# NETWORKS

**Q1) What is a computer Network? What are the advantages and disadvantages of using a computer network?**

**A computer network is a collection of interconnected computers and other devices that can communicate and share resources with each other. These networks can be as small as a couple of computers in a home or office or as large as a global network like the Internet. Computer networks are essential in modern computing because they enable data sharing, communication, and resource access among connected devices.**

## Advantages of using a computer network:

**Resource Sharing: Networks allow multiple users to share hardware resources such as printers, scanners, and storage devices. This reduces costs and makes efficient use of resources.**

**Data Sharing: Users on a network can easily share files and data, making collaboration and information exchange more straightforward.**

**Communication: Networks enable real-time communication through email, instant messaging, video conferencing, and VoIP (Voice over Internet Protocol) services, improving connectivity and collaboration.**

**Centralized Data Management: In a network, data can be centrally stored and managed, making it easier to back up, secure, and maintain data integrity.**

**Remote Access: Networks allow remote access to resources and data, enabling users to work from different locations and access their work-related information.**

**Scalability: Networks can be scaled up or down easily to accommodate growing or changing needs, making them flexible and adaptable.**

**Cost-Efficiency: Sharing resources and centralizing management can reduce costs associated with hardware and software.**

**Security: Networks can implement security measures such as firewalls, encryption, and access control to protect data and devices from unauthorized access.**

**Automation: Network management tools and protocols can automate tasks like software updates, monitoring, and troubleshooting, reducing administrative overhead.**

## Disadvantages of using a computer network:

**Security Concerns: Networks are vulnerable to security breaches, including hacking, malware, and data theft. Protecting networked systems is a constant challenge.**

**Complexity: Setting up and maintaining a network can be complex, requiring specialized knowledge and expertise. This complexity can result in higher costs.**

**Maintenance: Networks require regular maintenance to ensure optimal performance, which can be time-consuming and costly.**

**Downtime: Network failures or maintenance can lead to downtime, which can disrupt operations and productivity.**

**Compatibility Issues**: **Different devices and software on a network may not always be compatible, leading to integration challenges.**

**Privacy Concerns: In shared networks, there may be concerns about privacy, as others on the network could potentially access sensitive information**.

**Data Loss: Centralized data storage can pose a risk if there's a failure in the central server or storage device, potentially resulting in data loss.**

**Bandwidth Limitations**: **Network performance can suffer if there isn't enough bandwidth to handle the data traffic, leading to slowdowns and congestion**.

**Dependence on Infrastructure: Networks rely on physical infrastructure like cables and routers, which can be vulnerable to damage or natural disasters.**

**In summary, computer networks offer numerous advantages in terms of resource and data sharing, communication, and efficiency. However, they also come with challenges related to security, complexity, and maintenance. The benefits of a network typically outweigh the drawbacks, but careful planning and management are necessary to ensure a successful and secure network environment.**

**Q2) What are the features of LAN, MAN, and WAN?**

**LAN (Local Area Network), MAN (Metropolitan Area Network), and WAN (Wide Area Network) are three types of computer networks that differ in terms of their geographic scope and the features they offer. Here are the key features of each:**

**Local Area Network (LAN)**:

**1. Geographic Scope**: **LANs typically cover a relatively small geographic area, such as a single building, office, or campus.**
**2. Ownership: LANs are usually privately owned and operated by an organization or individual.**
**3. Data Transfer Rate: LANs offer high data transfer rates, often in the range of gigabits per second (gbps).**

**4. Topology: LANs commonly use bus, star, or ring topologies, depending on the specific network design.**
**5. Components: LANs typically include devices like computers, servers, switches, and routers, all connected within a confined area.**
**6. Distance: LANs have limited distance coverage, typically up to a few kilometers at most.**
**7. Use Cases: LANs are ideal for connecting devices within a single building or campus, enabling fast data transfer and resource sharing. They are commonly used in homes, offices, schools, and small businesses**.

