Computer Architecture of Networking

Q1. What is Internet ?

The **Internet** is a global network of interconnected computer networks that allows devices worldwide to communicate and share information. It is often referred to as the "network of networks" because it connects millions of private, public, academic, business, and government networks, enabling users to access information and services, exchange data, and interact in real-time.

Key Features of the Internet:

1. **Global Connectivity**: Links billions of devices, from computers to smartphones, regardless of location.
2. **Data Sharing**: Enables the transfer of text, images, videos, and other data formats.
3. **World Wide Web (WWW)**: A primary service of the Internet, allowing access to websites and web pages through browsers.
4. **Communication**: Facilitates email, social media, instant messaging, video calls, and more.
5. **Decentralized Structure**: Operates without a central governing authority, relying on standards and protocols like TCP/IP.

How It Works:

1. **Protocols**: The Internet uses protocols like **TCP/IP** to define how data is sent, received, and understood.
2. **IP Addresses**: Every connected device has a unique identifier called an **IP address**, which helps in locating and communicating with other devices.
3. **Routers and Servers**: Data is routed through interconnected networks and stored on servers, which host websites, applications, and files.
4. **Domain Names**: Human-friendly addresses like "google.com" map to numeric IP addresses via the **Domain Name System (DNS)**.

Applications of the Internet:

- Browsing information.
- Online shopping and banking.
- Streaming music, movies, and videos.
- Remote work and learning.
- IoT (Internet of Things) for smart devices.

Q2. What is computer Networking ?

Computer Networking refers to the practice of connecting multiple computing devices together to share resources, exchange data, and communicate efficiently. These networks can involve devices like computers, servers, printers, and other hardware, enabling them to work together as a unified system.

Key Components of Computer Networking:

1. **Nodes**: Devices such as computers, phones, and servers that are part of the network.
2. **Links**: The communication pathways between nodes, which can be wired (e.g., Ethernet cables) or wireless (e.g., Wi-Fi).
3. **Protocols**: Rules and standards (like TCP/IP) that govern how data is transmitted and received.
4. **Switches and Routers**:
    - **Switch**: Connects devices within a local network (LAN).
    - **Router**: Directs data between different networks and manages Internet connections.
5. **Network Interface Card (NIC)**: Hardware in devices that enables them to connect to a network.
6. **Firewall**: A security tool to monitor and control incoming and outgoing network traffic.

Types of Computer Networks:

1. **Local Area Network (LAN)**: Covers a small area, such as a home, office, or building.
2. **Wide Area Network (WAN)**: Spans large areas, connecting devices across cities or countries (e.g., the Internet).
3. **Metropolitan Area Network (MAN)**: Covers a city or campus.
4. **Personal Area Network (PAN)**: Covers a very small area, like a single room (e.g., Bluetooth devices).
5. **Virtual Private Network (VPN)**: Extends a private network over the Internet for secure communication.

Functions of Computer Networking:

- **Resource Sharing**: Share printers, storage, and software across devices.
- **Data Communication**: Exchange information between users and systems.
- **Centralized Management**: Control and manage devices from a central point.
- **Remote Access**: Allow users to connect to the network from distant locations.

Advantages of Networking:

1. **Efficiency**: Facilitates faster and more reliable data sharing.

2. **Cost-Effectiveness**: Reduces hardware and software duplication through shared resources.
3. **Scalability**: Easily expand the network as needed.
4. **Collaboration**: Enhances teamwork through shared access to files and communication tools.

Q3. Different types of network ?

Computer networks can be categorized based on their size, purpose, and geographical spread. Here are the most common **types of networks**:

---

1. Personal Area Network (PAN)

- **Scope**: Very small, typically within a single room.
- **Purpose**: Designed for a single user to connect personal devices like smartphones, tablets, and laptops.
- **Examples**:
    - Connecting a Bluetooth headset to a phone.
    - Synchronizing a smartwatch with a mobile phone.

---

2. Local Area Network (LAN)

- **Scope**: Covers a small, localized area such as a home, office, or building.
- **Purpose**: Connects devices within a single location for resource sharing, like printers and files.
- **Features**:
    - High-speed connections.
    - Typically uses Ethernet cables or Wi-Fi.
- **Examples**:
    - Office networks.
    - Home networks for gaming or file sharing.

---

3. Metropolitan Area Network (MAN)

- **Scope**: Covers a larger area than a LAN, such as a city or a campus.
- **Purpose**: Used to connect multiple LANs for citywide or regional communication.
- **Examples**:

    - A city's public Wi-Fi network.
    - University campus networks.

---

4. Wide Area Network (WAN)

- **Scope**: Covers large geographical areas, such as countries or continents.
- **Purpose**: Connects multiple LANs and MANs over long distances, often using leased telecommunication lines.
- **Examples**:
    - The Internet (largest WAN).
    - International corporate networks.

