Design issues of network layer

- **Routing:** How to find the best path for a packet to travel from source to destination.
- **Error handling:** How to deal with packets that are lost, corrupted, or delayed.
- **Congestion control:** How to prevent networks from becoming overloaded.
- **Addressing:** How to uniquely identify hosts and networks in a network.
- **Security:** How to protect packets from unauthorized access or modification.
- **Performance:** How to optimize the performance of the network layer, in terms of throughput, latency, and scalability.
- **Scalability:** How to design a network layer that can scale to meet the needs of a growing network.
- **Fault tolerance:** How to design a network layer that can continue to operate even if some of the nodes or links in the network fail.
- **Security:** How to protect the network layer from security threats, such as denial-of-service attacks or malicious code.

What is latency?

Latency in computer networks is the time it takes for a data packet to travel from one point to another. It is measured in milliseconds (ms). Latency is affected by a number of factors, including the distance between the sender and receiver, the type of network infrastructure, and the amount of traffic on the network.

Low latency is desirable for applications that require real-time communication, such as online gaming and video conferencing. High latency can cause delays and jitter, which can degrade the user experience.

It can be reduced by using fiber optic cables or reducing the amount of traffic on the network.

Differentiate between circuit and packet switching

Feature	Circuit switching	Packet switching
Connection	Dedicated	Virtual
Bandwidth	Guaranteed	Shared
Latency	Low	Variable
Applications	Voice, video, real-time data	Email, file sharing, bulk data
Examples	PSTN, ISDN	Internet, Ethernet

What are transmission impairments?

Transmission impairments are any factors that can degrade the quality of a signal as it travels through a transmission medium.

- **Attenuation:** This is the loss of signal strength as it travels through the medium. Attenuation is caused by the resistance of the medium to the flow of electrical current.
- **Distortion:** This is the alteration of the signal's shape or amplitude. Distortion can be caused by the non-linear characteristics of the medium or by interference from other signals.
- **Noise:** This is any unwanted signal that is added to the transmitted signal. Noise can be caused by thermal noise, shot noise, or interference from other sources.

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. Each signal is assigned a specific time slot, and only one signal is transmitted in each time slot.
- 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. Each signal is assigned a specific frequency band, and only one signal is transmitted in each frequency band.
- 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. Each signal is assigned a specific wavelength channel, and only one signal is transmitted in each wavelength channel.

What is tunnelling?

Tunnelling is a networking technique that allows data to be transmitted between two networks that are not directly connected. This is done by encapsulating the data from one network inside the data from another network. The encapsulated data is then transmitted over the public network, such as the Internet.

Tunnelling is used for a variety of purposes, like: Virtual private network (VPN), Remote access and Network extension

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

- **Minimum frame size: 64 bytes**
    - The minimum frame size is enforced by the preamble and start frame delimiter (SFD), which together take up 7 bytes.
    - The data field of the frame can be any size between 0 bytes and 46 bytes.
    - If the data field is 0 bytes, padding bytes are added to the end of the frame to bring the total frame size to 64 bytes.
- **Maximum frame size: 1518 bytes**
    - The maximum frame size is limited by the maximum transmission unit (MTU) of the network.
    - The MTU is the largest size of a frame that can be transmitted on the network without being fragmented.

- If the frame size exceeds the MTU, the frame will be fragmented into smaller frames that can be transmitted.

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

Explain the Layered approach of OSI Reference Model.

The seven layers of the OSI model are:

- **Physical layer:** This layer is responsible for the physical transmission of data over a network. It defines the electrical and mechanical characteristics of the network, such as the type of cable and the voltage levels.
- **Data link layer:** This layer is responsible for the reliable transmission of data over the physical layer. It provides error detection and correction, and it also manages the flow of data between devices.
- **Network layer:** This layer is responsible for routing data between different networks. It uses a routing protocol to determine the best path for data to travel.
- **Transport layer:** This layer is responsible for providing a reliable connection between two applications. It breaks data up into smaller units called segments, and it also handles error recovery and flow control.
- **Session layer:** This layer is responsible for managing the communication between two applications. It establishes and terminates sessions, and it also manages the synchronization of data between the two applications.
- **Presentation layer:** This layer is responsible for formatting data for presentation to the user. It translates data between different formats, such as ASCII and EBCDIC.
- **Application layer:** This layer is the interface between the user and the network. It provides services to the user, such as file transfer and email.

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 main components of Telephone system

The main components of a telephone system are:

- **End-user devices:** These are the devices that users use to make and receive calls. They can be landline phones, mobile phones, or VoIP phones.
- **Switching nodes:** These are the devices that connect end-user devices to each other. They can be located in central offices, local exchanges, or mobile switching centres.
- **Transmission media:** These are the physical media that carry the signals between switching nodes. They can be copper wires, optical fibres, or radio waves.
- **Signalling system:** This is the system that controls the flow of information between switching nodes. It uses a variety of protocols to establish and maintain connections, and to transfer data between devices.
- **Network management system:** This is the system that manages the telephone network. It monitors the network for problems, and it takes corrective action when necessary.