**Metropolitan Area Network (MAN):**

**1. Geographic Scope: MANs cover a larger geographic area than LANs but are smaller in scope compared to WANs. They typically span a city or a large metropolitan area.**
**2. Ownership: MANs can be owned and operated by a single organization or multiple organizations working together.**
**3. Data Transfer Rate: MANs offer moderate to high data transfer rates, typically in the range of megabits to gigabits per second.**
**4. Topology: The topology of a MAN can vary, including ring, star, or mesh configurations.**
**5. Components: MANs may include various network devices, including routers, switches, and fiber optic cables, to connect different parts of a city.**
**6. Distance: The distance coverage of a MAN can range from a few kilometers to tens of kilometers.**
**7. Use Cases: MANs are used to interconnect LANs within a city, enabling data exchange and resource sharing among different locations of a large organization or between multiple organizations.**

**Wide Area Network (WAN):**

**1. Geographic Scope: WANs cover a large geographic area, often spanning across cities, countries, or even continents.**
**2. Ownership: WANs can be owned and operated by private organizations, telecommunications companies, or public entities.**
**3. Data Transfer Rate: WANs can offer varying data transfer rates, which may range from kilobits per second (Kbps) to gigabits per second (Gbps), depending on the technology used and the network's size.**
**4. Topology: WANs typically use complex mesh or star topologies to interconnect a vast number of devices and networks.**
**5. Components: WANs comprise a wide range of components, including routers, switches, and leased lines, satellites, and undersea cables, to facilitate long-distance communication.**
**6. Distance: WANs can cover vast distances, making them suitable for connecting remote locations and providing global connectivity.**

**7. Use Cases: WANs are used for global data communication, connecting remote offices, data centers, and facilitating internet access. The internet itself is an example of a global WAN.**

**In summary, LANs are small-scale networks used for local connectivity, MANs cover larger areas within a city, and WANs span extensive geographic regions to provide long-distance communication. The choice of network type depends on the specific requirements of the organization or application in question.**

**Q3) Features, Advantages, and Disadvantages of Various Topologies:**

**Star Topology: Features**

- **In a star topology, all devices in the network are connected to a central hub or switch.**
- **The central hub acts as a central point of communication and controls the flow of data between devices.**
- **If one device fails, it doesn't affect the rest of the network; only the failed device loses connectivity.**
- **It is easy to add or remove devices in a star topology without disrupting the entire network.**
- **Commonly used in Ethernet networks, home networks, and small to medium-sized business networks.**

**Advantages:**

- **Easy to install, configure, and manage.**
- **Fault tolerance is very high since the failure of one device doesn't affect the others.**
- **Centralized control makes monitoring and troubleshooting more straightforward.**

**Disadvantages:**

- **Dependence on the central hub; if it fails, the entire network is affected.**
- **Costlier than other topologies due to the need for a central hub.**

**Ring Topology: Features**

- **In a ring topology, each device is connected to exactly two other devices, forming a closed loop.**
- **Data circulates in one direction through the ring, passing through each device until it reaches its destination.**

- **It requires a specific data token or frame to control access to the network, ensuring orderly data transmission.**
- **Failure of any device or connection in the ring can disrupt the entire network.**

**Advantages:**

- **It ensures fair access to the network as each device gets an equal opportunity to transmit data.**
- **Simple and predictable data flow.**

**Disadvantages:**

- **A single point of failure can bring down the entire network.**
- **Adding or removing devices can be challenging without disrupting the entire network.**
- **Not commonly used in modern network setups due to its limitations.**

**Bus Topology: Features**

- **In a bus topology, all devices are connected to a single central cable called the "bus."**
- **Data transmitted by one device travels along the bus and is received by all devices, but only the intended recipient processes it.**
- **Terminators are placed at both ends of the bus to prevent data reflections.**

**Advantages:**

- **Simple and inexpensive to set up, making it suitable for small networks.**
- **Well-suited for temporary networks or small office/home office (SOHO) environments.**

**Disadvantages:**

- **If the central bus cable fails, the entire network is affected.**
- **Adding or removing devices can be challenging as it requires temporarily disconnecting the entire network.**

**Mesh Topology: Features**

- **In a mesh topology, every device is connected to every other device in the network.**
- **This creates redundant connections, ensuring multiple paths for data to reach its destination.**

