COMPUTER NETWORKS

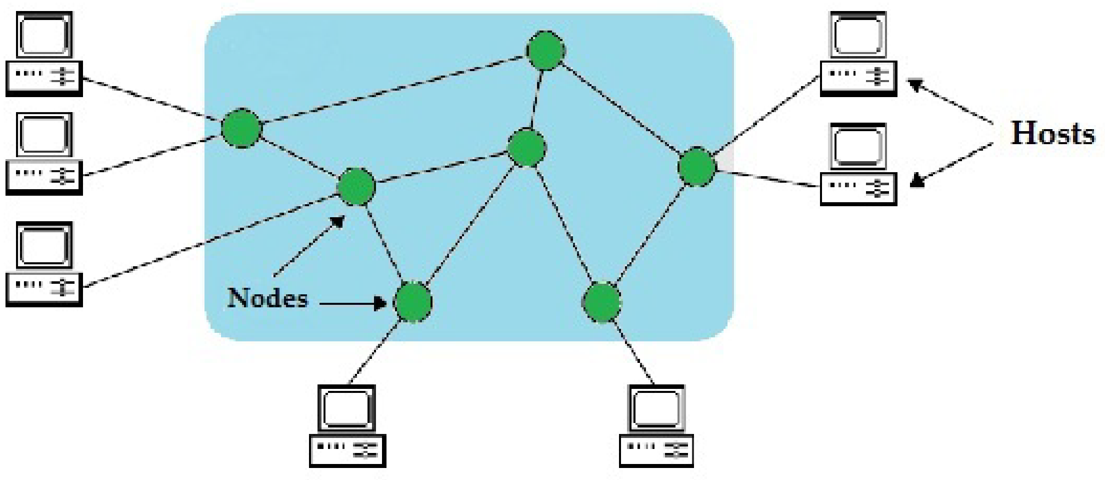
Make It Easy Education

Introduction

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.

Nodes and links are the basic building blocks in computer networking. A network node may be data communication equipment (DCE) such as a modem, hub or, switch, or data terminal equipment (DTE) such as two or more computers and printers. A link refers to the transmission media connecting two nodes. Links may be physical, like cable wires or optical fibres, or free space used by wireless networks.

In a working computer network, nodes follow a set of rules or protocols that define how to send and receive electronic data via the links. The computer network architecture defines the design of these physical and logical components. It provides the specifications for the network's physical components, functional organization, protocols, and procedures.



Computer Network

Components of Data Communication System

Data Communication is defined as exchange of data between two devices via some form of transmission media such as a cable, wire or it can be air or vacuum also. For occurrence of data communication, communicating devices must be a part of communication system made up of a combination of hardware or software devices and programs.

Data Communication System Components:

There are mainly five components of a data communication system:

```
1. Message
2. Sender
3. Receiver
4. Transmission Medium
5. Set of rules (Protocol)
```

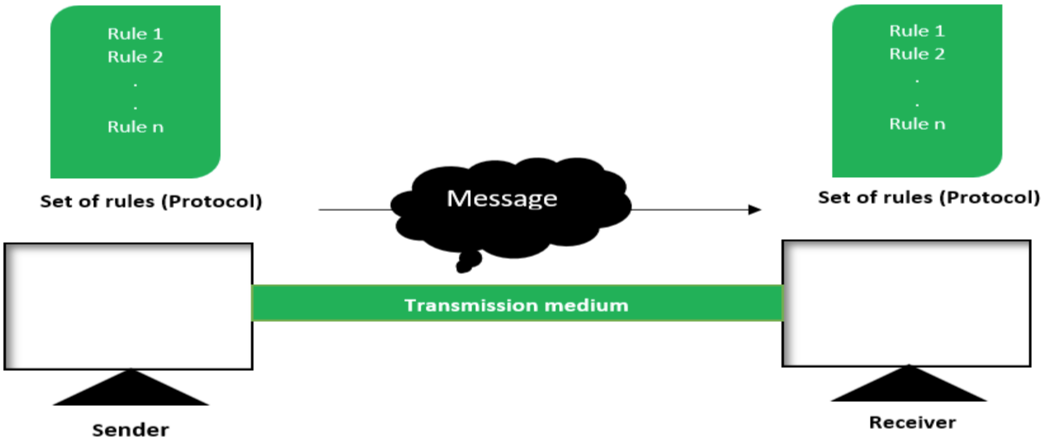


Figure – Components of Data Communication System

All above mentioned elements are described below:

1. **Message:**
   This is most useful asset of a data communication system. The message simply refers to data or piece of information which is to be communicated. A message could be in any form, it may be in form of a text file, an audio file, a video file, etc.

2. **Sender:**
   To transfer message from source to destination, someone must be there who will play role of a source. Sender plays part of a source in data communication system. It is simple a device that sends data message. The device could be in form of a computer, mobile, telephone, laptop, video camera, or a workstation, etc.

3. **Receiver:**
   It is destination where finally message sent by source has arrived. It is a device that receives message. Same as sender, receiver can also be in form of a computer, telephone mobile, workstation, etc.

