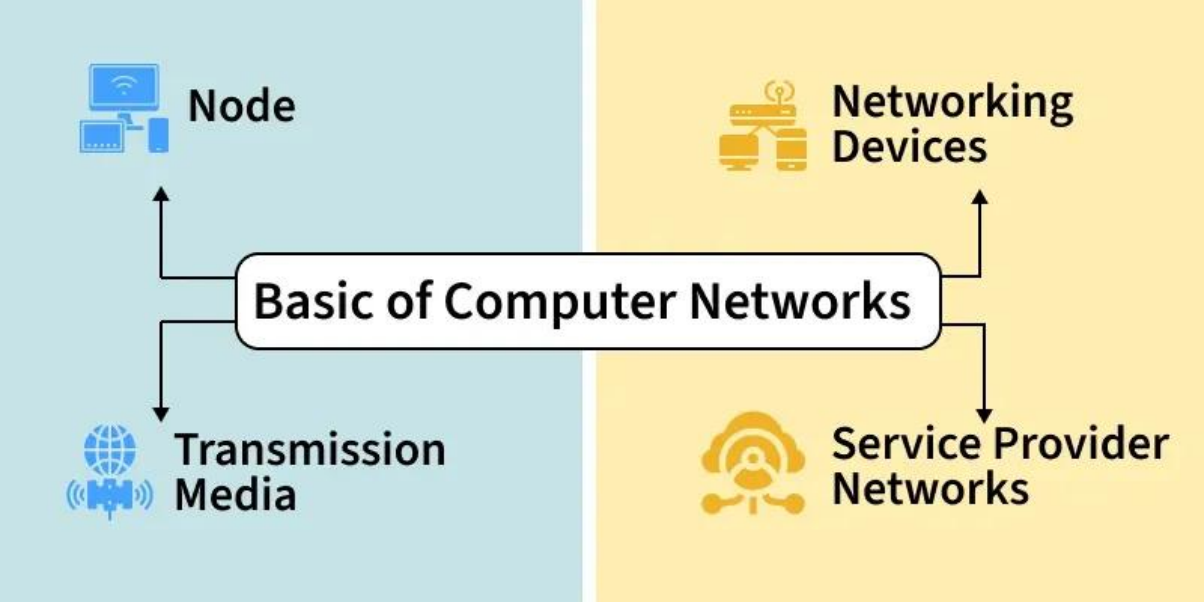
Basics of Computer Networking

A computer network is a collection of interconnected devices that share resources and information. These devices can include computers, servers, printers, and other hardware. Networks allow for the efficient exchange of data, enabling various applications such as email, file sharing, and internet browsing.

Basic Terminologies of Computer Networks

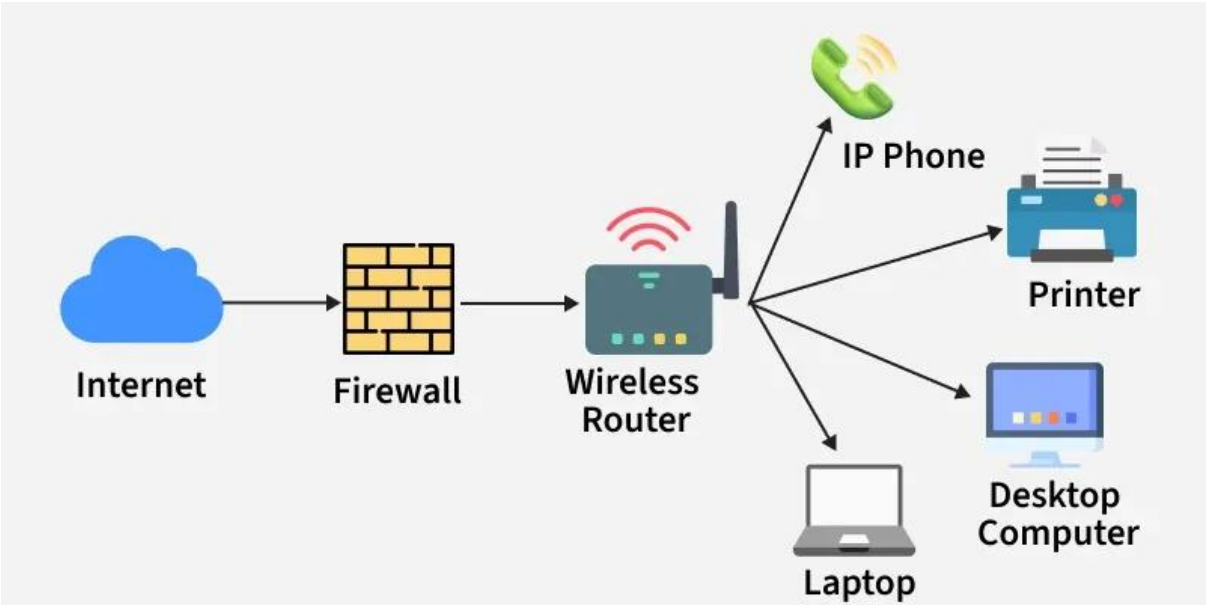


- **Network:** A group of connected computers and devices that can communicate and share data with each other.
- **Node:** Any device that can send, receive, or forward data in a network. This includes laptops, mobiles, printers, earbuds, servers, etc.
- **Networking Devices:** Devices that manage and support networking functions. This includes routers, switches, hubs, and access points.
- **Transmission Media:** The physical or wireless medium through which data travels between devices.
- **Wired media:** Ethernet cables, optical fibber**.**
- **Wireless media:** Wi-Fi, Bluetooth, infrared
- **Service Provider Networks:** Networks offered by external providers that allow users or organizations to lease network access and capabilities. This includes internet providers, mobile carriers, etc.

How Does a Computer Network Work

Basics building blocks of a computer network are Nodes and Links.

- A Network Node can be illustrated as Equipment for Data Communication like a Modem, Router, etc., or Equipment of a Data Terminal like connecting two computers or more.
- Link in Computer Networks can be defined as wires or cables or free space of wireless networks (as shown in the below diagram)
- The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate.
- Each device has an IP Address, that helps in identifying the device.
- A firewall is a network security device either hardware or software-based which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects, or drops that specific traffic.



