A computer network is a system of interconnected computers and devices that communicate and share resources using communication protocols over wired or wireless media.

LAN (Local Area Network): Covers up to 1 km; used in homes, schools, or offices.

MAN (Metropolitan Area Network): Covers 1–100 km; spans cities or large campuses.

WAN (Wide Area Network): Covers over 100 km; connects devices across countries or continents.

PAN (Personal Area Network): Range up to 10 meters; used for connecting personal devices like smartphones, laptops, etc.

CAN (Campus Area Network): Range up to 1–5 km; connects multiple LANs within a campus like a university or business park.

Network topologies refer to the physical or logical arrangement of devices in a computer network, defining how they are connected and how data flows between them.

1. **Bus Topology: All devices share a single communication line; cheap but prone to collisions.**
2. **Star Topology: All devices connect to a central hub; easy to manage, but hub failure affects entire network.**
3. **Ring Topology: Devices connected in a circular loop; data travels in one direction; one failure can affect the whole network.**
4. **Mesh Topology: Every device connects to every other; high reliability and fault tolerance.**
5. **Tree Topology: Combination of star and bus; hierarchical and scalable.**
6. **Hybrid Topology: Mix of two or more topologies; flexible and widely used.**

Transmission Modes

Simplex: Data flows in one direction only (e.g., keyboard to CPU).

Half-Duplex: Data flows in both directions, but one at a time (e.g., walkie-talkies).

Full-Duplex: Data flows in both directions simultaneously (e.g., telephone).

The OSI (Open Systems Interconnection) model is a 7-layer framework that standardizes network communication:

1. **Physical – Transmits raw bits (cables, signals)**
2. **Data Link – Error detection, MAC addressing**
3. **Network – Routing, IP addressing**

4. **Transport – Reliable data transfer (TCP/UDP)**
5. **Session – Manages sessions between applications**
6. **Presentation – Data translation, encryption, compression**
7. **Application – Interface for end-user services (HTTP, FTP)**

The TCP/IP model is a 4-layer networking framework used for the internet:

1. **Application Layer – Provides network services to users (HTTP, FTP, DNS)**
2. **Transport Layer – Ensures reliable data delivery (TCP) or fast delivery (UDP)**
3. **Internet Layer – Handles addressing and routing (IP)**
4. **Network Access Layer – Manages physical transmission over the network (Ethernet, Wi-Fi)**

Difference between OSI and TCP/IP Models (Paragraph-wise for 2 marks):

The **OSI model** has 7 layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. It is a **theoretical model** developed by ISO to standardize network communication.

The **TCP/IP model** has 4 layers: Network Access, Internet, Transport, and Application. It is a **practical model** developed by the U.S. Department of Defense and is used widely on the internet.

While OSI is **protocol-independent** and focuses on clear layer separation, TCP/IP is **protocol-oriented**, designed around standard internet protocols like TCP and IP.

The Data Link Layer is the 2nd layer of the OSI model. It is responsible for node-to-node communication, framing, error detection, and MAC addressing. It ensures reliable data transfer over the physical link by detecting and sometimes correcting errors from the Physical Layer.

Functions of Data Link Layer:

1. **Framing: Divides the data into frames for easier transmission.**
2. **Error Detection and Correction: Detects and sometimes corrects errors using techniques like CRC.**
3. **Flow Control: Manages data flow to prevent congestion.**
4. **MAC Addressing: Adds physical (MAC) addresses for node-to-node delivery.**
5. **Access Control: Determines which device has control over the channel in shared media.**

Byte Stuffing:
Byte stuffing is a technique used in data link layer to differentiate data from control information. A special byte (usually `ESC`) is inserted before any byte in the data that matches the flag byte (e.g., `FLAG`) used to mark the start and end of a frame.

Byte Unstuffing:
At the receiver's end, byte unstuffing removes the extra `ESC` bytes to recover the original data, ensuring correct interpretation.

