Computer Network: A computer network is a system of interconnected devices that communicate and share resources such as files, data, applications, and hardware like printers and servers. These networks can be wired or wireless and range from small, localized setups like a home or office network to extensive global systems like the internet. Networks operate using protocols, such as TCP/IP, to ensure seamless communication between devices. Depending on the scope and scale, networks are categorized into types like LAN (Local Area Network), WAN (Wide Area Network), or MAN (Metropolitan Area Network), enabling diverse functionalities such as collaboration, remote access, and data sharing.

Need of Computer Network: The need for computer networks arises from the growing demand for efficient communication and resource sharing in both personal and professional settings. They enable quick and seamless data transfer between users, facilitate collaboration through shared tools, and centralize resources like storage and printers, reducing redundancy and costs. Networks also support critical applications like cloud computing, remote work, and real-time communication, making them indispensable in today's connected world. By linking devices together, networks improve efficiency, scalability, and reliability, supporting modern demands for instant information access and global connectivity.

Network Architecture Models: Network architecture models define the framework and principles that dictate how devices in a network communicate and share resources. The two primary network architecture models are Peer-to-Peer (P2P) and Client-Server.

Peer-to-Peer Model (P2P): In this decentralized model, all devices, or nodes, are equal and can act as both clients and servers. Each node can initiate or respond to communication without relying on a central server. P2P networks are simple to set up and are commonly used in small-scale environments or for file-sharing applications, but they may lack security and scalability for larger systems.

Client-Server Model: This model features a centralized server that manages resources, data, and communication for multiple client devices. Clients request services, and the server processes and fulfills those requests. The client-server model is highly scalable, secure, and reliable, making it ideal for enterprise environments, web applications, and cloud-based systems.

Both models serve specific purposes, and the choice between them depends on factors like the size, complexity, and requirements of the network. Modern systems often combine elements of both to optimize performance and resource management.

Network Types: Networks are categorized based on their size, scope, and purpose, enabling various applications from small home setups to global communication. The primary network types are:

Local Area Network (LAN): LANs connect devices within a limited geographical area, such as an office, school, or home. They are typically used for resource sharing, such as printers and files, and provide high-speed connections. LANs are cost-effective and easy to manage, making them ideal for small-scale networks.

Metropolitan Area Network (MAN): MANs cover a larger area than LANs, such as a city or campus. They are used to connect multiple LANs using high-speed technologies like fiber optics. MANs are suitable for organizations that need to interlink offices in a specific region.

Wide Area Network (WAN): WANs span vast geographical areas, often connecting cities, countries, or continents. The internet is the largest example of a WAN. They rely on public or private telecommunications infrastructure and are used for global communication and resource sharing.

Personal Area Network (PAN): PANs are small networks designed for individual use, typically within a range of a few meters. They connect personal devices such as smartphones, laptops, and wearables using Bluetooth, Wi-Fi, or USB.

Campus Area Network (CAN): CANs connect multiple LANs within a limited geographical area, such as a university campus or business park. They are optimized for high performance within the campus and may rely on private infrastructure.

Storage Area Network (SAN): SANs are specialized networks that provide high-speed access to storage devices. They are used in enterprise environments for efficient and reliable data storage and management.

Topologies: Network topology refers to the physical or logical arrangement of devices (nodes) and connections in a network. It determines how data flows between devices, impacting performance, scalability, and fault tolerance. Common types of network topologies include:

Bus Topology: All devices are connected to a single central cable (the bus). Data travels along the cable, and each device checks if the data is intended for it. This topology is simple and cost-effective for small networks but can face performance bottlenecks and single points of failure.

Star Topology: Devices are connected to a central hub or switch. The hub acts as a communication point for all data exchanges. Star topology is highly reliable since failure in one device does not affect others, but the hub itself is a critical point of failure.

Ring Topology: Devices are connected in a closed loop, with each device linked to its two nearest neighbors. Data travels in one direction until it reaches its destination. While this topology ensures data consistency, a single point of failure can disrupt the entire network unless a dual-ring is used for redundancy.

Mesh Topology: Each device is connected to every other device in the network, either fully (all devices interconnected) or partially (selected devices interconnected). Mesh topology offers high reliability and fault tolerance but is expensive and complex to implement due to the large number of connections.

Tree Topology: Also known as hierarchical topology, it combines characteristics of star and bus topologies. Devices are arranged in a hierarchical structure with a central "root" node connected to multiple levels of subordinate nodes. Tree topology is scalable but dependent on the root node for stability.

Hybrid Topology: This topology combines two or more different topologies to create a flexible and scalable network. For example, a network may use a star topology in one section and a bus topology in another.

The choice of topology depends on factors like the size of the network, cost, scalability, fault tolerance, and ease of maintenance.

IP: An IP (Internet Protocol) address is a unique numerical identifier assigned to each device connected to a network. It enables devices to locate and communicate with each other over the internet or local networks. IP addresses function as virtual addresses, much like a home address, ensuring data is sent to the correct destination.There are two main versions of IP addresses:

IPv4 (Internet Protocol Version 4): The most commonly used version, IPv4 uses a 32-bit addressing scheme, allowing for approximately 4.3 billion unique addresses. An IPv4 address is represented in dotted-decimal format, such as 192.168.1.1.

IPv6 (Internet Protocol Version 6): Developed to address the limitations of IPv4, IPv6 uses a 128-bit addressing scheme, providing a vastly larger address pool. IPv6 addresses are represented in hexadecimal format, separated by colons, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

IP addresses are further classified into types:**Public IP**: Assigned by an Internet Service Provider (ISP), these addresses are unique and accessible over the internet.