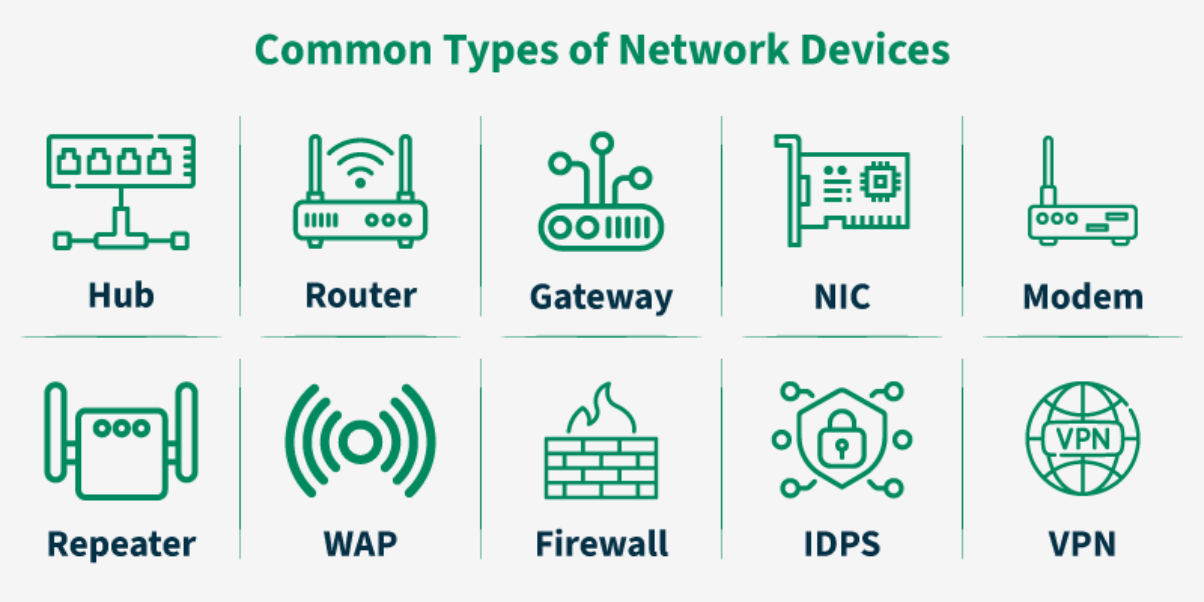
Types of Computer Network Architecture

Computer Network falls under these broad Categories:

- **Client-Server Architecture:**Client-Server Architecture is a type of Computer Network Architecture in which Nodes can be Servers or Clients. Here, the server node can manage the Client Node Behaviour.
- **Peer-to-Peer Architecture:** In P2P (Peer-to-Peer) Architecture, there is not any concept of a Central Server. Each device is free for working as either client or server.

Network Devices

An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as Network devices and include things such as routers, switches, hubs, and bridges.



Functions of Network Devices

- Network devices help to send and receive data between different devices.
- Network devices allow devices to connect to the network efficiently and securely.
- Network devices improve network speed and manage data flow better.
- It protects the network by controlling access and preventing threats.
- Expand the network range and solve signal problems.

Common Types of Networking Devices and Their Uses

Network devices work as a mediator between two devices for transmission of data, and thus play a very important role in the functioning of a computer network. Below are some common network devices used in modern networks:

- **Access Point**
- **Modems**
- **Firewalls**
- **Repeater**
- **Hub**
- **Bridge**
- **Switch**
- **Routers**
- **Gateway**
- **Brouter**

- **NIC**

Access Point

An access point in networking is a device that allows wireless devices, like smartphones and laptops, to connect to a wired network. It creates a Wi-Fi network that lets wireless devices communicate with the internet or other devices on the network. Access points are used to extend the range of a network or provide Wi-Fi in areas that do not have it. They are commonly found in homes, offices, and public places to provide wireless internet access.

Modems

Modem is also known as modulator/demodulator is a network device that is used to convert digital signal into analog signals of different frequencies and transmits these signals to a modem at the receiving location. These converted signals can be transmitted over the cable systems, telephone lines, and other communication mediums. A modem is also used to convert an analog signal back into digital signal. Modems are generally used to access the internet by customers of an Internet Service Provider (ISP).

Types of Modems

There are four main types of modems:

- **DSL Modem**: Uses regular phone lines to connect to the internet but it is slower compared to other types.
- **Cable Modem**: Sends data through TV cables, providing faster internet than DSL.
- **Wireless Modem**: Connects devices to the internet using Wi-Fi relying on nearby Wi-Fi signals.
- **Cellular Modem**: Connects to the internet using mobile data from a cellular network not Wi-Fi or fixed cables.

Firewalls

A firewall is a network security device that monitors and controls the flow of data between your computer or network and the internet. It acts as a barrier, blocking unauthorized access while allowing trusted data to pass through. Firewalls help protect your network from hackers, viruses, and other online threats by filtering traffic based on security rules. Firewalls can be physical devices (hardware), programs (software), or even cloud-based services, which can be offered as SaaS, through public clouds, or private virtual clouds.

Repeater

A repeater operates at the physical layer. Its main function is to amplify (i.e., regenerate) the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

Hub

A hub is 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, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub:** These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.

- **Passive Hub:** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

- **Intelligent Hub:** It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

Bridge

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It typically connects multiple network segments and each port is connected to different segment. A bridge is not strictly limited to two ports, it can have multiple ports to connect and manage multiple network segments. Modern multi-port bridges are often called Layer 2 switches because they perform similar functions.

Types of Bridges

- **Transparent Bridges:** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.

- **Source Routing Bridges:** In these bridges, routing operations is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

Switch

A switch is a multiport bridge with a buffer designed that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it

does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

Types of Switch

- **Unmanaged Switches:** These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.
- **Managed Switches:** These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.
- **Smart Switches:** These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.
- **Layer 2 Switches:** These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.
- **Layer 3 switches:** These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.
- **PoE Switches**: These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.
- **Gigabit switches:** These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.
- **Rack-Mounted Switches:** These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.
- **Desktop Switches:** These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.
- **Modular Switches**: These switches have modular design that allows for easy expansion or customization. They are suitable for large networks and data centers.

Router

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

Gateway

A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers.