4. Transmission Medium:
   In entire process of data communication, there must be something which could act as a bridge between sender and receiver, Transmission medium plays that part. It is physical path by which data or message travels from sender to receiver. Transmission medium could be guided (with wires) or unguided (without wires), for example, twisted pair cable, fiber optic cable, radio waves, microwaves, etc.

5. **Set of rules (Protocol):**
   To govern data communications, various sets of rules had been already designed by the designers of the communication systems, which represent a kind of agreement between communicating devices. These are defined as protocol. In simple terms, the protocol is a set of rules that govern data communication. If two different devices are connected but there is no protocol among them, there would not be any kind of communication between those two devices. Thus the protocol is necessary for data communication to take place.

A typical example of a data communication system is sending an e-mail. The user which send email act as sender, message is data which user wants to send, receiver is one whom user wants to send message, there are many protocols involved in this entire process, one of them is Simple Mail Transfer Protocol (SMTP), both sender and receiver must have an internet connection which uses a wireless medium to send and receive email.

Distributed Processing

Distributed computing refers to a system where processing and data storage is distributed across multiple devices or systems, rather than being handled by a single central device. In a distributed system, each device or system has its own processing capabilities and may also store and manage its own data. These devices or systems work together to perform tasks and share resources, with no single device serving as the central hub.

One example of a distributed computing system is a cloud computing system, where resources such as computing power, storage, and networking are delivered over the Internet and accessed on demand. In this type of system, users can access and use shared resources through a web browser or other client software.

Components

There are several key components of a Distributed Computing System

- **Devices or Systems:** The devices or systems in a distributed system have their own processing capabilities and may also store and manage their own data.
- **Network:** The network connects the devices or systems in the distributed system, allowing them to communicate and exchange data.
- **Resource Management:** Distributed systems often have some type of resource management system in place to allocate and manage shared resources such as computing power, storage, and networking.

The architecture of a Distributed Computing System is typically a Peer-to-Peer Architecture, where devices or systems can act as both clients and servers and communicate directly with each other.

Characteristics

There are several characteristics that define a Distributed Computing System

- **Multiple Devices or Systems:** Processing and data storage is distributed across multiple devices or systems.
- **Peer-to-Peer Architecture:** Devices or systems in a distributed system can act as both clients and servers, as they can both request and provide services to other devices or systems in the network.
- **Shared Resources:** Resources such as computing power, storage, and networking are shared among the devices or systems in the network.
- **Horizontal Scaling:** Scaling a distributed computing system typically involves adding more devices or systems to the network to increase processing and storage capacity. This can be done through hardware upgrades or by adding additional devices or systems to the network..

Advantages and Disadvantages

Some Advantages of the Distributed Computing System are:

- **Scalability:** Distributed systems are generally more scalable than centralized systems, as they can easily add new devices or systems to the network to increase processing and storage capacity.
- **Reliability:** Distributed systems are often more reliable than centralized systems, as they can continue to operate even if one device or system fails.
- **Flexibility:** Distributed systems are generally more flexible than centralized systems, as they can be configured and reconfigured more easily to meet changing computing needs.

There are a few limitations to Distributed Computing System

- **Complexity:** Distributed systems can be more complex than centralized systems, as they involve multiple devices or systems that need to be coordinated and managed.
- **Security:** It can be more challenging to secure a distributed system, as security measures must be implemented on each device or system to ensure the security of the entire system.

- **Performance:** Distributed systems may not offer the same level of performance as centralized systems, as processing and data storage is distributed across multiple devices or systems.

Applications

Distributed Computing Systems have a number of applications, including:

- **Cloud Computing:** Cloud Computing systems are a type of distributed computing system that are used to deliver resources such as computing power, storage, and networking over the Internet.
- **Peer-to-Peer Networks:** Peer-to-Peer Networks are a type of distributed computing system that is used to share resources such as files and computing power among users.
- **Distributed Architectures:** Many modern computing systems, such as micro services architectures, use distributed architectures to distribute processing and data storage across multiple devices or systems.

Network Topology

Network topology is the way devices are connected in a network. It defines how these components are connected and how data transfer between the network. Understanding the different types of network topologies can help in choosing the right design for a specific network. There are two major categories of Network Topology i.e. Physical Network topology and Logical Network Topology. Physical Network Topology refers to the actual structure of the physical medium for the transmission of data. Logical network Topology refers to the transmission of data between devices present in the network irrespective of the way devices are connected. The structure of the network is important for the proper functioning of the network. one must choose the most suitable topology as per their requirement.

