UNIT-I
Introduction to Computer Networks

Introduction

A Computer Network is a system that connects numerous independent computers in order 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.

A Computer Network consists of various kinds of nodes. Servers, networking hardware, personal computers, and other specialized or general-purpose hosts can all be nodes in a Computer Network. Host names and network addresses are used to identify them.

Computer Network Work

Computer Networks simply work using nodes and links. Data Communication Equipment is simply termed as Nodes. For example, Modems, Hubs, Switches, etc. whereas links in Computer Networks can be referred to as a connection between two nodes. We have several types of links like cable wires, optical fibers, etc.

Whenever a Computer Network is working, nodes have the work of sending and receiving data via the links. Computer Network provides some set of protocols that helps in following the rules and protocols.

Computer Networks are one of the important aspects of Computer Science. In the early days, it is used for data transmission on telephone lines and had a very limited use, but nowadays, it is used in a variety of places.

Computer Networks help in providing better connectivity that helps nowadays. Modern Computer Networks have the following functionality like

- Computer Networks help in operating virtually.
- Computer Networks integrate on a large scale.
- Computer Networks respond very quickly in case of conditions change.
- Computer Networks help in providing data security.

Criteria of a Good Network

- **Performance:** It can be measured in many ways, including transmit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of the network depends on a number of factors, including the number of users, the type of medium & Hardware
- **Reliability:** In addition to accuracy is measured by frequency of failure, the time it takes a link to recover from failure, and the network's robustness in catastrophe.
- **Security:** Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data loss.

Goals of Computer Networking

Programs do not have to execute on a single system because of resource and load sharing.

- Reduced costs – Multiple machines can share printers, tape drives, and other peripherals.
- Reliability – If one machine fails, another can take its place.
- Scalability (it's simple to add more processors or computers)
- Communication and mail (people living apart can work together)
- Information Access (remote information access, access to the internet, e-mail, video conferencing, and online shopping)
- Entertainment that is interactive (online games, videos, etc.)
- Social Networking

Types of Computer Networks

Division Based on the Communication Medium

- **Wired Network:** As we all know, "wired" refers to any physical medium made up of cables. Copper wire, twisted pair, or fiber optic cables are all options. A wired network employs wires to link devices to the Internet or another network, such as laptops or desktop PCs.
- **Wireless Network:** "Wireless" means without wire, media that is made up of Electromagnetic Waves (EM Waves) or infrared waves. Antennas or sensors will be present on all wireless devices. Cellular phones, wireless sensors, TV remotes, satellite dish receivers, and laptops with WLAN cards are all examples of wireless devices. For data or voice communication, a wireless network uses radio frequency waves rather than wires.

Division Based on Area Covered

1) **Local Area Network (LAN):** A LAN is a network that covers an area of around 10 kilometers. For example, a college network or an office network. Depending upon the needs of the organization, a LAN can be a single office, building, or Campus. We can have two PCs and one printer in-home office or it can extend throughout the company and include audio and video devices. Each host in LAN has an identifier, an address that defines hosts in LAN. A packet sent by the host to another host carries both the source host's and the destination host's address.
2) **Metropolitan Area Network (MAN):** MAN refers to a network that covers an entire city. For example: consider the cable television network.
3) **Wide Area Network (WAN):** WAN refers to a network that connects countries or continents. For example, the Internet allows users to access a distributed system called www from anywhere around the globe.WAN interconnects connecting devices such as switches, routers, or modems. A LAN is normally privately owned by an organization that uses it. We see two distinct examples of WANs today: point-to-point WANs and Switched WANs
    - **Point To Point**: Connects two connecting devices through transmission media.
    - **Switched:** A switched WAN is a network with more than two ends.

Based on Types of Communication

- **Point To Point networks:** Point-to-Point networking is a type of data networking that establishes a direct link between two networking nodes. A direct link between two devices, such as a computer and a printer, is known as a point-to-point connection.
- **Multipoint**: is the one in which more than two specific devices share links. In the multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection.
- **Broadcast networks:** In broadcast networks, a signal method in which numerous parties can hear a single sender. Radio stations are an excellent illustration of the "Broadcast Network" in everyday life. The radio station is a sender of data/signal in this scenario, and data is only intended to travel in one direction. Away from the radio transmission tower, to be precise.

Based on the Type of Architecture

- **P2P Networks:** Computers with similar capabilities and configurations are referred to as peers. "Peer to Peer" is the abbreviation for "peer to peer." The "peers" in a peer-to-peer network are computer systems that are connected to each other over the Internet. Without the use of a central server, files can be shared directly between systems on the network.
- **Client-Server Networks:** Each computer or process on the network is either a client or a server in a client-server architecture (client/server). The client asks for services from the server, which the server provides. Servers are high-performance computers or processes that manage disc drives (file servers), printers (print servers), or network traffic (network servers)
- **Hybrid Networks:** The hybrid model refers to a network that uses a combination of client-server and peer-to-peer architecture. Eg: Torrent.

Types of Computer Network Architecture

Computer Network Architecture is of two types. These types are mentioned below.

1) **Client-Server Architecture:** Client-Server Architecture is basically the architecture where the clients and the server are connected as two clients can communicate with each other and the devices present work as servers in the network.
2) **Peer-to-Peer Architecture:** Peer-to-Peer Architecture, computers are connected to each other and each computer is equally capable of working as there is no central server here. Each device present here can be used as a client or server.

Types of Enterprise Computer Networks

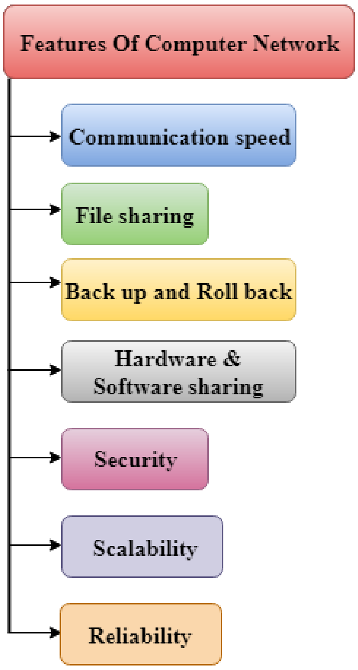
There are three main types of Enterprise Computer Networks which are mentioned below.

1) **Local Area Network (LAN):** Local Area Networks are small-scale networks used in small companies or as test networks. It has a limited size.
2) **Wide Area Networks (WAN):** Wide Area Networks are networks that are used for a larger area than local area networks and are used for long-distance communication.
3) **Service Provider Networks:** Service Provider Networks are the networks that help in wireless communication, high-speed internet access, etc.

Features of Computer Network

A list of Computer network features is given below

- **Communication speed -** Network provides us to communicate over the network in a fast and efficient manner. For example, we can do video conferencing, email messaging, etc. over the internet. Therefore, the computer network is a great way to share our knowledge and ideas.
- **File sharing** - File sharing is one of the major advantages of the computer network. Computer network provides us to share the files with each other.
- **Back up and Roll back is easy** - Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.
- **Software and Hardware sharing** - We can install the applications on the main server, therefore, the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.



- **Security** - Network allows the security by ensuring that the user has the right to access the certain files and applications.
- **Scalability** - Scalability means that we can add the new components on the network. Network must be scalable so that we can extend the network by adding new devices. But, it decreases the speed of the connection and data of the transmission speed also decreases, this increases the chances of error occurring. This problem can be overcome by using the routing or switching devices.
- **Reliability** - Computer network can use the alternative source for the data communication in case of any hardware failure.

Network Examples

Mathematically, a network is a **graph** G=(V,E), where **V** is a set of **nodes** and **E** is a set of pairs of nodes called **edges**. Edges can be *directed* or *undirected*, *weighted* or *unweighted*.

So, what's the difference between graphs and networks? While a graph is an abstract mathematical object, a network is a real-world web with **specific structural properties**. These properties has been exploited to investigate the origin and evolution of networks and to study the processes taking place on them. Let us give some remarkable examples of networks and briefly explain why they deserve attention:

- **The World Wide Web -** This is a directed network in which nodes represent Web pages and edges are the hyperlinks between pages. More precisely, there exists an edge from page **p** to page **q** if page **p** contains at least one hyperlink pointing to page **q**. Usually, the actual number of hyperlinks from **p** page **q** is not important and hence the network modeling the Web is unweighted.

