**Networking:**

* What is a network?

A computer network is a group of interconnected devices that are designed to communicate and share information with each other.

Uses of Computer networks

1. **Resource Sharing**: Computer networks allow different devices like computers, printers, and storage devices to share resources like files and software programs. For example, multiple users can access the same printer or files stored on a server.
2. **Communication**: Networks enable communication between devices and people. This can include sending emails, instant messages, video calls, or even sharing data between computers in different locations.
3. **Information Access**: With computer networks, users can access information from various sources such as websites, databases, and online services. This allows for quick and easy retrieval of information needed for work, study, or entertainment.
4. **Centralized Management**: Networks allow for centralized management of resources and data. This means administrators can control and monitor devices, users, and data from a central location, making it easier to manage large networks efficiently.
5. **Remote Access**: Computer networks enable remote access to resources and systems from anywhere with an internet connection. This allows users to work or access information from home, while traveling, or from any location outside of the physical office or network premises.

**Types of Networks:**

**LAN (local area network):**

LAN is the most frequently used network. A LAN is a computer network that connects computers through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi. It ranges up to 2km & transmission speed is very high with easy maintenance and low cost.

**Metropolitan Area Network (MAN):**

A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area. This network mainly used with a range from 5km to 50km. Its transmission speed is average. It is difficult to maintain and it comes with a high cost.

**Wide Area Network (WAN):**

A WAN is a network that spans over a large geographical area, such as a country or even globally. It connects multiple LANs and MANs across long distances using technologies like fiber optic cables, satellite links, or leased lines. The internet is the most common example of a WAN.

**Personal Area Network (PAN) :**

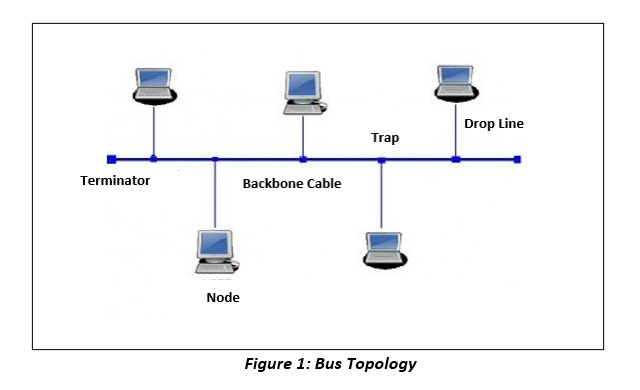
PAN is the most basic type of computer network. This network is restrained to a single person, that is, communication between the computer devices is centered only on an individual’s workspace. PAN offers a network range of 1 to 100 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost.

**Network Topologies :**

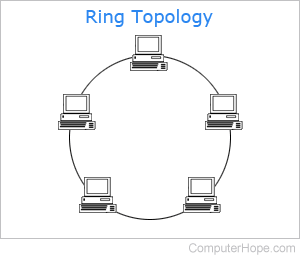
A network topology refers to how devices are connected in a network.

**Bus Topology:**

It is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

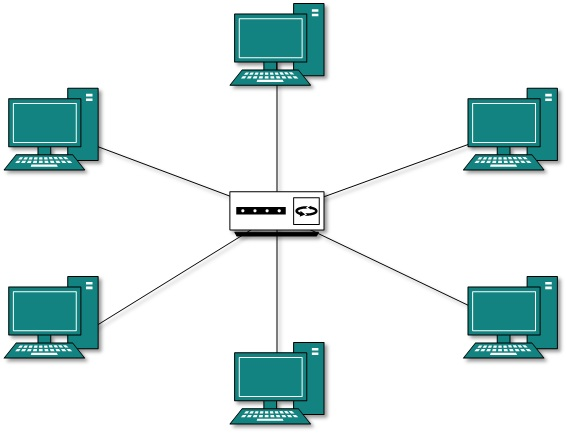
**Ring Topology:**

Picture a circle where everyone is holding hands with the person next to them. In a ring network, each device is connected to two others, forming a circular pathway. Data travels in one direction around the circle until it reaches its destination.