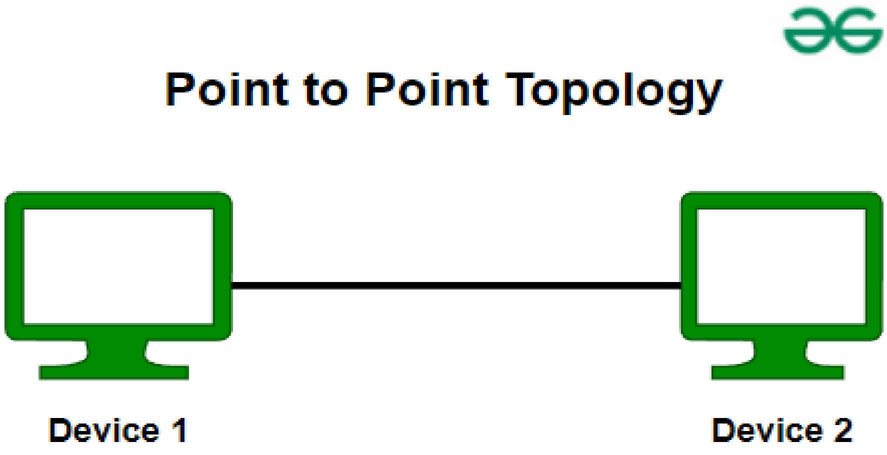
Types of Network Topology

Below mentioned are the types of Network Topology

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

Point to Point Topology

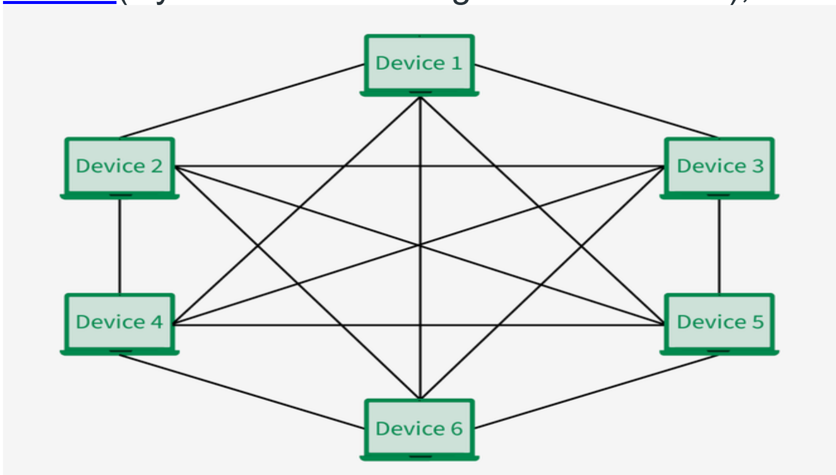
Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Point to Point Topology

Mesh Topology

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



Mesh Topology

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 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 $^NC_2$ 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.

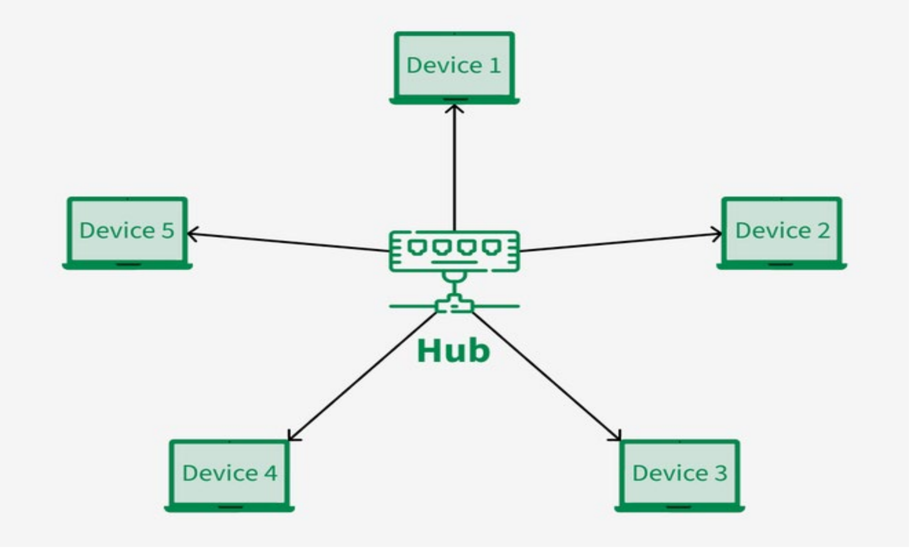
Disadvantages of Mesh Topology

- 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.

Star Topology

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



Star Topology

Advantages of Star Topology

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

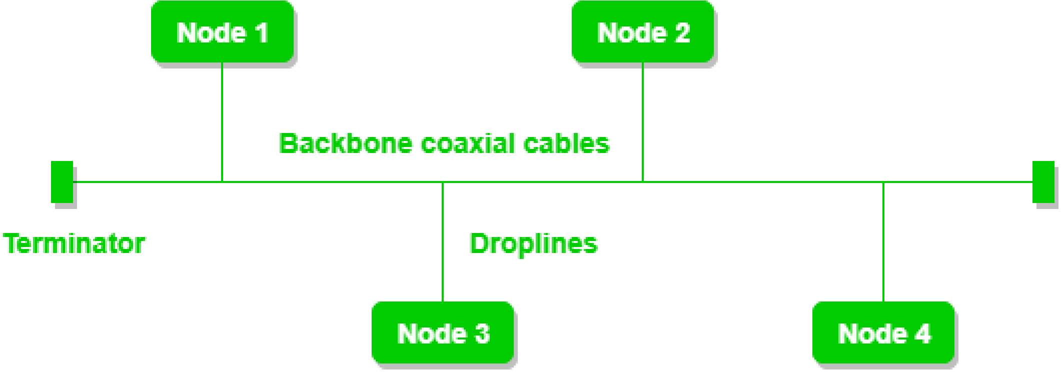
Disadvantages of Star Topology

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

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

Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.