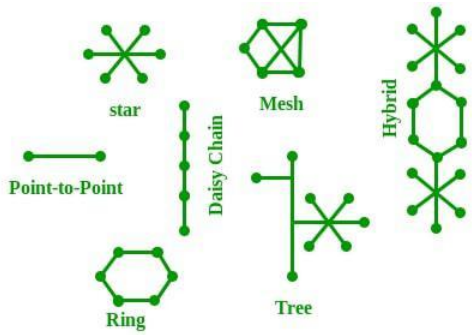
Brouter

It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as a bridge, it is capable of filtering local area network traffic.

NIC

NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique ID that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC is a layer 2 device which means that it works on both the physical and data link layers of the network model.

Network Topology



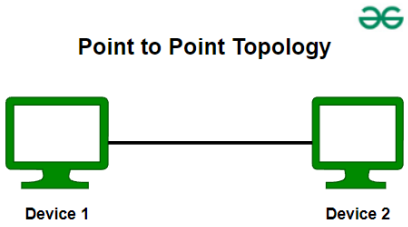
Network topology refers to the arrangement of different elements like nodes, links, or devices in a computer network. Common types of network topology include bus, star, ring, mesh, and tree topologies, each with its advantages and disadvantages. In this article, we will discuss different types of network topology in detail.

There are two major categories of Network Topology i.e. Physical Network topology and Logical Network Topology. Physical Network Topology refers to the actual structure of the physical medium for the transmission of data. Logical network Topology refers to the transmission of data between devices present in the network irrespective of the way devices are connected. The structure of the network is important for the proper functioning of the network. one must choose the most suitable topology as per their requirement.

Types of Network Topology

Point to Point Topology

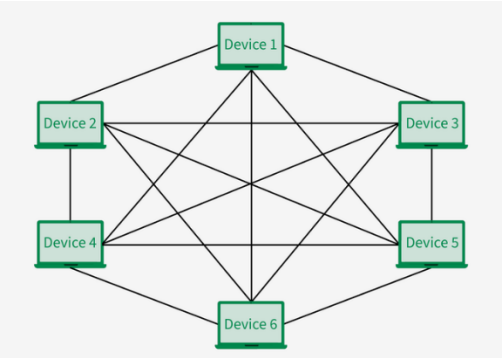
Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Point to Point Topology

Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. Every device is connected to another via dedicated channels. These channels are known as links. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



Mesh Topology

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure, there are 6 devices connected to each other, hence the total number of ports required by each device is 5. The total number of ports required = N * (N-1).

- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is ${}^{N}C_{2}$ i.e. N(N-1)/2. In Figure, there are 6 devices connected to each other, hence the total number of links required is 6*5/2 = 15.

Advantages of Mesh Topology

- Communication is very fast between the nodes.

- Mesh Topology is robust.

- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.

- Provides security and privacy.

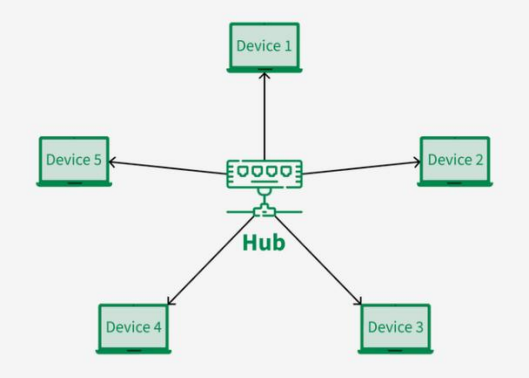
Disadvantages of Mesh Topology

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels. This topology is also used in military communication systems and aircraft navigation systems.

Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.



Star Topology

Advantages of Star Topology

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

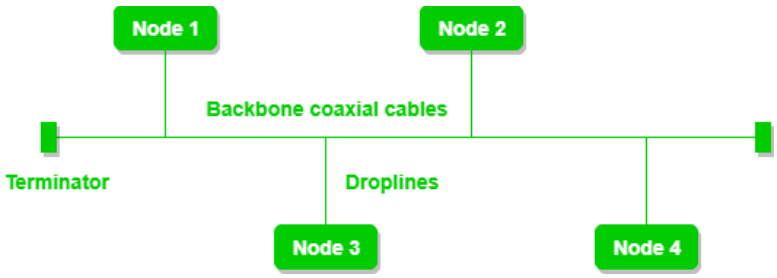
Disadvantages of Star Topology

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

A common example of star topology is a **local area network (LAN)** in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.

Bus Topology

Bus Topology 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. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.



Bus Topology

Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA is the most common method for this type of topology.

Disadvantages of Bus Topology

- A bus topology is quite simpler, but still, it requires a lot of cabling.

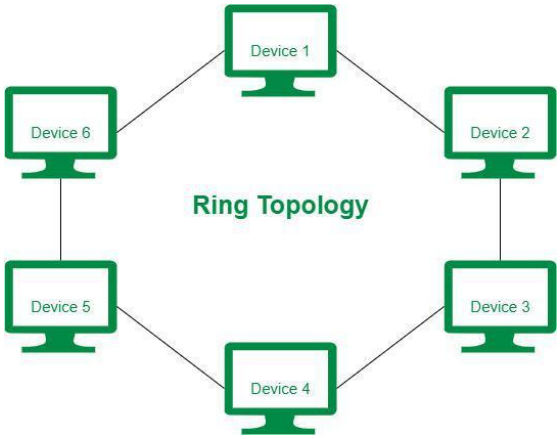
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks.

Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



Ring Topology

The most common access method of ring topology is token passing.

- **Token passing:** It is a network access method in which a token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

Operations of Ring Topology

- One station is known as a **monitor** station which takes all the responsibility for performing the operations.
- To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
- When no station is transmitting the data, then the token will circulate in the ring.
- There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delayed token release** releases the token after the acknowledgment is received from the receiver.

Advantages of Ring Topology

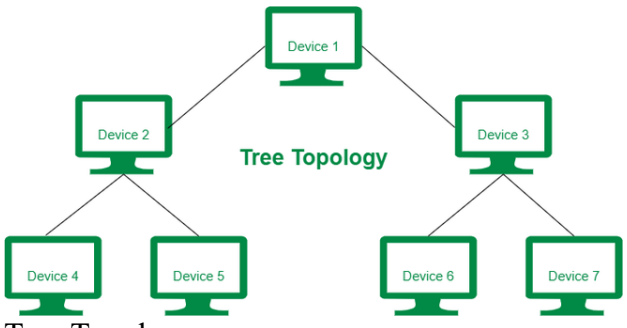
- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

Disadvantages of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

Tree Topology

Tree topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and **SAC (Standard Automatic Configuration)** are used.