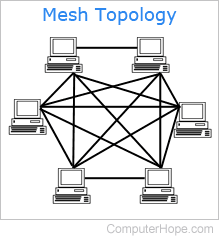
**Star Topology :**

Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer. The central computer is known as a server, and the peripheral devices attached to the server are known as clients.



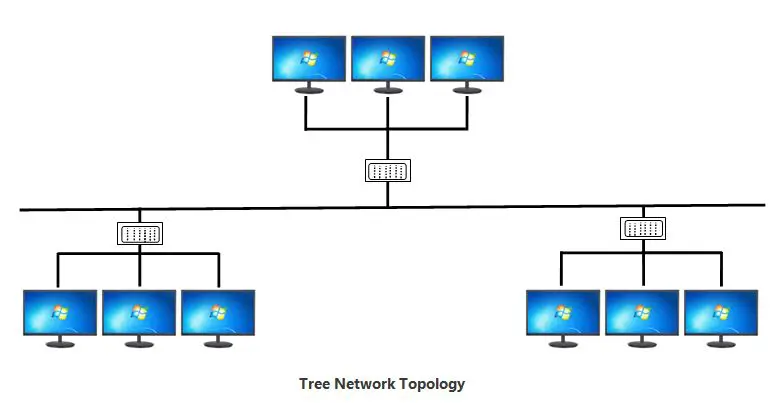
**Mesh Topology :**

A mesh topology is a type of computer network in which each node (computer or other device) is connected to every other node in the network. This type of network is often used in large organisations or companies because it can handle a large amount of data traffic and can be easily expanded.



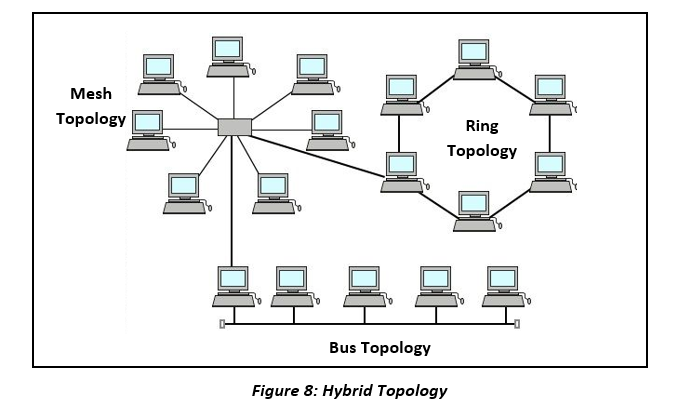
**Tree Topology :**

In tree topology nodes are connected in a hierarchical structure to form a tree. There is a root node in tree topology and the remaining nodes are considered as child nodes, basically it is a combination of star and bus topology. The central bus works as a communication pathway, and each star-configured network represents a level in the tree. In tree topology, a hierarchy is formed by the branching cable having no loops that connect the root with all other nodes for communication.



**Hybrid Topology:**

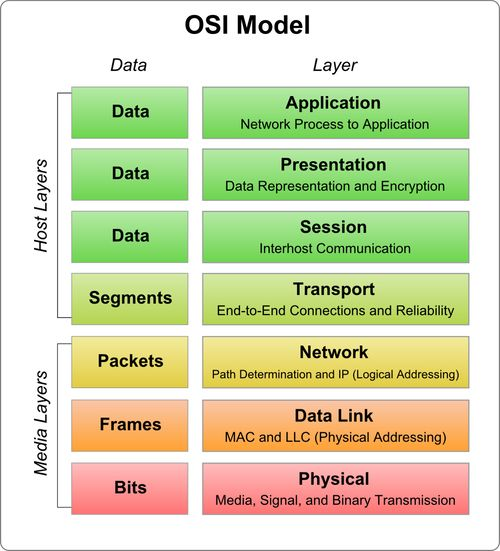
Hybrid topology is a network structure that combines two or more different types of topologies, such as star, ring, bus, or mesh. It's designed to leverage the strengths and minimize the weaknesses of the individual topologies it incorporates.