  Studying the Web as a network is of crucial importance in the field of Web information retrieval. Web search engines, for instance, heavily exploit the Web topology in order to rank Web pages that are returned to the user that issued a query. The Page Rank method, which is a major ingredient of Google search engine, is a fitting example.
- **The Internet -** This is a collection of routers linked by various physical lines. The Internet is a growing network with no central control authority. When adding a new node to the Internet, two factors mainly determine the router node to connect to: distance and bandwidth. While distance puts obvious constraints, bandwidth, a measure of connection speed of the router, is typically the dominant factor. This explains the emergence of hubs in the Internet. The study of Internet topology is crucial to investigate the robustness of the network under failures, which involve nodes randomly, and attacks, which purposely decimate network hubs. If the network is highly connected and dominated by few hubs, then random failures are generally not problematic, but attacks aimed to destroy the vital hubs might have Draconian effects.
- **Powerline and airline networks -** These are human-made networks that might be involved in random failures as well as targeted attacks. Failures may have cascading effects: the failure of one node may recursively provoke the failure of connected nodes. Clearly, such events on these networks might have catastrophic consequences. The topology of the network directly influences the magnitude and reach of such events.
- **Citation networks** - An article citation network links scholarly papers through bibliographic references contained in the bibliography of the papers. This network is directed and follows the temporal ordering of papers: we cite the past, not the future. Hence, cycles are very rare, and a citation network closely resembles a directed acyclic graph. Moreover, papers may be aggregated at different levels, forming bibliometric units like scholars and journals. These bibliometric units can play the role of nodes is a citation network, with edges representing the citations among them. For instance, in a journal citation network, nodes are academic journals, and there is an edge from journal **i** to journal j if some article published in **i** cites some article appearing in **j**. Usually, such a network is weighted, with the weight of an edge representing the number of citations between the journals participating in the edge.

  Citation networks are fundamental tools in *bibliometrics*, the discipline that concerns itself with the study of the dissemination of knowledge through academic publication. In particular, bibliometric indicators like the PageRank-inspired Eigenfactor take full advantage of the topology of journal citation networks. Citation networks arise also in different contexts like patents and corresponding citations and published opinions of judges and their citations within and across opinion circuits.

- **Language networks -** In these networks the nodes are words and the links represent relationships among words like significant co-occurrence in texts. The properties of this network suggest some unexpected features of language organization that might reflect the evolutionary and social history of lexicons and the origins of their flexibility and combinatorial nature. The known dramatic effects of disconnecting the most connected vertices in such networks can be identified in some language disorders like *agrammatism*, a kind of aphasia in which speech is non-fluent, laboured, halting and lacking in function words.
- **Food webs -** These are networks created by nature. In food webs, species are connected by links telling which species feeds on which other species. The links of these networks seldom go both ways, and hence food webs are also an example of directed networks. Studying food webs is important to understand the ecosystem dynamics. For instance, ecologists believe that hubs of food webs are the keystone species of the ecosystem, paramount in maintaining the stability of the ecosystem. The ecosystem can easily survive if random species are deleted; if, however, hub species are removed, the ecosystem dramatically collapses.
- **Economic networks -** Market can be viewed as a huge directed multi-relational network. Companies, firms, financial institutions, governments play the role of nodes. Links symbolize different interactions between them, for instance purchases and sales or financial loaning, and the weight of the links captures the value of the transaction. Viewing the economy as a network of interacting actors is useful to make sense of global financial meltdowns, which are provoked by a sequence of failures cascading over the highly connected and interdependent network economy.
- **Metabolic and protein networks -** The nodes of metabolic networks are simple molecules like water or ATP. The links are the biochemical reactions that take place between these molecules. Moreover, proteins can be viewed as nodes of a complex network in which two proteins are connected if they can physically interact. An important example is hemoglobin, a protein complex made of four proteins that attach together to transport oxygen in bloodstreams. The robustness of such life maps under failures determines our ability to survive various diseases, and the identification of hub molecules and proteins allow researchers to design effective drugs to cure diseases.
- **Social networks -** Social networks link people according to various social relationships, like acquaintance, friendship, collaboration, and sexual relation. They are of paramount importance to understand and anticipate the spread of ideas, innovations, fads, as well as biological and computer viruses. For instance, the dominant position of hubs in sexual networks -- people with an extraordinary number of sexual partners -- has been adopted as an explanation of the partially unexpected diffusion and persistence of AIDS epidemic, which defies the predictions of classical epidemic models based on the homogeneous, random network hypothesis. Indeed, due to their high connectivity, hubs are easy to be infected and, once infected; they potentially can pass the virus to all linked people.

Computer Networks and the Internet

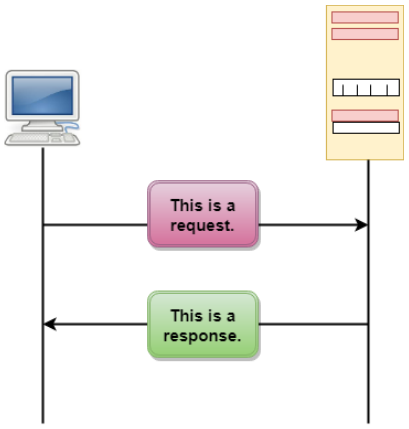
The Internet is the major example of a WAN, which connects billions of computers globally. Internet follows standard protocols that facilitate communication between these network devices. Those protocols include:

- **HTTP (Hypertext Transfer Protocol)**
  - ✓ HTTP stands for Hyper Text Transfer Protocol.
  - ✓ It is a protocol used to access the data on the World Wide Web (www).
  - ✓ The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
  - ✓ This protocol is known as Hyper Text Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
  - ✓ HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
  - ✓ HTTP is used to carry the data in the form of MIME-like format.
  - ✓ HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

Features of HTTP:

- ○ **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- ○ **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- ○ **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

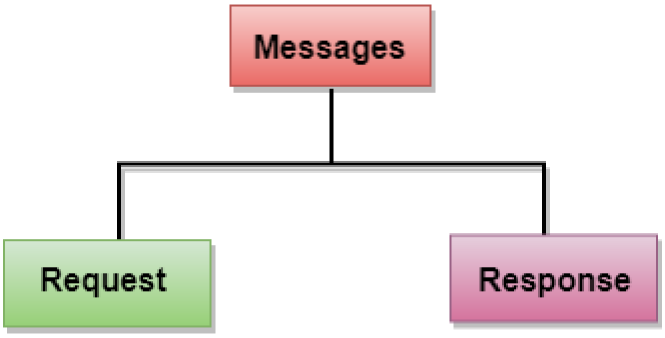
HTTP Transactions



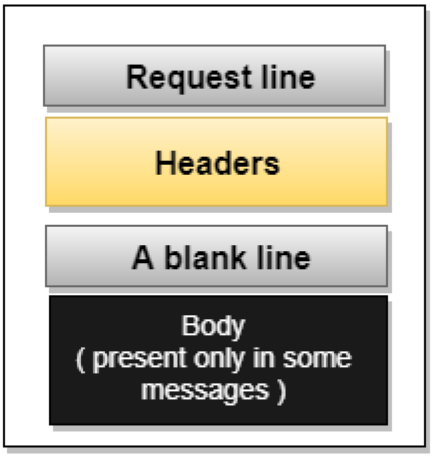
The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

Messages

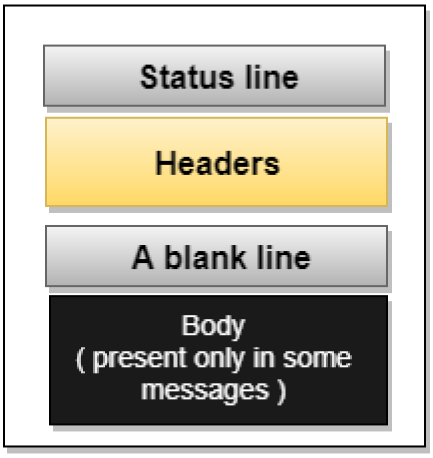
HTTP messages are of two types: request and response. Both the message types follow the same message format.



Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.

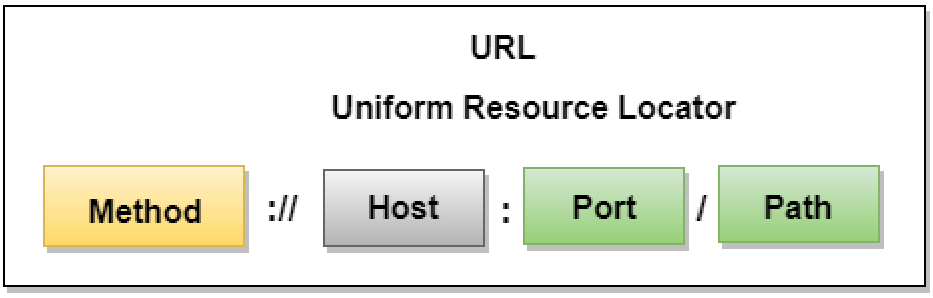


Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.



Uniform Resource Locator (URL)

- A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).
- The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.
- The URL defines four parts: method, host computer, port, and path.



- **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.
- **Host:** The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
- **Port:** The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
- **Path:** Path is the pathname of the file where the information is stored. The path itself contains slashes that separate the directories from the subdirectories and files.