Bus Topology

Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.

- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA is the most common method for this type of topology.

Disadvantages of Bus Topology

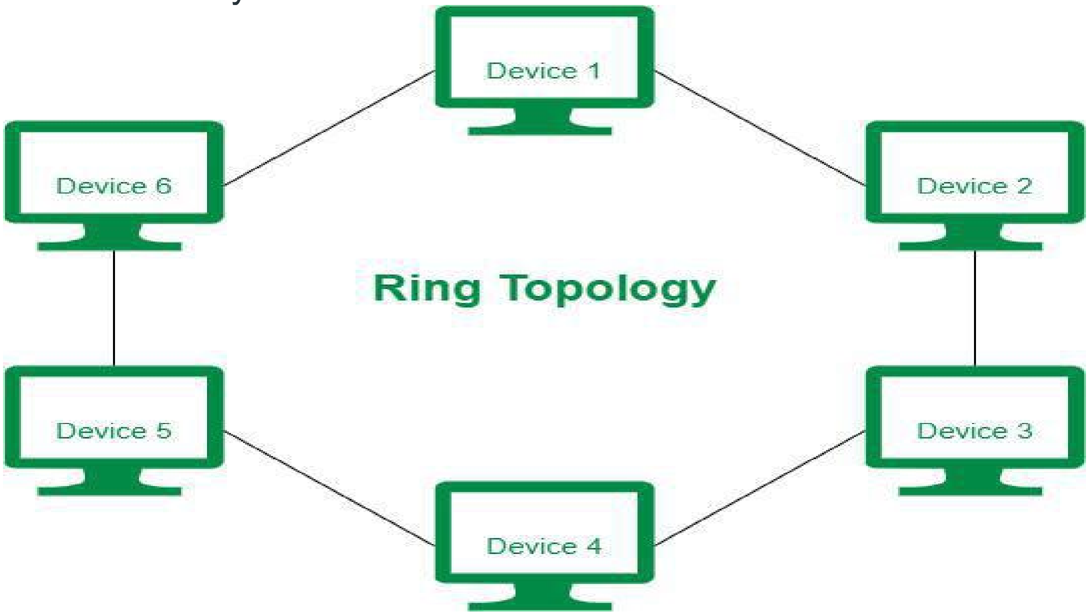
- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted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

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

Ring Topology

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

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



Ring Topology

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

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

Operations of Ring Topology

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

Advantages of Ring Topology

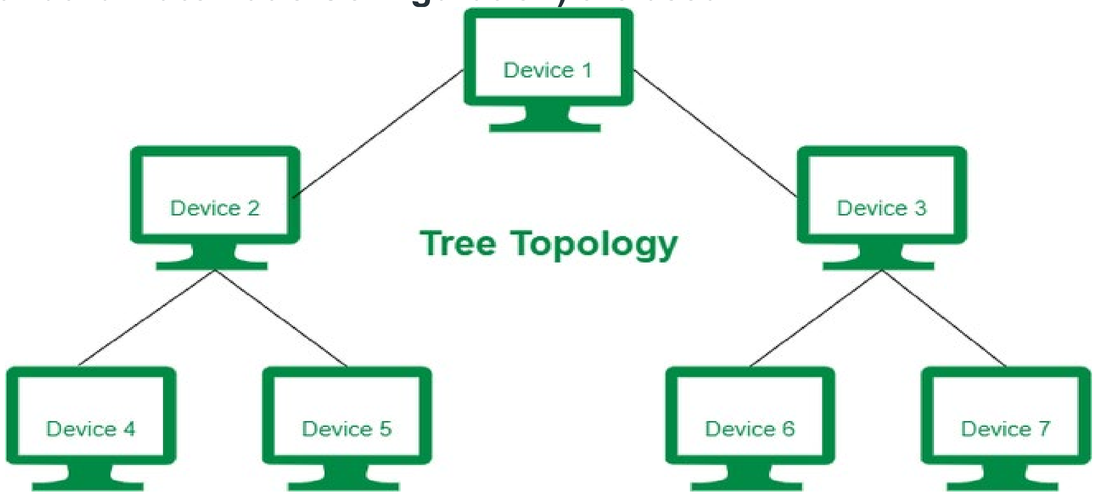
- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

Disadvantages of Ring Topology

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

Tree Topology

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



Tree Topology

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

Advantages of Tree Topology

- It allows more devices to be attached to a single central hub thus it decreases the distance that is 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.

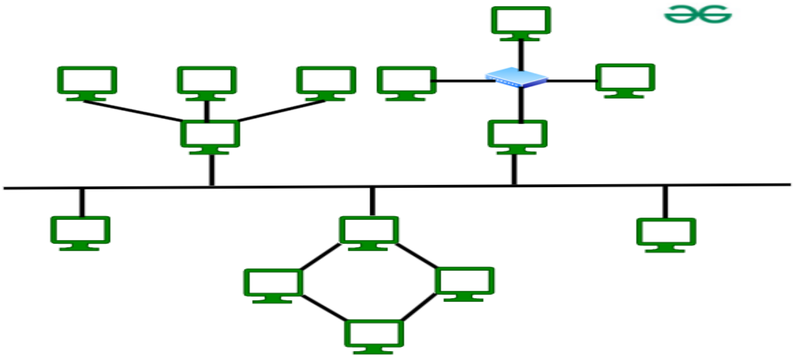
Disadvantages of Tree Topology

- 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.