**OSI Model:**

The OSI (Open Systems Interconnection) model is a conceptual framework for understanding how computer networks work.

It is composed of seven layers, each of which serves a specific purpose in the communication process.



**Physical Layer – Layer 1 :**

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

* It is the bottom-most or the first layer of the OSI Model
* It comprises the raw data which is further transmitted to the higher layers of the structure
* Preparing the physical devices in the network and accepting the received data for transmission
* The termination of connection between two nodes of a network also takes place at this stage
* This layer converts the digital bits into electrical, radio, or optical signals

**Data-Link Layer – Layer 2 :**

The data link layer ensures error-free node-to-node data transfer. It helps in data transfer between two devices on the same network. This layer takes packets from the network layer and converts them into smaller pieces called frames. It ensures flow control and error control in intra-network communication. This layer consists of two sub-layers:

* Access to get the data is achieved at this layer
* It breaks the input data into frames which makes analysing the data easier
* Ensures that the data received is free of any errors
* It controls the flow of data in the stipulated time duration and along with a set speed of transmission
* The data is sent to the next layer in the form of packets which are then reviewed for further processing

**3. Network Layer:**

The Network Layer is responsible for routing packets from the source to the destination across multiple networks. It provides logical addressing, which allows devices to be uniquely identified on a network. Key functions include:

Logical addressing (e.g., IP addresses).

Routing: Determining the best path for data packets.

Packet forwarding and delivery.

Fragmentation and reassembly of packets.

The Internet Protocol (IP) is the primary protocol at this layer.

**4. Transport Layer:**

The Transport Layer ensures reliable end-to-end communication between hosts. It segments and reassembles data from the upper layers and provides error detection and correction mechanisms. Key functions include:

* Segmentation and reassembly of data into manageable units (segments).
* Error detection and correction.
* Flow control to manage data transmission rates.
* Connection establishment, maintenance, and termination.

The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) operate at this layer.

**5. Session Layer:**

The Session Layer establishes, maintains, and terminates communication sessions between applications. It provides synchronization and dialog control between devices. Key functions include:

* Session establishment, maintenance, and termination.
* Dialog control (half-duplex or full-duplex communication).
* Synchronization of data exchange.

**6. Presentation Layer:**

The Presentation Layer ensures that data exchanged between systems is in a format that each system can understand. It is responsible for data translation, encryption, and compression. Key functions include:

* Data translation and formatting (e.g., ASCII to EBCDIC).
* Encryption and decryption of data for secure transmission.
* Compression to reduce the size of data for efficient transmission.

This layer enhances the compatibility and security of data exchange between systems.

**Application Layer:**

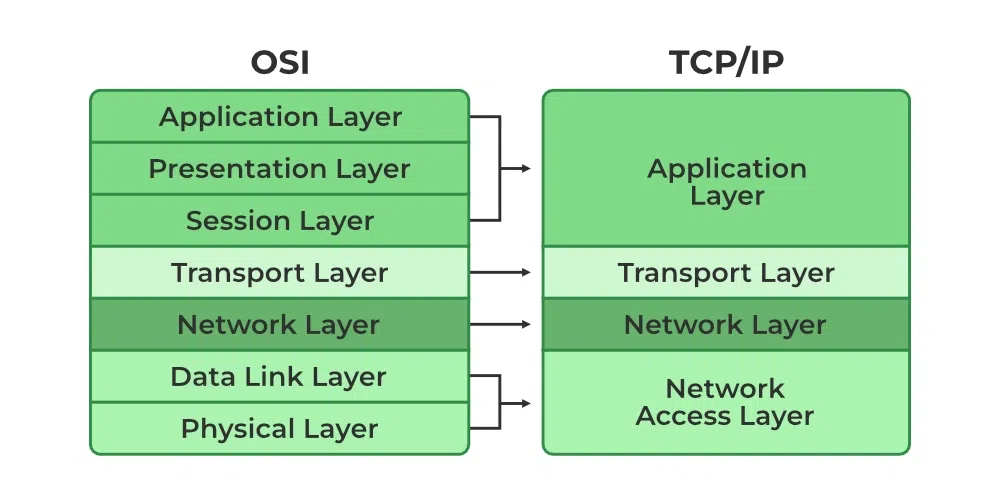
The Application Layer interacts directly with end-users and provides network services to applications. It enables communication between various software applications and network services. Key functions include:

* Providing network services to applications (e.g., email, web browsing).
* Interface between the network and application software.
* Protocols such as HTTP, FTP, SMTP, and DNS operate at this layer.

**TCP/IP Model:**

The TCP/IP (Transmission Control Protocol/Internet Protocol) model is a widely used networking model that provides a framework for communication over the internet.

It is composed of four layers, each with its own set of protocols and functions.



**1. Application Layer:**

The Application Layer in the TCP/IP model is similar to the OSI model's Application Layer. It's where communication services for applications reside. This layer provides interfaces for software to utilize network functionality, allowing programs to request network services such as file transfer, email, and remote login. Protocols operating at this layer include HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), and DNS (Domain Name System).

**2. Transport Layer:**

The Transport Layer in the TCP/IP model corresponds to the Transport Layer in the OSI model. Its primary purpose is to ensure end-to-end communication by providing reliable data transport services. The key protocols at this layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP ensures reliable, connection-oriented communication by providing features like flow control, error detection, and retransmission of lost packets. UDP, on the other hand, is connectionless and provides a simpler, faster transport mechanism without the overhead of TCP's reliability features.

**3. Internet Layer:**

The Internet Layer is equivalent to the Network Layer in the OSI model. It is responsible for routing packets between networks and across the internet. The Internet Protocol (IP) is the primary protocol at this layer. IP provides logical addressing (IPv4 or IPv6 addresses) to uniquely identify devices on a network, and it determines the best path for data packets to reach their destination. Additionally, ICMP (Internet Control Message Protocol) operates at this layer, facilitating error reporting and network diagnostics.

**4. Link Layer:**

The Link Layer is the lowest layer in the TCP/IP model, encompassing aspects of both the Data Link Layer and the Physical Layer of the OSI model. It deals with the physical connection to the network hardware and the transmission of data frames over the local network medium. Ethernet, Wi-Fi (IEEE 802.11), and PPP (Point-to-Point Protocol) are examples of link layer technologies. The Link Layer includes protocols for addressing (MAC addresses), framing, error detection, and media access control.

**Comparison with OSI Model:**

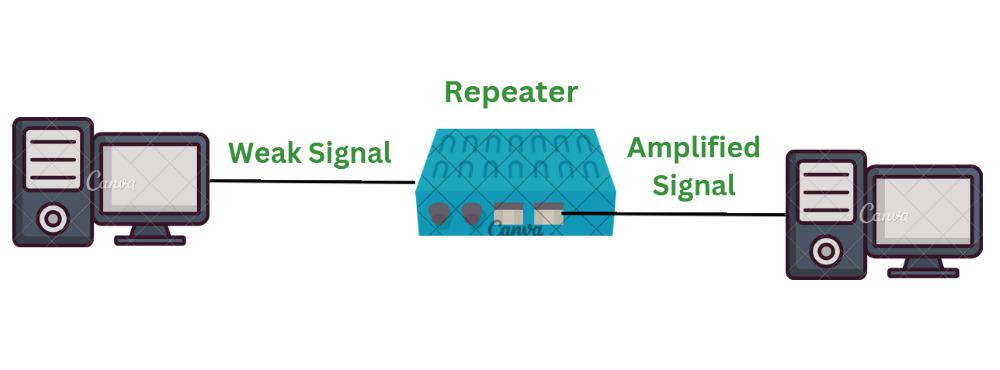
* The TCP/IP model has four layers, while the OSI model has seven layers. The TCP/IP model's layers are often more flexible and loosely defined.
* The TCP/IP model's Application Layer encompasses functions from both the OSI model's Application and Presentation Layers.
* The Transport Layer in the TCP/IP model is similar to the OSI model's Transport Layer.
* The Internet Layer in the TCP/IP model corresponds to the Network Layer in the OSI model.
* The Link Layer in the TCP/IP model combines aspects of the OSI model's Data Link and Physical Layers.