- **IP (Internet protocol or IP addresses)**

Here, IP stands for **internet protocol**. It is a protocol defined in the TCP/IP model used for sending the packets from source to destination. The main task of IP is to deliver the packets from source to the destination based on the IP addresses available in the packet headers. IP defines the packet structure that hides the data which is to be delivered as well as the addressing method that labels the datagram with a source and destination information.

An IP protocol provides the connectionless service, which is accompanied by two transport protocols, i.e., TCP/IP and UDP/IP, so internet protocol is also known as TCP/IP or UDP/IP.

The first version of IP (Internet Protocol) was IPv4. After IPv4, IPv6 came into the market, which has been increasingly used on the public internet since 2006

History of Internet Protocol

The development of the protocol gets started in 1974 by **Bob Kahn and Vint Cerf**. It is used in conjunction with the Transmission Control Protocol (TCP), so they together named the TCP/IP.

The first major version of the internet protocol was IPv4, which was version 4. This protocol was officially declared in RFC 791 by the Internet Engineering Task Force (IETF) in 1981.

After IPv4, the second major version of the internet protocol was IPv6, which was version 6. It was officially declared by the IETF in 1998. The main reason behind the development of IPv6 was to replace IPv4. There is a big difference between IPv4 and IPv6 is that IPv4 uses 32 bits for addressing, while IPv6 uses 128 bits for addressing.

Function

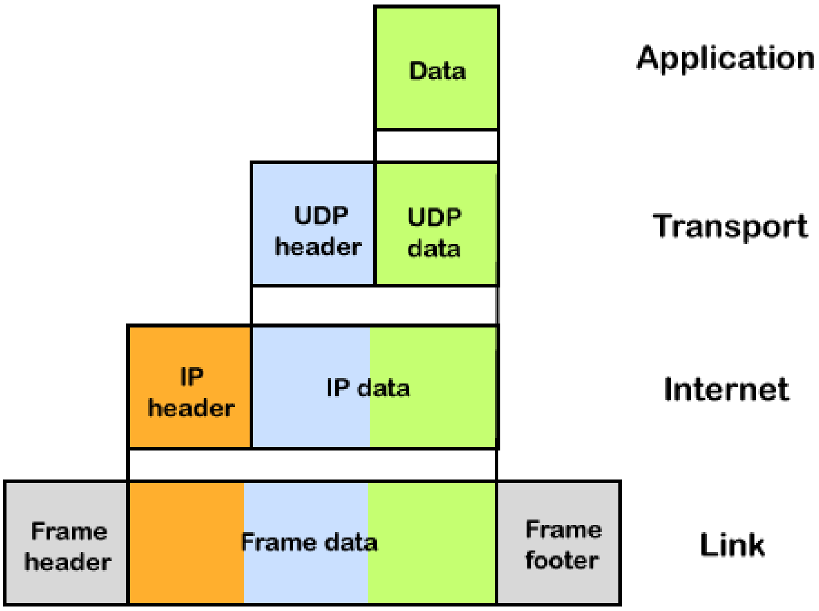
The main function of the internet protocol is to provide addressing to the hosts, encapsulating the data into a packet structure, and routing the data from source to the destination across one or more IP networks. In order to achieve these functionalities, internet protocol provides two major things which are given below.

An internet protocol defines two things:

- Format of IP packet
- IP Addressing system

IP packet

Before an IP packet is sent over the network, two major components are added in an IP packet, i.e., **header** and a **payload**.



An IP header contains lots of information about the IP packet which includes:

- Source IP address: The source is the one who is sending the data.
- Destination IP address: The destination is a host that receives the data from the sender.
- Header length
- Packet length
- TTL (Time to Live): The number of hops occurs before the packet gets discarded.
- Transport protocol: The transport protocol used by the internet protocol, either it can be TCP or UDP.

There is a total of 14 fields exist in the IP header, and one of them is optional.

Payload: Payload is the data that is to be transported.

How does the IP routing perform?

IP routing is a process of determining the path for data so that it can travel from the source to the destination. As we know that the data is divided into multiple packets, and each packet will pass through a web of the router until it reaches the final destination. The path that the data packet follows is determined by the routing algorithm. The routing algorithm considers various factors like the size of the packet and its header to determine the efficient route for the data from the source to the destination. When the data packet reaches some router, then the source address and destination address are used with a routing table to determine the next hop's address. This process goes on until it reaches the destination. The data is divided into multiple packets so all the packets will travel individually to reach the destination.

For example, when an email is sent from the email server, then the TCP layer in this email server divides the data into multiple packets, provides numbering to these packets and transmits them to the IP layer. This IP layer further transmits the packet to the destination email server. On the side of the destination server, the IP layer transmits these data packets to the TCP layer, and the TCP layer recombines these data packets into the message. The message is sent to the email application.

IP Addressing

An IP address is a unique identifier assigned to the computer which is connected to the internet. Each IP address consists of a series of characters like 192.168.1.2. Users cannot access the domain name of each website with the help of these characters, so DNS resolvers are used that convert the human-readable domain names into a series of characters. Each IP packet contains two addresses, i.e., the IP address of the device, which is sending the packet, and the IP address of the device which is receiving the packet.

Types of IP addresses

IPv4 addresses are divided into two categories:

a) **Public address -** The public address is also known as an external address as they are grouped under the WAN addresses. We can also define the public address as a way to communicate outside the network. This address is used to access the internet. The public address available on our computer provides the remote access to our computer. With the help of a public address, we can set up the home server to access the internet. This address is generally assigned by the ISP (Internet Service Provider).

   Key points related to public address are:

   - The scope of the public address is global, which means that we can communicate outside the network.
   - This address is assigned by the ISP (Internet Service Provider).
   - It is not available at free of cost.
   - We can get the Public IP by typing on Google "What is my IP".

b) **Private address -** A private address is also known as an internal address, as it is grouped under the LAN addresses. It is used to communicate within the network. These addresses are not routed on the internet so that no traffic can come from the internet to this private address. The address space for the private address is allocated using **InterNIC** to create our own network. The private addresses are assigned to mainly those computers, printers, smartphones, which are kept inside the home or the computers that are kept within the organization. For example, a private address is assigned to the printer, which is kept inside our home, so that our family member can take out the print from the printer.

If the computer is assigned with a private address, then the devices available within the local network can view the computer through the private ip address. However, the devices available outside the local network cannot view the computer through the private IP address, but they can access the computer if they know the router's public address. To access the computer directly, NAT (Network Address Translator) is to be used.

Key points related to private address are:

- Its scope is local, as we can communicate within the network only.
- It is generally used for creating a local area network.
- It is available at free of cost.
- We can get to know the private IP address by simply typing the "ipconfig" on the command prompt.

- **TCP (Transmission Control Protocol)**

TCP stands for **Transmission Control Protocol**. It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together; they are referred to as a TCP/IP.

The main functionality of the TCP is to take the data from the application layer. Then it divides the data into a several packets, provides numbering to these packets, and finally transmits these packets to the destination. The TCP, on the other side, will reassemble the packets and transmits them to the application layer. As we know that TCP is a connection-oriented protocol, so the connection will remain established until the communication is not completed between the sender and the receiver.

Features of TCP protocol

The following are the features of a TCP protocol:

- **Transport Layer Protocol -** TCP is a transport layer protocol as it is used in transmitting the data from the sender to the receiver.
- **Reliable -** TCP is a reliable protocol as it follows the flow and error control mechanism. It also supports the acknowledgment mechanism, which checks the state and sound arrival of the data. In the acknowledgment mechanism, the receiver sends either positive or negative acknowledgment to the sender so that the sender can get to know whether the data packet has been received or needs to resend.
- **Order of the data is maintained -** This protocol ensures that the data reaches the intended receiver in the same order in which it is sent. It orders and numbers each segment so that the TCP layer on the destination side can reassemble them based on their ordering.

- **Connection-oriented -** It is a connection-oriented service that means the data exchange occurs only after the connection establishment. When the data transfer is completed, then the connection will get terminated.
- **Full duplex -** It is a full-duplex means that the data can transfer in both directions at the same time.
- **Stream-oriented -** TCP is a stream-oriented protocol as it allows the sender to send the data in the form of a stream of bytes and also allows the receiver to accept the data in the form of a stream of bytes. TCP creates an environment in which both the sender and receiver are connected by an imaginary tube known as a virtual circuit. This virtual circuit carries the stream of bytes across the internet.

- **UDP (User Datagram Protocol)**

In computer networking, the UDP stands for User Datagram Protocol. The David P. Reed developed the UDP protocol in 1980. It is defined in RFC 768, and it is a part of the TCP/IP protocol, so it is a standard protocol over the internet. The UDP protocol allows the computer applications to send the messages in the form of datagram's from one machine to another machine over the Internet Protocol (IP) network. The UDP is an alternative communication protocol to the TCP protocol (transmission control protocol). Like TCP, UDP provides a set of rules that governs how the data should be exchanged over the internet. The UDP works by encapsulating the data into the packet and providing its own header information to the packet. Then, this UDP packet is encapsulated to the IP packet and sent off to its destination. Both the TCP and UDP protocols send the data over the internet protocol network, so it is also known as TCP/IP and UDP/IP. There are many differences between these two protocols. UDP enables the process to process communication, whereas the TCP provides host to host communication. Since UDP sends the messages in the form of datagrams, it is considered the best-effort mode of communication. TCP sends the individual packets, so it is a reliable transport medium. Another difference is that the TCP is a connection-oriented protocol whereas, the UDP is a connectionless protocol as it does not require any virtual circuit to transfer the data.

