What is a Network or Networking?

What is A Network?

A **network** is a set of devices connected by communication links. A network is simply two or more computers that are linked together. A node can be a computer, printer, or any other device capable of sending and receiving data generated by other nodes on the network.

Networks can be classified into several types including *Local Area Networks*, *Wide Area Networks, Metropolitan Area Networks*, and wireless networks such as *Wi-Fi and cellular networks*.

Network Criteria

A network must meet the following network criteria:

- **Performance –** It is measured by transit time and response time also depends on users, medium, hardware, and software.
- **Reliability –** reliability is measured by the frequency of failure.
- **Security –** Security protects data from unauthorized access.

Risks of Network Computing

The security of a computer network is challenged every day by:

- Equipment malfunctions
- System failures
- Computer hackers
- Virus attacks

Categories of Networks

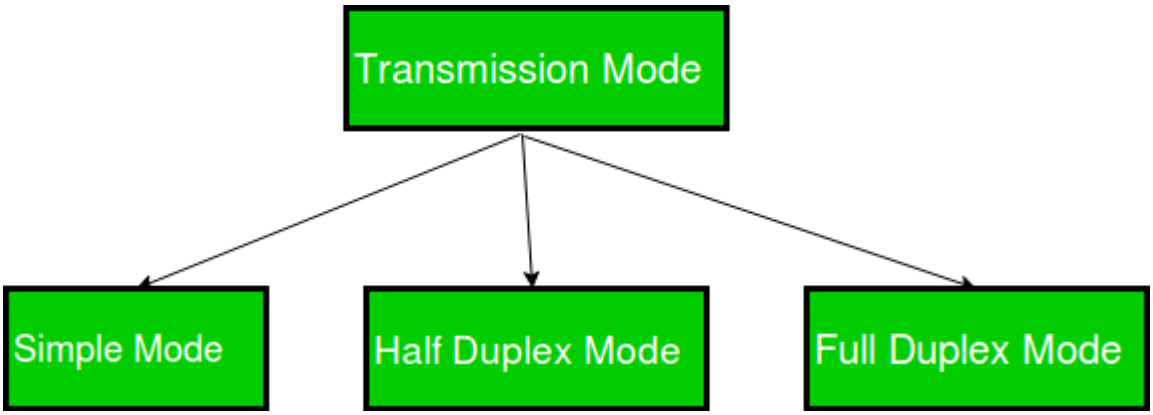
It is categorized into three types: LAN, MAN, WAN.

Into which categories of network falls is determined by its size, its ownership, the distance it covers, and its physical architecture.

Transmission Modes in Computer Networks (Simplex, Half-Duplex and Full-Duplex)

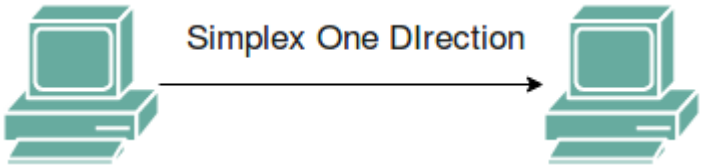
What is Transmission Modes?

Transmission mode means transferring data between two devices. It is also known as a communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected. **There are three types of transmission modes:**



Simplex Mode

In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.
Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.



Advantages of Simplex Mode

- Simplex mode is the easiest and most reliable mode of communication.
- It is the most cost-effective mode, as it only requires one communication channel.
- There is no need for coordination between the transmitting and receiving devices, which simplifies the communication process.
- Simplex mode is particularly useful in situations where feedback or response is not required, such as broadcasting or surveillance.

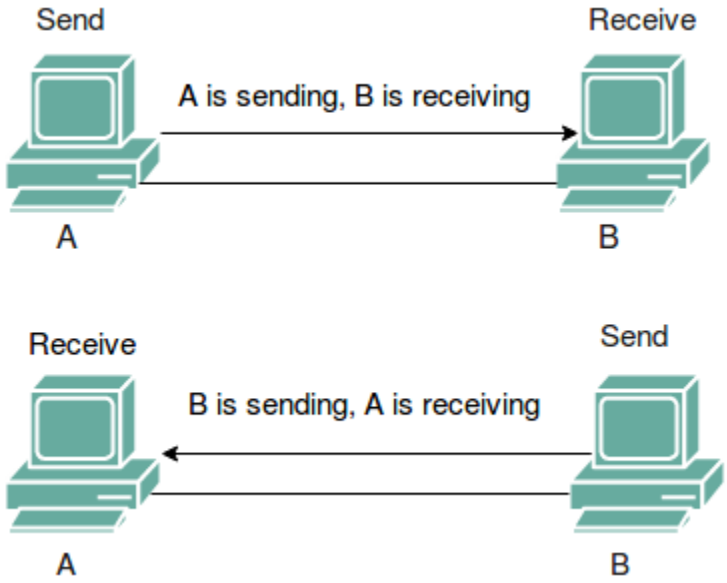
Disadvantages of Simplex Mode

- Only one-way communication is possible.
- There is no way to verify if the transmitted data has been received correctly.
- Simplex mode is not suitable for applications that require bidirectional communication.

Half-Duplex Mode

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.
Example: Walkie-talkie in which message is sent one at a time and messages are sent in both directions.

Channel capacity=Bandwidth * Propagation Delay



Advantages of Half Duplex Mode

- Half-duplex mode allows for bidirectional communication, which is useful in situations where devices need to send and receive data.
- It is a more efficient mode of communication than simplex mode, as the channel can be used for both transmission and reception.
- Half-duplex mode is less expensive than full-duplex mode, as it only requires one communication channel.

Disadvantages of Half Duplex Mode

- Half-duplex mode is less reliable than Full-Duplex mode, as both devices cannot transmit at the same time.
- There is a delay between transmission and reception, which can cause problems in some applications.
- There is a need for coordination between the transmitting and receiving devices, which can complicate the communication process.

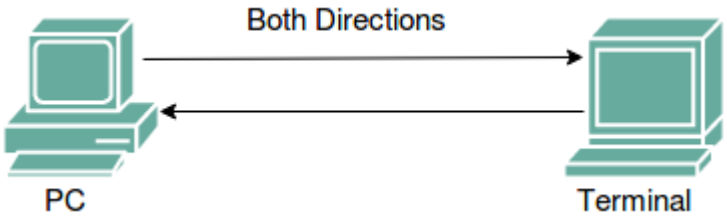
Full-Duplex Mode

In full-duplex mode, both stations can transmit and receive simultaneously. In full_duplex mode, signals going in one direction share the capacity of the link with signals going in another direction, this sharing can occur in two ways:

- Either the link must contain two physically separate transmission paths, one for sending and the other for receiving.
- Or the capacity is divided between signals traveling in both directions.

Full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.
Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.

Channel Capacity=2* Bandwidth*propagation Delay



Advantages of Full-Duplex Mode

- Full-duplex mode allows for simultaneous bidirectional communication, which is ideal for real-time applications such as video conferencing or online gaming.
- It is the most efficient mode of communication, as both devices can transmit and receive data simultaneously.
- Full-duplex mode provides a high level of reliability and accuracy, as there is no need for error correction mechanisms.

Disadvantages of Full-Duplex Mode

- Full-duplex mode is the most expensive mode, as it requires two communication channels.
- It is more complex than simplex and half-duplex modes, as it requires two physically separate transmission paths or a division of channel capacity.
- Full-duplex mode may not be suitable for all applications, as it requires a high level of bandwidth and may not be necessary for some types of communication.

Difference Between Simplex, Half duplex, and Full Duplex Transmission Modes

Parameters	Simplex	Half Duplex	Full Duplex
The direction of communication	Simplex mode is a uni-directional communication.	Half Duplex mode is a two-way directional communication but one at a time.	Full Duplex mode is a two-way directional communication simultaneously.
Sender and Receiver	In simplex mode, Sender can send the data but that sender can't receive the data.	In Half Duplex mode, Sender can send the data and also can receive the data but one at a time.	In Full Duplex mode, Sender can send the data and also can receive the data simultaneously.
Channel usage	Usage of one channel for the transmission of data.	Usage of one channel for the transmission of data.	Usage of two channels for the transmission of data.
Performance	The simplex mode provides less performance than half duplex and full duplex.	The Half Duplex mode provides less performance than full duplex.	Full Duplex provides better performance than simplex and half duplex mode.
Bandwidth Utilization	Simplex utilizes the maximum of a single bandwidth.	The Half-Duplex involves lesser utilization of single bandwidth at the time of transmission.	The Full-Duplex doubles the utilization of transmission bandwidth.
Suitable for	It is suitable for those transmissions when there is requirement of full bandwidth for delivering data.	It is suitable for those transmissions when there is requirement of sending data in both directions, but not at the same time.	It is suitable for those transmissions when there is requirement of sending and receiving data simultaneously in both directions.

Parameters	Simplex	Half Duplex	Full Duplex
Examples	Example of simplex mode are: Keyboard and monitor.	Example of half duplex mode is: Walkie-Talkies.	Example of full duplex mode is: Telephone.

Conclusion

Transmission modes enable communication between devices and are classified into three types: simplex mode, which allows unidirectional communication and is cost-effective but supports only one-way data transfer; half-duplex mode, which allows bidirectional communication but not simultaneously, offering a balance between efficiency and cost; and full-duplex mode, which enables simultaneous two-way communication, providing the highest efficiency and reliability but is the most complex and expensive.

Types of Computer Networks

A computer network is a cluster of computers over a shared communication path that works to share resources from one computer to another, provided by or located on the network nodes. In this article, we will discuss computer networks and their types.

What is a Computer Network?

A computer network is a system that connects many independent computers to share information (data) and resources. The integration of computers and other different devices allows users to communicate more easily. A computer network is a collection of two or more computer systems that are linked together. A network connection can be established using either cable or wireless media. Hardware and software are used to connect computers and tools in any network.

Basic Terminologies of Computer Networks

- **Network:** A network is a collection of computers and devices that are connected together to enable communication and data exchange.
- **Nodes:** Nodes are devices that are connected to a network. These can include computers, Servers, Printers, Routers, Switches, and other devices.
- **Protocol:** A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include TCP/IP, HTTP, and FTP.
- **Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh, and tree.
- **Service Provider Networks:** These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.
- **IP Address**: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.
- **DNS:** The Domain Name System (DNS) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.
- **Firewall:** A firewall is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

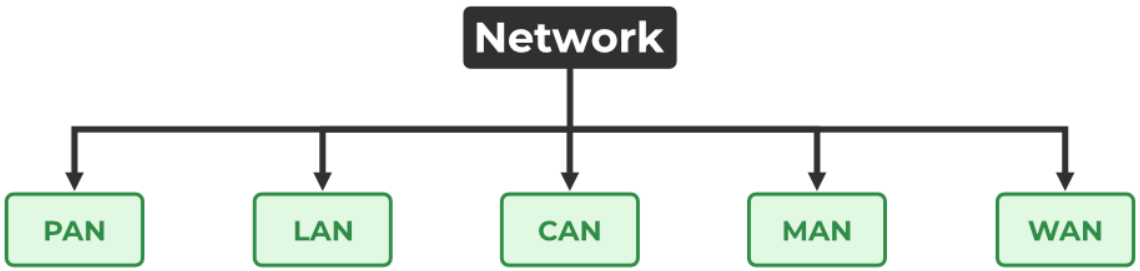
Uses of Computer Networks

- Communicating using email, video, instant messaging, etc.
- Sharing devices such as printers, scanners, etc.
- Sharing files.
- Sharing software and operating programs on remote systems.
- Allowing network users to easily access and maintain information.

Types of Computer Networks

There are mainly five types of Computer Networks

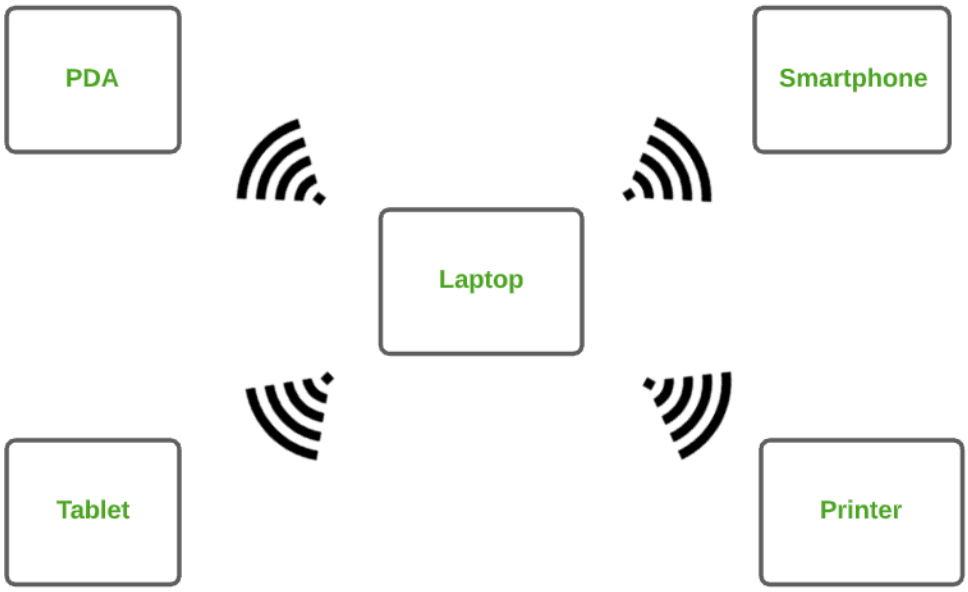
1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Campus Area Network (CAN)
4. Metropolitan Area Network (MAN)
5. Wide Area Network (WAN)



Types of Computer Networks

1. Personal Area Network (PAN)

PAN is the most basic type of computer network. It is a type of network designed to connect devices within a short range, typically around one person. It allows your personal devices, like smartphones, tablets, laptops, and wearables, to communicate and share data with each other. 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. This uses Bluetooth**,** IrDA**,** and Zigbee as technology. Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.



Personal Area Network (PAN)

Types of PAN

- **Wireless Personal Area Networks:** Wireless Personal Area Networks are created by simply utilising wireless technologies such as WiFi and Bluetooth. It is a low-range network.
- **Wired Personal Area Network:** A wired personal area network is constructed using a USB.

Advantages of PAN

- PAN is relatively flexible and provides high efficiency for short network ranges.
- It needs easy setup and relatively low cost.
- It does not require frequent installations and maintenance
- It is easy and portable.
- Needs fewer technical skills to use.

Disadvantages of PAN

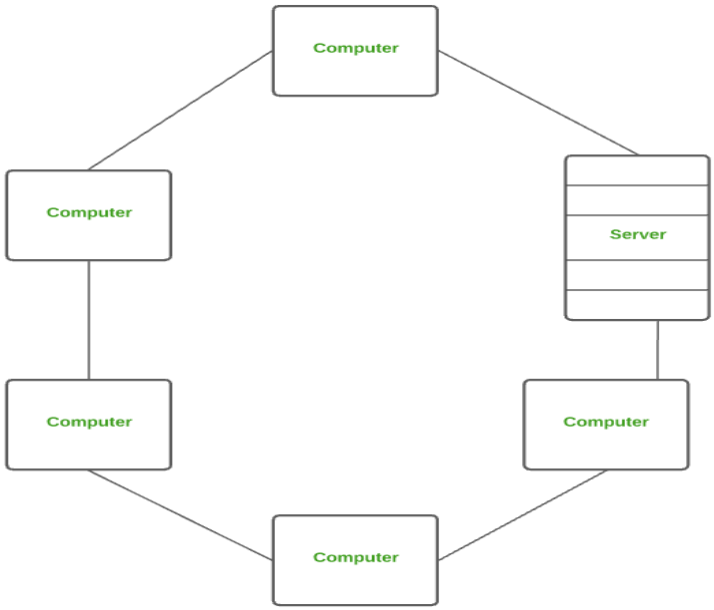
- Low network coverage area/range.
- Limited to relatively low data rates.
- Devices are not compatible with each other.
- Inbuilt WPAN devices are a little bit costly.