Tree Topology

In tree topology, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of Tree Topology

- It allows more devices to be attached to a single central hub thus it decreases the distance that is travelled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add **new devices to the existing network.**
- **Error detection** and **error correction** are very easy in a tree topology.

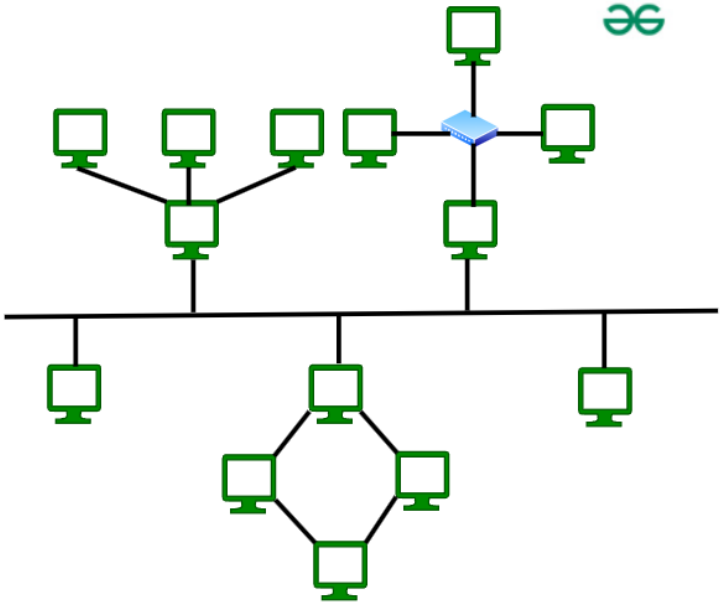
Disadvantages of Tree Topology

- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

A common example of a tree topology is the hierarchy in a large organization. At the top of the tree is the CEO, who is connected to the different departments or divisions (child nodes) of the company. Each department has its own hierarchy, with managers overseeing different teams (grandchild nodes). The team members (leaf nodes) are at the bottom of the hierarchy, connected to their respective managers and departments.

Hybrid Topology

Hybrid Topology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



Hybrid Topology

The above figure shows the structure of the Hybrid topology. As seen, it contains a combination of all different types of networks.

Advantages of Hybrid Topology

- This topology is **very flexible.**
- The size of the network can be easily expanded by **adding new devices.**

Disadvantages of Hybrid Topology

- It is challenging **to design the architecture** of the Hybrid Network.
- **Hubs** used in this topology are **very expensive.**
- The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices.**

A common example of a hybrid topology is a university campus network. The network may have a backbone of a star topology, with each building connected to the backbone through a switch or router. Within each building, there may be a bus or ring topology connecting the different rooms and offices. The wireless access points also create a mesh topology for wireless devices. This hybrid topology allows for efficient communication between different buildings while providing flexibility and redundancy within each building.

Why is Network Topology Important?

Network Topology is important because it defines how devices are connected and how they communicate in the network. Here are some points that defines why network topology is important.

- **Network Performance:** Upon choosing the appropriate topology as per requirement, it helps in running the network easily and hence increases network performance.
- **Network Reliability:** Some topologies like Star, Mesh are reliable as if one connection fails, they provide an alternative for that connection, hence it works as a backup.
- **Network Expansion**: Choosing correct topology helps in easier expansion of Network as it helps in adding more devices to the network without disrupting the actual network.
- **Network Security:** Network Topology helps in understanding how devices are connected and hence provides a better security to the network.

OSI Model

The **OSI (Open Systems Interconnection)** Model is a set of rules that explains how different computer systems communicate over a network. OSI Model was developed by the **International Organization for Standardization (ISO)**. The OSI Model consists of 7 layers and each layer has specific functions and responsibilities. This layered approach makes it easier for different devices and technologies to work together. OSI Model provides a clear structure for data transmission and managing network issues. The OSI Model is widely used as a reference to understand how network systems function.

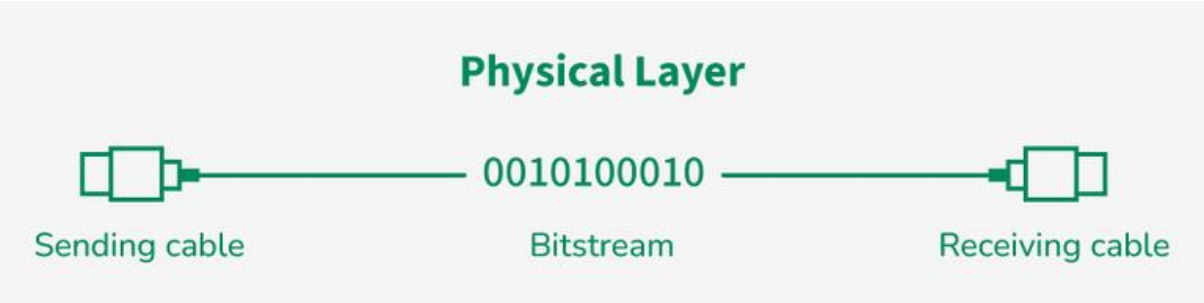
Layers of the OSI Model

There are 7 layers in the OSI Model and each layer has its specific role in handling data. All the layers are mentioned below:

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Layer 1: Physical Layer

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.** Physical Layer 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. Common physical layer devices are Hub, Repeater, Modem, and Cables.



Functions of the Physical Layer

- **Bit Synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
- **Bit Rate Control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- **Physical Topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus topology, star topology, or mesh topology.
- **Transmission Mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full duple

Layer 2: Data Link Layer (DLL)

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address. Packet in the Data Link layer is referred to as Frame**.** Switches and Bridges are common Data Link Layer devices.

The Data Link Layer is divided into two sublayers:

- Logical Link Control (LLC)
- Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of the **NIC (Network Interface Card)**. DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP (Address Resolution Protocol) request onto the wire asking, "Who has that IP address?" and the destination host will reply with its MAC address.

Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

- **Physical Addressing:** After creating frames, the Data link layer adds physical addresses (MAC **addresses)** of the sender and/or receiver in the header of each frame.