Explain different types of Transmission media.

Guided media are those that confine the signal to a specific path. They are also known as wired or bounded transmission media. The most common types of guided media are:

- **Twisted-pair cable:** This is the most common type of guided media. It consists of two insulated copper wires twisted together. Twisted-pair cables are relatively inexpensive and easy to install. However, they have a relatively low bandwidth.
- **Coaxial cable:** This type of cable consists of a central copper conductor surrounded by an insulating layer, a conducting shield, and an outermost plastic sheath. Coaxial cables have a higher bandwidth than twisted-pair cables and are less susceptible to interference. However, they are also more expensive and difficult to install.

- **Optical fiber:** This type of cable consists of a thin strand of glass or plastic that carries light signals. Optical fibers have the highest bandwidth of any guided media and are very resistant to interference. However, they are also the most expensive and difficult to install.

Unguided media are those that do not confine the signal to a specific path. They are also known as wireless or unbounded transmission media. The most common types of unguided media are:

- **Radio waves:** These are electromagnetic waves that can propagate through the air. Radio waves are used for a variety of wireless applications, including cellular networks, Wi-Fi, and satellite communication.
- **Microwaves:** These are high-frequency radio waves that can be used to transmit data over long distances. Microwaves are used for applications such as point-to-point communication and satellite communication.
- **Infrared light:** This is a type of electromagnetic radiation that can propagate through the air. Infrared light is used for applications such as remote controls and wireless networking.

Explain sliding window protocols.

- Sliding window protocols are a way to improve the efficiency of data transmission over a network.
- They allow the sender to send multiple packets before receiving an acknowledgment from the receiver.
- The size of the window determines how many packets the sender can send before receiving an acknowledgment.
- The receiver acknowledges the packets that it has received, and the sender then slides the window forward to include the acknowledged packets.
- If a packet is lost or corrupted, the receiver will not acknowledge it. The sender will then resend the lost or corrupted packet.
- Sliding window protocols are a valuable tool for improving the efficiency of data transmission. They are used in a variety of network protocols, including the Transmission Control Protocol (TCP).

There are two main types of sliding window protocols: Go-Back-N ARQ and Selective Repeat ARQ.

- **Go-Back-N ARQ** is a simple sliding window protocol in which the sender sends all of the packets in the window before receiving an acknowledgment. If any packet is lost or corrupted, the receiver will send an acknowledgment for all of the packets up to the lost or corrupted packet. The sender will then resend all of the packets from the lost or corrupted packet onwards.
- **Selective Repeat ARQ** is a more sophisticated sliding window protocol in which the sender only resends the packets that have been lost or corrupted. This is more efficient than Go-Back-N ARQ, as it does not require the sender to resend all of the packets in the window.

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

Error correction and detection are important techniques used in computer networks to ensure that data is transmitted without errors. Error correction and detection are typically implemented in the data link layer.

There are two main types of error correction techniques: forward error correction (FEC) and backward error correction (BEC).

- **Forward error correction (FEC)** adds redundant bits to the data stream before transmission. The receiver can use these redundant bits to correct errors that have occurred during transmission. FEC is more efficient than BEC, but it can only correct a limited number of errors.
- **Backward error correction (BEC)** requires the receiver to request the sender to retransmit the data if an error is detected. BEC is less efficient than FEC, but it can correct a wider range of errors.

Various error correction techniques are:

- **Parity check:** This is the simplest form of error detection. A parity bit is added to the data stream, and the receiver can use this bit to detect whether an even or odd number of bits have been flipped.
- **Cyclic redundancy check (CRC):** This is a more sophisticated error detection technique. A CRC code is generated from the data stream, and the receiver can use this code to detect and correct errors.
- **Hamming code:** This is a forward error correction technique. Hamming codes can correct up to one-bit error in a data word.

Explain channel allocation problem.

It deals with the allocation of channels to users. The goal of channel allocation is to maximize the utilization of channels while minimizing interference between users.

There are two main types of channel allocation problems: static and dynamic.

- **Static channel allocation** is the process of allocating channels to users at the beginning of a communication session. Once channels are allocated, they cannot be changed. Static channel allocation is often used in applications where the number of users and their traffic patterns are known in advance.
- **Dynamic channel allocation** is the process of allocating channels to users as needed. Dynamic channel allocation is often used in applications where the number of users and their traffic patterns are not known in advance.

Some of the most common algorithms include:

- **First-come, first-served (FCFS):** This algorithm allocates channels to users in the order in which they request them.
- **Shortest remaining time first (SRTF):** This algorithm allocates channels to users with the shortest remaining transmission time.
- **Max-min fairness (MMF):** This algorithm allocates channels to users in a way that maximizes the minimum throughput of all users.

Discuss frame format of HDLC protocol.