Private IP: Used within private networks, such as homes or offices, and not routable on the internet.

Static IP: Fixed and manually assigned, often used for servers or devices requiring a consistent address

.**Dynamic IP**: Automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server and can change over time. **CLASSES:** addresses are divided into five classes (A, B, C, D, and E) based on their range and intended use:**Class A** (1.0.0.0 to 127.255.255.255): Used for large networks, with a default subnet mask of 255.0.0.0. Class A supports over 16 million hosts on a single network.**Class B** (128.0.0.0 to 191.255.255.255): Designed for medium-sized networks, with a default subnet mask of 255.255.0.0, allowing for up to 65,000 hosts.**Class C** (192.0.0.0 to 223.255.255.255): Commonly used for small networks, with a default subnet mask of 255.255.255.0, supporting up to 254 hosts.**Class D** (224.0.0.0 to 239.255.255.255): Reserved for multicast addresses, used for sending data to multiple recipients.**Class E** (240.0.0.0 to 255.255.255.255): Reserved for experimental purposes and future use, not used in standard network configurations.

Interconnectivity Devices: Interconnectivity devices are hardware components used to connect and enable communication between different parts of a network. These devices ensure data flows efficiently between devices, networks, and systems, playing a vital role in modern networking. Below are common types of interconnectivity devices:

Hub:A hub is a basic networking device that connects multiple devices in a network. It broadcasts data received from one device to all others connected to it. Hubs work at the physical layer of the OSI model and are suitable for small, simple networks.

Switch:A switch connects multiple devices within a local area network (LAN) and forwards data to the intended recipient based on MAC addresses. It provides efficient and secure communication compared to a hub. Switches operate at the data link layer (Layer 2) or network layer (Layer 3) in managed versions.

Router:A router connects different networks and routes data packets based on IP addresses. It enables communication between devices and provides internet access. Routers operate at the network layer (Layer 3) and offer features like dynamic routing and network security.

Modem:A modem (modulator-demodulator) converts digital signals to analog for transmission over telephone or cable lines and vice versa. It connects a device or network to the internet. Modems operate at the physical and data link layers.

Access Point: An access point provides wireless connectivity by extending a wired network. It allows devices like laptops and smartphones to connect wirelessly. Access points are commonly used in Wi-Fi networks to enhance coverage.

Gateway:A gateway connects two networks with different protocols, translating data between them. It enables communication between incompatible networks, such as a LAN and the internet. Gateways can operate across all OSI layers depending on the application.

Bridge:A bridge connects two local area network (LAN) segments, making them function as a single network. It filters and forwards traffic to improve network performance. Bridges operate at the data link layer (Layer 2).

Repeater:A repeater amplifies and regenerates weak signals to extend the range of a network. It ensures data integrity and prevents signal loss over long distances. Repeaters work at the physical layer (Layer 1) of the OSI model.

OSI Model

The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and implement network communication between systems. It divides the communication process into seven distinct layers, each with specific functions:

Physical Layer (Layer 1):
This layer deals with the physical connection between devices, including cables, switches, and the transmission of raw binary data over physical mediums (electrical signals, radio waves, etc.).

Data Link Layer (Layer 2):
The data link layer ensures reliable data transfer over the physical layer. It handles error detection, correction, and the framing of data. Devices like switches and network interface cards (NICs) operate at this layer.

Network Layer (Layer 3):
Responsible for routing data across different networks, the network layer uses IP addresses to determine the best path for data to travel. Routers work at this layer.

Transport Layer (Layer 4):
The transport layer ensures reliable data transfer by providing error recovery and flow control. It divides data into smaller packets and ensures they arrive in the correct order. Protocols like TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) operate here.

Session Layer (Layer 5):
The session layer manages sessions or connections between applications. It ensures that data exchange occurs in an organized and synchronized manner, handling issues like session establishment, maintenance, and termination.

Presentation Layer (Layer 6):
This layer translates data into a format that the application layer can understand. It deals with data encryption, compression, and translation between different data formats (e.g., converting ASCII to EBCDIC).

Application Layer (Layer 7):
The topmost layer, it interacts directly with end-user applications. It provides network services to applications like web browsers (HTTP), email (SMTP), and file transfer (FTP).

TCP/IP Model

The **TCP/IP (Transmission Control Protocol/Internet Protocol) model** is a simpler, more streamlined model used to describe the networking protocols used on the internet. Unlike the OSI model, which has seven layers, the TCP/IP model consists of **four layers**:

Network Interface Layer (Link Layer):
This corresponds to the OSI's physical and data link layers. It deals with the physical transmission of data and the protocols for communication within a network segment.

Internet Layer:
This layer corresponds to the OSI's network layer. It handles logical addressing, routing, and the delivery of data across multiple networks. The primary protocol at this layer is **IP (Internet Protocol)**.

Transport Layer:
Similar to the OSI model's transport layer, this layer ensures reliable data transfer between devices. It includes protocols like **TCP (Transmission Control Protocol)** for connection-oriented communication and **UDP (User Datagram Protocol)** for connectionless communication.

Application Layer:
The top layer of the TCP/IP model, which directly interfaces with the end-user applications. It includes all protocols that support application-level communication, such as **HTTP**, **FTP**, **SMTP**, and **DNS**. This layer combines the functionality of the OSI's application, presentation, and session layers.

Key Differences between OSI and TCP/IP Models:

- **Layer Count**: OSI has 7 layers, while TCP/IP has 4 layers.
- **Protocol Focus**: OSI is a theoretical model, while TCP/IP is practical and based on real-world protocols.
- **Development**: OSI was developed by ISO, while TCP/IP was developed by DARPA for the ARPANET and later became the foundation of the internet.