- **Error Control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

- **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.

- **Access Control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

Layer 3: Network Layer

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender and receiver's IP address are placed in the header by the network layer. Segment in the Network layer is referred to as Packet**.** Network layer is implemented by networking devices such as routers and switches.

Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.

- **Logical Addressing:** To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender and receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.
- **Layer 4: Transport Layer**
- The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as **Segments**. It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits

the data if an error is found. Protocols used in Transport Layer are TCP, UDP NetBIOS, PPTP.

Network Protocols

A protocol is a set of rules or algorithms which define the way how two entities can communicate across the network and there exists a different protocol defined at each layer of the OSI model. A few such protocols are TCP, IP, UDP, ARP, DHCP, FTP, and so on.

- **Transmission Control Protocol/Internet Protocol (TCP/IP):**TCP/IP is the foundational protocol suite of the internet, enabling reliable communication. TCP Ensures data is delivered reliably and in order and IP routes data packets to their destination based on IP addresses.

- **Hypertext Transfer Protocol (HTTP) and HTTPS:** HTTP and HTTPS protocols used for transmitting web pages. **In HTTP** communication is unsecured and in **HTTPS** secured communication using SSL/TLS encryption.

- **Simple Mail Transfer Protocol (SMTP):** SMTP protocol used to send email. SMTP protocol works with other protocols like POP3 and IMAP for email retrieval.

- **File Transfer Protocol (FTP):** FTP protocol used for transferring files between computers. Includes commands for uploading, downloading, and managing files on a remote server.

- **Dynamic Host Configuration Protocol (DHCP):** DHCP protocol automatically assigns IP addresses to devices on a network. Reduces manual configuration and IP address conflicts.

- **Domain Name System (DNS):** DNS Translates human-friendly domain names into IP addresses. Ensures seamless navigation on the internet.

At the sender's side, the transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow and error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

- Generally, this destination port number is configured, either by default or manually. For example, when a web application requests a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

At the Receiver's side, Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

Functions of the Transport Layer

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.

- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus, by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services Provided by Transport Layer

- Connection-Oriented Service

- Connectionless Service

Layer 5: Session Layer

Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices. It also provides authentication and security. Protocols used in the Session Layer are NetBIOS, PPTP.

Functions of the Session Layer

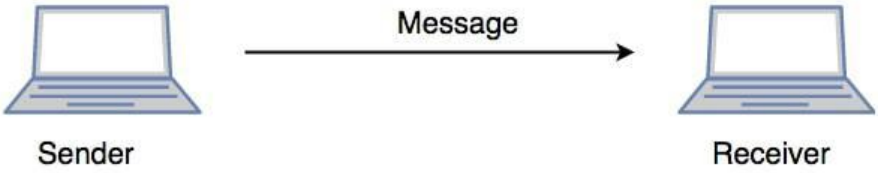
- **Session Establishment, Maintenance, and Termination:** The layer allows the two processes to establish, use, and terminate a connection.

- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely, and data loss is avoided.

- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full duplex.

Example

Let us consider a scenario where a user wants to send a message through some Messenger application running in their browser. The "**Messenger**" here acts as the application layer which provides the user with an interface to create the data. This message or so-called **Data** is compressed, optionally encrypted (if the data is sensitive), and converted into bits (0's and 1's) so that it can be transmitted.



Layer 6: Presentation Layer

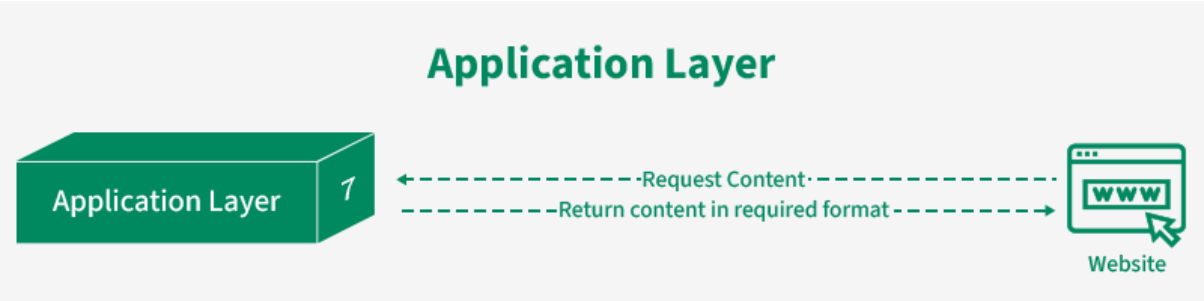
The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. Protocols used in the Presentation Layer are TLS/SSL (Transport Layer Security / Secure Sockets Layer).JPEG, MPEG, GIF, are standards or formats used for encoding data, which is part of the presentation layer's role.

Functions of the Presentation Layer

- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext, and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** Reduces the number of bits that need to be transmitted on the network.

Layer 7: Application Layer

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user. Protocols used in the Application layer are SMTP, FTP, DNS, etc.



Application Layer

Functions of the Application Layer

The main functions of the application layer are given below.

- **Network Virtual Terminal (NVT):** It allows a user to log on to a remote host.

- **File Transfer Access and Management (FTAM):** This application allows a user to access files in a remote host, retrieve files in a remote host, and manage or control files from a remote computer.

- **Mail Services: Provide email service.**

- Directory Services: This application provides distributed database sources and access for global information about various objects and services.

How Data Flows in the OSI Model?

When we transfer information from one device to another, it travels through 7 layers of OSI model. First data travels down through 7 layers from the sender's end and then climbs back 7 layers on the receiver's end.

Data flows through the OSI model in a step-by-step process:

- Application Layer: Applications create the data.

- Presentation Layer: Data is formatted and encrypted.

- Session Layer: Connections are established and managed.