Applications of PAN

- Home and Offices
- Organizations and the Business sector
- Medical and Hospital
- School and College Education
- Military and Defense

2. Local Area Network (LAN)

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. Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.



Local Area Network (LAN)

Advantages of a LAN

- **Privacy:** LAN is a private network, thus no outside regulatory body controls it, giving it a privacy.
- **High Speed:** LAN offers a much higher speed(around 100 mbps) and data transfer rate comparatively to WAN.
- **Supports different transmission mediums:** LAN support a variety of communications transmission medium such as an Ethernet cable (thin cable, thick cable, and twisted pair), fiber and wireless transmission.

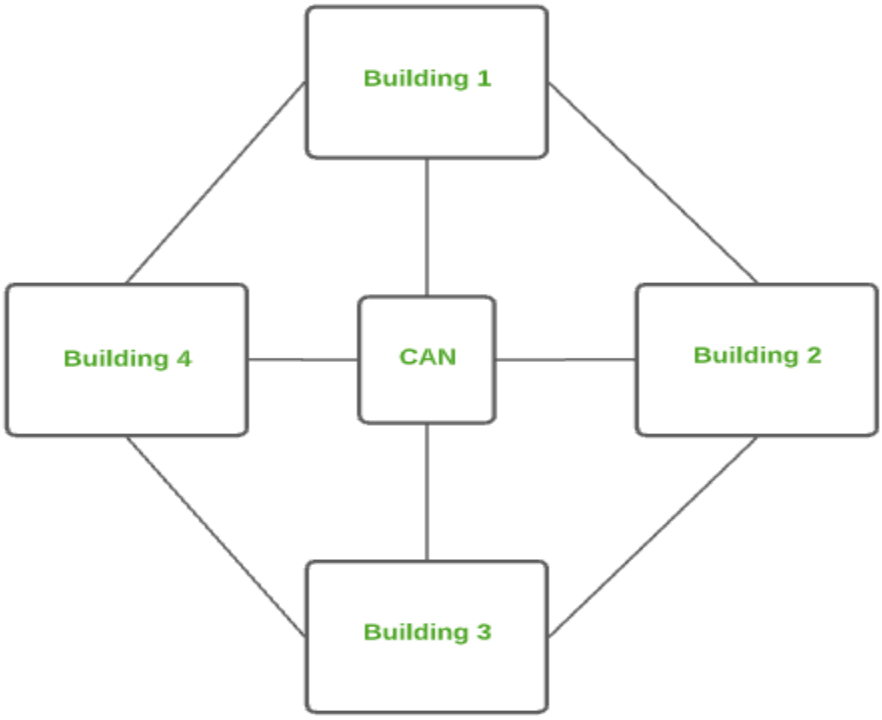
- **Inexpensive and Simple:** A LAN usually has low cost, installation, expansion and maintenance and LAN installation is relatively easy to use, good scalability.

Disadvantages of LAN

- The initial setup costs of installing Local Area Networks is high because there is special software required to make a server.
- Communication devices like an ethernet cable, switches, hubs, routers, cables are costly.
- LAN administrator can see and check personal data files as well as Internet history of each and every LAN user. Hence, the privacy of the users are violated
- LANs are restricted in size and cover only a limited area
- Since all the data is stored in a single server computer, if it can be accessed by an unauthorized user, can cause a serious data security threat.

3. Campus Area Network (CAN)

CAN is bigger than a LAN but smaller than a MAN. This is a type of computer network that is usually used in places like a school or colleges. This network covers a limited geographical area that is, it spreads across several buildings within the campus. CAN mainly use Ethernet technology with a range from 1km to 5km. Its transmission speed is very high with a moderate maintenance cost and moderate cost. Examples of CAN are networks that cover schools, colleges, buildings, etc.



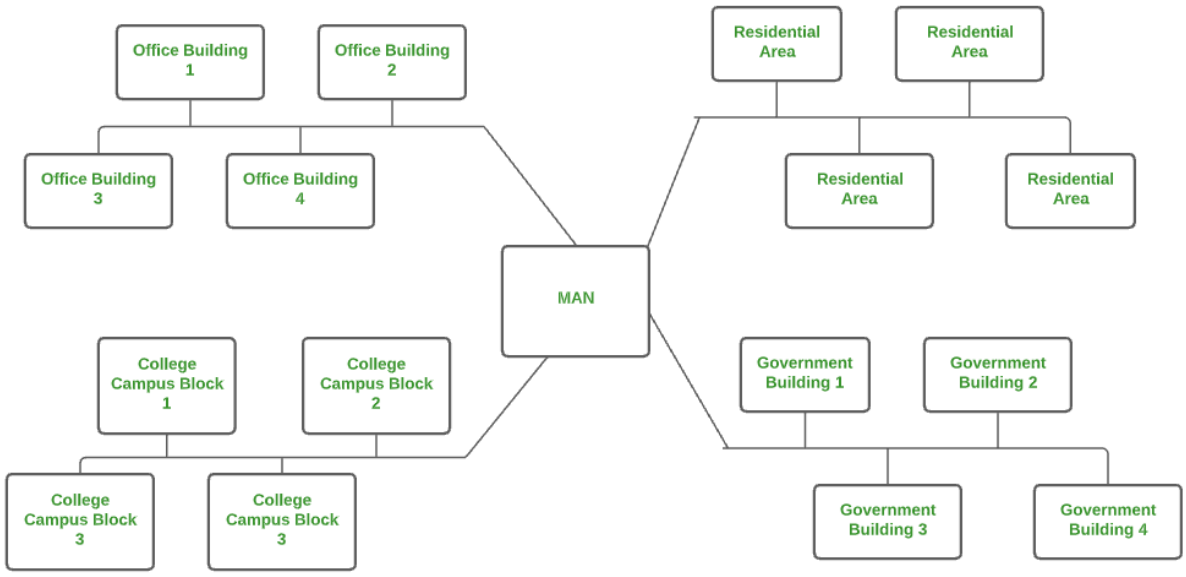
Campus Area Network (CAN)

Advantages of CAN

- **Speed:** Communication within a CAN takes place over Local Area Network (LAN) so data transfer rate between systems is little bit fast than Internet.
- **Security:** Network administrators of campus take care of network by continuous monitoring, tracking and limiting access. To protect network from unauthorized access firewall is placed between network and internet.
- **Cost effective:** With a little effort and maintenance, network works well by providing fast data transfer rate with multi-departmental network access. It can be enabled wirelessly, where wiring and cabling costs can be managed. So to work with in a campus using CAN is cost-effective in view of performance

4. 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 uses FDDI, CDDI, and ATM as the technology with a range from 5km to 50km. Its transmission speed is average. It is difficult to maintain and it comes with a high cost. Examples of MAN are networking in towns, cities, a single large city, a large area within multiple buildings, etc.



Metropolitan Area Network (MAN)

Advantages of MAN

- MAN offers high-speed connectivity in which the speed ranges from 10-100 Mbps.
- The security level in MAN is high and strict as compared to WAN.

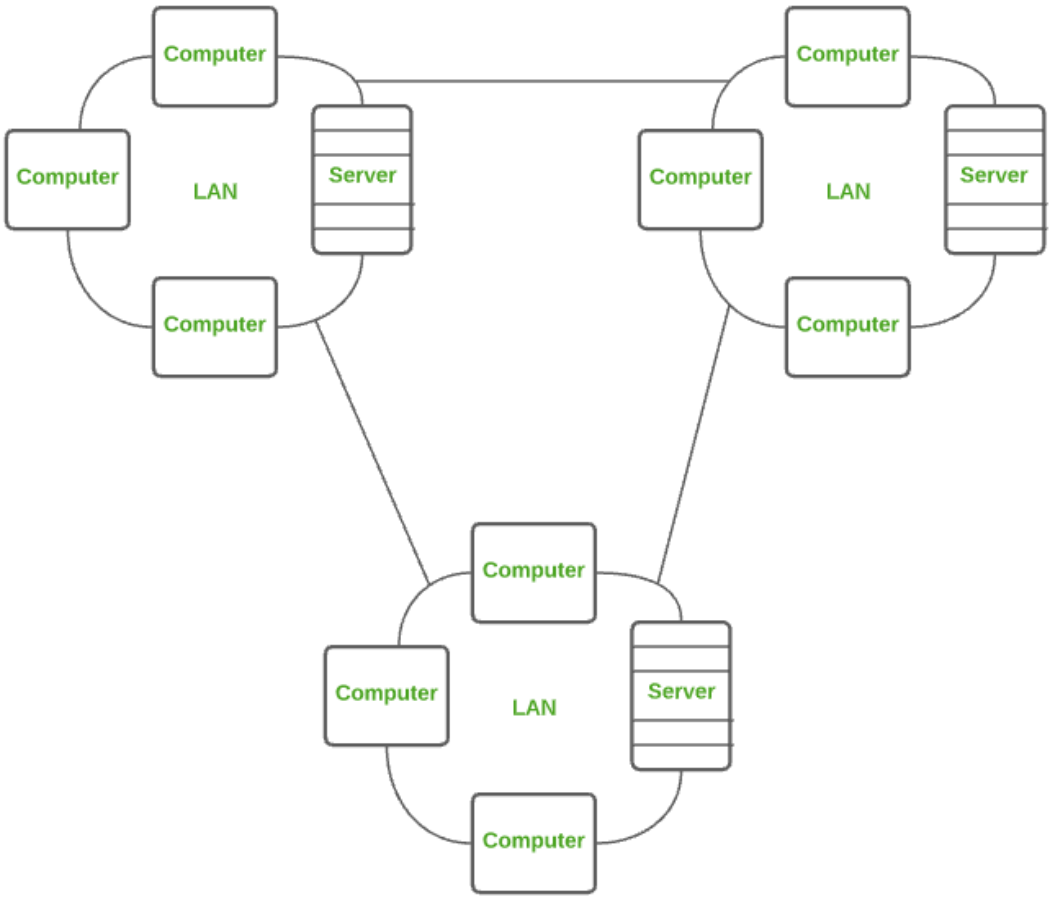
- It support to transmit data in both directions concurrently because of dual bus architecture.
- MAN can serve multiple users at a time with the same high-speed internet to all the users.
- MAN allows for centralized management and control of the network, making it easier to monitor and manage network resources and security.

Disadvantages of MAN

- The architecture of MAN is quite complicated hence, it is hard to design and maintain.
- This network is highly expensive because it required the high cost to set up fiber optics.
- It provides less fault tolerance.
- The Data transfer rate in MAN is low when compare to LANs.

5. Wide Area Network (WAN)

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. WAN can also be defined as a group of local area networks that communicate with each other with a range above 50km. Here we use Leased-Line & Dial-up technology. Its transmission speed is very low and it comes with very high maintenance and very high cost. The most common example of WAN is the Internet.



Wide Area Network (WAN)

Advantages of WAN

- It covers large geographical area which enhances the reach of organisation to transmit data quickly and cheaply.
- The data can be stored in centralised manner because of remote access to data provided by WAN.
- The travel charges that are needed to cover the geographical area of work can be minimised.
- WAN enables a user or organisation to connect with the world very easily and allows to exchange data and do business at global level.

Disadvantages of WAN

- Traffic congestion in Wide Area Network is very high.
- The fault tolerance ability of WAN is very less.
- Noise and error are present in large amount due to multiple connection point.
- The data transfer rate is slow in comparison to LAN because of large distances and high number of connected system within the network.

Comparison between Different Computer Networks

Parameters	PAN	LAN	CAN	MAN	WAN
Full Name	Personal Area Network	Local Area Network	Campus Area Network	Metropolitan Area Network	Wide Area Network
Technology	Bluetooth, IrDA,Zigbee	Ethernet & Wifi	Ethernet	FDDI, CDDi. ATM	Leased Line, Dial-Up
Range	1-100 m	Upto 2km	1 – 5 km	5-50 km	Above 50 km
Transmission Speed	Very High	Very High	High	Average	Low
Ownership	Private	Private	Private	Private or Public	Private or Public
Maintenance	Very Easy	Easy	Moderate	Difficult	Very Difficult
Cost	Very Low	Low	Moderate	High	Very High

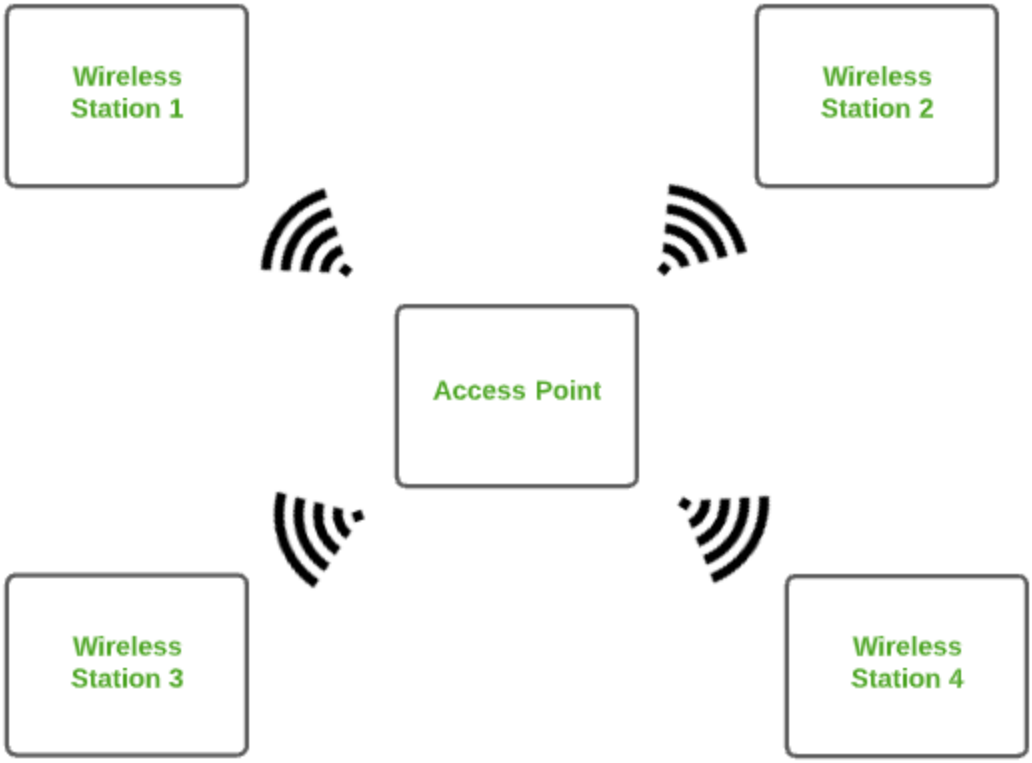
Other Types of Computer Networks

- Wireless Local Area Network (WLAN)
- Storage Area Network (SAN)
- System-Area Network (SAN)
- Passive Optical Local Area Network (POLAN)
- Enterprise Private Network (EPN)
- Virtual Private Network (VPN)

- Home Area Network (HAN)

1. Wireless Local Area Network (WLAN)

WLAN is a type of computer network that acts as a local area network but makes use of wireless network technology like Wi-Fi. This network doesn't allow devices to communicate over physical cables like in LAN but allows devices to communicate wirelessly. The most common example of WLAN is Wi-Fi.