- **Mesh topologies can be full mesh (every device is connected to every other device) or partial mesh (only some devices have multiple connections).**
- **High redundancy provides fault tolerance and robustness but can be costly and complex to implement.**

### Advantages:

- **High fault tolerance; even if multiple devices fail, alternative paths are available for data transmission.**
- **High scalability and performance in large networks.**

### Disadvantages:

- **Expensive to set up due to the large number of interconnections required.**
- **Difficult to manage and maintain in large-scale deployments.**

**Each topology has its strengths and weaknesses, and the choice of which one to use depends on the specific requirements and constraints of the network being implemented.**

**Examples of Star topology, Bus Topology Ring topology, and Mesh topology**

**Star Topology:**

- **Home Network: In a typical home network, you might have a wireless router (central hub) that connects all your devices like laptops, smartphones, smart TVs, and IOT devices wirelessly. The router acts as the central point of communication, and each device communicates directly with the router.**
- **Office LAN: In a small to medium-sized office, a network switch serves as the central hub. All computers, printers, and other networked devices are connected to the switch using Ethernet cables, forming a star topology.**

**Bus Topology:**

- **Ethernet LAN: In traditional Ethernet LANs, computers and devices are connected to a single coaxial cable, acting as the central "bus." Each device taps into the cable to send and receive data. However, bus topology is less common in modern LAN setups.**

**Ring Topology:**

- **Token Ring Network: Token Ring was a popular network technology where devices were connected in a ring-like fashion. Each device in the ring had two neighbors to which it could pass data. Devices had to wait for a special token to access the network, ensuring orderly data transmission. However,**

**the Token Ring is now mostly obsolete, and ring topologies are less commonly used in modern networks.**

**Mesh Topology:**

- **Military Communication Network: In military communication networks, mesh topology is often used to ensure high reliability and fault tolerance. Different military installations or units are interconnected with multiple communication links, providing redundant paths for data transmission.**
- **Internet Backbone: The global internet backbone is an example of a complex mesh topology. Large network providers and internet exchange points are interconnected with redundant links, allowing data to take multiple paths between different parts of the world.**

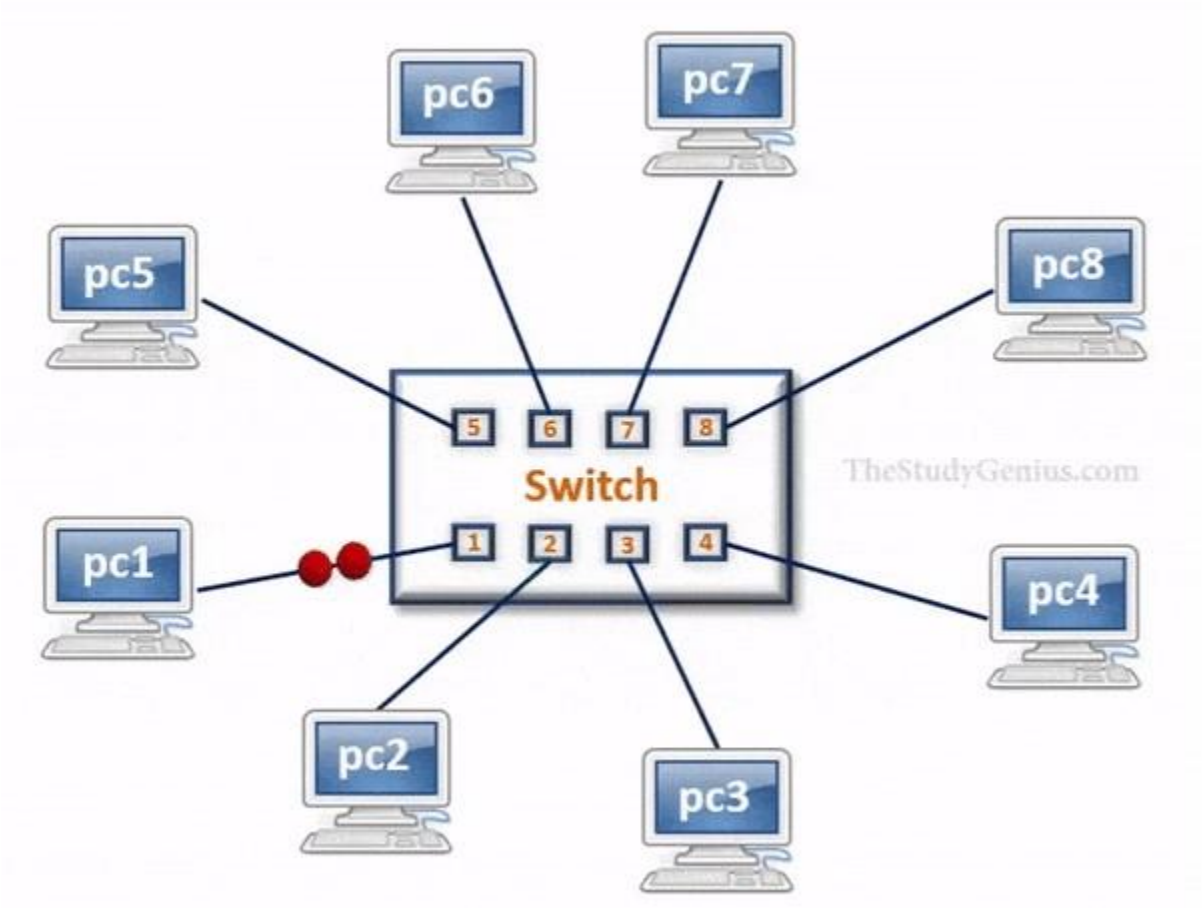
**In real-world scenarios, network topologies are often a combination of these basic topologies to achieve the desired balance of performance, fault tolerance, and cost-effectiveness.**