Error Detection Techniques:

1. **Parity Bit:** Adds an extra bit to make the number of 1s even (even parity) or odd (odd parity).
2. **Checksum:** Sums data segments and sends the result for error checking at the receiver.
3. **Cyclic Redundancy Check (CRC):** Uses polynomial division to detect burst errors.
4. **Longitudinal Redundancy Check (LRC):** Applies parity check on blocks of data.

Error Correction Techniques:

1. **Hamming Code:** Detects and corrects single-bit errors using redundant bits.
2. **Reed-Solomon Code:** Corrects burst errors; used in CDs, DVDs, and QR codes.
3. **Forward Error Correction (FEC):** Adds redundant data so the receiver can correct errors without retransmission.

Pure ALOHA:

- Users transmit data whenever they want without checking the channel.
- High chance of collisions; efficiency is about **18.4%**.
- Simpler but less efficient.

Slotted ALOHA:

- Time is divided into equal slots; data is sent only at the beginning of a slot.
- Reduces collisions; efficiency is about **36.8%**.
- More efficient than Pure ALOHA but needs time synchronization.

Stop and Wait ARQ is an error control protocol in which the sender transmits one frame at a time and waits for an acknowledgment (ACK) before sending the next frame.

If the ACK is not received within a timeout, the sender retransmits the same frame. It ensures reliable data transfer but is inefficient for high-latency networks due to idle waiting time.

Selective Repeat ARQ is an error control protocol where the sender can send multiple frames before needing an acknowledgment, but only the erroneous or lost frames are retransmitted.

The receiver stores frames in a buffer and sends ACKs for correctly received ones. This method improves efficiency by avoiding unnecessary retransmissions, especially in noisy channels.

Go-Back-N ARQ is an error control protocol where the sender can transmit multiple frames (up to a window size) without waiting for individual ACKs.

If an error is detected or a frame is lost, the receiver discards that frame and all subsequent frames. The sender then **goes back** and retransmits from the erroneous frame onward. It is simpler than Selective Repeat but less efficient.

Circuit Switching is a communication method where a dedicated communication path is established between sender and receiver before data transfer begins.

Packet Switching is a communication method where data is divided into small packets, each transmitted independently over the network.

Packets may take different paths and are reassembled at the destination. It is efficient, supports multiple users, and is used in the internet, but may cause delays and packet loss.

Network Layer is the 3rd layer of the OSI model. It is responsible for **routing**, **logical addressing (IP addresses)**, and **packet forwarding** between devices across different networks.

It ensures that data is sent from the source to the destination, even if they are on different networks. Key protocols include **IP**, **ICMP**, and **ARP**.

Switch: Operates at Data Link Layer; connects devices in a LAN and forwards data based on MAC addresses.

Router: Operates at Network Layer; routes data between different networks using IP addresses.

Repeater: Operates at Physical Layer; regenerates and amplifies signals to extend network range.

Hub: Operates at Physical Layer; broadcasts data to all devices, no filtering or addressing.

Bridge: Operates at Data Link Layer; connects two LANs and filters traffic using MAC addresses.

Gateway: Operates at all layers; connects different networks using different protocols (e.g., LAN to internet).

Functions of Network Layer:

1. **Routing:** Determines the best path for data to travel from source to destination.
2. **Logical Addressing:** Assigns IP addresses to devices for unique identification across networks.
3. **Packet Forwarding:** Moves packets from one node to another toward the destination.
4. **Fragmentation and Reassembly:** Breaks large packets into smaller ones and reassembles them at the destination.
5. **Error Handling and Diagnostics:** Uses protocols like ICMP to report errors and provide network diagnostics.

IPv4 (Internet Protocol version 4) is the fourth version of the Internet Protocol used to identify devices on a network using a 32-bit address.

It provides around **4.3 billion unique addresses**, written in **dotted decimal format** (e.g., 192.168.0.1). IPv4 supports packet routing, fragmentation, and addressing but has limited address space, leading to the development of IPv6.