**Network Devices**

These are physical devices that allow hardware on a computer network to communicate and interact with one another.

Example: Hub, Switch, Router, etc.

1. **Repeater –** A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do no amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.



1. **Hub –** A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.



1. **Switch:** A switch is a multi-port device designed to transmit incoming data packets to correct ports or devices based on the destination MAC or hardware address. It’s typically more intelligent than a hub as it can improve the network performance with advanced features such as intelligent packet forwarding and full-duplex communication. It can also control access to various parts of the network, thereby enhancing network security. Multi-layer switches can operate as a router and thereby known as advanced network devices.



1. **Router:** A router is popular networking hardware that can connect two network segments or subnets to create an extensive network. As a network layer device, the router collects and stores information such as the IP address of its connected devices in a routing table and uses it for packet forwarding to the right destination. Routers can operate with static and dynamic routing. Static routing requires manual configuration and is less effective in dynamic networks. In contrast, dynamic routing allows routers to exchange information with other routers using special routing protocols and identify the most optimal path for data transfer.



**Network Protocols:**

Network protocols define how data is transmitted, received, and processed between devices.

They are essential for ensuring that devices can communicate with each other.

**1. Address Resolution Protocol (ARP)**

A communication layer protocol (mapping process between the data link layer and network layer) which is used to identify a media access control (MAC) address given the IP address. There is no way that the host can validate where the network packet came from in the peer to peer network. This is a vulnerability and gives rise to ARP spoofing. The attacker can exploit this if the attacker is on the same LAN as the target or uses a compromised machine that is on the same network. The idea is that the attacker associates his MAC address with the IP address of the target so that any traffic meant for the target is received by the attacker.

**2. Domain Name System (DNS)**

IP addresses are of numerical format and hence they are not easily readable or remember-able to humans. DNS is a hierarchical system that converts these IP addresses into a human-readable hostname. The most common vulnerability in DNS is cache poisoning. Here the attacker replaces the legitimate IP address to send the target audience to malicious websites. DNS amplification can also be exploited on a DNS server which permits recursive lookups and uses recursion to amplify the magnitude of the attack.

**3.Simple Mail Transfer Protocol (SMTP)**

It is a communication application layer protocol and is used to send emails. Spammers and hackers can use an e-mail server to send spam or malware through email under the guise of the unsuspecting open-relay owner. Hackers also perform a directory harvest attack, which is a way of gleaning valid email addresses from a server or domain for hackers to use. Vulnerabilities also include buffer overflow attacks, trojan horse attacks, shell script attacks, etc.

**4. Secure SHell (SSH)**

It is a cryptography-based network protocol for operating network services securely and reliably over an unsecured network. Some particular applications include remote command-line, remote command execution, login, but any network service can be made secure with the help of SSH. A man-in-the-middle(MITM) attack may allow the adversary to completely destabilize and bring down encryption and may gain access to the encrypted contents that can include passwords. A successful adversary is a cable to inject commands into the terminal to modify or alter data in transit or to steal data. The attack can also allow the injection of harmful malware into any binary files and other software updates downloaded through the system. This technique has been used by various attack groups and malware packages in the past.

**Wireless Networks**

A wireless network is a type of computer network that uses radio waves instead of physical cables to connect devices. Wireless networks are commonly used for internet access, as well as for sharing files, printers, and other resources between devices.