UDP also provides a different port number to distinguish different user requests and also provides the checksum capability to verify whether the complete data has arrived or not; the IP layer does not provide these two services.

Features of UDP protocol

The following are the features of the UDP protocol:

- **Transport layer protocol -** UDP is the simplest transport layer communication protocol. It contains a minimum amount of communication mechanisms. It is considered an unreliable protocol, and it is based on best-effort delivery services. UDP provides no acknowledgment mechanism, which means that the receiver does not send the acknowledgment for the received packet, and the sender also does not wait for the acknowledgment for the packet that it has sent.
- **Connectionless -** The UDP is a connectionless protocol as it does not create a virtual path to transfer the data. It does not use the virtual path, so packets are sent in different paths between the sender and the receiver, which leads to the loss of packets or received out of order.

- **Ordered delivery of data is not guaranteed -** In the case of UDP, the datagram's are sent in some order will be received in the same order is not guaranteed as the datagram's are not numbered.
- **Ports -** The UDP protocol uses different port numbers so that the data can be sent to the correct destination. The port numbers are defined between 0 and 1023.
- **Faster transmission -** UDP enables faster transmission as it is a connectionless protocol, i.e., no virtual path is required to transfer the data. But there is a chance that the individual packet is lost, which affects the transmission quality. On the other hand, if the packet is lost in TCP connection, that packet will be resent, so it guarantees the delivery of the data packets.
- **Acknowledgment mechanism -** The UDP does have any acknowledgment mechanism, i.e., there is no handshaking between the UDP sender and UDP receiver. If the message is sent in TCP, then the receiver acknowledges that I am ready, then the sender sends the data. In the case of TCP, the handshaking occurs between the sender and the receiver, whereas in UDP, there is no handshaking between the sender and the receiver.
- **Segments are handled independently -** Each UDP segment is handled individually of others as each segment takes different path to reach the destination. The UDP segments can be lost or delivered out of order to reach the destination as there is no connection setup between the sender and the receiver.
- **Stateless -** It is a stateless protocol that means that the sender does not get the acknowledgement for the packet which has been sent.

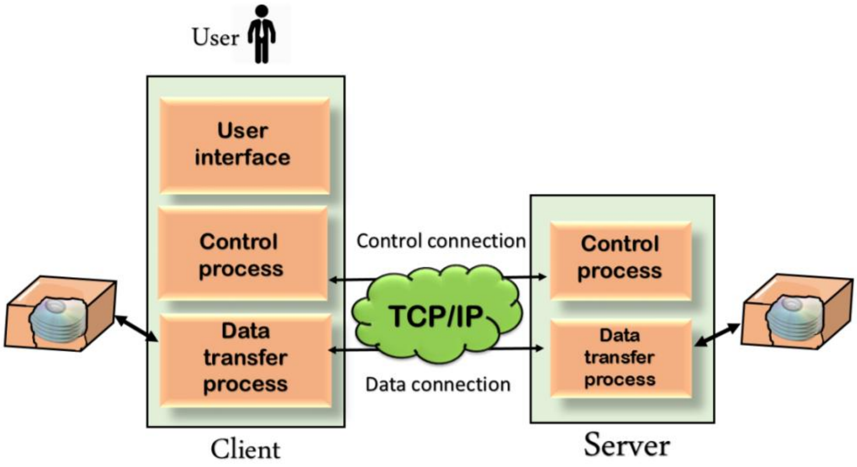
- **FTP (File Transfer Protocol)**
  - FTP stands for File transfer protocol.
  - FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
  - It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
  - It is also used for downloading the files to computer from other servers.

Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

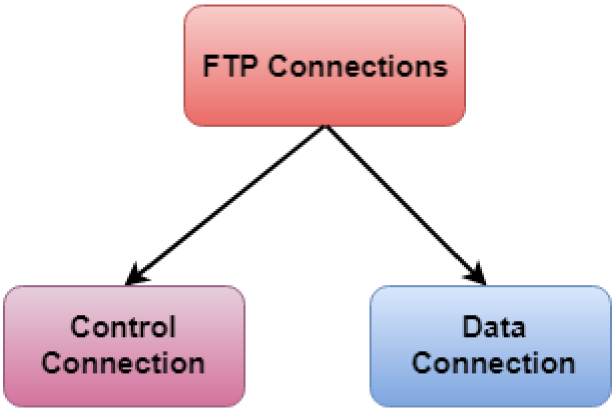
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Mechanism of FTP



The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

There are two types of connections in FTP:



a) **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.

b) **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients

FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.

- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

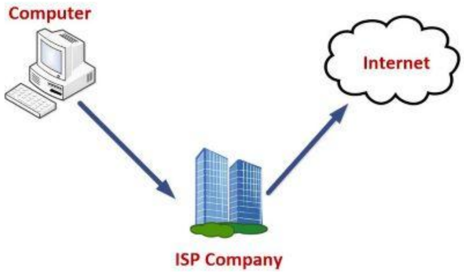
- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

- **ISPs (Internet Service Providers)**

ISP stands for Internet Service Provider. It is a company that provides access to the internet and similar services such as Website designing and virtual hosting. For example, when you connect to the Internet, the connection between your Internet-enabled device and the internet is executed through a specific transmission technology that involves the transfer of information packets through an Internet Protocol route.



Data is transmitted through different technologies, including cable modem, dial-up, DSL, high speed interconnects. Accordingly, based on the method of data transmission, the Internet access provided by ISPs can be divided into many types, some of which are as follows:

- **Dial-up Internet access:** It is the oldest technology to provide Internet access by modem to modem connection using telephone lines. In this method, the user's computer is connected to a modem with a telephone line. This method has become outdated today due to slow connection speed. However, in remote areas, this method can be used where the broadband network is not available.

- **DSL:** DSL, which stands for 'digital subscriber line' is an advanced version of the dial-up Internet access method. It uses high frequency to execute a connection over the telephone network and allows the internet and the phone connection to run on the same telephone line. This method offers an Asymmetric Digital Subscriber (ADSL), where the upload speed is less than the download speed, and a Symmetric Digital Subscriber Line (SDSL), which offers equal upload and download speeds. Out of these two, ADSL is more popular among users and is popularly known as DSL.
- **Wireless Broadband (WiBB):** It is a modern broadband technology for Internet access. It allows high-speed wireless internet within a large area. To use this technology, you are required to place a dish on the top of your house and point it to the transmitter of your Wireless Internet Service Provider (WISP).
- **Wi-Fi Internet:** It is the short form for "wireless fidelity," which is a wireless networking technology that provides wireless high-speed Internet connections using radio waves. To use the internet, you are required to be within the range of wi-fi network. It is commonly used in public places such as hotels, airports, restaurants to provide internet access to customers.
- **ISDN:** It is a short form of Integrated Services Digital Network. It is a telephone system network which integrates a high-quality digital transmission of voice and data over the same standard phone line. It offers a fast upstream and downstream Internet connection speed and allows both voice calls and data transfer.
- **Ethernet:** It is a wired LAN (Local Area Network) where computers are connected within a primary physical space. It enables devices to communicate with each other via a protocol (a set of rules or common network language). It may provide different speeds such as 10 Mbps, 100 Mbps and 10 Gbps.

- **NSPs (Network Service Providers)** effectively support the internet infrastructure.

  To fully understand what **NSP** is. Firstly, we have to know about what is a Network and what are network services.

  Network - A Network is a connection of two or more devices which communicate with each other for sharing images, files, audio, videos, and resources.

  The devices that want to transmit data and resources are connected via twisted-pair cables, optical fiber cables, co-axial cable, radio waves, and Bluetooth technology

  The best example of a network is the Internet, which connects thousands even millions of users across the globe via their network devices.

  Following are some network devices which can communicate with each other with the physical medium:

  - Laptops, tablets, computers, and mobile phones.
  - Hubs and switches.
  - Firewalls.
  - Routers and Modems.
  - Network Interface Card, etc.

Network Services

- Those applications, functions, and services of the network which are managed by the IT service providers for their clients and customers are called network services.
- Enterprises and consumers can purchase the services of the network directly from MSPs (Managed Service Providers) and NSPs (Network Service Providers).
- Network services include various network operations, security and performance services, and communication methods.

NSP - NSP is a short form of '**Network Service Provider'**.