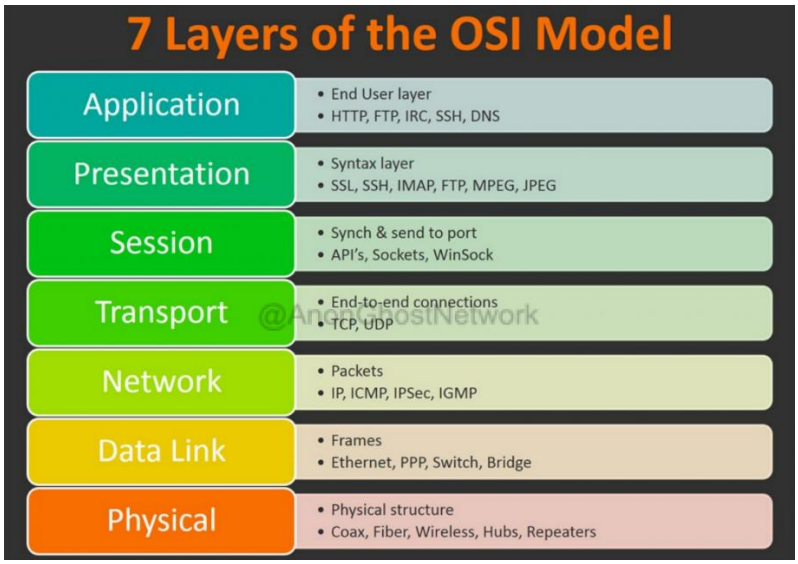
- Transport Layer: Data is broken into segments for reliable delivery.

- Network Layer: Segments are packaged into packets and routed.

- Data Link Layer: Packets are framed and sent to the next device.

- Physical Layer: Frames are converted into bits and transmitted physically.

Each layer adds specific information to ensure the data reaches its destination correctly, and these steps are reversed upon arrival.



We can understand how data flows through OSI Model with the help of an example mentioned below.

Let us suppose, **Person A** sends an e-mail to his friend **Person B**.

Step 1: Person A interacts with e-mail application like **Gmail**, **outlook**, etc. Writes his email to send. (This happens at **Application Layer**).

Step 2: At Presentation Layer, Mail application prepares for data transmission like encrypting data and formatting it for transmission.

Step 3: At Session Layer, there is a connection established between the sender and receiver on the internet.

Step 4: At Transport Layer, Email data is broken into smaller segments. It adds sequence number and error-checking information to maintain the reliability of the information.

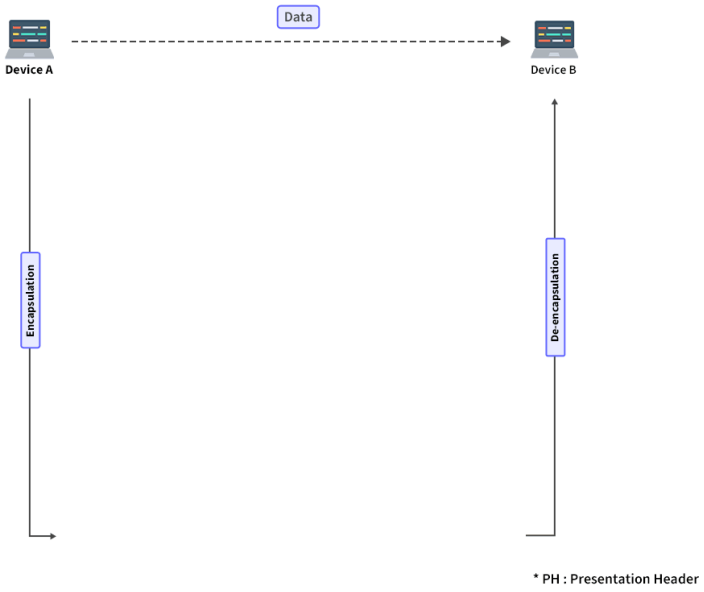
Step 5: At Network Layer, addressing of packets is done in order to find the best route for transfer.

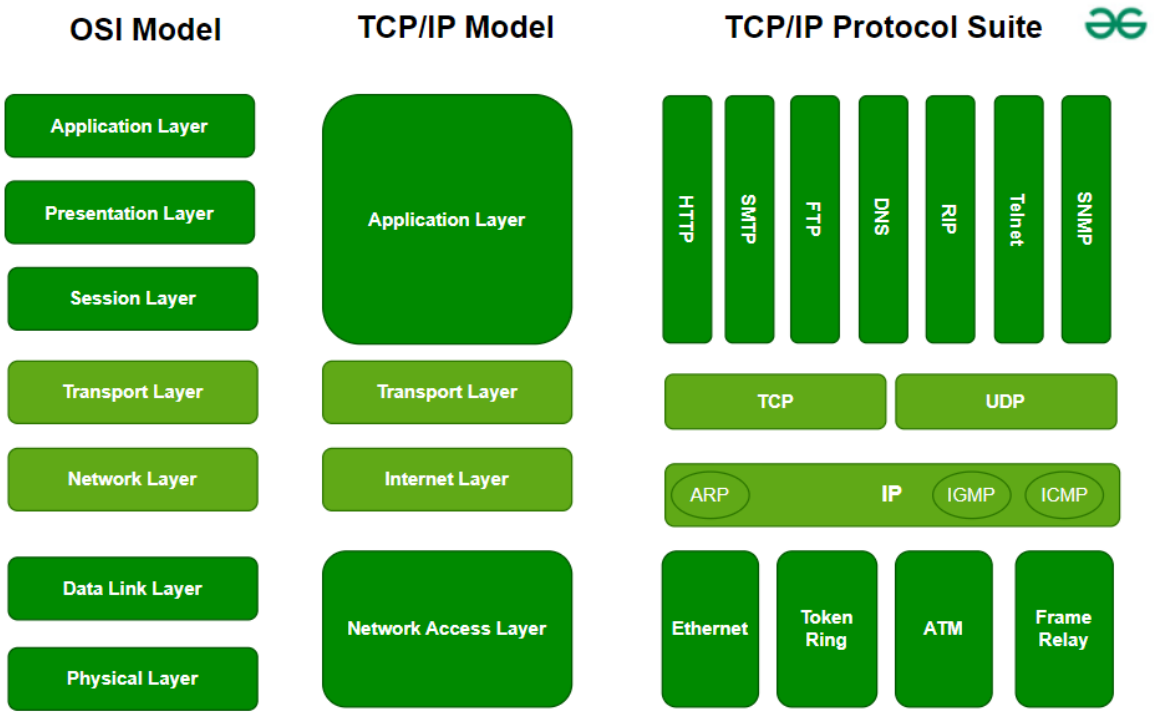
Step 6: At Data Link Layer, data packets are encapsulated into frames, then MAC address is added for local devices and then it checks for error using error detection.