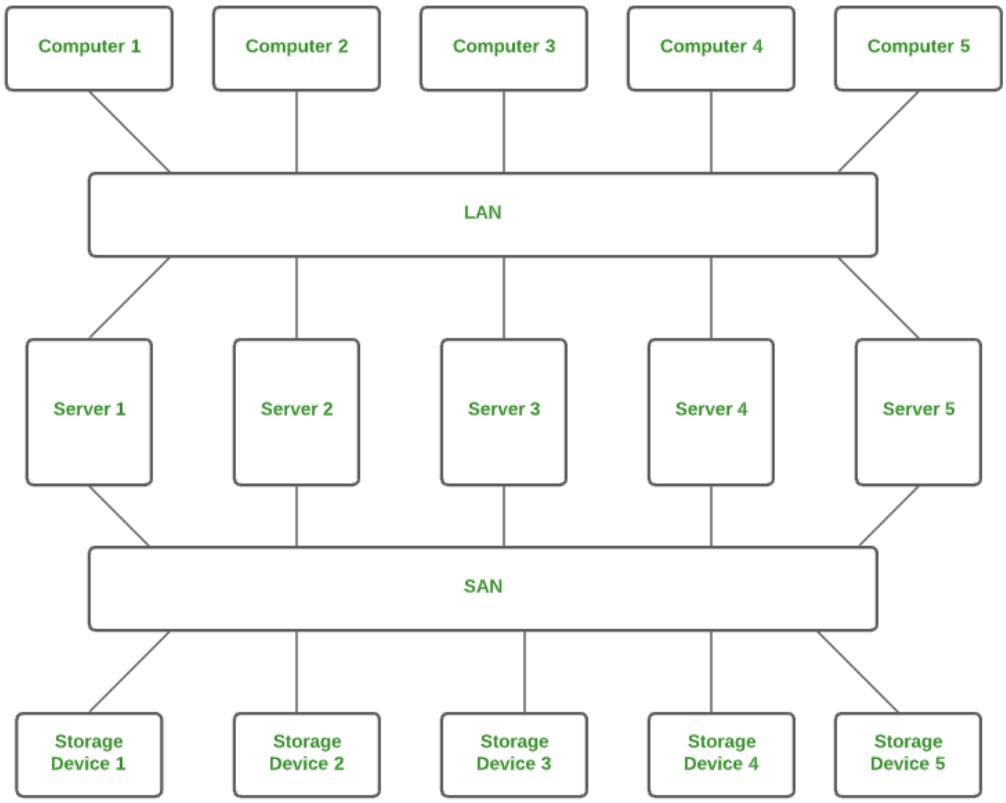


Wireless Local Area Network (WLAN)

There are several computer networks available; more information is provided below.

2. Storage Area Network (SAN)

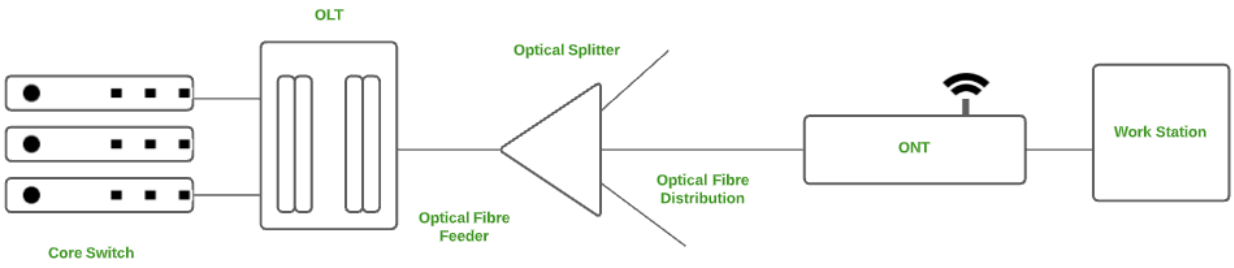
SAN is a type of computer network that is high-speed and connects groups of storage devices to several servers. This network does not depend on LAN or WAN. Instead, a SAN moves the storage resources from the network to its high-powered network. A SAN provides access to block-level data storage. Examples of SAN are a network of disks accessed by a network of servers.



Storage Area Network (SAN)

3. Passive Optical Local Area Network (POLAN)

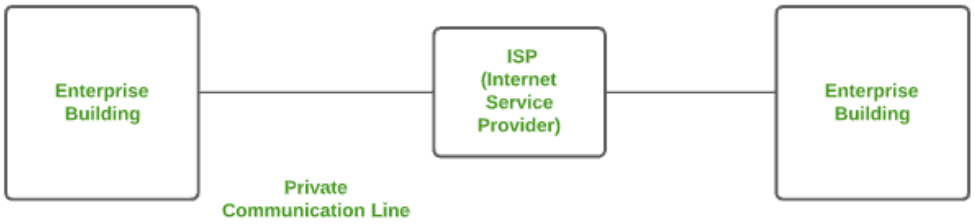
A POLAN is a type of computer network that is an alternative to a LAN. POLAN uses optical splitters to split an optical signal from a single strand of single-mode optical fiber to multiple signals to distribute users and devices. In short, POLAN is a point to multipoint LAN architecture.



Passive Optical Local Area Network (POLAN)

4. Enterprise Private Network (EPN)

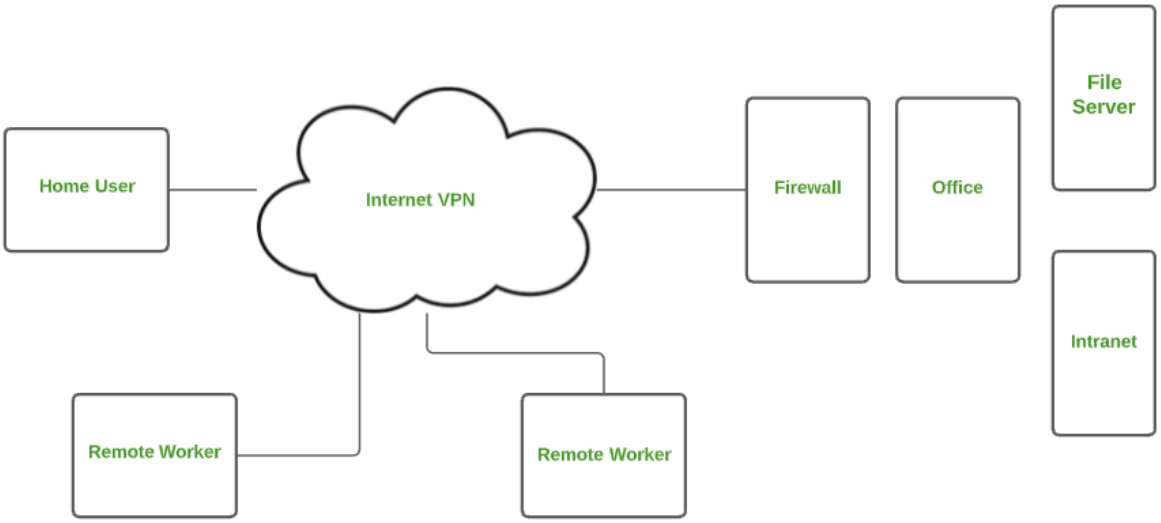
EPN is a type of computer network mostly used by businesses that want a secure connection over various locations to share computer resources.



Enterprise Private Network (EPN)

5. Virtual Private Network (VPN)

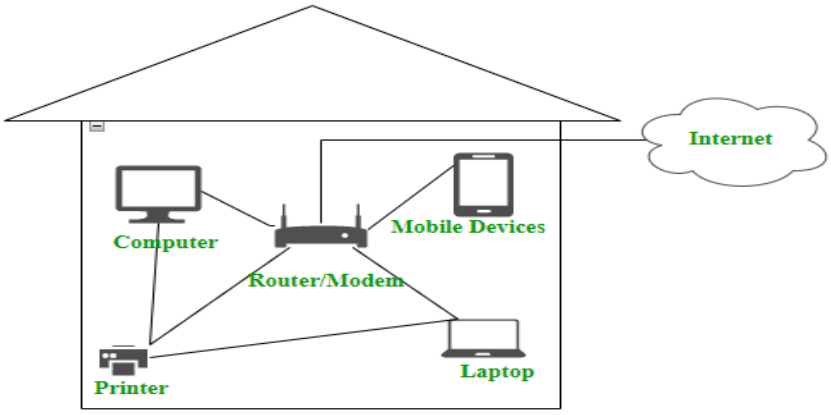
A VPN is a type of computer network that extends a private network across the internet and lets the user send and receive data as if they were connected to a private network even though they are not. Through a virtual point-to-point connection users can access a private network remotely. VPN protects you from malicious sources by operating as a medium that gives you a protected network connection.



Virtual Private Network (VPN)

6. Home Area Network (HAN)

Many of the houses might have more than a computer. To interconnect those computers and with other peripheral devices, a network should be established similar to the local area network (LAN) within that home. Such a type of network that allows a user to interconnect multiple computers and other digital devices within the home is referred to as Home Area Network (HAN). HAN encourages sharing of resources, files, and programs within the network. It supports both wired and wireless communication.



Home Area Network

Home Area Network (HAN)

Internetwork

An internet network is defined as two or more computer network LANs, WANs, or computer network segments that are connected by devices and configured with a local addressing system. The method is known as internetworking. There are two types of Internetwork.

- **Intranet**: An internal network within an organization that enables employees to share data, collaborate, and access resources. Intranets are not accessible to the public and use private IP addresses.
- **Extranet**: Extranets extend the intranet to authorized external users, such as business partners or clients. They provide controlled access to specific resources while maintaining security.

Advantages of Computer Network

- **Central Storage of Data:** Files are stored on a central storage database which helps to easily access and available to everyone.
- **Connectivity:** A single connection can be routed to connect multiple computing devices.
- **Sharing of Files:** Files and data can be easily shared among multiple devices which helps in easily communicating among the organization.
- **Security through Authorization:** Computer Networking provides additional security and protection of information in the system.

Disadvantages of Computer Network

- **Virus and Malware:** A virus is a program that can infect other programs by modifying them. Viruses and Malware can corrupt the whole network.
- **High Cost of Setup:** The initial setup of Computer Networking is expensive because it consists of a lot of wires and cables along with the device.
- **loss of Information:** In case of a System Failure, might lead to some loss of data.
- **Management of Network:** Management of a Network is somehow complex for a person, it requires training for its proper use.

What is Network Topology?

Network topology refers to the arrangement of different elements like nodes, links, or devices in a computer network. It defines how these components are connected and interact with each other. Understanding various types of network topologies helps in designing efficient and robust networks. Common types include bus, star, ring, mesh, and tree topologies, each with its own advantages and disadvantages. In this article, we are going to discuss different types of network topology their advantages and disadvantages in detail.

Types of Network Topology

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology** . The various network topologies are:

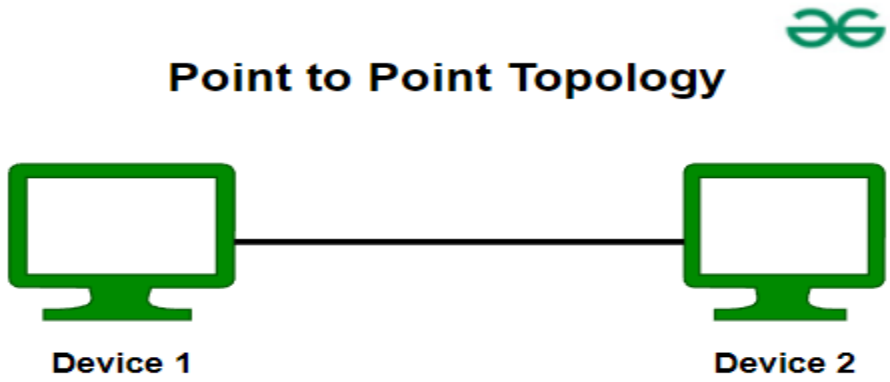
- Point to Point Topology
- Mesh Topology
- Star Topology
- Bus Topology
- Ring Topology

- Tree Topology
- Hybrid Topology

A strong understanding of network topologies is essential for competitive exams like GATE, where computer networks are a significant subject. To deepen your knowledge and enhance your exam preparation, consider enrolling in the GATE CS Self-Paced Course . This course covers all critical networking concepts, including detailed explanations of various network topologies, equipping you with the expertise needed to excel in your exams.

Point to Point Topology

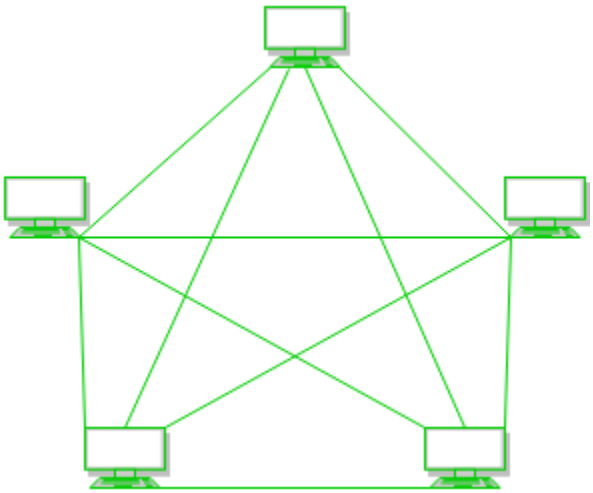
Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Point to Point Topology

Mesh Topology

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



Mesh Topology

Figure 1 : Every device is connected to another via dedicated channels. These channels are known as links.

- 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 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. 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 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.

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

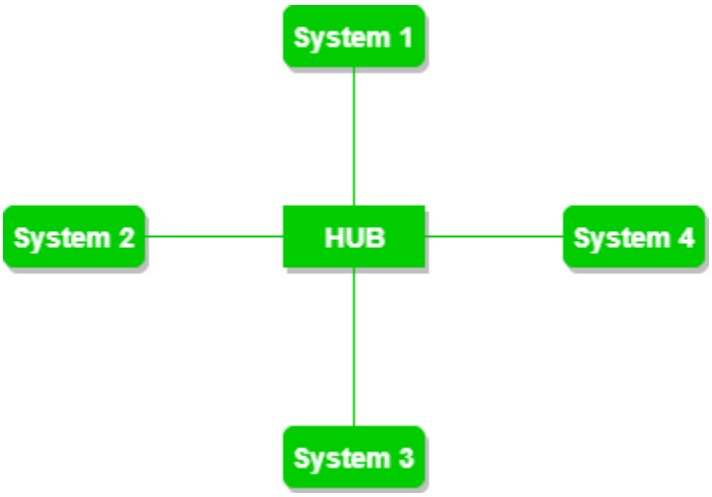
- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

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.

For more, refer to the Advantages and Disadvantages of Mesh Topology .

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

Figure 2 : A star topology having four systems connected to a single point of connection i.e. hub.

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

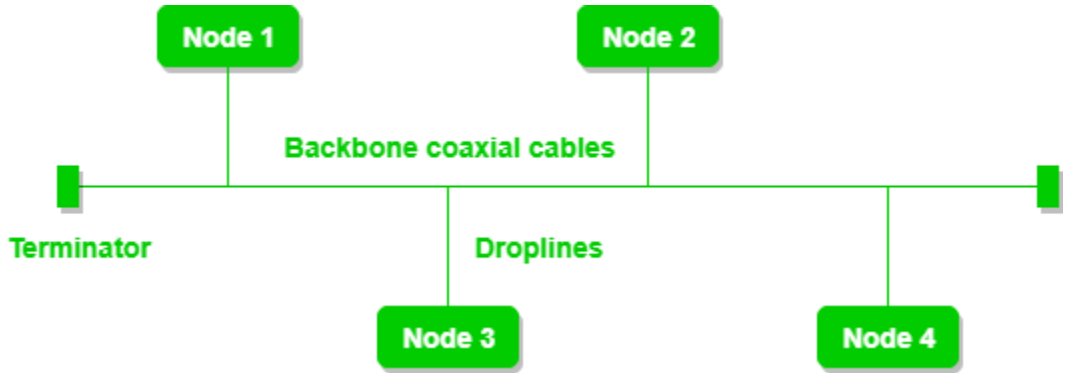
- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

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.