- It is a business or company that sells the bandwidth by supplying the Internet backbone to the Internet Service Providers and large organizations directly for the consumer's use. Sometimes, NSP is also called backbone service providers.
- Network Service Providers are considered the same as ISPs, but in many situations, they provide Internet access to the ISPs.
- NSPs establish and manage the primary infrastructure of the Internet across the world. This service provider includes the fiber optic line which gives the high bandwidth of thousands of gigabits per second.
- When we use a cable modem and DSL modem for Internet connection, then we connect to the ISP, and the ISP automatically establishes a connection with the internet backbone of NSP.
- The responsibility of network service providers is to make sure that the network across the globe is reliable and performs decently.
- The reliability feature is serious for the telecommunication organizations which offer high-speed internet access to the consumers.
- NSP routes all the traffic and builds its infrastructure to meet the traffic demands.
- ISPs purchase cloud-based services from the NSPs for offering the services to their users, businesses, and consumers.
- In the United States, MCI, Verizon, AGIS, BBN, Sprint, and AT & T are the major network service providers.

The infrastructure allows the transportation of data packets to the recipient device over the Internet.

Internet Based Applications

Internet Applications can be described as the type of applications that use the internet for operating successfully, that is, by using the internet for fetching, sharing and displaying the information from the respective server systems. It can be accessed only with the help of the internet facility, and it cannot be functional without the internet. These applications can be classified as electronic devices based, automated digital technology, industrial internet, smart phones based, smart home-based, smart grids, smart city, and other major applications.

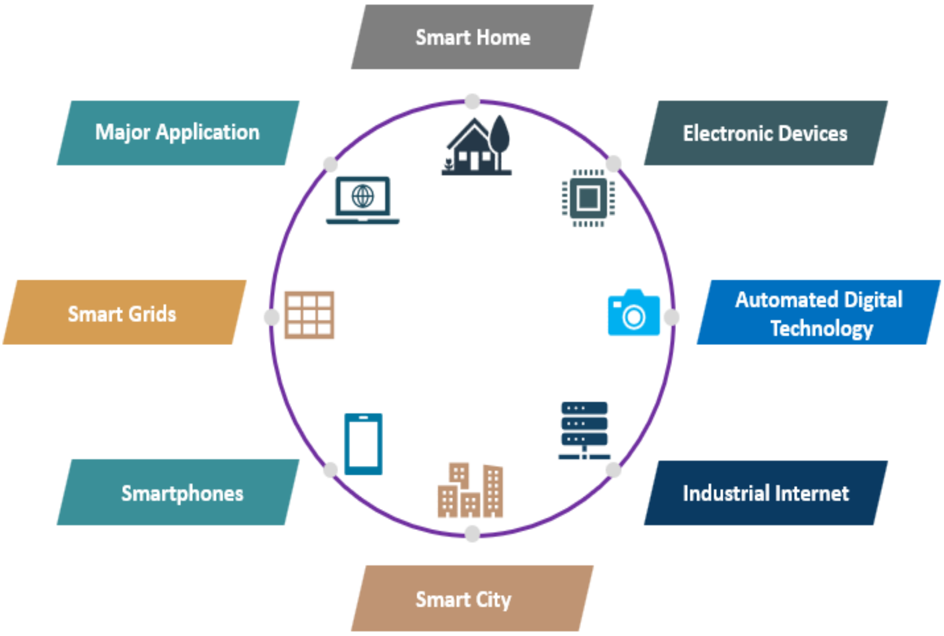
Services of Internet Application

Some of the internet applications are:

- The internet has many few major applications like electronic mail services, web browsing, and peer to peer networking. The use of email increases because of its several features like attachments, messages, data usage.
- The attachment feature such as word documents, excel sheets, and graphical media is possible because of Multipurpose Internet Mail Extensions, but the result is traffic volume caused by mail is calibrated in terms of data packets in the network.
- Electronic mail services became a vital part of personal and professional communication method, and its time and cost consuming. The data is transmitted and received **securely by encryption**. The price of tickets for transport and sport are received in the mail.
- The web browser is a critical application of the internet and is highly commercial dominated by Microsoft and highly influenced by WWW – World Wide Web.
- The web browser is free and available as an open-source model that enriches the minds of future generations. The open-source has been developed and deployed on a modular basis since the source code is accessible only with few usage restrictions. The open-source feature has been **integrated to file managers** and web browsers.
- Other important applications and potentially needed in Internet application is peer-to-peer networking. This P2P networking is a dynamic method that is based on the exchanging of physical resources like hard drives, files, processors and other intelligent features.
- Each group of peer to peer networking has equal responsibility and functions. Peer-to-peer applications based on the internet locate the computer at the focus of the computing matrix based on cross-network protocols like SOAP Simple Object Access Protocol or Remote Procedure Calling XML-**RPC the user** to enter on the Internet more proactively.

Top Application of Internet

1) **Smart Home -** Smart Home has become the evolutionary ladder in residential and developing as common as smartphones. It is a special feature of Google and now deployed in many areas to make life convenient and user-friendly. The smart home is designed to save time, money and energy.
2) **Electronic Devices -** Electronic devices like wearables are installed with different sensors and software, which gather data and information of the user where data is processed to give required info about the user. The devices mainly used to monitor fitness, entertainment, and health. They mostly work on ultra-low power and available in small sizes.



3) **Automated Digital Technology -** The automated digital technology has concentrated on the optimization of vehicles and their internal functions. the automated car is designed with special features that give a comfort zone to passengers with onboard sensors and internet establishment. Popular companies like Tesla, Apple, BMW, Google is yet to aboard their revolution in the automobile industry by installing excellent features.
4) **Industrial Internet -** The industrial internet is investing in industrial engineering with Artificial intelligence and data analytics to build brilliant machines. The important moto is to build smart machines that are accurate and compatible with a human. It holds vast potential with good quality and reliability. The applications are deployed for tracing the goods to be delivered, real-time data regarding retails and supplies that increase the efficiency of the business's supply chain and productivity.
5) **Smart City -** A smart city is another major implementation of the internet, which is employed for smart surveillance, water distribution, automatic transportation, environment monitoring. People are prone to pollution, improper supplies and shortage of sources, and the installation of traffic sensors solves irregular traffic flow, and the app is developed to report the municipal systems. Citizens can able to diagnose simple malfunctions in meter and can report to the electricity system via electricity board applications or websites, and they can also find available slots for vehicle parking easily in sensor systems.
6) **Smartphones -** Smartphones are also used for retailers and customers to stay connected for their business transactions, even out of the store. They have using Beacon technology to help business people to provide smart service to the client. They can track the products and enhance the store dashboard and deliver premium order before the scheduled date, even in congested traffic areas.
7) **Smart Grids -** The idea applied in smart grids is to gather data in an automated way to analyze the attribute of electricity. Consumers to improve the efficiency and economics

of usage. Smart grids can easily detect the power outage and shortage quickly and fix them shortly.

8) **Major Application -** Another major application of the internet is in healthcare as it is smart medical systems installed to diagnose and cure the disease at an earlier stage. Many **machine learning** algorithms are used in image processing and classification to detect the fetus's abnormalities before birth. The main aim applied in the medical field is to provide a healthier life for all by wearing connected devices. The gathered medical data of patients made the treatment easier, and a monitoring device is installed to track the sugar and blood pressure.

Advantages of the internet

- The internet is a suitable environment to work with people all over the world through instant communication that can provide products and services easier and faster.
- An internet connection made the employees work from the option to create a virtual office at home.
- The internet connection connects your laptop or pc to internet aided devices to **access cloud computing** and cloud storage.
- The internet can build a supercomputer to perform and manage complex task.

Network Devices in Networking

Functions of Network devices

- Networking devices serve the following general purposes:
- Facilitate data transmission and communication between devices
- Enable efficient and secure network connectivity
- Enhance network performance and optimize traffic flow
- Provide network security by enforcing access control and threat prevention
- Simplify network management and configuration
- Extend network coverage and overcome signal limitations

1: Hub.

What do you understand by the word Hub in the world of computing?Hub (computing) refers to the connection point in a system which is the melting pot as data from many directions is converged here and further sent out in many varied directions. A hub also often acts as a switch by stopping certain data packets from reaching their destinations.

Types of Hubs:

1) Active Hub.
2) Intelligent Hub.
3) Passive Hub.

Configuration:

- The runtime that has been set by the environment data hub needs to be shared on DASD in a SYSPLEX environment.
- To make a high availability hub that enables movement from one LPAR to another, whilst a recovery switchover. The hub host address needs to be defined by the means of Dynamic VIPA (DVIP).

Need of Hub in Networking:

- Multiple devices are connected by the means of a hub.
- It also qualifies as a repeater as it amplifies signals which have deteriorated after traveling over connecting cables.
- Hubs are the easiest in the entire family of network connecting a hub is the simplest in the family of network connecting devices because it connects LAN components with identical protocols.

2: Switches

Switches are devices that are operating a secondary data link layer in the OSI model. They establish connectivity in any network and by the means of a packet data is received and sent. Multiple computers are plugged into it as it has many ports.