Step 7: At Physical Layer, Frames are transmitted in the form of electrical/ optical signals over a physical network medium like ethernet cable or WiFi.

After the email reaches the receiver i.e. **Person B**, the process will reverse and decrypt the e-mail content. At last, the email will be shown on **Person B** email client.

Please refer the below animation for detailed flow.





Advantages of OSI Model

The OSI Model defines the communication of a computing system into 7 different layers. Its advantages include:

- It divides network communication into 7 layers which makes it easier to understand and troubleshoot.
- It standardizes network communications, as each layer has fixed functions and protocols.
- Diagnosing network problems is easier with the **OSI model.**
- It is easier to improve with advancements as each layer can get updates separately.

Disadvantages of OSI Model

- The OSI Model has seven layers, which can be complicated and hard to understand for beginners.
- In real-life networking, most systems use a simpler model called the Internet protocol suite (TCP/IP), so the OSI Model is not always directly applicable.
- Each layer in the OSI Model adds its own set of rules and operations, which can make the process more time-consuming and less efficient.
- The OSI Model is more of a theoretical framework, meaning it's great for understanding concepts but not always practical for implementation.

Network Protocols

A protocol is a set of rules or algorithms which define the way how two entities can communicate across the network and there exists a different protocol defined at each layer of the OSI model. A few such protocols are TCP, IP, UDP, ARP, DHCP, FTP, and so on.

- **Transmission Control Protocol/Internet Protocol (TCP/IP):**TCP/IP is the foundational protocol suite of the internet, enabling reliable communication. TCP Ensures data is delivered reliably and in order and IP routes data packets to their destination based on IP addresses.

- **Hypertext Transfer Protocol (HTTP) and HTTPS:** HTTP and HTTPS protocols used for transmitting web pages. **In HTTP** communication is unsecured and in **HTTPS** secured communication using SSL/TLS encryption.

- **Simple Mail Transfer Protocol (SMTP):** SMTP protocol used to send email. SMTP protocol works with other protocols like POP3 and IMAP for email retrieval.

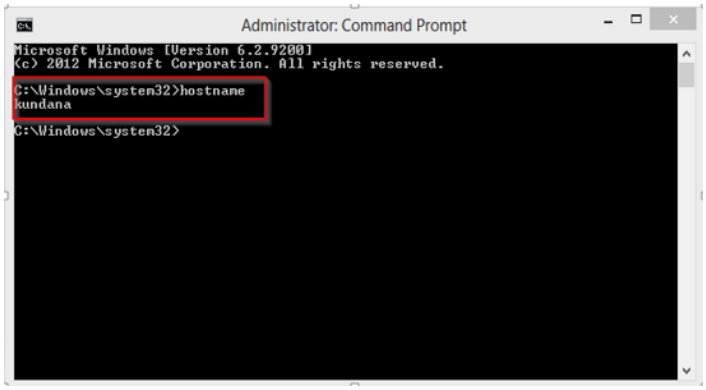
- **File Transfer Protocol (FTP):** FTP protocol used for transferring files between computers. Includes commands for uploading, downloading, and managing files on a remote server.

- **Dynamic Host Configuration Protocol (DHCP):** DHCP protocol automatically assigns IP addresses to devices on a network. Reduces manual configuration and IP address conflicts.

- **Domain Name System (DNS):** DNS Translates human-friendly domain names into IP addresses. Ensures seamless navigation on the internet.

Unique Identifiers of Network

Hostname: Each device in the network is associated with a unique device name known as Hostname. Type “hostname” in the command prompt (Administrator Mode) and press ‘Enter’, this displays the hostname of your machine.



IP Address (Internet Protocol address): Also known as the Logical Address, the IP Address is the network address of the system across the network. To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4)

address as a unique identifier to each device on the Internet. The length of an IPv4 address is 32 bits, hence, we have 2^{32} IP addresses available. The length of an IPv6 address is 128 bits.

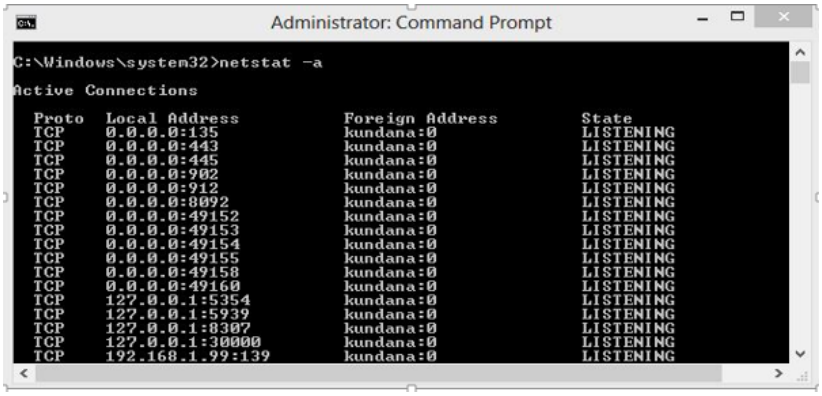
In **Windows** Type “ipconfig” in the command prompt and press ‘Enter’, this gives us the IP address of the device. For **Linux,** type “ifconfig” in the terminal and press ‘Enter’ this gives us the IP address of the device.

Port: A port can be referred to as a logical channel through which data can be sent/received to an application. Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.

A port number is a 16-bit integer; hence, we have 2^{16} ports available which are categorized as shown below:

Port Types	Range
Well known Ports	0 – 1023
Registered Ports	1024 – 49151
Ephemeral Ports	49152 - 65535