For more, refer to the Advantages and Disadvantages of Star Topology.

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

Figure 3 : A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

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

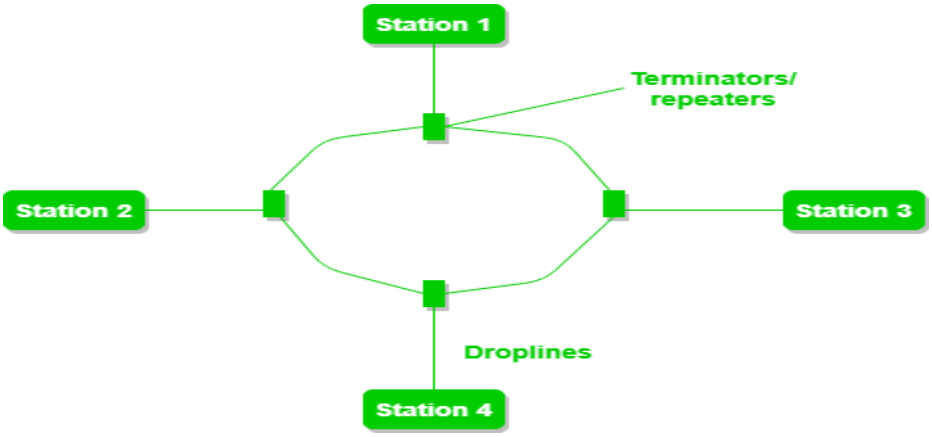
- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted 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. For more, refer to the Advantages and Disadvantages of Bus Topology .

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

Figure 4 : A ring topology comprises 4 stations connected with each forming a ring.

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

1. One station is known as a **monitor** station which takes all the responsibility for performing the operations.
2. 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.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. 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

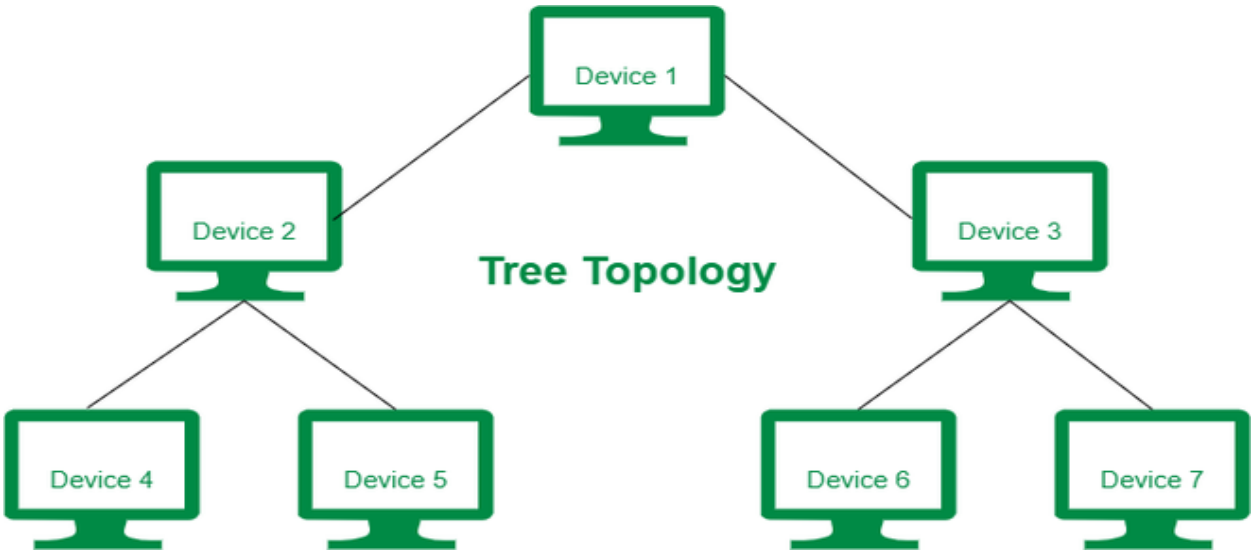
- The failure of a single node in the network can cause the entire network to fail.

- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

For more, refer to the Advantages and Disadvantages of Ring Topology .

Tree Topology

This 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

Figure 5 : In this, 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 traveled 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.

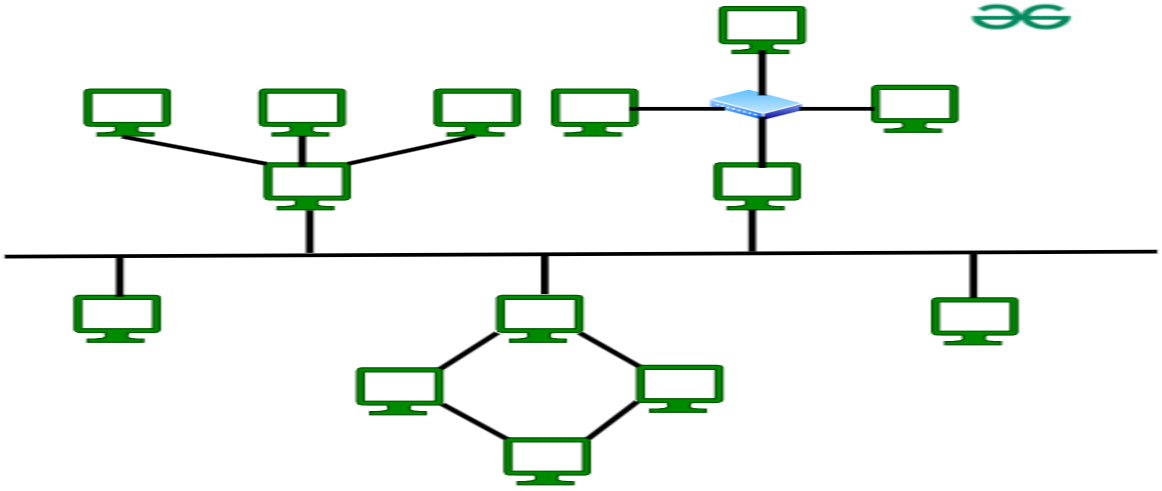
- If new devices are added, it becomes difficult to reconfigure.

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.

For more, refer to the Advantages and Disadvantages of Tree Topology .

Hybrid Topology

This topological technology 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.

For more, refer to the Advantages and Disadvantages of Hybrid Topology .

Conclusion

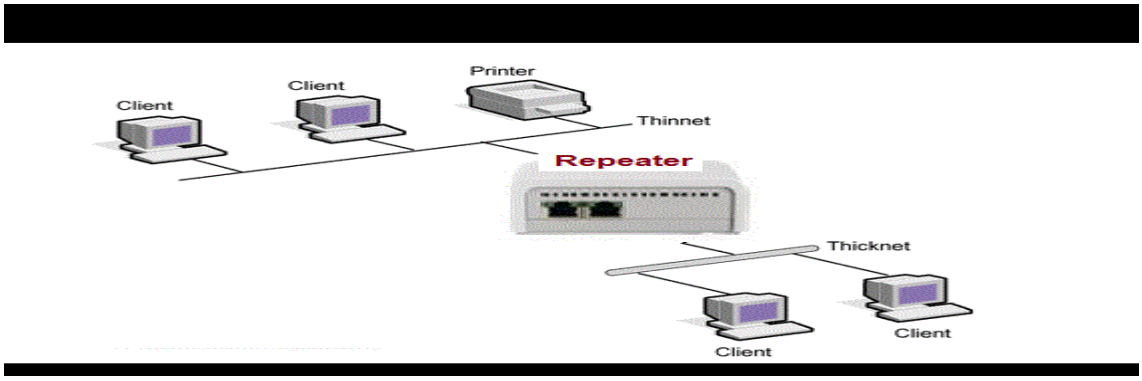
In conclusion, network topologies play a crucial role in determining the efficiency and reliability of a computer network. Each topology, whether it's bus, star, ring, mesh, or tree, offers unique benefits and potential drawbacks. By understanding these different arrangements, network designers can choose the most appropriate topology to meet the specific needs of their systems, ensuring optimal performance and connectivity.

Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter)

Network Devices: Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

1. Repeater – A repeater operates at the physical layer. Its job is to amplifies (i.e., regenerates) 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.

Understanding network devices is key to mastering networking concepts, which are heavily tested in exams like GATE. To ensure you're fully prepared, consider the GATE CS Self-Paced Course . This course offers in-depth coverage of networking topics, including detailed tutorials on the various network devices, helping you build the expertise needed to excel in your exams.

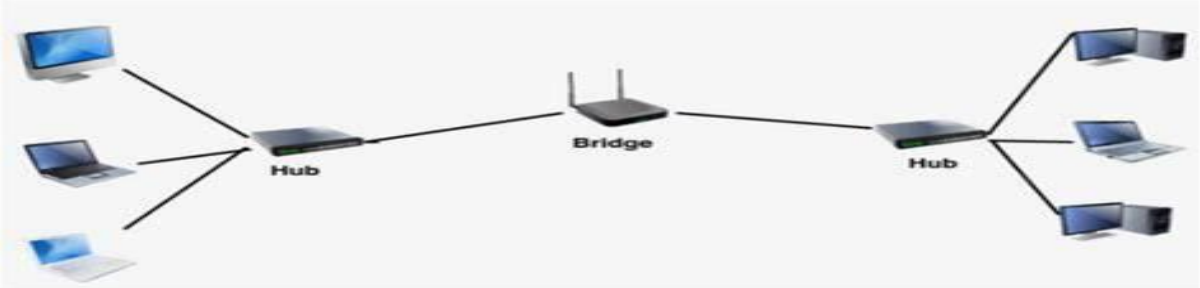


2. Hub – A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain 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.

3. 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 has a single input and single output port, thus making it a 2 port device.



Types of Bridges

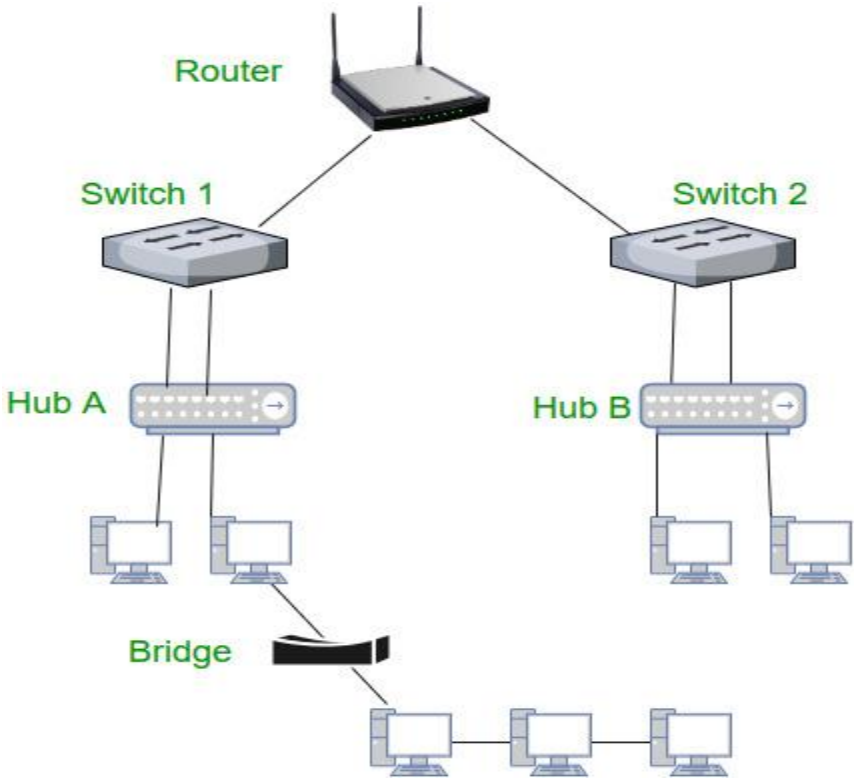
- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and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

4. Switch – A switch is a multiport bridge with a buffer and a design 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.

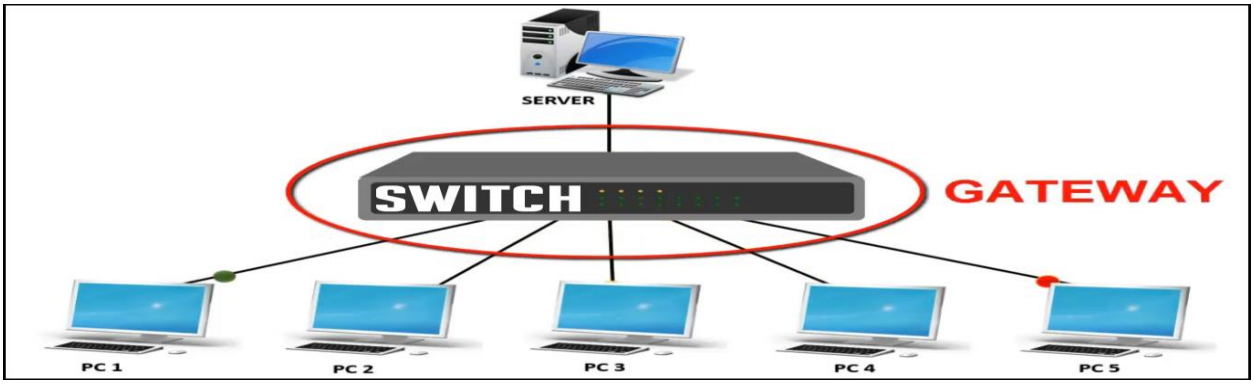
Types of Switch

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. Gigabit switches: These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.
8. 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.
9. 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.
10. Modular switches: These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centers.

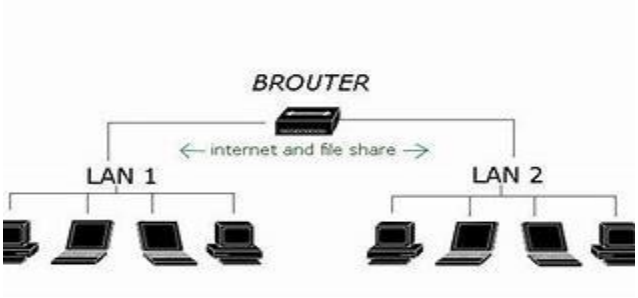
5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router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



6. 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.