Hybrid Topology

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



Hybrid Topology

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

Advantages of Hybrid Topology

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

Disadvantages of Hybrid Topology

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

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

Categories/Types of Computer Network

The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN, and WAN are the three major types of networks designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area, **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.

Local Area Network (LAN) –

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.

Data transmits at a very fast rate as the number of computers linked is limited. By definition, the connections must be high-speed and relatively inexpensive hardware (Such as hubs, network adapters, and Ethernet cables). LANs cover a smaller geographical area (Size is limited to a few kilometres) and are privately owned. One can use it for an office building, home, hospital, school, etc. LAN is easy to design and maintain. A Communication medium used for LAN has twisted-pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.

Early LANs had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN. The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. LAN has a range up to 2km. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. The fault tolerance of a LAN is more and there is less congestion in this network. For example A bunch of students playing Counter-Strike in the same room (without internet).

Advantages:

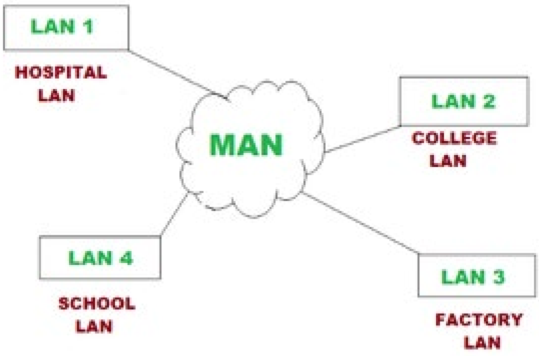
- Provides fast data transfer rates and high-speed communication.
- Easy to set up and manage.
- Can be used to share peripheral devices such as printers and scanners.
- Provides increased security and fault tolerance compared to WANs.

Disadvantages:

- Limited geographical coverage.
- Limited scalability and may require significant infrastructure upgrades to accommodate growth.
- May experience congestion and network performance issues with increased usage.

Metropolitan Area Network (MAN) –

MAN or Metropolitan area Network covers a larger area than that covered by a LAN and a smaller area as compared to WAN. MAN has a range of 5-50km. It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need high-speed connectivity. Speeds of MAN range in terms of Mbps. It’s hard to design and maintain a Metropolitan Area Network.



The fault tolerance of a MAN is less and also there is more congestion in the network. It is costly and may or may not be owned by a single organization. The data transfer rate and the propagation delay of MAN are moderate. Devices used for transmission of data through MAN are Modem and Wire/Cable. Examples of a MAN are part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

Advantages:

- Provides high-speed connectivity over a larger geographical area than LAN.
- Can be used as an ISP for multiple customers.
- Offers higher data transfer rates than WAN in some cases.

Disadvantages:

- Can be expensive to set up and maintain.
- May experience congestion and network performance issues with increased usage.
- May have limited fault tolerance and security compared to LANs.

Wide Area Network (WAN) –

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. WAN has a range of above 50 km. A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high-speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN(Public Switched Telephone Network) or Satellite Link. Due to long-distance transmission, the noise and error tend to be more in WAN.

WAN’s data rate is slow about a 10th LAN’s speed since it involves increased distance and increased number of servers and terminals etc. The speed of WAN ranges from a few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for the transmission of data through WAN are Optic wires, Microwaves, and Satellites. An example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is a dial-up line that connects a home computer to the Internet.

Advantages:

- Covers large geographical areas and can connect remote locations.
- Provides connectivity to the internet.
- Offers remote access to resources and applications.

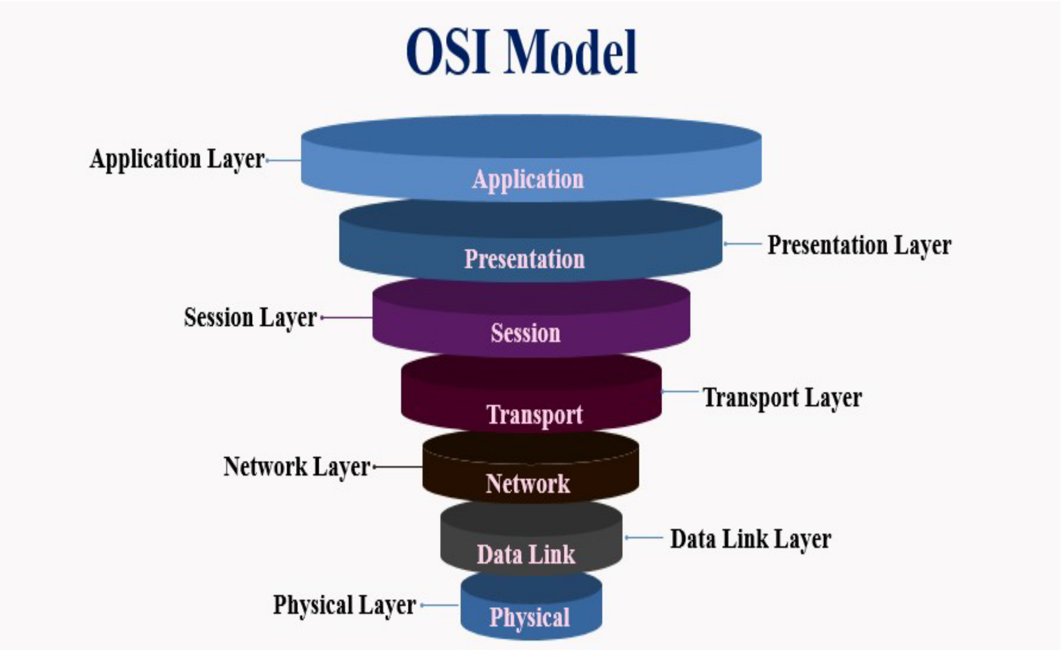
- Can be used to support multiple users and applications simultaneously.