Types of switches:

1) KVM switch
2) Managed switch
3) Unmanaged switch
4) Smart switch
5) PoE Switch

Configuration

- The most number of small switches are employed by small businesses. They are also used at homes and office spaces. These require no configuration as they are plug and play.
- However, plug and play doesn't always work. Small switches don't offer any troubleshooting, logging, security, or manageability whatsoever.

Need For a Switch:

- Switches are key building blocks for any network. They connect multiple devices, such as computers, wireless access points, printers, and servers; on the same network within a building or campus. A switch enables connected devices to share information and talk to each other.

3: Router

Router is defined as a networking device that sends data packets further between computer networks. They are able to perform traffic directing functions over the internet.

Types of Routers:

1) Edge routers
2) VPN routers.
3) Wired routers
4) Core routers

Configuration:

- The process to configure a router begins by unplugging or switching off the cable or DSL modem. Firstly, unplug or turn off the cable or DSL modem. Then the wireless router has to be plugged in and connected to the network cable into the port over the router that is labeled as 'internet' or' WAN'. The other end is to be connected to the cable or DSL modem and the modem has to be started.

Need for a router:

- The router is one of the integral parts of a computing system.
- It works to manage traffic between networks by forwarding data packets to the IP address designated to them and also allowing multiple devices to use the same internet connection as well.

4: Bridge.

A bridge is another device that is used to connect LAN cable segments together. The bridge is operational at the data link layer of an OSI model. Bridges also facilitate packet filtering at the data link layer, which means that it can only pass the packets that are meant for the other side of the network.

Configuration:

- Bridging is one of the features that can be employed to establish a connection between 2 or more layer 2 interfaces together that too from the single broadcast domain.
- This then further forwards packets in software, basing it upon the layer 2 header. This resembles quite a lot to forward the logic to layer 2 switching. From where they get ahead into hardware.

Need for configuration:

There is a need for bridges as:

- Bridges happen to connect two or more different LANs that have a similar protocol and further provide communication between the devices in them.
- Bridges help in multiplying the network capacity of a single LAN by joining multiple LANs.

5: Gateway.

A gateway can be defined as a network node that is employed in telecommunications that it tends to connect two networks which possess varying transmission protocols alongside. network as it's important for all data to communicate with the gateway before it begins to get routed.

Configuration

- To configure a Gateway the following steps are needed:
- Primarily install and configure the second network adapter.
- Install and configure the second network adapter, if you have not done so already. (See Installing a network adapter and Adapter management and configuration.)
- Choose an IP address for the second network interface, and then configure the network interface by following the instructions in Network interface management.

Need of a gateway:

- A gateway is a network node that is used to connect two networks with varying transmission protocols together, in telecommunications.

6: Modem

A modem is defined as a network device that both modulates and also demodulates analog carrier signals known as signals or sine waves, for encoding and decoding digital information for processing. Modems efficiently accomplish both tasks.

Configuration

- Whilst using any device with a browser, you have to connect it to the WiFi network of that particular modem.
- Open the browser and then enter the gateway address which is written at the back of that modem.
- Now the final step is to enter the modem username and password, which should also be on the modem.

Need for a MODEM:

- We need a modem to be able to send and receive data from two different networking routes; the internet provider's connection and also one's home network's connection as well.

7: Repeater.

A repeater is implemented in a system's network to facilitate A repeater is implemented in computer networks to expand the coverage area of the network, repropagate a weak or broken signal and or service remote nodes. Repeaters amplify the received/input signal to a higher frequency domain so that it is reusable, scalable and available.

Configuration

- When in repeater mode, the access point tends to extend the range of any existing WiFi network.
- This mode is most preferred if a person is in a no Wifi zone or a place that has really poor reception.

8: Access Point

An access point is identified as a device that creates a wireless local area network, or WLAN, that often exists in an office or large building. An access point establishes a connection with a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.

Configuration

- The access point has to be connected to one of the ports of one's existing wired/wireless router and then the access point's wireless settings have to be configured.
- Now web point's web -based setup page is opened by entering the default IP address.
- On the web-based setup page, click on Wireless
- Enter the Network Name (SSID).

Need for an access point:

- Access points are useful for extending the wireless coverage of any existent network and further increasing the number of users that shall be connected to it.
- Hopefully you were able to know the networking devices essential to perform and carry out daily and advanced computing as well. The devices are absolutely crucial for carrying out smooth working be it for individuals or organizations.

9: WLC - Wireless LAN Controller

Cisco Wireless LAN Controller (WLAN), wireless controller, provides wireless performance of all mobile devices, offers limited hotspot coverage and more.

Configuration:

- A wireless LAN controller (WLC) is a network component that is capable of managing wireless network access points and allows wireless devices to connect to the network.
- It offers central control over network elements, simplifies individual component monitoring.

Need for WLC:

- WLCs (Cisco WLC) are commonly used to have control over one's routers, switches, firewalls, gateways etc. Monitoring Cisco WLC helps you determine the performance and efficiency of every device.

10: NIC - Network Interface Card:

A network interface card (NIC) is a hardware component, typically a circuit board or chip, which is installed on a computer so it can connect to a network.

Configuration of NIC:

- To configure NIC firstly the control panel has to be opened. Then orderly, set View by to Category.
- Click Network and Internet.
- Click Network and Sharing Center.
- Select the local area network connection that is connected to the radio hardware and then select properties.
- If an unused network connection is available, the local area connection appears as an unidentified network.
- If you plan to reuse your network connection, select the local area connection that you plan to use for the radio hardware.
- If you have only one network connection, check if you can connect wirelessly to the existing local area network. If you can, you can use the network connection for the radio

hardware.

A pluggable USB is used as a Gigabit Ethernet LAN adapter instead of a NIC. All options except Internet Protocol Version 4 (TCP/IPv4) are to be cleared.

- Often it is observed that services like antiviral software can cause intermittent connection problems with the radio hardware.

Need of NIC:

- A NIC is competent enough to provide computers with a dedicated , full- time connection from the network.
- It works to implement the physical layer circuitry which is hailed as essential for communicating with a data link layer standard. \
- Each card represents a device and can prepare, transmit and control the flow of data on the network.

11: Load Balancer:

Load balancer is defined as the traffic cop, sitting in front of any server and routing client requests across all servers that are capable of fulfilling the former request. It is done in a way that maximizes speed and capacity utilization and ensures that no server happens to be overburdened.

Configuration:

- A load balancer is configured with a protocol and a port for front-end (client to load balancer) connections and also a protocol and a port for back-end (load balancer to instance) connections.

Need for A load balancer:

- Load balancers let you evenly distribute network traffic to prevent failure that can be caused by overloading a particular resource.
- The employed strategy improves the performance and also the availability of applications, databases and other varied computing resources.
- It also aids processing user requests quickly and accurately.

12. Firewalls

A firewall restricts the internet traffic of a private network, controlling what goes in and out. They analyze and restrict data packets based on programmed parameters, either white lists or blacklists. White lists only allow information that falls within a certain set of parameters, while blacklists deny all information that falls inside the parameters.

Firewalls are essential for private networks, especially those operating with sensitive information. They are also used within internal networks to block access between subgroups, such as a sales department being denied access to files pertaining to IT or HR.

Several types of firewalls exist, and which one is right for you depends on your operation. Some of the most common firewall types include:

- Packet filtering: Acts as a network layer checkpoint, analyzing data packets by IP address, packet type, port number or network protocols
- Stateful inspection: Analyzes data at network and transport layers, inspecting source IP, destination IP, source port and destination port
- Next-generation: Analyzes actual packet content and all TCP handshake checks, checking for malware, and detects advanced threats (see the section on IDS and IPS below)

Any type of firewall is helpful, but packet filtering is the most basic. A stateful inspection takes defenses to the next level. Next-generation firewall methods are the most thorough and secure, often used in highly regulated industries like finance and healthcare.

Network interface cards (NICs)
A network interface card is an internal hardware chip that connects a device to the internet. At the TCP/IP layer, the NIC connects a device to a network. At the physical layer, the NIC transmits a signal that sends information to the network layer. Then all data passes through the NIC to the server and back to the device.

There are two main types of NICs:

- An Ethernet NIC comes with an 8P8C socket for connecting an ethernet cable.
- A Wi-Fi NIC connects to a wireless network.

Mobile devices have only a wireless NIC, but most computers still incorporate an Ethernet chip. Ethernet ports are more reliable but limit a user's mobility while handling the device.

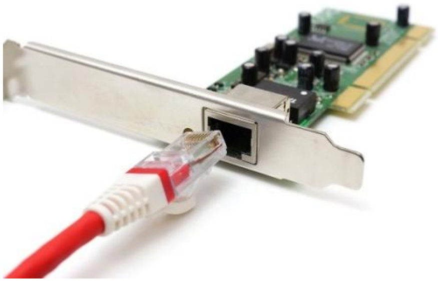
Wireless access points (WAPs)
A wireless access point consists of a transceiver (transmitter and receiver) device used to create a wireless LAN (WLAN). WAPs are separate network devices with a built-in antenna, transmitter and adapter. WAPs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired ethernet LAN. They also have several ports, allowing you to expand the network to support additional clients.

