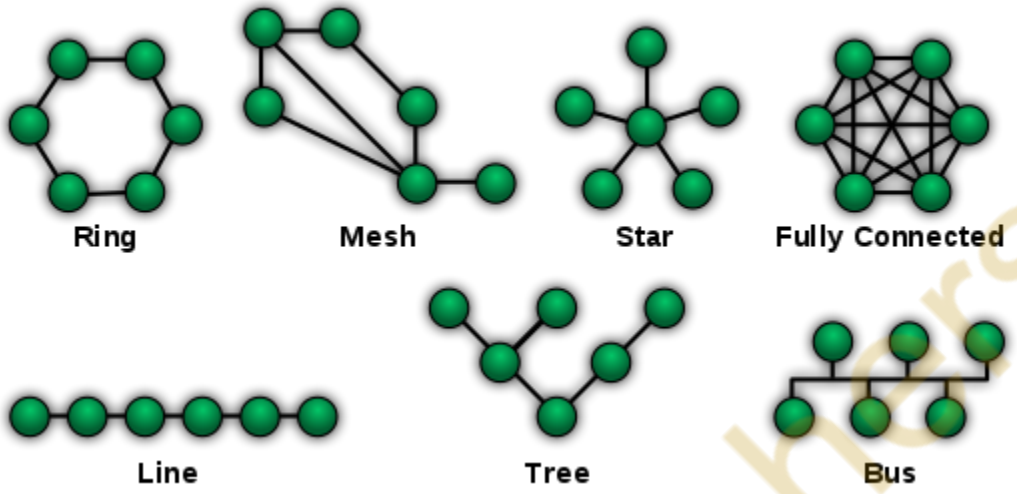
1. What is Computer Networks ?

A computer network is a collection of computers and other devices that are interconnected to share resources and information. In simpler terms, it's like a digital highway that allows different devices to communicate and exchange data with each other.

2. What is LAN , MAN And WAN ?

Aspect	LAN (Local Area Network)	WAN (Wide Area Network)	MAN (Metropolitan Area Network)
Definition	Network within a limited area (e.g., home, office, school).	Spans a large geographical area, connecting multiple LANs or networks.	Covers a larger geographic area than LAN, typically within a city or town.
Scope	Limited geographical area.	Global or regional coverage.	City or metropolitan area coverage.
Speed	Typically high-speed connections.	Speeds vary based on infrastructure and distance.	Speeds similar to LAN or WAN, depending on infrastructure.
Ownership	Owned and managed by a single organization.	May be owned and managed by multiple organizations.	Usually owned and managed by a single organization or consortium.
Example	Home network, office network.	Internet.	Network connecting multiple university campuses within a city.
Technology	Ethernet, Wi-Fi.	Fiber optics, satellite links.	Ethernet, fiber optics.

3. Explain All Network Topologies



Star: Devices are connected to a central hub or switch, like in a typical home or office network.

Bus: Devices are connected to a single cable, often used in Ethernet networks.

Ring: Devices are connected in a closed loop, where data flows in one direction, like in Token Ring networks.

Mesh: Devices are connected to each other directly, creating multiple paths for data transmission.

Tree: Combines characteristics of star and bus topologies, often used in large networks like hierarchical organizational setups.

4. Explain OSI Model in detail

The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven distinct layers. Here's a brief explanation of each layer:

1. Physical Layer:

What it does: Deals with the physical connection between devices.
Example: It defines how cables are connected and how bits are transmitted over the network.

2. Data Link Layer:
What it does: Ensures reliable transmission of data across a physical link.
Example: It handles framing, error detection, and flow control.

3. Network Layer:
What it does: Manages the addressing and routing of data packets between different networks.
Example: It determines the best path for data to travel from source to destination.

4. Transport Layer:
What it does: Provides endtoend communication between devices.

Example: It ensures data is delivered reliably and in the correct order, handling issues like congestion and flow control.

5. Session Layer:
What it does: Manages communication sessions between applications.
Example: It establishes, maintains, and terminates connections between devices.

6. Presentation Layer:
What it does: Deals with data formatting and conversion, ensuring compatibility between different systems.
Example: It translates data into a format that the application layer can understand.