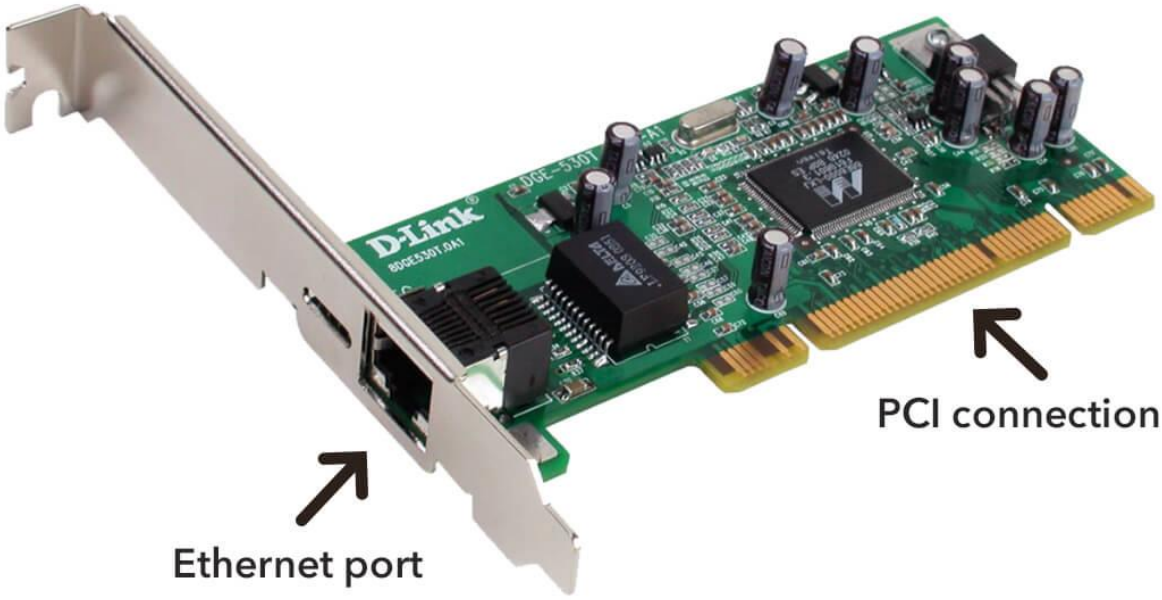


7. Brouter – It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as the bridge, it is capable of filtering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



8. 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 card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

Gigabit Ethernet NIC

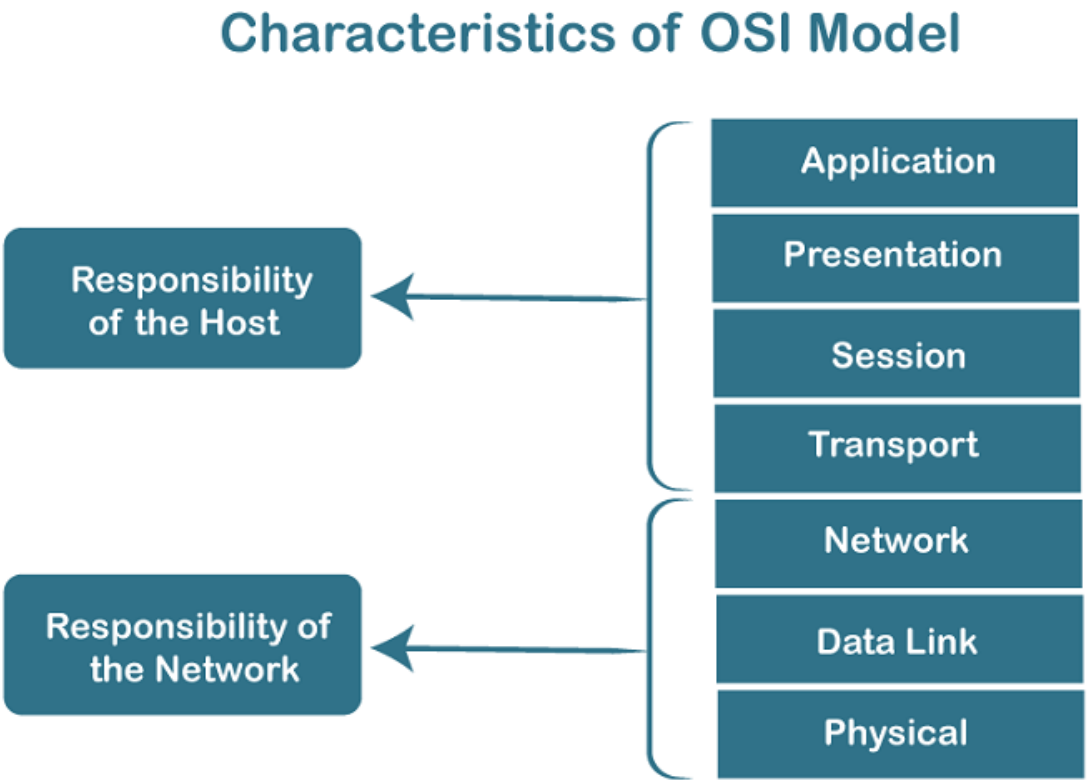


TechTerms.com

OSI Model

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:



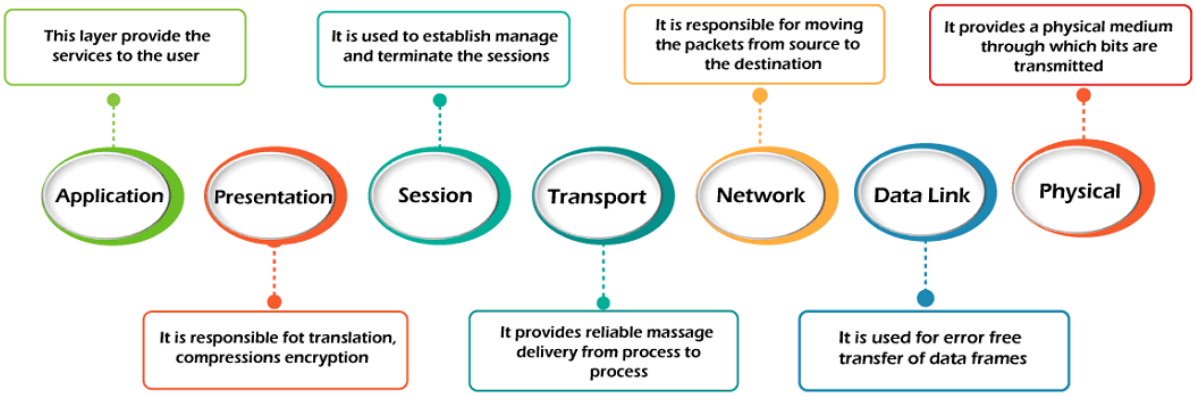
- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer

of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

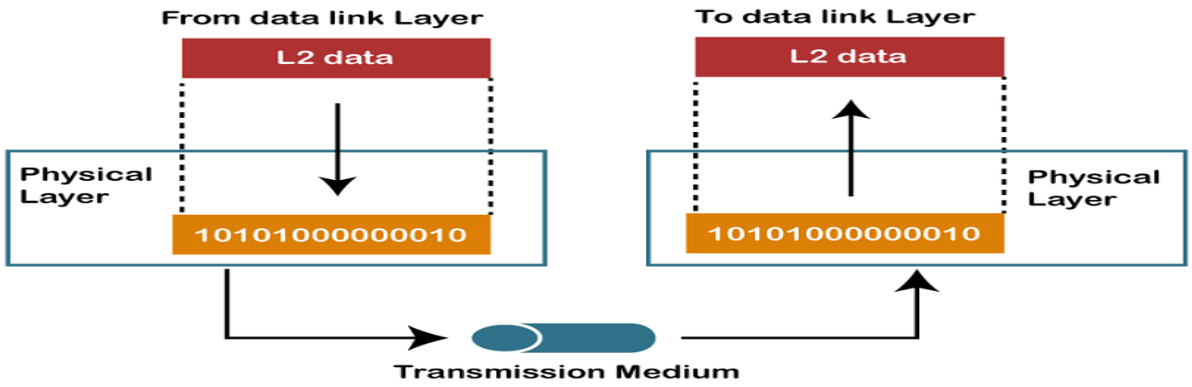
7 Layers of OSI Model

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



1) Physical layer



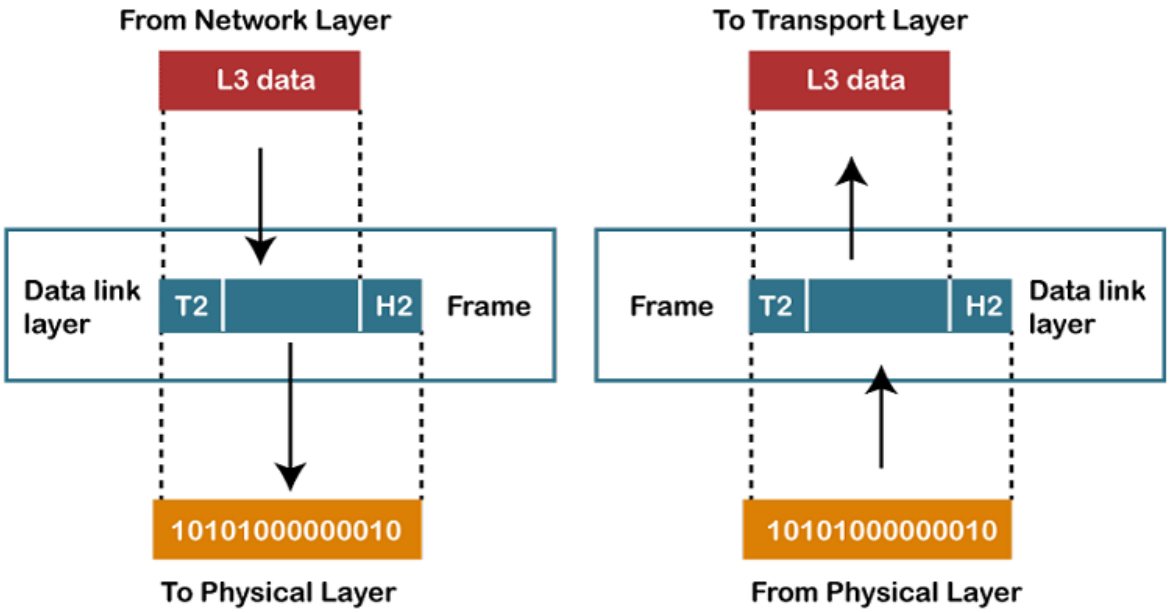
- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.

- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- Data Transmission**:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- Topology**:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

2) Data-Link Layer((2) Data Link Layer In OSI Model | Data Link Layer In Computer Networks | Networking Basics |Simplilearn - YouTube**)**



- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:

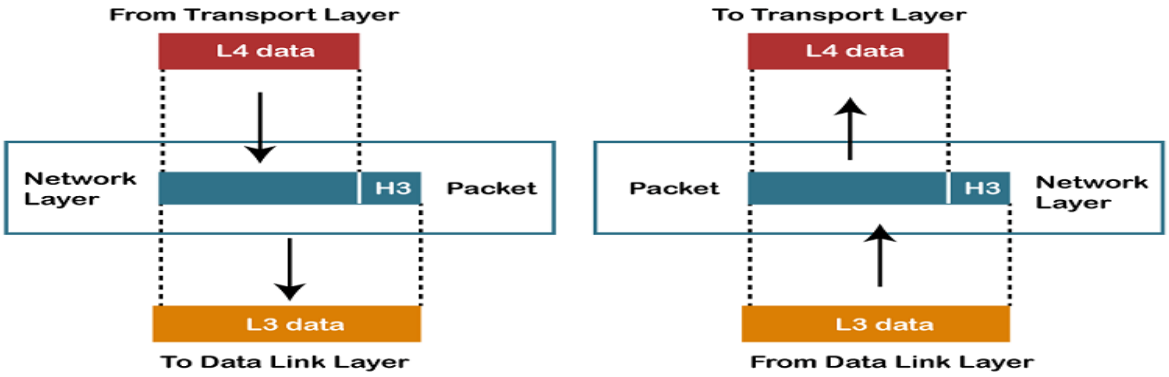
- **Logical Link Control Layer**
    - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
    - It identifies the address of the network layer protocol from the header.
    - It also provides flow control.
- **Media Access Control Layer**
    - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
    - It is used for transferring the packets over the network.

Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

3) Network Layer

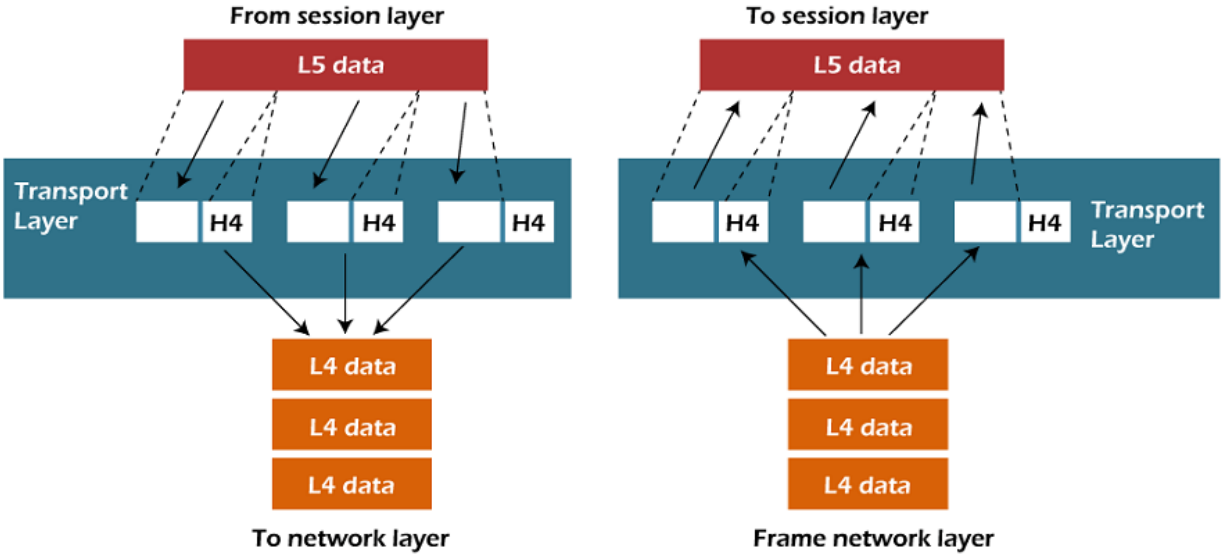


- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- Addressing**:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- Routing**:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

4) Transport Layer



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

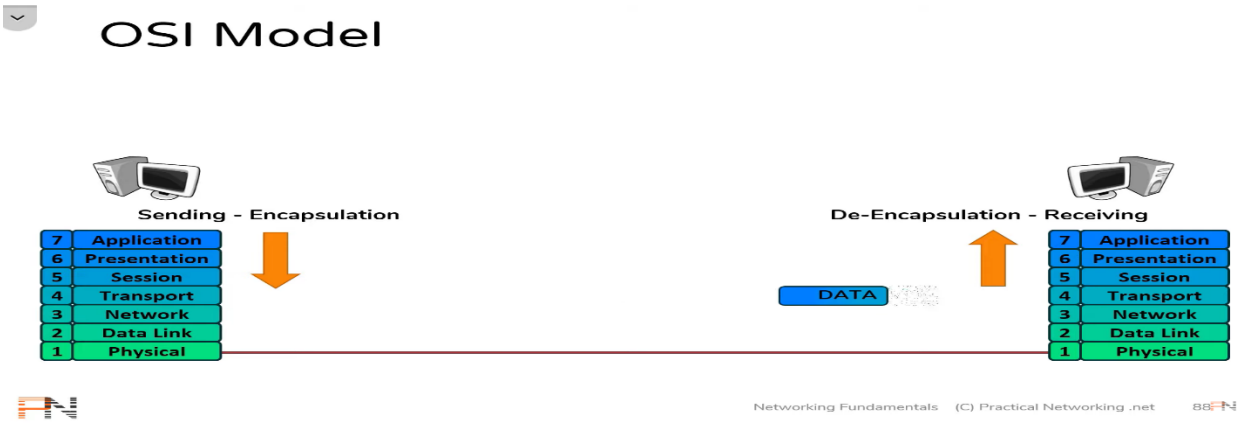
- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