Depending on the size of the network, one or more WAPs might be required to provide full coverage. Additional WAPs allow access to more wireless clients and expand the wireless network range. The distance depends on the wireless standard, the obstructions and the environmental conditions between the client and the WAP. Higher-end WAPs have high-powered antennas, enabling them to extend how far the wireless signal can travel.

13. RJ45 Connector

RJ45 is the acronym for **Registered Jack 45. RJ45 connector** is an 8-pin jack used by devices to physically connect to **Ethernet** based **local area networks (LANs)**. **Ethernet** is a technology that defines protocols for establishing a LAN. The cable used for Ethernet LANs are twisted pair ones and have **RJ45 connector pins** at both ends. These pins go into the corresponding socket on devices and connect the device to the network.

14. Ethernet Card



Ethernet card, also known as **network interface card (NIC)**, is a hardware component used by computers to connect to **Ethernet LAN** and communicate with other devices on the LAN. The earliest **Ethernet cards** were external to the system and needed to be installed manually. In modern computer systems, it is an internal hardware component. The NIC has **RJ45 socket** where network cable is physically plugged in.

Ethernet card speeds may vary depending upon the protocols it supports. Old Ethernet cards had maximum speed of **10 Mbps**. However, modern cards support fast Ethernets up to a speed of **100 Mbps**. Some cards even have capacity of **1 Gbps**.

Internet

The Internet is a larger network that allows Computer Networks controlled by enterprises, governments, colleges, and other organizations all over the world to communicate with one another. As a result, there is a tangle of cables, computers, data centers, routers, servers, repeaters, satellites, and Wi-Fi towers that allow digital data to go around the world.

The Internet is a vast network of networks that functions as a networking infrastructure. It links millions of computers throughout the world, creating a network in which any computer can talk with any other computer as long as they are both linked to the Internet.

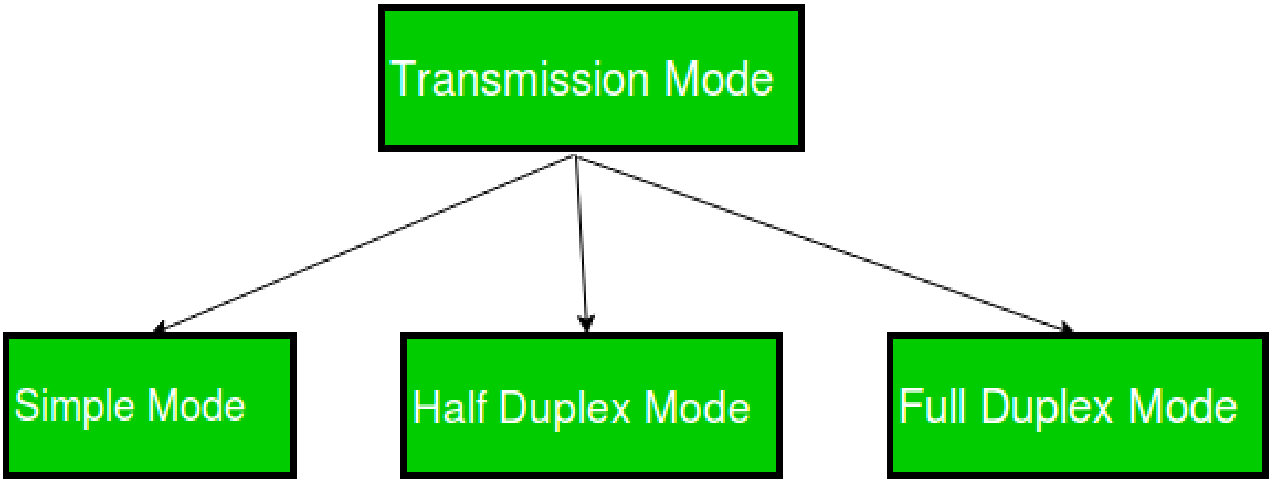
The Internet is a global network of interconnected computers that communicate and share information using a standardized Internet Protocol Suite.

Transmission Modes in Computer Networks

(Simplex, Half-Duplex and Full-Duplex)

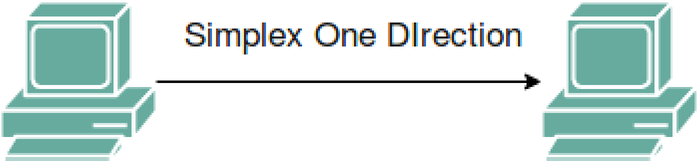
Transmission mode means transferring data between two devices. It is also known as a communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected.

There are three types of transmission mode:-



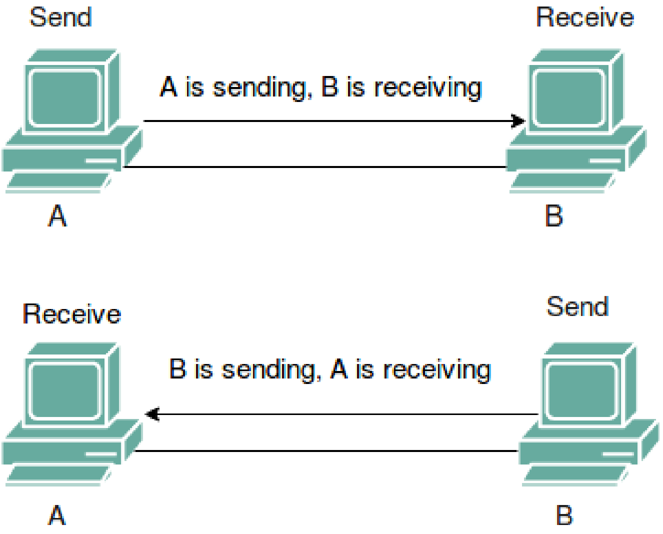
These are explained as following below.

1) **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:**
  - 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:**
  - 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.

2) **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

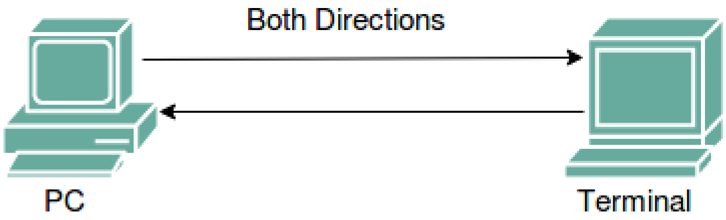


- **Advantages:**
  - Half-duplex mode allows for bidirectional communication, which is useful in situations where devices need to send and receive data.
  - It is a more efficient mode of communication than simplex mode, as the channel can be used for both transmission and reception.
  - Half-duplex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

3) **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:**
  - 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:**
  - 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.

Network Topology

In Computer Network, there are various ways through which different components are connected to one another. **Network Topology** is the way that defines the structure, and how these components are connected to each other.

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:

1) Point to Point Topology
2) Bus Topology
3) Ring Topology
4) Star Topology
5) Mesh Topology
6) Tree Topology
7) Hybrid Topology

Point-to-Point Topology

In a point-to-point topology, two nodes (computers, routers, hubs, etc.) form a computer network. Both connect to each other directly by LAN cables or any other physical medium.

Creating a computer network using this method is the simplest and most cost-effective method. The sender writes to one end, and the receiver receives from another end without requiring any intermediate routing decisions.

A dedicated channel connects the two hosts. Therefore, the entire capacity of the underline medium is reserved for communication. A major disadvantage of this network is that there can only be a maximum of two nodes.

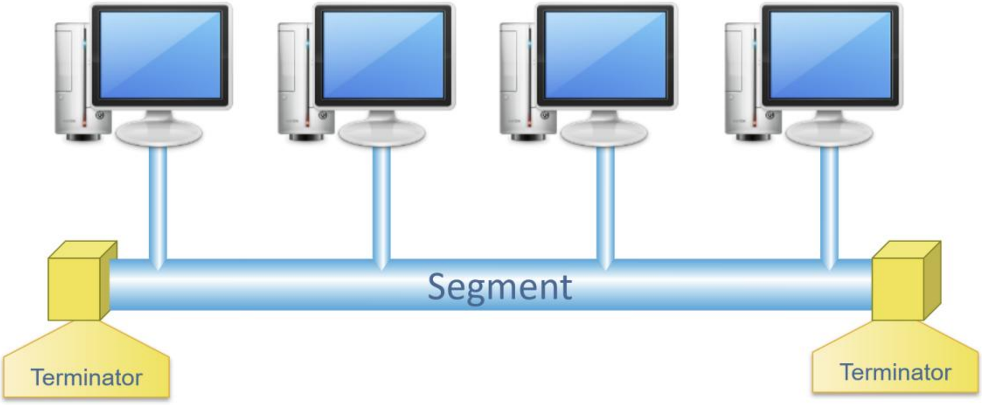
Example is the home's remote control for the air conditioner, which operates through a point-to-point connection.