Disadvantages:

- Can be expensive to set up and maintain.
- Offers slower data transfer rates than LAN or MAN.
- May experience higher latency and longer propagation delays due to longer distances and multiple network hops.
- May have lower fault tolerance and security compared to LANs.

OSI Model

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



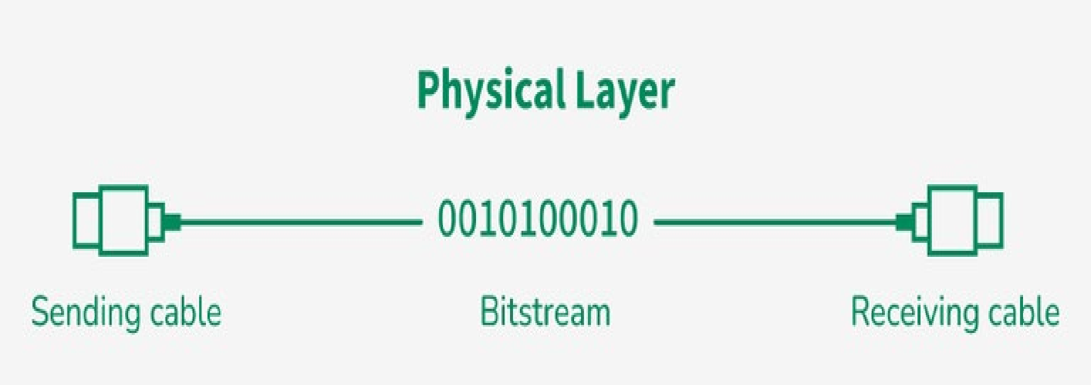
Layers of the OSI Model

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

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

Layer 1 – Physical Layer

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



Physical Layer

Functions of the Physical Layer

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

Layer 2 – Data Link Layer (DLL)

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

The Data Link Layer is divided into two sublayers:

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

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

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

Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- **Physical Addressing:** After creating frames, the Data link layer adds physical addresses (MAC **addresses)** of the sender and/or receiver in the header of each frame.
- **Error Control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
- **Access Control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

Layer 3 – Network Layer

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

Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- **Logical Addressing:** To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender and receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Layer 4 – Transport Layer

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as **Segments**. It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found. Protocols used in Transport Layer are TCP, UDP NetBIOS, PPTP.

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

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

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

Functions of the Transport Layer

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus, by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services Provided by Transport Layer

- Connection-Oriented Service
- Connectionless Service

Layer 5 – Session Layer

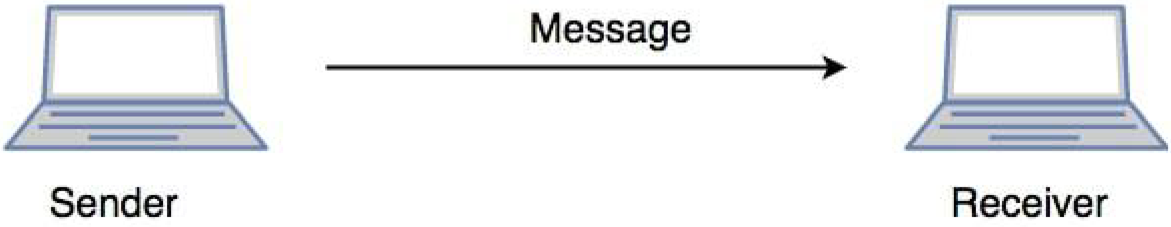
Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices. It also provides authentication and security. Protocols used in the Session Layer are NetBIOS, PPTP.

Functions of the Session Layer

- **Session Establishment, Maintenance, and Termination:** The layer allows the two processes to establish, use, and terminate a connection.
- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely, and data loss is avoided.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full duplex.

