detect errors in the frame.

Discuss briefly about the high speed networks.

High-speed networks are a type of network that can transmit data at very high speeds. They are often used for applications that require a lot of bandwidth, such as video streaming, online gaming, and cloud computing.

Some high speed technologies are:

- **Fiber optic:** Fiber optic cables are made of glass or plastic and can transmit data at very high speeds. They are often used for long-distance networks.
- **Ethernet:** Ethernet is a wired networking technology that can transmit data at speeds up to 100 Gbps. It is a popular choice for high-speed networks in businesses and homes.
- **Wireless:** Wireless networks can transmit data at high speeds using radio waves. They are a popular choice for high-speed networks in mobile devices and laptops.

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

(a) Datagram format

It consists of a header and a data payload. The header contains information about the datagram, such as the source and destination addresses, the length of the datagram, and the type of service. The data payload is the actual data that is being transmitted.

The IPv4 header is 20 bytes long. It is divided into the following fields:

- **Version:** This field specifies the version of the IPv4 protocol.
- **IHL:** This field specifies the length of the IPv4 header in bytes.
- **Type of Service:** This field specifies the type of service that is requested for the datagram.
- **Total Length:** This field specifies the length of the datagram, including the header and the data payload.
- **Identification:** This field is used to identify the datagram.
- **Flags:** This field contains flags that control the fragmentation and reassembly of the datagram.
- **Fragment Offset:** This field specifies the offset of the datagram in the original datagram.
- **Time to Live:** This field specifies the number of hops that the datagram can travel before it is discarded.
- **Protocol:** This field specifies the upper-layer protocol that is used for the data payload.
- **Header Checksum:** This field is used to verify the integrity of the IPv4 header.

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

The following fields in the IPv4 header are related to fragmentation and reassembly of an IPv4 datagram:

- **Flags:** This field contains two flags that control fragmentation and reassembly:
    - **The More Fragments bit (MF bit):** This bit is set if there are more fragments of the original datagram.
    - **The Don't Fragment bit (DF bit):** This bit is set if the datagram should not be fragmented.
- **Fragment Offset:** This field specifies the offset of the datagram in the original datagram.

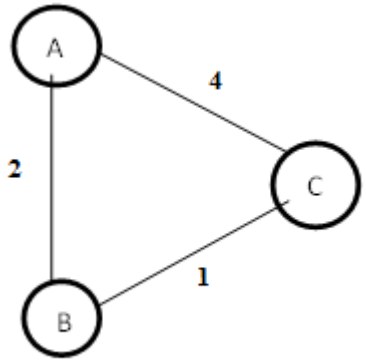
Explain the working of distance vector routing protocol with an example.

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