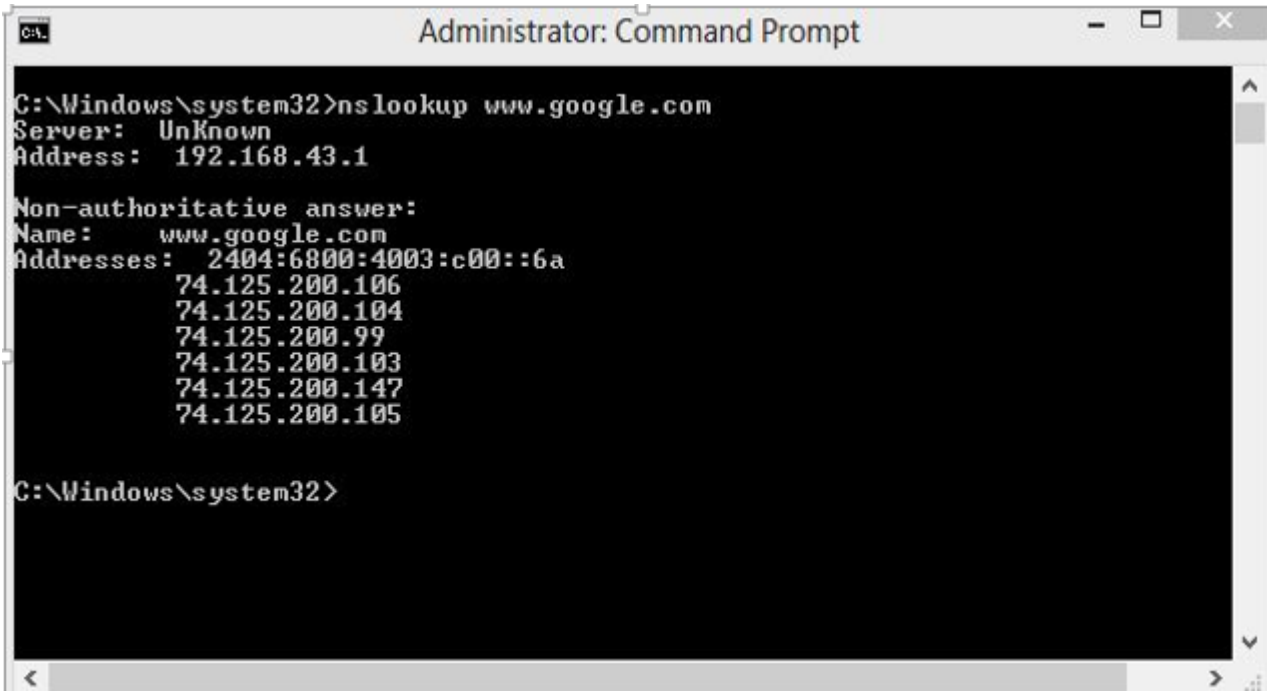
Number of ports: 65,536
Range: 0 – 65535
Type “netstat -a” in the command prompt and press ‘Enter’, this lists all the ports being used.



Socket: The unique combination of IP address and Port number together is termed a Socket.

Other Related Concepts

DNS Server: DNS stands for **Domain Name System**. DNS is basically a server that translates web addresses or URLs (ex: www.google.com) into their corresponding IP addresses. We don’t have to remember all the IP addresses of each and every website. The command ‘**nslookup**’ gives you the IP address of the domain you are looking for. This also provides information on our DNS Server. \



Domain IP Address

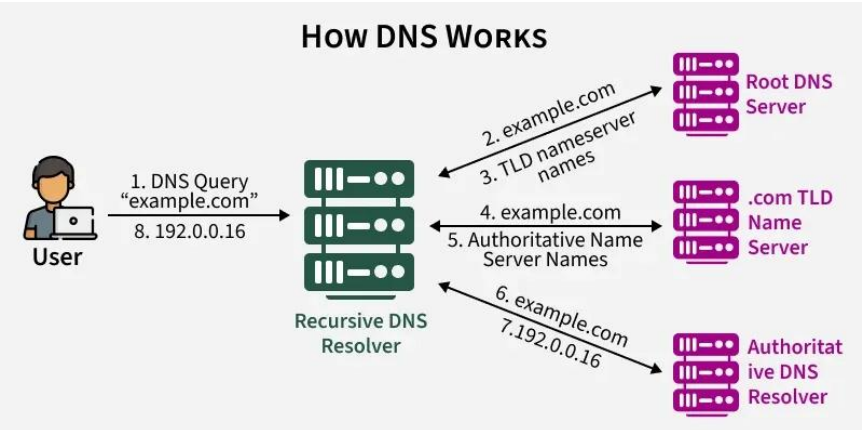
ARP: ARP stands for **Address Resolution Protocol**. It is used to convert an IP address to its corresponding physical address(i.e., MAC Address). ARP is used by the Data Link Layer to identify the MAC address of the Receiver's machine.

RARP: RARP stands for **Reverse Address Resolution Protocol**. As the name suggests, it provides the IP address of the device given a physical address as input. But RARP has become obsolete since the time DHCP has come into the picture.

The Domain Name System (DNS) is a critical component of computer networking. It converts easily recognizable domain names, such as www.example.com, into numerical IP addresses that computers use to identify each other on the network.

How DNS Works?

DNS works efficiently, translating user-friendly domain names into IP addresses, allowing seamless navigation on the internet. Below step by step working of DNS:



- **User Input:** When a user enters a domain name in a browser, the system needs to find its IP address.
- **DNS Query:** The user's device sends a DNS query to the DNS resolver.
- **Resolver Request:** The DNS resolver checks its cache for the IP address. If not found, it forwards the request to the root DNS server.
- **Root DNS Server:** The root DNS server provides the address of the TLD (Top-Level Domain) server for the specific domain extension (e.g., .com).
- **TLD DNS Server:** The TLD server directs the resolver to the authoritative DNS server for the actual domain.
- **Authoritative DNS Server:** The authoritative DNS server knows the IP address for the domain and provides it to the resolver.
- **Response to User:** The resolver stores the IP address in its cache and sends it to the user's device.
- **Access Website**: With the IP address, the user's device can access the desired website.

Network Security

Ensuring the security of a network is crucial to protect data and resources from unauthorized access and attacks. Key aspects of network security include:

- **Firewalls:** Devices or software that monitor and control incoming and outgoing network traffic based on security rules.
- **Encryption:** The process of encoding data to prevent unauthorized access. Commonly used in VPNs, HTTPS, and secure email.
- **Intrusion Detection Systems (IDS):** Tools that monitor network traffic for suspicious activity and potential threats.
- **Access Control:** Mechanisms that restrict access to network resources based on user identity and role.
- **Regular Updates and Patching:** Keeping software and hardware up to date to protect against vulnerabilities.

Characteristics of Computer Networks

Computer networks are systems that connect multiple devices to facilitate communication, resource sharing, and data transfer. They possess several key characteristics that ensure efficient and secure operations. These characteristics include Security, Reliability, Scalability, Performance, Fault Tolerance, and hardware and software support.