IPv6 (Internet Protocol version 6) is the latest version of the Internet Protocol designed to replace IPv4.

It uses **128-bit addresses**, allowing a vastly larger number of unique IP addresses (2^{128}). IPv6 is written in **hexadecimal format** (e.g., 2001:0db8::1), supports **better security**, **simplified headers**, and eliminates the need for NAT (Network Address Translation).

Network address - It identifies a network on internet. Using this, we can find range of addresses in the network and total possible number of hosts in the network.

Mask - It is a 32-bit binary number that gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.

The default mask in different classes are :

Class A - 255.0.0.0

Class B - 255.255.0.0

Class C - 255.255.255.0

Classless Addressing is a method of IP addressing where addresses are not divided into fixed classes (A, B, C).

It uses **CIDR (Classless Inter-Domain Routing)** notation, like 192.168.1.0/24, where /24 indicates the number of bits used for the network part.

This allows more efficient IP address allocation and reduces wastage compared to classful addressing.

Subnetting is the process of dividing a large IP network into smaller, manageable **sub-networks (subnets)**.

It improves network efficiency, security, and organization by separating devices into different groups. Subnetting uses a **subnet mask** to determine the network and host portions of an IP address

Network Address Translation (NAT) is a technique used to map **private IP addresses** within a local network to a **single public IP address** before sending data to the internet.

It helps conserve public IP addresses and adds a layer of security by hiding internal network details from external users.

Classless Inter-Domain Routing (CIDR) is an IP addressing method that replaces traditional class-based addressing.

It uses **prefix notation** (e.g., 192.168.1.0/24) to define the number of bits in the network portion, allowing **flexible allocation** of IP addresses and reducing wastage. CIDR improves **routing efficiency** and supports **subnetting and supernetting**.

Transport Layer is the 4th layer of the OSI model. It is responsible for **end-to-end communication**, **reliable data transfer**, **flow control**, and **error control** between source and destination systems.

Key protocols include:

- **TCP (Transmission Control Protocol):** Reliable, connection-oriented.
- **UDP (User Datagram Protocol):** Unreliable, connectionless, faster.

Functions of Transport Layer:

1. **Segmentation and Reassembly:** Divides large data into smaller segments and reassembles them at the receiver.
2. **End-to-End Communication:** Ensures complete data transfer between sender and receiver.
3. **Flow Control:** Prevents sender from overwhelming the receiver with too much data.
4. **Error Control:** Ensures error-free delivery using acknowledgment and retransmission.
5. **Connection Control:** Manages connection setup, maintenance, and termination (in TCP).
6. **Multiplexing:** Allows multiple applications to use the network simultaneously using port numbers.

TCP (Transmission Control Protocol) is a **connection-oriented** and **reliable** transport layer protocol.

It ensures **error-free**, **ordered**, and **complete delivery** of data using acknowledgments, sequencing, and retransmissions. TCP is used in applications like **HTTP, FTP, and Email** where reliability is critical.

UDP (User Datagram Protocol) is a **connectionless** and **unreliable** transport layer protocol.

It sends data without acknowledgments or retransmissions, making it **faster** but less reliable than TCP. UDP is used in applications like **video streaming, online gaming, and DNS**, where speed is more important than reliability.

Application Layer is the **7th and topmost layer** of the OSI model. It provides **network services directly to users and applications**.

It enables functions like **email (SMTP)**, **file transfer (FTP)**, and **web browsing (HTTP)**. It also handles data formatting, user authentication, and network resource access.

Functions of Application Layer:

1. **User Interface:** Provides services directly to user applications.
2. **Resource Sharing:** Allows access to remote files and printers.

3. **Email Services:** Supports email protocols like SMTP, POP3.
4. **File Transfer:** Enables file sharing using protocols like FTP.
5. **Web Services:** Provides access to websites using HTTP/HTTPS.
6. **Network Management:** Assists in managing and monitoring network operations.