## Elements of Network Hardware

Network hardware refers to the physical devices that are used to build and operate a computer network. These devices enable communication, data transfer, and connectivity between different computers and network devices. Here are some essential elements of network hardware:

a. **Network Interface Card (NIC):** A Network Interface Card, also known as a network adapter, is a hardware component that allows a computer to connect to a network. It is responsible for converting data between the computer's internal bus and the network medium (like Ethernet or Wi-Fi).
b. **Router:** A router is a networking device that forwards data packets between different networks. It acts as a central point for directing network traffic and determines the best path for data to travel from one network to another. Home networks and businesses often use routers to connect to the internet and create local area networks (LANs).
c. **HUB:** Though less commonly used in modern networks, a hub is a basic networking device that connects multiple devices in a network. Unlike a switch, a hub broadcasts data to all connected devices, which can lead to more collisions and reduced efficiency.

d. **Switch:** A network switch is a device that connects multiple devices within a local area network (LAN). Unlike a hub, which broadcasts data to all connected devices, a switch intelligently forwards data only to the device for which it is intended, reducing unnecessary network traffic and increasing efficiency.




e. **Modem:** A modem (modulator-demodulator) is a device that converts digital data from a computer into analog signals for transmission over

analog communication lines (such as telephone lines) and vice versa. Modems are used to conn1ect to the internet through dial-up, DSL, or cable connections.

f. **Access Point (AP):** An access point is a wireless networking device that allows Wi-Fi-enabled devices to connect to a wired network. It serves as a central hub for wireless communication and enables devices like laptops, smartphones, and tablets to access the network without the need for physical cables.
g. **Network Cables:** Various types of cables are used to connect network devices. Common network cable types include Ethernet cables (e.g., Cat 5e, Cat 6, Cat 6a) for wired connections and fiber optic cables for high-speed, long-distance data transmission.
h. **Firewall**: A firewall is a security device that filters network traffic, controlling the flow of data between networks and devices. It helps protect the network from unauthorized access and potential cyber threats.
i. **Network Attached Storage (NAS)**: A NAS device is a specialized file storage system connected to a network that allows multiple devices to access and share files and data. It provides a centralized and efficient way to store and manage data.
j. **Network Printer**: A network printer is a printer that is directly connected to the network and can be accessed and used by multiple devices without the need for a direct connection.

These are some of the fundamental elements of network hardware that are commonly used to build and maintain computer networks of various sizes and complexities.