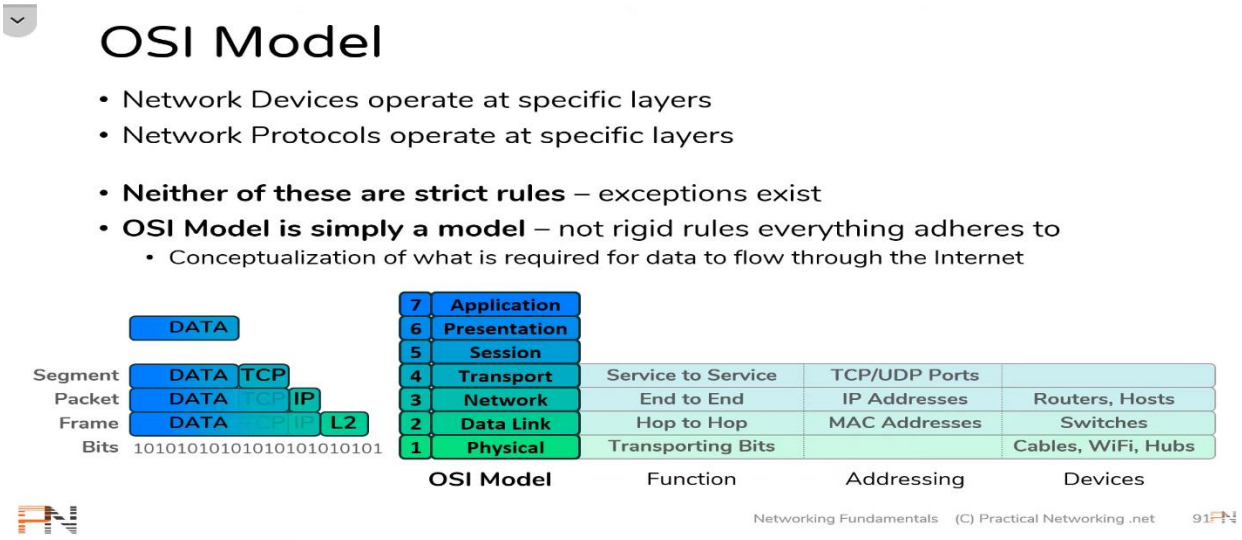
Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another

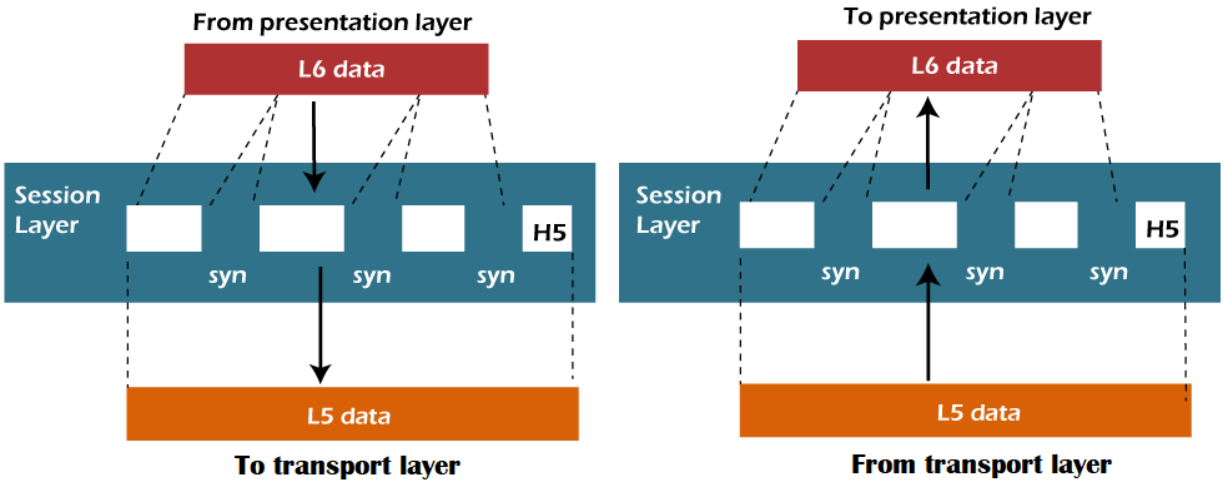
computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.

- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.





5) Session Layer

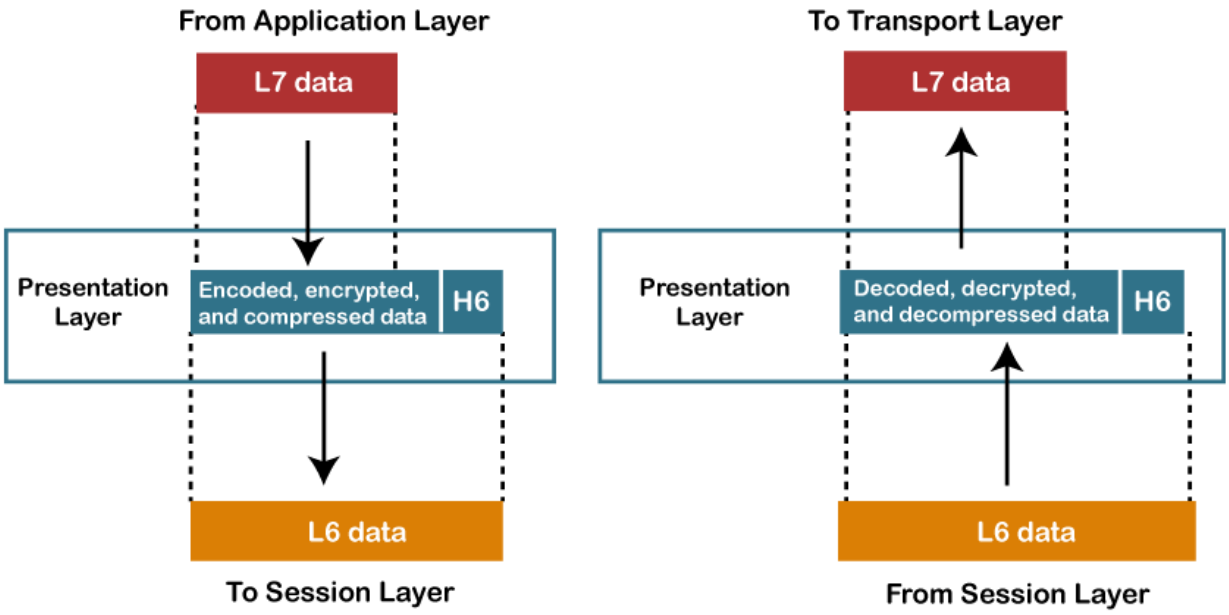


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6) **Presentation Layer**

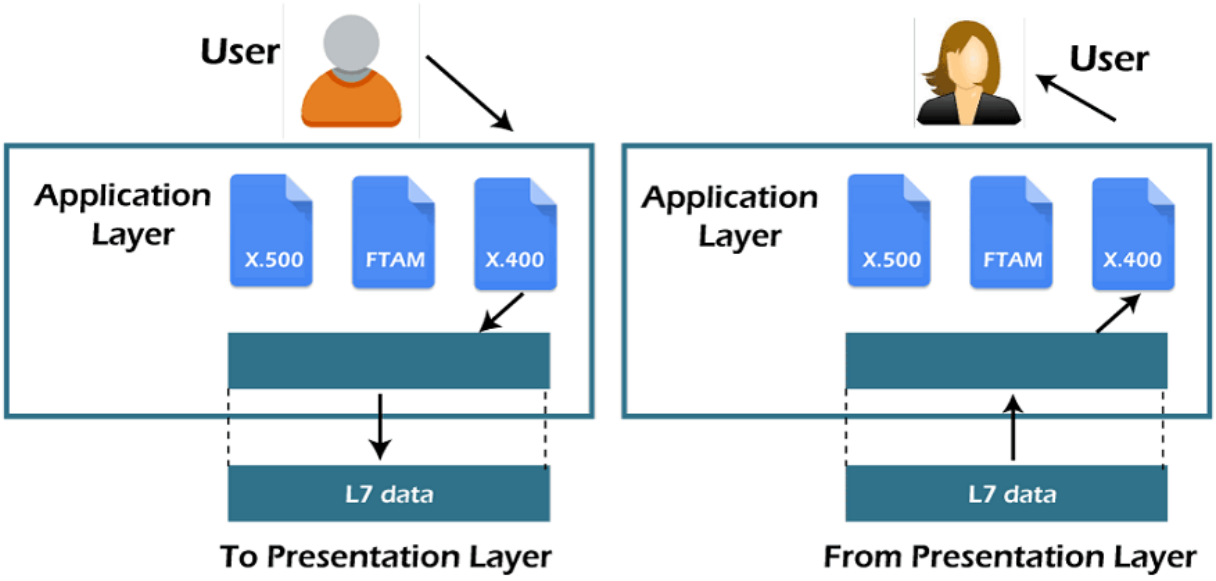


- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

7) Application Layer



- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Functions of Application layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

TCP/IP MODEL

The TCP/IP model is a fundamental framework for computer networking. It stands for Transmission Control Protocol/Internet Protocol, which are the core protocols of the Internet. This model defines how data is transmitted over networks, ensuring reliable communication between devices. It consists of four layers: the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer. Each layer has specific functions that help manage different aspects of network communication, making it essential for understanding and working with modern networks.

TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model. In this article, we are going to discuss the TCP/IP model in detail.

TCP/IP model was developed alongside the creation of the ARPANET, which later became the foundation of the modern internet. It was designed with a focus on the practical aspects of networking at the time. The lower-level hardware details and physical transmission medium were largely abstracted away in favor of higher-level networking protocols.

What Does TCP/IP Do?

The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end. The TCP/IP model is used in the context of the real-world internet, where a wide range of physical media and network technologies are in use. Rather than specifying a particular Physical Layer, the TCP/IP model allows for flexibility in adapting to different physical implementations.

Difference Between TCP and IP

Feature	TCP (Transmission Control Protocol)	IP (Internet Protocol)
Purpose	Ensures reliable, ordered, and error-checked delivery of data between applications.	Provides addressing and routing of packets across networks.
Type	Connection-oriented	Connectionless
Function	Manages data transmission between devices, ensuring data integrity and order.	Routes packets of data from the source to the destination based on IP addresses.

Feature	TCP (Transmission Control Protocol)	IP (Internet Protocol)
Error Handling	Yes, includes error checking and recovery mechanisms.	No, IP itself does not handle errors; relies on upper-layer protocols like TCP.
Flow Control	Yes, includes flow control mechanisms.	No
Congestion Control	Yes, manages network congestion.	No
Data Segmentation	Breaks data into smaller packets and reassembles them at the destination.	Breaks data into packets but does not handle reassembly.
Header Size	Larger, 20-60 bytes	Smaller, typically 20 bytes
Reliability	Provides reliable data transfer	Does not guarantee delivery, reliability, or order.
Transmission Acknowledgment	Yes, acknowledges receipt of data packets.	No

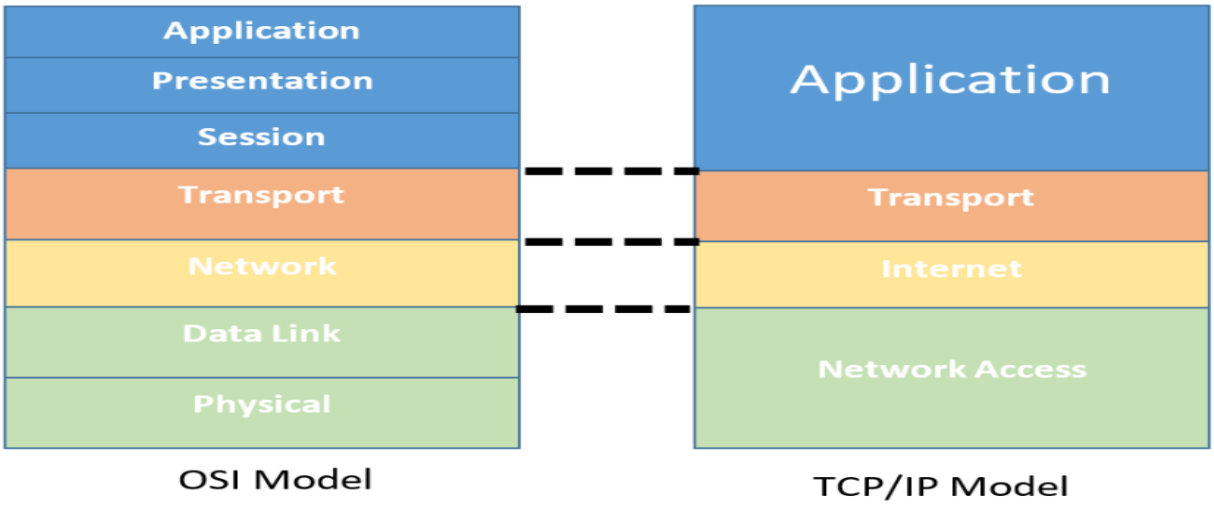
How Does the TCP/IP Model Work?

Whenever we want to send something over the internet using the TCP/IP Model, the TCP/IP Model divides the data into packets at the sender's end and the same packets have to be recombined at the receiver's end to form the same data, and this thing happens to maintain the accuracy of the data. TCP/IP model divides the data into a 4-layer procedure, where the data first go into this layer in one order and again in reverse order to get organized in the same way at the receiver's end. For more, you can refer to TCP/IP in Computer Networking.

Layers of TCP/IP Model

- Application Layer
- Transport Layer(TCP/UDP)
- Network/Internet Layer(IP)
- Network Access Layer

The diagrammatic comparison of the **TCP/IP and OSI** model is as follows:



TCP/IP and OSI

1. Network Access Layer

It is a group of applications requiring network communications. This layer is responsible for generating the data and requesting connections. It acts on behalf of the sender and the Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

The packet's network protocol type, in this case, TCP/IP, is identified by network access layer. Error prevention and "framing" are also provided by this layer. Point-to-Point Protocol (PPP) framing and Ethernet IEEE 802.2 framing are two examples of data-link layer protocols.

2. Internet or Network Layer

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for the logical transmission of data over the entire network. The main protocols residing at this layer are as follows:

- **IP:** IP stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.
- **ICMP:** ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
- **ARP:** ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.

The Internet Layer is a layer in the Internet Protocol (IP) suite, which is the set of protocols that define the Internet. The Internet Layer is responsible for routing packets of data from one device to another across a

network. It does this by assigning each device a unique IP address, which is used to identify the device and determine the route that packets should take to reach it.

Example: Imagine that you are using a computer to send an email to a friend. When you click "send," the email is broken down into smaller packets of data, which are then sent to the Internet Layer for routing. The Internet Layer assigns an IP address to each packet and uses routing tables to determine the best route for the packet to take to reach its destination. The packet is then forwarded to the next hop on its route until it reaches its destination. When all of the packets have been delivered, your friend's computer can reassemble them into the original email message.

In this example, the Internet Layer plays a crucial role in delivering the email from your computer to your friend's computer. It uses IP addresses and routing tables to determine the best route for the packets to take, and it ensures that the packets are delivered to the correct destination. Without the Internet Layer, it would not be possible to send data across the Internet.

3. Transport Layer

The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error. End-to-end communication is referred to as such. Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).

- **TCP:** Applications can interact with one another using TCP as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission.
- **UDP:** The datagram delivery service is provided by UDP, the other transport layer protocol. Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP rather than TCP because it eliminates the processes of establishing and validating connections.

4. Application Layer

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The three main protocols present in this layer are:

- **HTTP and HTTPS:** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions.
- **SSH:** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
- **NTP:** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions.

Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

The host-to-host layer is a layer in the OSI (Open Systems Interconnection) model that is responsible for providing communication between hosts (computers or other devices) on a network. It is also known as the transport layer.