HTTP (HyperText Transfer Protocol) is an **application layer protocol** used for **transferring web pages** and other resources over the internet.

It is a **stateless**, **request-response** protocol where a client (browser) sends a request and the server responds with data (like HTML, images, etc.). It typically uses **port 80** (or 443 for HTTPS).

HTTPS (HyperText Transfer Protocol Secure) is the **secure version of HTTP** that uses **SSL/TLS encryption** to protect data during transmission.

It ensures **confidentiality**, **integrity**, and **authentication** of data between client and server. HTTPS typically uses **port 443**.

TELNET (Terminal Network) is an **application layer protocol** used for **remote login and command execution** on another computer over a network.

It provides a **text-based interface** but transmits data in **plain text**, making it insecure. It typically uses **port 23** and is largely replaced by **SSH** for secure communication.

FTP (File Transfer Protocol) is an **application layer protocol** used to **transfer files** between a client and a server over a network.

It supports **uploading, downloading, renaming, and deleting files** and typically uses **port 21**. FTP is not secure by default, so **FTPS** or **SFTP** is preferred for secure file transfers.

SMTP (Simple Mail Transfer Protocol) is an **application layer protocol** used to **send and forward emails** between mail servers.

It works over **port 25** (or 587 for secure transmission) and is used only for **sending** emails, not receiving. For receiving, protocols like **POP3** or **IMAP** are used.

DNS (Domain Name System) is an **application layer protocol** that translates **domain names** (like www.example.com) into **IP addresses** (like 192.0.2.1).

It acts like the internet's phonebook and typically works over **port 53**. DNS allows users to access websites using easy-to-remember names instead of numeric IPs.

DHCP (Dynamic Host Configuration Protocol) is an **application layer protocol** used to **automatically assign IP addresses** and other network configuration settings (like subnet mask, gateway, DNS) to devices on a network.

Purpose of Each Class of IP Network:

1. **Class A**
    - **Range:** 1.0.0.0 to 126.0.0.0
    - **Purpose:** Designed for **very large networks** (e.g., multinational companies)
    - **Hosts per network:** ~16 million
2. **Class B**
    - **Range:** 128.0.0.0 to 191.255.0.0
    - **Purpose:** Used for **medium-sized networks** (e.g., universities, large businesses)
    - **Hosts per network:** ~65,000
3. **Class C**
    - **Range:** 192.0.0.0 to 223.255.255.0
    - **Purpose:** Intended for **small networks** (e.g., small businesses)
    - **Hosts per network:** 254
4. **Class D**
    - **Range:** 224.0.0.0 to 239.255.255.255
    - **Purpose:** Used for **multicasting** (sending data to a group of systems)
5. **Class E**
    - **Range:** 240.0.0.0 to 255.255.255.255
    - **Purpose: Reserved** for **experimental and research** purposes.

Data Rate in terms of transmission refers to the **amount of data transmitted per unit time** over a communication channel.

Intradomain Routing Algorithm is used to determine the best path for data **within a single autonomous system (AS)** or network domain. E.g Distance Vector Routing, Link State Routing.

VPN (Virtual Private Network) is a technology that creates a **secure and encrypted connection** over a public network (like the Internet), allowing users to **safely access private networks** remotely.

Piggybacking in networking refers to the technique where the **acknowledgment (ACK)** of received data is **combined with outgoing data** in the same frame.

The **ARP (Address Resolution Protocol)** is used to get the **MAC address** corresponding to a given **IP address** within a local network.

The **Transport Layer** is responsible for **host-to-host delivery** of data in the OSI model.

A **Firewall** is a **network security system** that monitors and controls **incoming and outgoing network traffic** based on **predefined security rules**.

It acts as a **barrier** between a trusted internal network and untrusted external networks (like the internet), helping to **prevent unauthorized access**.