---

5. Storage Area Network (SAN)

- **Scope**: Dedicated high-speed network for storage devices.
- **Purpose**: Provides centralized access to storage resources for servers.
- **Examples**:
    - Data centers.
    - Enterprise storage solutions.

---

6. Virtual Private Network (VPN)

- **Scope**: Virtual, spanning across public networks like the Internet.
- **Purpose**: Extends a private network over the Internet, encrypting data for secure communication.
- **Examples**:
    - Remote work connections to office servers.
    - Secure browsing on public Wi-Fi.

---

7. Wireless Local Area Network (WLAN)

- **Scope**: Similar to LAN but wireless.
- **Purpose**: Connects devices wirelessly within a small area.
- **Examples**:
    - Wi-Fi networks in homes, cafes, or airports.

---

8. Global Area Network (GAN)

- **Scope**: A network that connects WANs worldwide.
- **Purpose**: Facilitates communication and resource sharing on a global scale.
- **Example**: Satellite communication networks.

---

9. Campus Area Network (CAN)

- **Scope**: Covers a campus or group of buildings.
- **Purpose**: Connects LANs within a confined geographical area.
- **Examples**:
    - University networks.
    - Hospital networks.

---

10. Enterprise Private Network (EPN)

- **Scope**: Private networks owned and operated by a single organization.
- **Purpose**: Used by businesses to securely connect multiple locations.
- **Examples**:
    - Internal corporate networks connecting branch offices.

Comparison Table:

Type	Coverage	Example	Technology
PAN	Room-level	Bluetooth devices	Bluetooth, USB
LAN	Building-level	Office/home network	Ethernet, Wi-Fi
WLAN	Building-level	Home Wi-Fi	Wi-Fi
MAN	City-level	City-wide ISP network	Fiber optics, Ethernet
WAN	Country/continent	Internet	Fiber optics, satellites
SAN	Data center-specific	Enterprise storage	Fiber Channel
VPN	Virtual/global	Remote work networks	Encryption protocols
GAN	Worldwide	Satellite communications	Satellite technologies

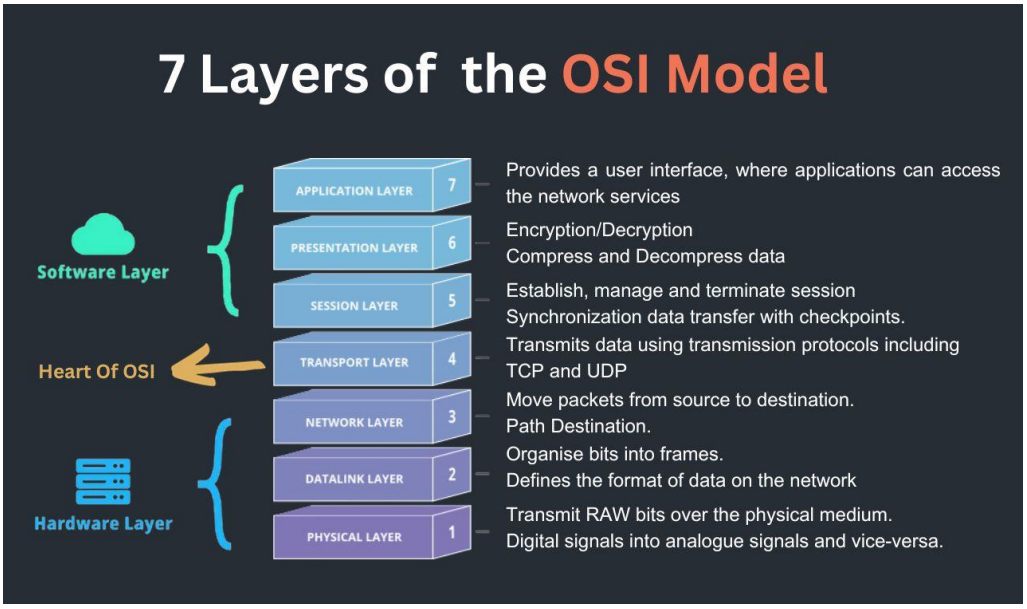
Q5. Write some network terminologies ?

