What is the significance of twisting in twisted pair cable?

- **Reduces EMI:** As mentioned earlier, twisting in twisted pair cable helps to reduce EMI by cancelling out the EMI that is induced in each wire. This makes the cable less susceptible to noise from nearby electrical devices.
- **Improves signal quality:** The twisting also helps to improve signal quality by reducing crosstalk. Crosstalk is a type of interference that can occur when two wires are close together. The twisting helps to keep the wires separate, which reduces the amount of crosstalk.
- **Increases bandwidth:** The twisting also helps to increase bandwidth by reducing attenuation. Attenuation is the loss of signal strength over distance. The twisting helps to keep the signal from spreading out, which reduces the amount of 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 in computer networking to divide a network into smaller subnetworks. This is done by using a subnet mask to identify which bits of an IP address belong to the network and which bits belong to the host.
- The subnet mask is a 32-bit number that is used to divide an IP address into two parts: the network address and the host address. The network address is the part of the IP address that identifies the network, and the host address is the part of the IP address that identifies the individual host on the network.
- The subnet mask is a bitmask, which means that it is a sequence of 1s and 0s. The 1s in the subnet mask represent the bits of the IP address that belong to the network address, and the 0s represent the bits of the IP address that belong to the host address.
- For example, the subnet mask 255.255.255.0 has 24 1s in the beginning, which means that the first 24 bits of the IP address belong to the network address. The remaining 8 bits of the IP address belong to the host address.

What is the difference between packet switching and circuit switching?

Feature	Packet Switching	Circuit Switching
Data transmission	Data is divided into small chunks called packets.	A dedicated connection is established between the sender and the receiver.
Data delivery	Packets are routed through the network independently of each other.	Data is transmitted continuously until it reaches the destination.
Efficiency	Efficient for bursty traffic.	Efficient for continuous traffic.
Reliability	Less reliable than circuit switching.	More reliable than packet switching.
Cost	Less expensive than circuit switching.	More expensive than packet switching.
Examples	Internet, LANs	Telephone network, WANs

What is early token release?

Early token release (ETR) is a technique used in token ring networks that allows a station to release a new token onto the ring immediately after transmitting, instead of waiting for the first frame to return. This feature can increase the total bandwidth on the ring.

ETR is not enabled by default on token ring networks. It must be enabled by the network administrator.

Explain the three types of frames in HDLC.

- **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.

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.

Sure. Slow start is a congestion control algorithm used in the Transmission Control Protocol (TCP). It is a conservative algorithm that starts with a small amount of data and gradually increases the amount of data sent over time. This helps to prevent the network from becoming congested.

Slow start is divided into two phases:

- **Phase 1:** The sender starts by sending a single packet. If the packet is acknowledged, the sender sends two packets in the next round. The sender continues to double the number of packets sent in each round until it reaches a threshold.
- **Phase 2:** Once the threshold is reached, the sender enters the congestion avoidance phase. In this phase, the sender continues to send packets, but it does not double the number of packets sent in each round. Instead, the sender adds a small amount of data to each round.

Explain the various layers present in TCP/IP reference model and their functions. (b) Explain the three types of transmission impairment?

The four layers of TCP/IP protocol are −

- **Host-to- Network Layer −**It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.
- **Internet Layer −**It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.
- **Transport Layer −** It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **Application Layer −** This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

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 the difference between guided media and unguided media. Briefly explain any three methods used for data transmission using guided media and any two methods used for data transmission using unguided media.

Guided media use a physical path to transmit data, such as a copper cable or a fiber optic cable. The data travels through the medium in the form of electrical or optical signals. Guided media are typically used for point-to-point communication, such as between two computers or between a computer and a router.

Unguided media do not use a physical path to transmit data. Instead, the data is transmitted through the air or space in the form of electromagnetic waves. Unguided media are typically used for broadcast communication, such as radio or television.

Methods used for data transmission using guided media are:

- **Twisted pair:** Twisted pair is a type of cable that consists of two insulated copper wires twisted around each other. Twisted pair cables are commonly used for telephone and Ethernet networks.
- **Coaxial cable:** Coaxial cable is a type of cable that consists of a central conductor surrounded by a dielectric insulator and a braided metal shield. Coaxial cables are commonly used for cable television and high-speed Ethernet networks.

- **Fiber optic cable:** Fiber optic cable is a type of cable that consists of a central core of glass or plastic surrounded by a cladding layer. Fiber optic cables are used for high-speed data transmission over long distances.

Methods used for data transmission using unguided media are:

- **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.

- IEEE 802.11 uses 48-bit MAC addresses to uniquely identify devices on a wireless network.
- The MAC address is used for addressing and authentication purposes.
- The MAC address is a globally unique identifier that can be used to track devices on a wireless network.
- The MAC address is divided into two parts: the Organizationally Unique Identifier (OUI) and the device identifier.
- The OUI is assigned by the IEEE to organizations that manufacture networking devices.
- The device identifier is assigned by the organization to the individual device.

Explain in detail the problems associated with IEEE 802.11 standard.

- **Security:** The IEEE 802.11 standard does not provide strong security out of the box. 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, which can degrade the performance of the wireless network.
- **Range:** The range of a wireless network is limited by the power of the transmitter and the environment. In some cases, the range may be too short to cover the desired area.
- **Performance:** The performance of a wireless network can be affected by a number of factors, such as 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.

Feature	CSMA/CD	CSMA/CA
Name	Carrier Sense Multiple Access with Collision Detection	Carrier Sense Multiple Access with Collision Avoidance
Purpose	To prevent collisions on a shared medium	To minimize collisions on a shared medium
Efficiency	Less efficient than CSMA/CA	More efficient than CSMA/CD
Recovery time	Slow	Fast
Used in	Wired networks	Wireless networks

Explain the loop problem associated with bridges.

A loop problem is a condition that can occur in a network when there are two or more bridges connected in a way that creates a loop.

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

- **Packet loss:** Data packets can be lost as they are sent around the loop.
- **Performance degradation:** The performance of the network can degrade as the bridges try to process the packets that are being sent around the loop.
- **Instability:** The network can become unstable as the bridges try to resolve the loop.

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

Feature	Classful Addressing	Classless Addressing
Network ID	Fixed length	Variable length
Host ID	Fixed length	Variable length

Number of networks	5	Unlimited
Number of hosts per network	Varies by class	Unlimited
Efficiency	Less efficient	More efficient
Scalability	Not scalable	Scalable
Support for VLSM	No	Yes

Find the netid and hostid of the following IP addresses: (i) 114.34.2.8 (ii) 208.34.54.12

IP Address	NetID	HostID
114.34.2.8	114.34.2	8
208.34.54.12	208.34.54	12

Explain the principles of congestion control in TCP.

Congestion control in TCP is a set of mechanisms that prevents network congestion by ensuring that the sender does not send more data than the network can handle. Congestion can occur when too many packets are sent to a router or link, and the router is unable to forward them all in a timely manner. This can lead to packet loss, which can further degrade performance.

TCP congestion control is based on the following principles:

- **Additive Increase/Multiplicative Decrease (AIMD).** This is a simple algorithm that starts with a small window size and increases it by one after each acknowledgment. If a packet is lost, the window size is decreased by half.
- **Slow start.** This is a special phase that is used when the sender is first starting to send data. In this phase, the window size is increased exponentially, which allows the sender to quickly ramp up its sending rate.
- **Congestion avoidance.** This is the normal phase of congestion control. In this phase, the window size is increased by one after each acknowledgment, as long as no packets are lost.