7. Application Layer:
What it does: Provides network services directly to endusers or applications.
Example: It includes protocols like HTTP, FTP, SMTP, etc., used for email, web browsing, file transfer, etc.

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

5. Explain Difference bw TCP And UDP Protocols

Feature	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Connection	Connection-oriented: Requires establishing a connection before data transfer.	Connectionless: No prior connection setup; data can be sent without establishing a connection.
Reliability	Reliable: Guarantees delivery of data packets, with acknowledgment and retransmission mechanisms.	Unreliable: Does not guarantee delivery; packets may be lost without notification.
Ordering	Preserves packet order; data arrives in the same order as sent.	No guarantee of packet order; packets may arrive out of order.
Header Size	Larger header size due to additional control information for sequencing and error detection.	Smaller header size, as there is less control information needed.

6. What is An IP Address ?

An IP address is like a house address for devices on a network. It's a unique number that identifies a device, allowing it to communicate with other devices over the internet or a local network.

Example: Just like each house on a street has its own address (like 123 Main Street), each device on a network has its own IP address (like 192.168.1.1).

7. Difference Bw Ip Address and Mac Address

Feature	IP Address	MAC Address
Definition	A numerical label assigned to each device	A unique identifier assigned to network interfaces
Purpose	Identifies a device in a network	Identifies a device in a local network segment
Layer	Works at the network layer (Layer 3)	Works at the data link layer (Layer 2)
Type	Logical address	Physical address
Assigned by	Assigned by the network administrator or DHCP	Assigned by the manufacturer of the network adapter
Format	Consists of four sets of numbers separated by periods (e.g., 192.168.1.1)	Consists of six pairs of hexadecimal characters separated by colons or dashes (e.g., 00:1A:2B:3C:4D:5E)
Changeability	Can be changed or reassigned	Generally cannot be changed

8. What is a Subnet Mask ?

A subnet mask is a number used in computer networking to divide an IP address into two parts: the network address and the host address.

Purpose : It helps identify which part of an IP address belongs to the network and which part belongs to a specific device within that network.

Example : If you have an IP address like 192.168.1.100 and a subnet mask of 255.255.255.0, the first three numbers (192.168.1) are the network address, and the last number (100) is the host address.

9. What Is DNS And Its Purpose ?

DNS stands for Domain Name System. It's like a phone book for the internet. Here's a simple explanation:

What It Is : DNS is a system that translates humanreadable domain names (like google.com) into numerical IP addresses (like 172.217.6.238) that computers understand.

Purpose : It helps you access websites by typing in easytoremember domain names instead of complicated IP addresses.

Example : When you type "google.com" into your web browser, DNS translates it to the IP address "172.217.6.238" so your browser can connect to Google's servers and load the webpage.

10. What Is DHCP And How Does It Works ?

DHCP stands for Dynamic Host Configuration Protocol. It's like a manager for assigning IP addresses to devices on a network. Here's a simple explanation:

What It Does: DHCP automatically gives devices on a network their unique IP addresses, so they can communicate with each other and the internet.

How It Works: When a device connects to the network, it sends a request to the DHCP server asking for an IP address. The DHCP server then assigns an available IP address to the device for a specific period (lease time).

Example: Imagine you join a new WiFi network at a cafe. Your device automatically gets an IP address from the cafe's DHCP server, allowing you to browse the internet and connect with other devices on the network without manually configuring anything.

11. What is ARP And How Does It Works ?

ARP stands for Address Resolution Protocol. It's a communication protocol used to map IP addresses to MAC addresses on a local network. Here's a simple explanation:

What It Does : ARP helps devices find each other's physical (MAC) addresses when only their IP addresses are known.

How It Works : When a device wants to communicate with another device on the same network, it sends out an ARP request asking, "Who has this IP address?" The device with that IP address responds with its MAC address.

Example : Imagine you want to send a message to your friend's computer in the same WiFi network. You know their IP address but need their MAC address to send the message. So, you send out an ARP request to the network asking for the MAC address corresponding to your friend's IP address. Your friend's computer receives the request and replies with its MAC address. Now, you can send the message using their MAC address.