### Differences between Router, Switch, hub, and Modem

Router, switch, hub, and modem are all essential network hardware devices, but they serve different purposes and have distinct functionalities. Here are the key differences between them:

1. **Router**:
    - Purpose: A router is a networking device that connects different networks together and forwards data packets between them. It determines the best path for data to travel from one network to another, making it a vital component for connecting networks and accessing the internet.

- Functionality: Routers operate at the network layer (Layer 3) of the OSI model and use IP addresses to direct traffic. They have the ability to make decisions about the most efficient path for data transmission.
- Example: Home Wi-Fi routers, enterprise routers, and internet service provider (ISP) routers.

**2. Switch:**

- Purpose: A switch is a networking device used to connect multiple devices within a local area network (LAN). It creates a network segment and intelligently forwards data only to the intended recipient, reducing unnecessary network traffic and improving efficiency.
- Functionality: Switches operate at the data link layer (Layer 2) of the OSI model and use MAC addresses to determine where to send data packets within the local network.
- Example: Ethernet switches commonly used in home networks, offices, and data centers.

**3. Hub:**

- Purpose: A hub is an older networking device used to connect multiple devices within a LAN. It is a simple device that broadcasts data to all connected devices, leading to more collisions and reduced network efficiency compared to switches.
- Functionality: Hubs operate at the physical layer (Layer 1) of the OSI model and do not possess any intelligence to manage network traffic.
- Note: Hubs are mostly outdated and have been largely replaced by switches.

**4. Modem:**

Purpose: A modem (modulator-demodulator) is a device used to modulate digital data from a computer into analog signals suitable for transmission over analog communication lines (e.g., telephone lines or cable lines). It also demodulates analog signals back into digital data at the receiving end.

- Functionality: Modems are used to establish a connection to the internet or other networks through various means such as dial-up, DSL, or cable connections.
- Example: Cable modems, DSL modems, and dial-up modems.

In summary, a router connects different networks together and forwards data between them, a switch connects devices within a local network segment and intelligently forwards data to the intended recipient, a hub connects devices within a network but broadcasts data to all connected

devices, and a modem facilitates the connection between a computer or network and an external network (like the internet) through various transmission media. As technology advances, switches, and routers have become more prevalent due to their efficiency and intelligence in managing network traffic, while hubs are no longer commonly used.

## Features and Function of OSI Layers

## Physical Layer

The physical layer helps you to define the electrical and physical specifications of the data connection. This level establishes the relationship between a device and a physical transmission medium. The physical layer is not concerned with protocols or other such higher-layer items.

Examples of hardware in the physical layer are network adapters, ethernet, repeaters, networking hubs, etc.

**Bit Encoding and Signaling:** The Physical Layer converts digital data (0s and 1s) generated by the higher layers into signals suitable for transmission over the physical medium. It determines how bits are represented electrically, optically, or through other means, such as voltage levels or light pulses.

**Transmission Media Selection**: It specifies the type of physical medium used for data transmission, which can include copper wires, optical fibers, coaxial cables, radio waves (wireless communication), and more. The choice of medium affects data rates, distance, and reliability.

**Data Rate (Transmission Speed)**: The Physical Layer defines the data rate at which bits are transmitted over the medium. It sets the maximum transmission speed (e.g., in bits per second or baud rate) based on the medium's characteristics and network requirements.

**Synchronization:** It ensures that the sender and receiver are synchronized in terms of bit timing, so that data can be correctly interpreted at the receiving end.

**Data Transmission Mode:** The Physical Layer defines the transmission mode, which can be simplex (one-way communication), half-duplex (bidirectional but not simultaneously), or full-duplex (bidirectional and simultaneous).

**Error Detection and Correction:** Some error detection and correction mechanisms may be implemented at the Physical Layer to identify and, in some cases, correct errors in the received data.

**Noise and Interference Handling:** It deals with noise and interference on the physical medium, employing techniques like shielding, filtering, and error recovery to maintain signal integrity.

# Data Link Layer:

Data link layer corrects errors which can occur at the physical layer. The layer allows you to define the protocol to establish and terminates a connection between two connected network devices.