Example

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



Communication in Session Layer

Layer 6 – Presentation Layer

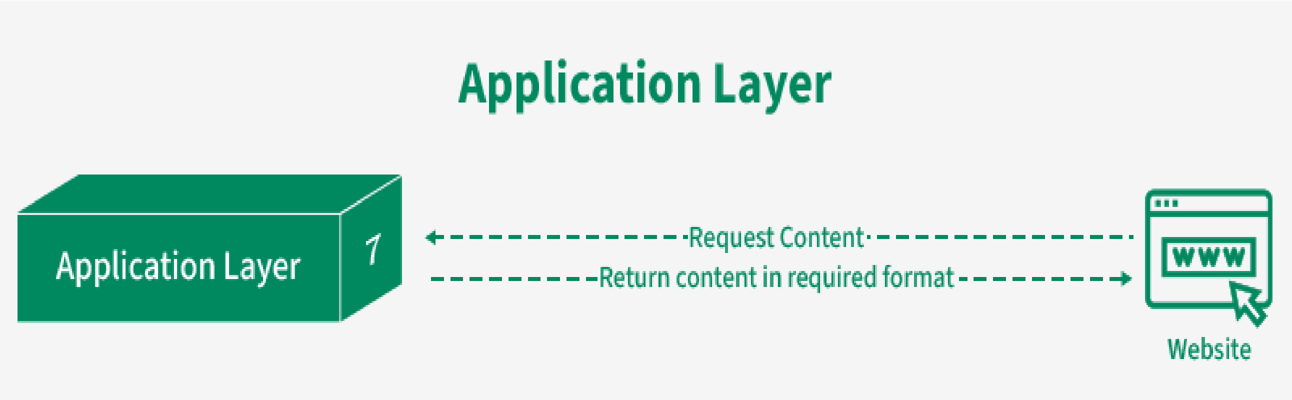
The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. Protocols used in the Presentation Layer are JPEG, MPEG, GIF, TLS/SSL, etc.

Functions of the Presentation Layer

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

Layer 7 – Application Layer

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



Application Layer

Functions of the Application Layer

The main functions of the application layer are given below.

- **Network Virtual Terminal (NVT):** It allows a user to log on to a remote host.
- **File Transfer Access and Management (FTAM):** This application allows a user to access files in a remote host, retrieve files in a remote host, and manage or control files from a remote computer.
- **Mail Services:** Provide email service.
- **Directory Services:** This application provides distributed database sources and access for global information about various objects and services.

Advantages of OSI Model

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

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

Disadvantages of OSI Model

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

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.

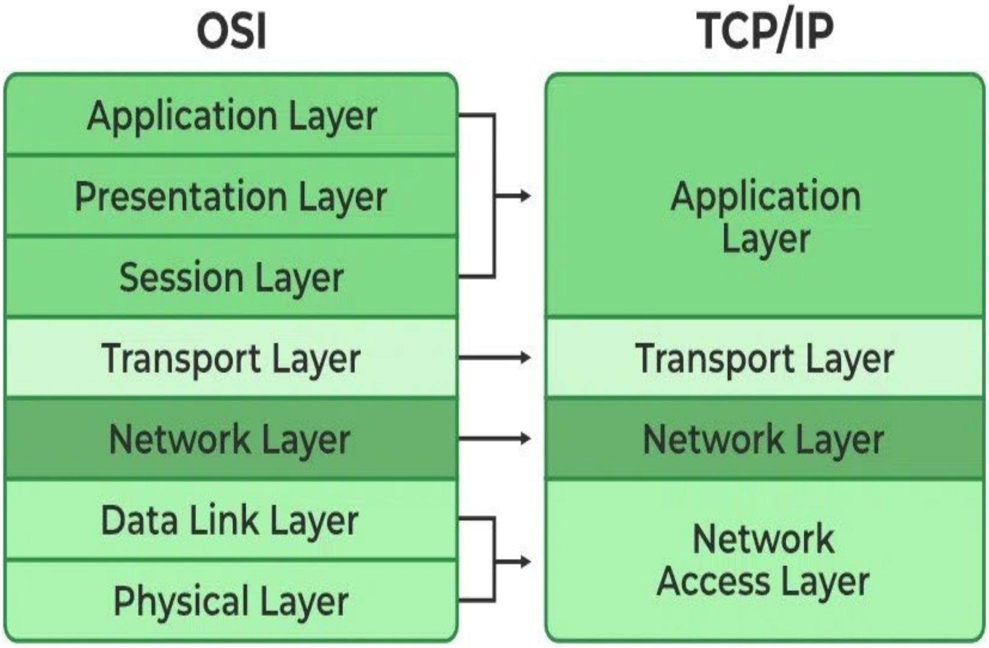
What Does TCP/IP Do?

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.

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



1. Network Access Layer

The Network Access Layer represents a collection of applications that require network communication. This layer is responsible for generating data and initiating connection requests. It operates on behalf of the sender to manage data transmission, while the Network Access layer on the receiver's end processes and manages incoming data. In this article, we will focus on its role from the receiver's perspective.

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

The Application Layer in the TCP/IP model combines the functions of three layers from the **OSI model**: the **Application**, **Presentation**, and **Session** layers. 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.

Digital Transmission

Modem

A modem and router are two of the most frequent components in a home network configuration. A router establishes a local area network (LAN), whereas a modem connects to an internet service provider (ISP). For a home network to work, both devices are necessary.

What is a Modem?

Modem stands for Modulator/Demodulator. The modem is defined as a networking device that is used to connect devices connected in the network to the internet. The main function of a modem is to convert the analog signals that come from telephone wire into a digital form. In digital form, these converted signals are stored in the form of 0s and 1s. The modem can perform both the task of modulation and demodulation simultaneously. Modems are majorly used to transfer digital data in personal systems. The modem is also known as a signal translator as it translates one signal into another signal by modulating the digital signal into an analog signal for transmission and then demodulates receiving analog signals into digital signals.