Some common use cases for the host-to-host layer include:

- **Reliable Data Transfer:** The host-to-host layer ensures that data is transferred reliably between hosts by using techniques like error correction and flow control. For example, if a packet of data is lost during transmission, the host-to-host layer can request that the packet be retransmitted to ensure that all data is received correctly.
- **Segmentation and Reassembly:** The host-to-host layer is responsible for breaking up large blocks of data into smaller segments that can be transmitted over the network, and then reassembling the data at the destination. This allows data to be transmitted more efficiently and helps to avoid overloading the network.
- **Multiplexing and Demultiplexing:** The host-to-host layer is responsible for multiplexing data from multiple sources onto a single network connection, and then demultiplexing the data at the destination. This allows multiple devices to share the same network connection and helps to improve the utilization of the network.
- **End-to-End Communication:** The host-to-host layer provides a connection-oriented service that allows hosts to communicate with each other end-to-end, without the need for intermediate devices to be involved in the communication.

Example: Consider a network with two hosts, A and B. Host A wants to send a file to host B. The host-to-host layer in host A will break the file into smaller segments, add error correction and flow control information, and then transmit the segments over the network to host B. The host-to-host layer in host B will receive the segments, check for errors, and reassemble the file. Once the file has been transferred successfully, the host-to-host layer in host B will acknowledge receipt of the file to host A.

In this example, the host-to-host layer is responsible for providing a reliable connection between host A and host B, breaking the file into smaller segments, and reassembling the segments at the destination. It is also responsible for multiplexing and demultiplexing the data and providing end-to-end communication between the two hosts.

Why TCP/IP Model Does Not Have Physical Layer

The physical layer is not covered by the TCP/IP model because the data link layer is considered the point at which the interface occurs between the TCP/IP stock and the underlying network hardware. Also, it is designed to be independent of the underlying physical media. This allows TCP/IP to be flexible and adaptable to different types of physical connections, such as Ethernet, Wi-Fi, fiber optics, or even older technologies like dial-up modems. The physical layer is typically handled by hardware components and standards specific to the physical medium being used, like Ethernet cables or radio waves for Wi-Fi.

Other Common Internet Protocols

TCP/IP Model covers many Internet Protocols. The main rule of these Internet Protocols is how the data is validated and sent over the Internet. Some Common Internet Protocols include:

- **HTTP (Hypertext Transfer Protocol):** HTTP takes care of Web Browsers and Websites.
- **FTP (File Transfer Protocol):** FTP takes care of how the file is to be sent over the Internet.
- **SMTP (Simple Mail Transfer Protocol):** SMTP is used to send and receive data.

Difference between TCP/IP and OSI Model

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP uses both the session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP follows connectionless a horizontal approach.	OSI follows a vertical approach.
The Transport layer in TCP/IP does not provide assurance delivery of packets.	In the OSI model, the transport layer provides assurance delivery of packets.
Protocols cannot be replaced easily in TCP/IP model.	While in the OSI model, Protocols are better covered and are easy to replace with the technology change.
TCP/IP model network layer only provides connectionless (IP) services. The transport layer (TCP) provides connections.	Connectionless and connection-oriented services are provided by the network layer in the OSI model.

Advantages of TCP/IP Model

- **Interoperability**: The TCP/IP model allows different types of computers and networks to communicate with each other, promoting compatibility and cooperation among diverse systems.
- **Scalability**: TCP/IP is highly scalable, making it suitable for both small and large networks, from local area networks (LANs) to wide area networks (WANs) like the internet.
- **Standardization**: It is based on open standards and protocols, ensuring that different devices and software can work together without compatibility issues.

- **Flexibility**: The model supports various routing protocols, data types, and communication methods, making it adaptable to different networking needs.
- **Reliability**: TCP/IP includes error-checking and retransmission features that ensure reliable data transfer, even over long distances and through various network conditions.

Disadvantages of TCP/IP Model

- **Complex Configuration**: Setting up and managing a TCP/IP network can be complex, especially for large networks with many devices. This complexity can lead to configuration errors.
- **Security Concerns**: TCP/IP was not originally designed with security in mind. While there are now many security protocols available (such as SSL/TLS), they have been added on top of the basic TCP/IP model, which can lead to vulnerabilities.
- **Inefficiency for Small Networks**: For very small networks, the overhead and complexity of the TCP/IP model may be unnecessary and inefficient compared to simpler networking protocols.
- **Limited by Address Space**: Although IPv6 addresses this issue, the older IPv4 system has a limited address space, which can lead to issues with address exhaustion in larger networks.
- **Data Overhead**: TCP, the transport protocol, includes a significant amount of overhead to ensure reliable transmission. This can reduce efficiency, especially for small data packets or in networks where speed is crucial.

Conclusion

In conclusion, the TCP/IP model is the backbone of modern internet communication, allowing different devices and networks to connect and share information reliably. Despite some complexity and security concerns, its flexibility, scalability, and widespread adoption make it essential for both small and large networks. Overall, the TCP/IP model is crucial for ensuring efficient and effective network communication.

IP Address (Internet Protocol Address):

An IP address is a numerical label assigned to each device connected to a network that uses the Internet Protocol for communication. It serves as a unique identifier for devices to send and receive data over a network.

- **Purpose**: Identifies a device on a network.
- **Type**: Logical address assigned to each device connected to a network (e.g., computers, routers, servers).
- **Format**: Two main versions are IPv4 (e.g., 192.168.1.1) and IPv6 (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- **Use**: Helps route data between devices over the internet or local networks.

This address is just a string of numbers written in a certain format. It is generally expressed in a set of numbers for example 192.155.12.1. Here each number in the set is from 0 to 255 range. Or we can say that a full IP address ranges from 0.0.0.0 to 255.255.255.255. And these IP addresses are assigned by IANA(known as Internet Corporation For Internet Assigned Numbers Authority).

But what is Internet protocol? This is just a set of rules that makes the internet work. You are able to read this article because your computer or phone has a unique address where the page that you requested (to read this article from GeeksforGeeks) has been delivered successfully.

Working of IP addresses

The working of IP addresses is similar to other languages. It can also use some set of rules to send information. Using these protocols we can easily send, and receive data or files to the connected devices. There are several steps behind the scenes. Let us look at them

- Your device directly requests your Internet Service Provider which then grants your device access to the web.
- And an IP Address is assigned to your device from the given range available.
- Your internet activity goes through your service provider, and they route it back to you, using your IP address.
- Your IP address can change. For example, turning your router on or off can change your IP Address.
- When you are out from your home location your home IP address doesn't accompany you. It changes as you change the network of your device.

Types of IP Address

IP Address is of two types:

1. IPv4: Internet Protocol version 4. It consists of 4 numbers separated by the dots. Each number can be from 0-255 in decimal numbers. But computers do not understand decimal numbers, they instead change them to binary numbers which are only 0 and 1. Therefore, in binary, this (0-255) range can be written as (00000000 – 11111111). Since each number N can be represented by a group of 8-digit binary digits. So, a whole IPv4 binary address can be represented by 32-bits of binary digits. In IPv4, a unique sequence of bits is assigned to a computer, so a total of (2^32) devices approximately = 4,294,967,296 can be assigned with IPv4.

IPv4 can be written as:

189.123.123.90

Classes of IPv4 Address: There are around 4.3 billion IPv4 addresses and managing all those addresses without any scheme is next to impossible. Let's understand it with a simple example. If you have to find a word from a language dictionary, how long will it take? Usually, you will take less than 5 minutes to find that word. You are able to do this because words in the dictionary are organized in alphabetical order. If you have to find out the same word from a dictionary that doesn't use any sequence or order to organize

the words, it will take an eternity to find the word. If a dictionary with one billion words without order can be so disastrous, then you can imagine the pain behind finding an address from 4.3 billion addresses. For easier management and assignment IP addresses are organized in numeric order and divided into the following 5 classes :

IP Class	Address Range	Maximum number of networks
Class A	1-126	126 (2^7-2)
Class B	128-191	16384
Class C	192-223	2097152
Class D	224-239	Reserve for multitasking
Class E	240-254	Reserved for Research and development

The 0.0.0.0 is a Non-routable address is that indicates an invalid, or inapplicable end-user address.

A loopback address is a distinct reserved IP address range that starts from 127.0.0.0 ends at 127.255.255.255 though 127.255.255.255 is the broadcast address for 127.0.0.0/8. The loopback addresses are built into the IP domain system, enabling devices to transmit and receive the data packets. The loopback address 127.0.0.1 is generally known as localhost.

2. IPv6: But, there is a problem with the IPv4 address. With IPv4, we can connect only the above number of 4 billion devices uniquely, and apparently, there are much more devices in the world to be connected to the internet. So, gradually we are making our way to **IPv6 Address** which is a 128-bit IP address. In human-friendly form, IPv6 is written as a group of 8 hexadecimal numbers separated with colons(:). But in the computer-friendly form, it can be written as 128 bits of 0s and 1s. Since, a unique sequence of binary digits is given to computers, smartphones, and other devices to be connected to the internet. So, via IPv6 a total of (2^128) devices can be assigned with unique addresses which are actually more than enough for upcoming future generations.

IPv6 can be written as:

2011:0bd9:75c5:0000:0000:6b3e:0170:8394

Classification of IP Address

An IP address is classified into the following types:

1. Public IP Address: This address is available publicly and it is assigned by your network provider to your router, which further divides it to your devices. Public IP Addresses are of two types,

- **Dynamic IP Address:** When you connect a smartphone or computer to the internet, your Internet Service Provider provides you an IP Address from the range of available IP Addresses. Now, your device has an IP Address and you can simply connect your device to the Internet and send and receive data to and from your device. The very next time when you try to connect to the internet with the same device, your provider provides you with different IP Addresses to the same device and also from the same available range. Since IP Address keeps on changing every time when you connect to the internet, it is called a Dynamic IP Address.
- **Static IP Address:** Static address never changes. They serve as a permanent internet address. These are used by DNS servers. What are DNS servers? Actually, these are computers that help you to open a website on your computer. Static IP Address provides information such as device is located on which continent, which country, which city, and which Internet Service Provider provides internet connection to that particular device. Once, we know who is the ISP, we can trace the location of the device connected to the internet. Static IP Addresses provide less security than Dynamic IP Addresses because they are easier to track.

2. Private IP Address: This is an internal address of your device which are not routed to the internet and no exchange of data can take place between a private address and the internet.

3. Shared IP addresses: Many websites use shared IP addresses where the traffic is not huge and very much controllable, they decide to rent it to other similar websites so to make it cost-friendly. Several companies and email sending servers use the same IP address (within a single mail server) to cut down the cost so that they could save for the time the server is idle.

4. Dedicated IP addresses: A dedicated IP Address is an address used by a single company or an individual which gives them certain benefits using a private Secure Sockets Layer (SSL) certificate which is not in the case of a shared IP address. It allows to access the website or log in via File Transfer Protocol (FTP) by IP address instead of its domain name. It increases the performance of the website when the traffic is high. It also protects from a shared IP address that is black-listed due to spam.

Lookup IP addresses

To know your public IP, you can simply search “What is my IP?” on google. Other websites will show you equivalent information: they will see your public IP address because, by visiting the location, your router has made an invitation/request and thus revealed the information. the location IP location goes further by showing the name of your Internet Service Provider and your current city.

Finding your device’s private IP Address depends on the OS or platform you are using.

- **On Windows:** Click Start and type “cmd” in the search box and run the command prompt. In the black command prompt dialog box type “ipconfig” and press enter. You will be able to see your IP Address there.
- **On Mac:** Go to system preferences and select Network, you will be able to see the information regarding your network which includes your IP Address.

IP address security threats

Each IP address is associated with virtual ports in a computer that acts as a doorway that allows web applications or websites to send and receive data or information on your device. If after the connection is terminated the ports remain open somehow, might allow hackers to get into your device. Once, a hacker gets access to your device remotely through various tools and viruses, they would be able to access all

your stored files and data and your computer hardware as well, which includes your webcam, mic, speaker, and all your browsing history, your emails and saved passwords. These are some serious threats from which we need to be extra careful.

Various online activities can reveal your IP address from playing games or accepting bad cookies from a trap website or commenting on a website or forum. Once, they have your IP, there are websites that help them get a decent idea of your location. They can further use social media websites to track your online presence and cross verify everything that they got from these sites and use your information for their benefits or can sell these data collected on the dark web which can further exploit you.

The worst which I have seen in my friend's pc got infected while he was installing an application that he downloaded from a pirated website. The moment he hit install, a number of command prompt boxes started appearing, tens of commands started running and after a while, it was back to normal. Some malware was installed in the process. After a few days, someone was trying to log in to his social media account and other accounts using his computer as a host pc (his own IP address) but his computer was idle. The hacker was using his pc and his network, i.e., his IP address to do some serious stuff. He formatted his computer then and there, secured all his emails and other accounts, and changed all the passwords and all the security measures that had to be taken.

Cybercriminals use different techniques to get hands-on with your IP address and know your location, get into your network and hack into your computers. For instance, they will find you through Skype which uses IP addresses to speak. If you are using these apps, it's important to notice that your IP address might be vulnerable. Attackers can use the various tools, where they will find your IP address. Some of the threats are: Online stalking, downloading illegal content using your IP address, tracking your location, directly attacking your network, and hacking into your device.

Protect and hide IP address

To secure and hide your IP address from unwanted people always remember the following points:

- Use a proxy server.
- Use a virtual private network (VPN) when using public Wi-Fi, you are traveling, working remotely, or just want some privacy.
- Change privacy settings on instant messaging applications.
- Create unique passwords.
- Beware of phishing emails and malicious content.
- Use a good and paid antivirus application and keep it up to date.
- When you are using public wifi in a cafe or station or anywhere, you must hide your IP address by using VPN. Getting your IP from public wifi is just a cakewalk for these hackers and they are very good at stealing all your information while using your computer's address. There are different phishing techniques in which they email you, call you, and SMS you about giving vital information about you. They give links to vicious websites which are pre-rigged. The moment you open these websites, they steal all your device's information revealing all the information about you and your device which are to be kept private. These leaks help the hackers to exploit your device and install or download some spyware and malware on your device. But using a good

anti-virus gives you web security as well, which will prevent those websites to launch and warn you about the information being passed to these websites.

- It is also not recommended to use torrent or pirated websites which are a threat to your online identity and can compromise your device or emails or any other information about you.

2. MAC Address (Media Access Control Address):

- **Purpose**: Identifies the physical hardware of a device.
- **Type**: Physical address permanently assigned to a device's network interface controller (NIC) by the manufacturer.
- **Format**: 48-bit hexadecimal format, e.g., 00:1A:2B:3C:4D:5E.
- **Use**: Used within a local network for data transfer between devices (Layer 2 of OSI Model). It's unique to each device.

3. Port Address:

- **Purpose**: Identifies specific services or processes running on a device.
- **Type**: Logical construct used by the transport layer (Layer 4 of OSI Model) to distinguish different processes.
- **Format**: A number ranging from 0 to 65535 (e.g., HTTP uses port 80, HTTPS uses port 443).
- **Use**: Helps direct incoming and outgoing network traffic to the right service or application running on a device.

In summary:

- **IP Address** helps devices communicate over networks.
- **MAC Address** identifies the physical hardware of a device on a local network.
- **Port Address** distinguishes specific applications or services on a device.

IP Address (Internet Protocol Address):

An IP address is a numerical label assigned to each device connected to a network that uses the Internet Protocol for communication. It serves as a unique identifier for devices to send and receive data over a network.

MAC Address (Media Access Control Address):

A MAC address is a unique identifier assigned to the network interface card (NIC) of a device at the time of manufacturing. It is used to identify the hardware of a device within a local network.