General Networking Terms

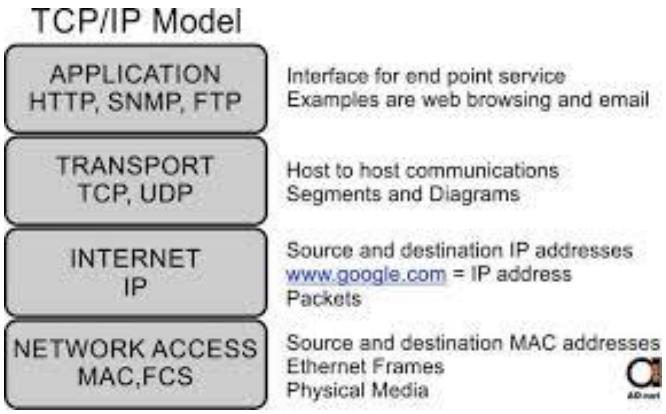
1. **Node**: Any device connected to a network, such as a computer, printer, or smartphone.
2. **Host**: A device on a network that provides services or resources (e.g., a web server).
3. **Client**: A device or application that requests resources or services from a server.
4. **Server**: A computer or device that provides resources, data, or services to other devices (clients) in the network.
5. **Protocol**: A set of rules and standards that allow devices to communicate over a network (e.g., HTTP, TCP/IP).
6. **Packet**: A small unit of data transmitted over a network.
7. **Bandwidth**: The maximum amount of data that can be transmitted over a network in a given time, usually measured in bits per second (bps).
8. **Latency**: The delay or time it takes for data to travel from the source to the destination.
9. **IP Address**: A unique identifier assigned to each device in a network (e.g., IPv4: 192.168.1.1).
10. **MAC Address**: A unique hardware address assigned to a network interface card (NIC), used for communication within a LAN.

Networking Models and Architectures

1. **OSI Model**: A framework with seven layers (Physical, Data Link, Network, Transport, Session, Presentation, Application) that standardize network communication.



2. **TCP/IP Model**: A simplified networking model used for the Internet with four layers (Link, Internet, Transport, Application).



3. **LAN**: Local Area Network; a network confined to a small area, such as a home or office.
4. **WAN**: Wide Area Network; a network spanning large geographical areas, like the Internet.

Network Devices

1. **Router**: A device that forwards data packets between networks, enabling Internet connectivity.
2. **Switch**: A device that connects devices within a LAN and manages data transmission.
3. **Hub**: A simple network device that connects devices and broadcasts data to all ports.
4. **Access Point (AP)**: A device that provides wireless connectivity to devices within a network.
5. **Firewall**: A security device or software that monitors and controls incoming and outgoing traffic based on predefined rules.

Security and Authentication

1. **Firewall**: A system that protects a network by controlling incoming and outgoing traffic.
2. **VPN (Virtual Private Network)**: A secure connection that encrypts data and allows remote access to a network.
3. **SSL/TLS**: Encryption protocols used to secure communication over the Internet (e.g., HTTPS).
4. **Authentication**: The process of verifying the identity of a user or device before granting access.
5. **Encryption**: The process of encoding data to prevent unauthorized access.

Data Transmission

1. **DNS (Domain Name System)**: Translates human-readable domain names (e.g., google.com) into IP addresses.
2. **DHCP (Dynamic Host Configuration Protocol)**: Assigns IP addresses dynamically to devices on a network.

3. **HTTP/HTTPS**: Protocols used for transferring web pages (HTTPS is secure with encryption).
4. **FTP (File Transfer Protocol)**: A protocol used for transferring files over a network.
5. **Ping**: A tool used to test the reachability and response time of a device on a network.

Wireless Networking

1. **SSID (Service Set Identifier)**: The name of a wireless network.
2. **WEP/WPA/WPA2**: Security protocols used to protect wireless networks.
3. **Wi-Fi**: A technology that allows wireless networking within a limited area.
4. **Bluetooth**: A wireless technology for short-range communication between devices.

Network Configurations

1. **Subnet**: A smaller network created within a larger network, separated for organizational or security purposes.
2. **Gateway**: A device that connects two different networks, often providing access to the Internet.
3. **Proxy Server**: Acts as an intermediary between a client and a server to enhance security, control, or caching.

Performance and Metrics

1. **Throughput**: The actual amount of data successfully transmitted over a network in a given time.
2. **Jitter**: The variation in time delay for data packets during transmission.
3. **Collision**: Occurs when two devices attempt to send data over the network simultaneously.

Q 6. WRITE AND EXPLAIN THE NETWORK TOPOLOGY TYPES:

ANSWER:

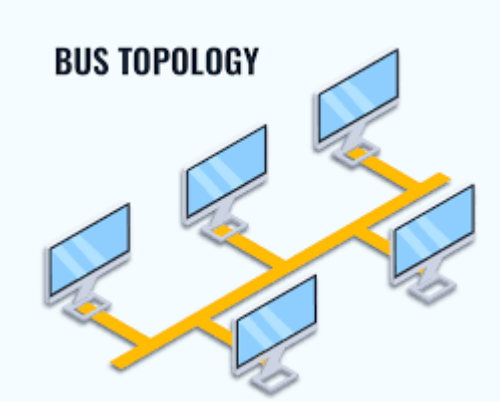
Network Topologies: A Visual Guide

Network topology refers to the physical or logical arrangement of devices in a network. The choice of topology impacts factors like performance, reliability, and cost. Here are some common network topologies:

1. Bus Topology

- **Description:** Devices are connected to a single cable, like computers on a bus.
- **Advantages:** Simple to implement, inexpensive.