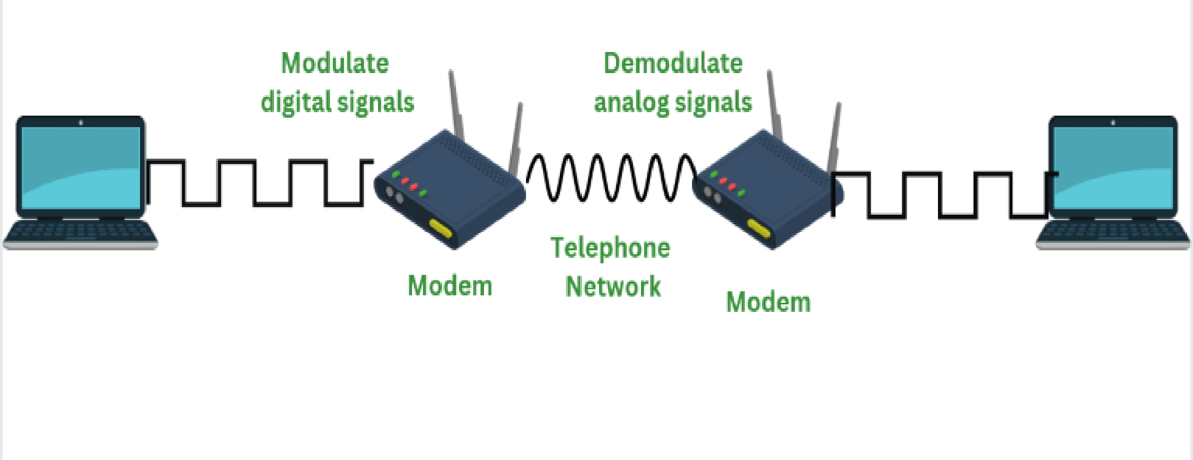
Features of Modem

- Modems can modulate as well as demodulate the signals simultaneously.
- Modem allows to connect only a specific number of devices to the internet.
- According to the features of modem, it’s price ranges.
- Modems can be upgraded with the help of a specific software patch.
- To use the devices over the internet with a modem devices need to be configured with an Internet Service Provider(ISP).

- When the modem is connected to Hub it slows down its process.

Working of Modem

The two main components of a modem are modulation and demodulation. Where the modem can perform both tasks simultaneously. The step-by-step working of the modem is given below:



Step 1: Data Generation: When data needs to be transmitted it is first generated. Therefore computer system generated the data which is in digital form of 0s and 1s.

Step 2: Modulation: Modulation is defined as a process of converting digital data signals of the computer into analog data signals so that these signals can travel on the internet. The digital data is encoded onto a carrier wave.

Step 3: Transmission: The resultant of modulation that is modulated data is transmitted over the communication line to the modem that is receiving it.

Step 4: Demodulation: Demodulation is defined as a process in which analog data signals from the internet are converted into digital data signals so they can be understood by computer systems. In the process of demodulation the digital data from the carrier wave is decoded.

Step 5: Decoding: The resultant of demodulation that is demodulated data is being sent to the computer systems for their further use.

Types of Modem

There are different types of modems available. Each modem has different features and provides with different benefits. Below are the different types of modems:

1. Optical Modem

In modem, different type of media is used to transfer the signals. Optical Modem is the type of modem that makes use of optical cables instead of using another metallic type of media. The digital data is converted into the pulse of light that is transmitted on the optical fiber used in the optical Modem.

2. Digital Modem

Digital Modem is defined as a type of modem that is used to convert digital data into digital signals. Digital data is in form of 0s and 1s. For this, it performs the process of modulation. Digital Modem modulates the digital data on digital carrier signals for transmission.

3. Cable Modem

Cable modems are defined as a type of modem used to establish a communication between computer systems and the Internet Service Providers. A cable modem helps to access high-speed data through cable TV networks. Such modems are usually connected to desktops or systems and work like external devices.

4. Satellite Modem

Satellite Modems are defined as a type of modem that provides with the internet connection through satellite dishes. This type of modem works by sending the input bits into output radio signals and vice versa. The internet network that is provided by such types of modems is more reliable and efficient as compared to other types of modems.

5. Dial Modem

A Dial Modem is a type of modem that converts data used in telephone and data used on computers. In short dial modem converts between analog form and digital form. The networking devices connected to the computer are all at one end and the telephone line is at another end. This type of modem transmits the data at a speed of 56000 per/sec.

Advantages of Modem

- A modem converts digital signals into an analog signal.
- The cost of a modem increases according to the features it has.
- The modem helps to connect the LAN to the internet.
- Modem performs both modulation and demodulation processes simultaneously

Disadvantages of Modem

- The working of the modem slows down when connected to the hub.
- The modem cannot track the traffic between the LAN and the internet.
- When using a modem a limited number of network devices can be connected to the internet.
- Modems have a high rock of security-related attacks.
- The modem does not provide maintenance of traffic.