Port Address:

A port address is a numerical identifier in networking used to specify a particular process or service running on a device. It allows different applications to communicate over the internet or local networks by routing data to the correct process

PROTOCOLS

1. DNS (Domain Name System)

- **Purpose**: Translates domain names (e.g., www.example.com) into IP addresses.
- **Working**:
    1. A user types a domain name into the browser.
    2. The browser sends a DNS query to resolve the domain name.
    3. If the browser cache doesn't have it, it queries the local DNS server (ISP).
    4. If the local server doesn't have it, the request goes to root servers, then top-level domain (TLD) servers, and finally the authoritative server.
    5. The authoritative server returns the IP address, and the user's browser connects to it.

2. DHCP (Dynamic Host Configuration Protocol)

- **Purpose**: Automatically assigns IP addresses and other network configurations (like gateway, DNS server) to devices on a network.
- **Working**: A client sends a request for an IP address (DHCPDISCOVER), the server responds with a DHCPOFFER, and the client accepts by sending a DHCPREQUEST. Finally, the server confirms with a DHCPACK.

3. TCP (Transmission Control Protocol)

- **Purpose**: Ensures reliable, ordered, and error-checked delivery of data.
- **Working**:
    1. Connection setup using a **three-way handshake** (SYN, SYN-ACK, ACK).
    2. Data transfer with guaranteed delivery, retransmission of lost packets.
    3. Connection termination with a **four-way handshake** (FIN, ACK, FIN, ACK).
        - **Connection-oriented**: TCP establishes a connection between a client and a server before transmitting data, ensuring reliable communication.
        - **Reliable**: It guarantees that data is delivered in the same order it was sent. If data is lost or corrupted, TCP will retransmit it.
        - **Flow control**: TCP controls the rate of data transmission based on network conditions to avoid overwhelming the receiver.
        - **Use cases**: Web browsing (HTTP/HTTPS), email (SMTP), file transfer (FTP).

4. UDP (User Datagram Protocol)

- **Purpose**: Provides a faster, connectionless communication but without guarantees on delivery or ordering.

- **Working**: Data is sent as packets (datagrams) without establishing a connection. Useful for applications like streaming where speed is more critical than reliability.
    - **Connectionless**: UDP does not establish a connection before sending data. It sends data packets (called datagrams) independently.
    - **Unreliable**: There's no guarantee that the data will be delivered, or that it will arrive in the correct order.
    - **Faster**: Due to the lack of reliability features, UDP is faster and has lower overhead.
    - **Use cases**: Real-time applications like video streaming, online gaming, DNS queries, VoIP.

5. SMTP (Simple Mail Transfer Protocol)

- **Purpose**: Transfers emails from clients to mail servers and between mail servers.
- **Working**: Operates over TCP port 25. It connects to the server, sends the sender and recipient information, transfers the message, and terminates the session.

6. ARP (Address Resolution Protocol)

- **Purpose**: Resolves the IP address to a MAC address within a local network.
- **Working**: A device broadcasts an ARP request asking for the MAC address corresponding to an IP. The device with the matching IP replies with its MAC.

7. ICMP (Internet Control Message Protocol)

- **Purpose**: Used for network diagnostics (e.g., ping, traceroute).
- **Working**: Sends error messages and operational information, such as "destination unreachable" or "time exceeded" messages.

8. POP3 (Post Office Protocol v3)

- **Purpose**: Downloads emails from a remote server to a local client.
- **Working**: Once downloaded, the email is usually deleted from the server, so the client is meant for offline use.

9. IMAP (Internet Message Access Protocol)

- **Purpose**: Manages emails on a remote server, allowing multiple clients to access the same mailbox.
- **Working**: Emails stay on the server unless explicitly deleted, and the user can manage mailboxes across multiple devices.

10. FTP (File Transfer Protocol)

- **Purpose**: Transfers files between a client and a server over a network.
- **Working**: Requires a control connection for sending commands and a separate data connection for file transfer. Operates over TCP port 21.

11. HTTP (Hypertext Transfer Protocol)

- **Purpose**: Transfers hypertext documents (webpages) across the web.
- **Working**: Works on a request-response model. A browser (client) sends a request, the server processes it and returns the webpage.

12. HTTPS (HTTP Secure)

- **Purpose**: Same as HTTP, but adds encryption via TLS/SSL for secure communication.
- **Working**: Encrypts the data exchanged between client and server, protecting against interception.

13. Telnet

- **Purpose**: Provides command-line interface access to remote devices.
- **Working**: Sends commands and receives responses in plain text, which makes it insecure (data, including passwords, is sent unencrypted).

Types of Network Protocols and Their Uses

Network protocols are a set of rules that are responsible for the communication of data between various devices in the network. These protocols define guidelines and conventions for transmitting and receiving data, ensuring efficient and reliable data communication.

What is Network Protocol?

A network protocol is a set of rules that govern data communication between different devices in the network. It determines what is being communicated, how it is being communicated, and when it is being communicated. It permits connected devices to communicate with each other, irrespective of internal and structural differences.

How do Network Protocols Work ?

It is essential to understand how devices communicate over a network by recognizing network protocols. The Open Systems Interconnection (OSI), the most widely used model, illustrates how computer systems interact with one another over a network. The communication mechanism between two network devices is shown by seven different layers in the OSI model. Every layer in the OSI model works based on different network protocols. At every layer, one or more protocols are there for network communication. To enable network-to-network connections, the Internet Protocol (IP), for instance, routes data by controlling information like the source and destination addresses of data packets. It is known as a network layer protocol.

Types of Network Protocols

In most cases, communication across a network like the Internet uses the OSI model. The OSI model has a total of seven layers. Secured connections, network management, and network communication are the three main tasks that the network protocol performs. The purpose of protocols is to link different devices.

The protocols can be broadly classified into three major categories:

- Network Communication
- Network Management
- Network Security

1. Network Communication

Communication protocols are really important for the functioning of a network. They are so crucial that it is not possible to have computer networks without them. These protocols formally set out the rules and formats through which data is transferred. These protocols handle syntax, semantics, error detection, synchronization, and authentication. Below mentioned are some network communication protocol:

Hypertext Transfer Protocol(HTTP)

It is a layer 7 protocol that is designed for transferring a hypertext between two or more systems. HTTP works on a client-server model, most of the data sharing over the web is done through using HTTP.

Transmission Control Protocol(TCP)

TCP layouts a reliable stream delivery by using sequenced acknowledgment. It is a connection-oriented protocol i.e., it establishes a connection between applications before sending any data. It is used for communicating over a network. It has many applications such as emails, FTP, streaming media, etc.

User Datagram Protocol(UDP)

It is a connectionless protocol that lay-out a basic but unreliable message service. It adds no flow control, reliability, or error-recovery functions. UPD is functional in cases where reliability is not required. It is used when we want faster transmission, for multicasting and broadcasting connections, etc.

Border Gateway Protocol(BGP)

BGP is a routing protocol that controls how packets pass through the router in an independent system one or more networks run by a single organization and connect to different networks. It connects the endpoints of a LAN with other LANs and it also connects endpoints in different LANs to one another.

Address Resolution Protocol(ARP)

ARP is a protocol that helps in mapping logical addresses to the physical addresses acknowledged in a local network. For mapping and maintaining a correlation between these logical and physical addresses a table known as ARP cache is used.

Internet Protocol(IP)

It is a protocol through which data is sent from one host to another over the internet. It is used for addressing and routing data packets so that they can reach their destination.

Dynamic Host Configuration Protocol(DHCP)

it's a protocol for network management and it's used for the method of automating the process of configuring devices on IP networks. A DHCP server automatically assigns an IP address and various other

configurational changes to devices on a network so they can communicate with other IP networks. it also allows devices to use various services such as NTP, DNS, or any other protocol based on TCP or UDP.

2. Network Management

These protocols assist in describing the procedures and policies that are used in monitoring, maintaining, and managing the computer network. These protocols also help in communicating these requirements across the network to ensure stable communication. Network management protocols can also be used for troubleshooting connections between a host and a client.

Internet Control Message Protocol(ICMP)

It is a layer 3 protocol that is used by network devices to forward operational information and error messages. ICMP is used for reporting congestions, network errors, diagnostic purposes, and timeouts.

Simple Network Management Protocol(SNMP)

It is a layer 7 protocol that is used for managing nodes on an IP network. There are three main components in the SNMP protocol i.e., SNMP agent, SNMP manager, and managed device. SNMP agent has the local knowledge of management details, it translates those details into a form that is compatible with the SNMP manager. The manager presents data acquired from SNMP agents, thus helping in monitoring network glitches, and network performance, and troubleshooting them.

Gopher

It is a type of file retrieval protocol that provides downloadable files with some description for easy management, retrieving, and searching of files. All the files are arranged on a remote computer in a stratified manner. Gopher is an old protocol and it is not much used nowadays.

File Transfer Protocol(FTP)

FTP is a Client/server protocol that is used for moving files to or from a host computer, it allows users to download files, programs, web pages, and other things that are available on other services.

Post Office Protocol(POP3)

It is a protocol that a local mail client uses to get email messages from a remote email server over a TCP/IP connection. Email servers hosted by ISPs also use the POP3 protocol to hold and receive emails intended for their users. Eventually, these users will use email client software to look at their mailbox on the remote server and to download their emails. After the email client downloads the emails, they are generally deleted from the servers.

Telnet

It is a protocol that allows the user to connect to a remote computer program and to use it i.e., it is designed for remote connectivity. Telnet creates a connection between a host machine and a remote endpoint to enable a remote session.

3. Network Security

These protocols secure the data in passage over a network. These protocols also determine how the network secures data from any unauthorized attempts to extract or review data. These protocols make sure that no unauthorized devices, users, or services can access the network data. Primarily, these protocols depend on encryption to secure data.

Secure Socket Layer(SSL)

It is a network security protocol mainly used for protecting sensitive data and securing internet connections. SSL allows both server-to-server and client-to-server communication. All the data transferred through SSL is encrypted thus stopping any unauthorized person from accessing it.

Hypertext Transfer Protocol(HTTPS)

It is the secured version of HTTP. this protocol ensures secure communication between two computers where one sends the request through the browser and the other fetches the data from the web server.

Transport Layer Security(TLS)

It is a security protocol designed for data security and privacy over the internet, its functionality is encryption, checking the integrity of data i.e., whether it has been tampered with or not, and authentication. It is generally used for encrypted communication between servers and web apps, like a web browser loading a website, it can also be used for encryption of messages, emails, and VoIP.

Some Other Protocols

Internet Message Access Protocol (IMAP)

- ICMP protocol is used to retrieve message from the mail server. By using ICMP mail user can view and manage mails on his system.

Session Initiation Protocol (SIP)

- SIP is used in video, voice, and messaging application. This protocol is used to initiating, Managing, Terminating the session between two users while they are communicating.

Real-Time Transport Protocol (RTP)

- This protocol is used to forward audio, video over IP network. This protocol is used with SIP protocol to send audio, video at real-time.

Rout Access Protocol (RAP)

- RAP is used in network management. It helps to user for accessing the nearest router for communication. RAP is less efficient as compared to SNMP.

Point To Point Tunnelling Protocol (PPTP)

- It is used to implement VPN (Virtual Private Network). PPTP protocol append PPP frame in IP datagram for transmission through IP based network.

Trivial File Transfer Protocol (TFTP)

- TFTP is the simplified version of FTP. TFTP is also used to transfer file over internet

Resource Location Protocol (RLP)

- RLP is used to assign the resource such as server, printer, or other devices over the internet to the user. It is used to locate the resource to the client for broadcast query

What is a Subnet?

A **subnet** (short for subnetwork) is a segmented piece of a larger network, typically used to improve performance, security, and organization within a network. In simple terms, it divides a large IP network into smaller, more manageable sections. Each subnet can function independently, but it remains part of the larger network.

What is Subnetting?

Subnetting is the process of dividing a network into smaller sub-networks (subnets). Subnetting allows an organization to better utilize IP address ranges and enhance network management. Each subnet has its own range of IP addresses, improving efficiency and allowing different departments or areas of an organization to have their own distinct subnet.

Need for Subnetting:

1. **Efficient IP Address Usage**: Subnetting reduces wastage of IP addresses. It allows the use of smaller IP ranges for specific areas rather than assigning large ranges to networks that don't need them.
2. **Improved Network Management**: Subnetting breaks a network into smaller, logical segments, making it easier to manage and troubleshoot.
3. **Enhanced Security**: By isolating subnets, you can apply security policies or firewall rules on a per-subnet basis, protecting parts of the network.
4. **Reduced Network Congestion**: Since traffic is localized within subnets, it can help reduce network congestion and broadcast traffic.
5. **Custom Network Sizes**: Different departments or functions in an organization may have different requirements for the number of devices (hosts). Subnetting allows flexibility to create custom network sizes.

How Subnetting is Done:

Subnetting involves borrowing bits from the host portion of an IP address to create additional network addresses.

For example, in an IPv4 address, there are 32 bits. The IP address is typically divided into two parts: the **network portion** (identifies the network) and the **host portion** (identifies specific devices within the network). Subnetting adjusts the boundaries between these parts by borrowing bits from the host portion and using them to create new network identifiers.

Key Components of Subnetting:

1. **Subnet Mask**: A 32-bit number that defines how the IP address is split between the network and host portions. A subnet mask contains a sequence of 1's (for the network portion) followed by a sequence of 0's (for the host portion). For example, 255.255.255.0 (also represented as /24) means the first 24 bits are for the network, and the remaining 8 bits are for hosts.
2. **Network Address**: The first address in a subnet used to identify the subnet itself.

3. **Broadcast Address**: The last address in the subnet, used for sending traffic to all devices within the subnet.
4. **Number of Subnets**: The number of subnets you can create depends on how many bits you borrow from the host portion.
5. **Hosts per Subnet**: The number of usable IP addresses per subnet is calculated as 2number of host bits−22^{\text{number of host bits}} - 22number of host bits−2 (subtracting 2 accounts for the network and broadcast addresses).

Subnetting IP Addresses of Different Classes:

1. **Class A (1.0.0.0 to 126.0.0.0)**:
    - Default Subnet Mask: 255.0.0.0 (/8)
    - Subnets: By borrowing bits from the host portion, you can create smaller networks.
    - Example: Borrowing 8 bits gives a subnet mask of 255.255.0.0 (/16), creating 256 subnets with 65,534 hosts each.
2. **Class B (128.0.0.0 to 191.255.0.0)**:
    - Default Subnet Mask: 255.255.0.0 (/16)
    - Example: Borrowing 8 bits from the host portion gives a subnet mask of 255.255.255.0 (/24), creating 256 subnets with 254 hosts each.
3. **Class C (192.0.0.0 to 223.255.255.0)**:
    - Default Subnet Mask: 255.255.255.0 (/24)
    - Example: Borrowing 2 bits from the host portion gives a subnet mask of 255.255.255.192 (/26), creating 4 subnets with 62 hosts each.

Example:

For a Class C network, if you have the network 192.168.1.0 with a default subnet mask /24, but you want to create 4 subnets, you need to borrow 2 bits from the host portion:

- New Subnet Mask: /26 or 255.255.255.192
- Subnets:
    - 192.168.1.0/26
    - 192.168.1.64/26
    - 192.168.1.128/26
    - 192.168.1.192/26

Each subnet will have 62 usable IP addresses.

Summary:

- Subnetting divides a larger network into smaller, more manageable pieces.

- It helps in IP address management, security, and network performance.
- The subnet mask is key to subnetting, as it defines the division between network and host bits.

RECORDS https://youtu.be/JRZiQFVWpi8?si=3mpMrkxICMY1nD2f

Record types:-