The High-level Data Link Control (HDLC) protocol is a bit-oriented data link layer protocol that is used to transmit data between two nodes on a network. The HDLC frame format is as follows:

- **Flag:** The flag is an 8-bit sequence that marks the beginning and end of the frame.
- **Address:** The address field is 8 bits long and identifies the destination of the frame.
- **Control:** The control field is 8 bits long and specifies the type of frame and the actions that the receiver should take.
- **Information:** The information field contains the data that is being transmitted. The length of the information field can vary.
- **FCS:** The Frame Check Sequence (FCS) is a 2-byte or 4-byte field that is used to detect errors in the frame.
- **Flag:** The flag is an 8-bit sequence that marks the end of the frame.

There are three types of frames in HDLC:

- **I-frames:** Information frames carry user data.
- **S-frames:** Supervisory frames are used for flow control and error control.
- **U-frames:** Unnumbered frames are used for miscellaneous purposes, such as link establishment and teardown.

Explain IEEE 802.3 standard.

The IEEE 802.3 standard is a set of specifications for Ethernet, a local area network (LAN) technology. The standard defines the physical layer and data link layer of the OSI model.

The physical layer defines the electrical and mechanical characteristics of the network, while the data link layer defines the framing and error control mechanisms.

Various 802.3 standards:

- **10Base-T (IEEE 802.3):** 10 Mbps with category 3 unshielded twisted pair (UTP) wiring, up to 100 meters long.
- **100Base-TX (IEEE 802.3u):** Known as Fast Ethernet, uses category 5, 5E, or 6 UTP wiring, up to 100 meters long.
- **1000Base-T (IEEE 802.3ab):** Gigabit Ethernet, uses category 5e or 6 UTP wiring, up to 100 meters long.
- **10GBASE-T (IEEE 802.3an):** 10 Gigabit Ethernet, uses category 6a UTP wiring, up to 100 meters long.
- **2.5GBASE-T (IEEE 802.3bz):** 2.5 Gigabit Ethernet, uses category 6a UTP wiring, up to 100 meters long.
- **5GBASE-T (IEEE 802.3bz):** 5 Gigabit Ethernet, uses category 6a UTP wiring, up to 100 meters long.

- **10GBASE-SR (IEEE 802.3ae):** 10 Gigabit Ethernet, uses single-mode fiber optic cable, up to 300 meters long.
- **10GBASE-LR (IEEE 802.3ae):** 10 Gigabit Ethernet, uses multimode fiber optic cable, up to 2 kilometers long.

What are functions of MAC layer of IEEE 802.11

The MAC layer of IEEE 802.11 is responsible for the following functions:

- **Medium access control (MAC):** The MAC layer is responsible for controlling access to the shared medium. This is done using a variety of techniques, such as CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).
- **Addressing:** The MAC layer is responsible for addressing frames. This is done using MAC addresses, which are 48-bit identifiers assigned to each wireless device.
- **Frame delimiting and framing:** The MAC layer is responsible for delimiting and framing frames. This means that it is responsible for identifying the beginning and end of frames, as well as for adding header and trailer information to frames.
- **Error detection and correction:** The MAC layer is responsible for error detection and correction. This is done using a variety of techniques, such as CRC (cyclic redundancy check).
- **Flow control:** The MAC layer is responsible for flow control. This is done to ensure that the sender does not send data faster than the receiver can receive it.
- **Security:** The MAC layer is responsible for security. This is done by providing mechanisms for authentication, encryption, and data integrity.

Explain fragmentation

Fragmentation is the process of dividing a large data packet into smaller pieces, called fragments, so that the resulting pieces can travel across a link with a smaller maximum transmission unit (MTU) than the original packet size.

Fragmentation is typically done in the network layer of the OSI model. The network layer is responsible for routing data packets between different networks. If the MTU of a link is smaller than the size of the data packet, the network layer will fragment the data packet into smaller pieces so that the pieces can be routed across the link.

The fragments are then reassembled at the destination network layer. The destination network layer will reassemble the fragments into the original data packet.

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 a system of addresses, called IP addresses. IP addresses are unique identifiers that are assigned to each device on the Internet.
- **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 using a variety of techniques, such as error detection and correction, and retransmission.
- **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 algorithms change their routing paths based on the current network conditions, while non-adaptive algorithms use a static routing table that does not change.

Adaptive algorithms:

- **OSPF (Open Shortest Path First):** OSPF is an adaptive routing algorithm that uses a link state routing protocol. OSPF routers exchange information about the links in their networks, and they use this information to calculate the shortest paths between all pairs of routers.
- **BGP (Border Gateway Protocol):** BGP is an adaptive routing algorithm that uses a path vector routing protocol. BGP routers exchange information about the routes they know, and they use this information to build a routing table that includes the best routes to all destinations.

Non-adaptive algorithms:

- **Static routing:** Static routing is a non-adaptive routing algorithm that uses a static routing table. The routing table is created manually by the network administrator, and it does not change unless the network administrator manually updates it.
- **Distance vector routing:** Distance vector routing is a non-adaptive routing algorithm that uses a distance vector routing protocol. Distance vector routers exchange information about the distances to their neighbors, and they use this information to update their routing tables.