12. What is Difference Bw Hub , Switch And Router

Feature	Router	Hub	Switch
Function	Routes data between different networks.	Broadcasts data to all connected devices.	Directs data to specific devices on a network.
Intelligence	Intelligent; makes decisions based on IP addresses.	Dumb; simply broadcasts data to all ports.	Intelligent; learns MAC addresses and forwards data accordingly.
Addressing	Uses IP addresses.	Does not understand IP addresses.	Uses MAC addresses.
Ports	Usually has fewer ports.	Can have many ports.	Can have multiple ports.
Example	Your home Wi-Fi router.	An old Ethernet hub.	A modern Ethernet switch.
Usage	Connects multiple networks in a home or office.	Rarely used due to inefficiency.	Connects devices within a local network.

13. What is Firewall And Why Its Used ?

A firewall is a security system that controls and monitors incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access while allowing legitimate communication to pass through.

Example: Imagine a firewall as a security guard at the entrance of a building. The guard checks everyone's ID before allowing them to enter. Similarly, a firewall examines data packets entering and leaving a network, allowing only authorized traffic to pass through while blocking malicious or unauthorized traffic.

14. What is NAT And why its Used ?

NAT (Network Address Translation) is a process used in computer networking to translate private IP addresses into public IP addresses and vice versa. Here's a simple explanation:

What It Is: NAT allows multiple devices in a local network to share a single public IP address when accessing the internet.

How It Works: When a device in the local network sends data to the internet, NAT changes the source IP address in the outgoing packets to the public IP address of the router. When the response

comes back, NAT translates the destination IP address back to the private IP address of the original device.

Example: Imagine you have a home network with several devices (computers, smartphones, etc.). Your router uses NAT to translate the private IP addresses of these devices into the single public IP address assigned by your internet service provider (ISP) when accessing websites or online services.

15. What Is The Difference Bw IPV4 And IPV6

Feature	IPv4	IPv6
Address Length	32 bits (4 bytes).	128 bits (16 bytes).
Address Format	Dotted-decimal format (e.g., 192.168.1.1).	Hexadecimal format separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
Address Space	Limited address space (about 4.3 billion addresses).	Vast address space (approximately 340 undecillion addresses).
Header Size	Fixed header size of 20 bytes.	Variable header size (40 bytes for basic header).
Header Fields	Contains fields like version, header length, TTL, protocol, checksum, etc.	Additional fields like flow label and extension headers.
Security Features	Relies on external security measures like IPSec.	Built-in support for IPSec.
Fragmentation	Routers perform fragmentation.	End-to-end fragmentation.

16. What Is Packet And How Does It Differ From Frame ?

A **packet** is a unit of data that is transmitted over a network. It consists of two main parts: the header, which contains control information like source and destination addresses, and the payload, which contains the actual data being transmitted.

A **frame**, on the other hand, is a unit of data at the data link layer of the OSI model. It includes the header, which contains control information like source and destination MAC addresses, and the payload, which contains the packet.

In short, a packet is a unit of data at the network layer, while a frame is a unit of data at the data link layer. Frames encapsulate packets for transmission over a network.

17. Explain Wireless Network

A wireless network is a type of computer network that allows devices to connect to the internet or communicate with each other without using wires or cables.

How it works:

Wireless networks use radio waves or infrared signals to transmit data between devices.

Devices like smartphones, laptops, tablets, and routers have builtin antennas to send and receive signals.

A wireless router acts as the central hub, transmitting data between devices and connecting them to the internet.

When a device wants to send or receive data, it sends signals to the router, which then broadcasts the data to other devices in the network.

Example:

WiFi networks in homes, cafes, and offices are common examples of wireless networks.

When you connect your smartphone to a WiFi network to browse the internet or stream videos, you're using a wireless network.

18. Explain Important Protocols in Networking

TCP/IP: Fundamental protocol for communication on the Internet and local networks.

HTTP: Used for transferring web pages and content on the World Wide Web.

HTTPS: Secure version of HTTP, providing encrypted communication over networks.

DNS: Translates domain names into IP addresses for accessing websites.

SMTP: Used for sending email messages between servers.

POP3 / IMAP: Protocols for retrieving email messages from a mail server.