It is IP address understandable layer, which helps you to define logical addressing so that any endpoint should be identified.

The layer also helps you implement routing of packets through a network. It helps you to define the best path, which allows you to take data from the source to the destination.

The data link layer is subdivided into two types of sublayers:

1. Media Access Control (MAC) layer- It is responsible for controlling how device in a network gain access to medium and permits to transmit data.
2. Logical link control layer- This layer is responsible for identity and encapsulating network-layer protocols and allows you to find the error.

## Important Functions of the Datalink Layer:

- Framing which divides the data from the Network layer into frames.
- Allows you to add a header to the frame to define the physical address of the source and the destination machine
- Adds Logical addresses of the sender and receivers

- It is also responsible for the sourcing process to the destination process delivery of the entire message.
- It also offers a system for error control in which it detects and retransmits damaged or lost frames.
- Datalink layer also provides a mechanism to transmit data over independent networks which are linked together.

# Transport Layer:

The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine. It is hosted using single or multiple networks, and also maintains the quality of service functions.

It determines how much data should be sent where and at what rate. This layer builds on the messages which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.

Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or de-segmentation.

The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer.

## Important functions of Transport Layers:

- It divides the message received from the session layer into segments and numbers them to make a sequence.
- Transport layer makes sure that the message is delivered to the correct process on the destination machine.
- It also makes sure that the entire message arrives without any error else it should be retransmitted.

# Network Layer:

The network layer provides the functional and procedural means of transferring variable length data sequences from one node to another connected in “different networks”.

Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol.

Layer-management protocols that belong to the network layer are:

1. routing protocols
2. multicast group management
3. network-layer address assignment.

# Session Layer

Session Layer controls the dialogues between computers. It helps you to establish starting and terminating the connections between the local and remote application.

This layer request for a logical connection which should be established on end user's requirement. This layer handles all the important log-on or password validation.

Session layer offers services like dialog discipline, which can be duplex or half-duplex. It is mostly implemented in application environments that use remote procedure calls.

## Important function of Session Layer:

- It establishes, maintains, and ends a session.
- Session layer enables two systems to enter into a dialog
- It also allows a process to add a checkpoint to steam of data.

# Presentation Layer

Presentation layer allows you to define the form in which the data is to exchange between the two communicating entities. It also helps you to handles data compression and data encryption.

This layer transforms data into the form which is accepted by the application. It also formats and encrypts data which should be sent across all the networks. This layer is also known as a **syntax layer**.

### The function of Presentation Layers:

- Character code translation from ASCII to EBCDIC.
- Data compression: Allows to reduce the number of bits that needs to be transmitted on the network.
- Data encryption: Helps you to encrypt data for security purposes — for example, password encryption.
- It provides a user interface and support for services like email and file transfer.

## Application Layer

Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI layer, which is closest to the end-user. It means OSI application layer allows users to interact with other software application.

Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model.

Example of the application layer is an application such as file transfer, email, remote login, etc.

### The function of the Application Layers are:

- Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
- It allows users to log on to a remote host
- This layer provides various e-mail services
- This application offers distributed database sources and access for global information about various objects and services.

## Interaction Between OSI Model Layers

Information sent from a one computer application to another needs to pass through each of the OSI layers.

This is explained in the below-given example:

- Every layer within an OSI model communicates with the other two layers which are below it and its peer layer in some another networked computing system.
- In the below-given diagram, you can see that the data link layer of the first system communicates with two layers, the network layer and the physical layer of the system. It also helps you to communicate with the data link layer of, the second system.

- **Protocols supported at various levels**

| Layer | Name | Protocols |
|---|---|---|
| Layer 7 | Application | SMTP, HTTP, FTP, POP3, SNMP |
| Layer 6 | Presentation | MPEG, ASCH, SSL, TLS |
| Layer 5 | Session | NetBIOS, SAP |
| Layer 4 | Transport | TCP, UDP |
| Layer 3 | Network | IPV5, IPV6, ICMP, IPSEC, ARP, MPLS. |
| Layer 2 | Data Link | RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc. |
| Layer 1 | Physical | RS232, 100BaseTX, ISDN, 11. |