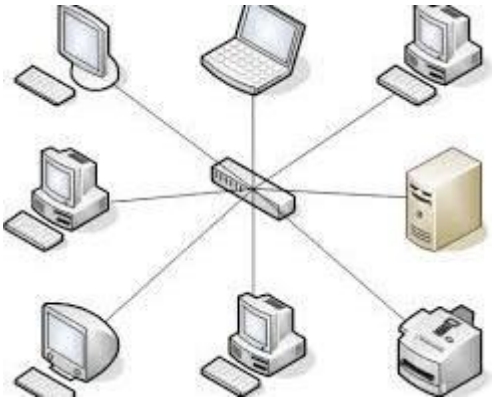
- **Disadvantages:** Single point of failure, limited scalability.



Bus Topology

2. Star Topology

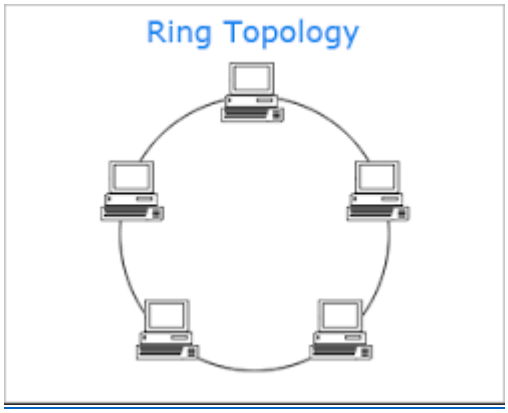
- **Description:** Devices are connected to a central hub or switch.
- **Advantages:** Easy to add or remove devices, centralized management, fault isolation.
- **Disadvantages:** Reliance on the central device.



Star Topology

3. Ring Topology

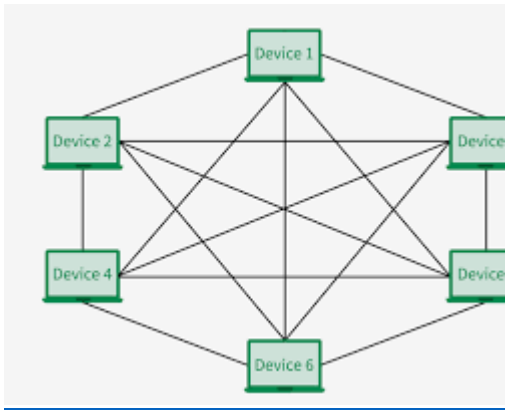
- **Description:** Devices are connected in a circular fashion, with each device connected to two neighbors.
- **Advantages:** High bandwidth, fault tolerance.
- **Disadvantages:** Complex installation, failure of one device can affect the entire network.



Ring Topology

4. Mesh Topology

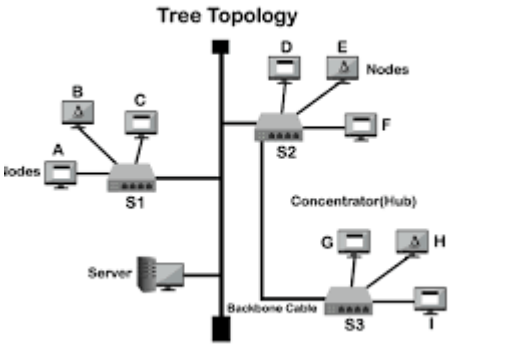
- **Description:** Every device is connected to every other device.
- **Advantages:** High reliability, fault tolerance, high bandwidth.
- **Disadvantages:** Expensive to implement, complex to manage.



Mesh Topology

5. Tree Topology

- **Description:** Hierarchical structure, with a root node branching out to multiple levels.
- **Advantages:** Scalable, organized, easy to troubleshoot.
- **Disadvantages:** Reliance on the root node.



Tree Topology

Choosing the Right Topology The choice of topology depends on factors like:

- **Network size:** Smaller networks may benefit from simpler topologies like bus or star. Larger networks might require more robust topologies like mesh or tree.
- **Performance:** Mesh and star topologies generally offer better performance due to multiple paths for data transmission.
- **Reliability:** Mesh and ring topologies are more fault-tolerant as they have multiple paths for data to flow.
- **Cost:** Bus topology is generally the most cost-effective, while mesh topology is the most expensive.
- **Scalability:** Star and tree topologies are more scalable as devices can be easily added or removed.