- **Advantages of Point-to-Point Topology**
  - Very easy to maintain. You can replace a wire within a few seconds if the wire has a problem.
  - Maximum utilization of the underlying connecting link bandwidth.
  - This is the simplest topology compared to any other network topology type.
  - Least minor delays in communication as compared to any other network connection type.
  - Low-cost option when you have only two nodes to connect
- **Disadvantages of Point-to-Point Topology**
  - The network performance depends on a single link only. If the link is down, the entire network stops working.
  - Because of the need for a direct connection, topology cannot be expanded to a large area. E.g., if there is a multistory building, two computers may be far apart.

- There is only one server or client. If anyone fails, all will stop working. You cannot take advantage of the network cluster. Not suitable for any database servers.
- Only applicable when the two devices are in proximity to each other such as connecting a printer.

Bus Topology

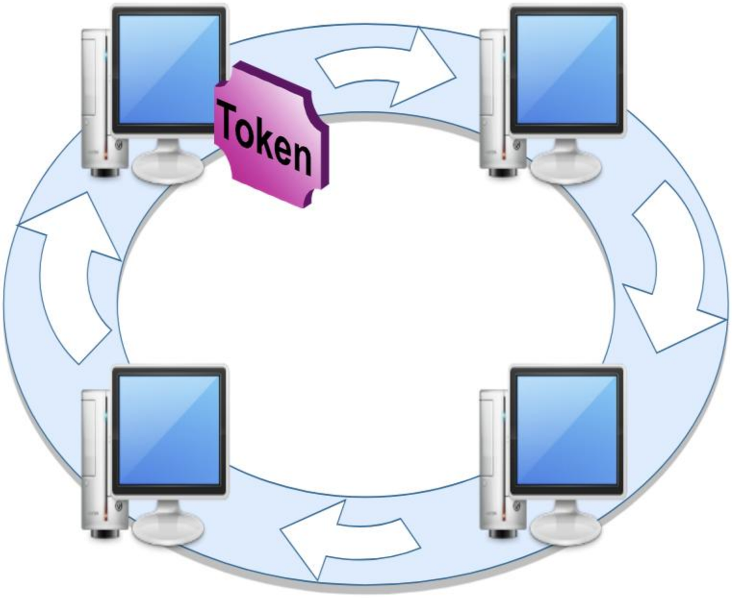
Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are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



- **Advantages of Bus Topology :**
  - It is the easiest network topology for connecting peripherals or computers in a linear fashion.
  - It works very efficiently well when there is a small network.
  - The length of cable required is less than a star topology.
  - It is easy to connect or remove devices in this network without affecting any other device.
  - Very cost-effective as compared to other network topology i.e. mesh and star
  - It is easy to understand topology.
  - Easy to expand by joining the two cables together.
- **Disadvantages of Bus Topology :**
  - Bus topology is not great for large networks.
  - Identification of problems becomes difficult if the whole network goes down.
  - Troubleshooting individual device issues is very hard.
  - Need terminators are required at both ends of the main cable.
  - Additional devices slow the network down.
  - If the main cable is damaged, the whole network fails or splits into two.
  - Packet loss is high.
  - This network topology is very slow as compared to other topologies.

Ring Topology

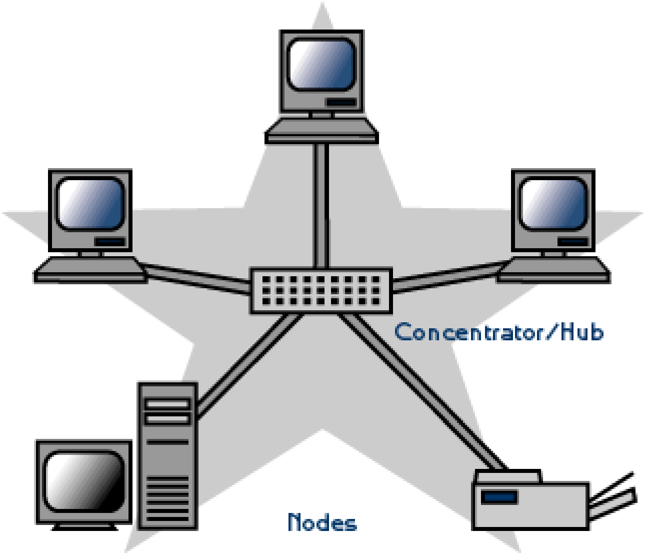
The topology is named ring topology because one computer is connected to another, with the final one being connected to the first. Exactly two neighbors for each device. A signal is passed along the ring in one direction. Each ring incorporates a repeater.



- **Advantages of Ring topology :**
  - In this data flows in one direction which reduces the chance of packet collisions.
  - In this topology additional workstations can be added after without impacting performance of the network.
  - Equal access to the resources.
  - There is no need of server to control the connectivity among the nodes in the topology.
  - It is cheap to install and expand.
  - Minimum collision.
  - Speed to transfer the data is very high in this type of topology.
  - Due to the presence of token passing the performance of ring topology becomes better than bus topology under heavy traffic.
  - Easy to manage.
  - Ring network is extremely orderly organized where every device has access to the token and therefore the opportunity to transmit.
- **Disadvantages of Ring topology :**
  - Due to the Uni-directional Ring, a data packet (token) must have to pass through all the nodes.
  - If one workstation shuts down, it affects whole network or if a node goes down entire network goes down.
  - It is slower in performance as compared to the bus topology
  - It is Expensive.
  - Addition and removal of any node during a network is difficult and may cause issue in network activity.
  - Difficult to troubleshoot the ring.
  - In order for all the computer to communicate with each other, all computer must be turned on.
  - Total dependence in on one cable.
  - They were not Scalable.

Star Topology

Each device in a star topology has a dedicated point-to-point link to a central controller, which is commonly referred to as the HUB. There is no direct connection between the devices. Traffic between the devices is not allowed in this topology. As an exchange, the controller is used.

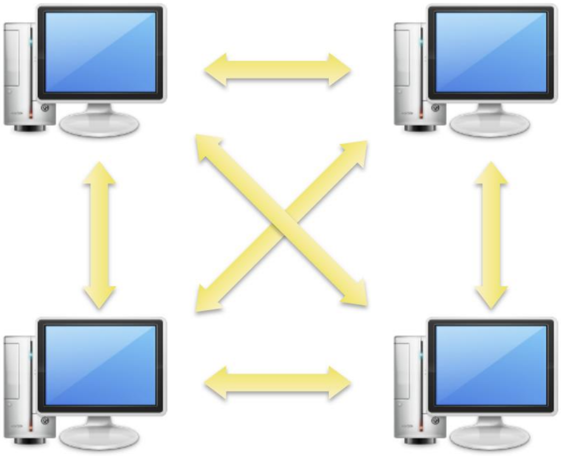


- **Advantages of Star Topology**
  - It is very reliable – if one cable or device fails then all the others will still work
  - It is high-performing as no data collisions can occur
  - Less expensive because each device only need one I/O port and wishes to be connected with hub with one link.
  - Easier to put in
  - Robust in nature
  - Easy fault detection because the link are often easily identified.
  - No disruptions to the network when connecting or removing devices.
  - Each device requires just one port i.e. to attach to the hub.
  - If N devices are connected to every other in star, then the amount of cables required to attach them is N. So, it's easy to line up.
- **Disadvantages of Star Topology**
  - Requires more cable than a linear bus .
  - If the connecting network device (network switch) fails, nodes attached are disabled and can't participate in network communication.
  - More expensive than linear bus topology due to the value of the connecting devices (network switches)
  - If hub goes down everything goes down, none of the devices can work without hub.
  - Hub requires more resources and regular maintenance because it's the central system of star .
  - Extra hardware is required (hubs or switches) which adds to cost
  - Performance is predicated on the one concentrator i.e. hub.

Example: Used in high-speed LANs

Mesh Topology

Every device in a mesh topology has dedicated point-to-point connectivity to every other device. The term “dedicated” refers to the fact that the link exclusively transports data between the two devices it links. To connect n devices, a fully connected mesh network contains n *(n-1)/2 physical channels.



There are two types of Mesh topologies –

a) Fully-connected Mesh Topology
b) Partially-connected Mesh Topology

a) **Full Mesh Topology:** All the nodes within the network are connected with every other If there are n number of nodes during a network, each node will have an n-1 number of connections. A full mesh provides an excellent deal of redundancy, but because it is prohibitively expensive to implement, it’s usually reserved for network backbones.
Total number of links required for the mesh topology is [n(n-1)]/2.

b) **Partial Mesh Topology:** The partial mesh is more practical as compared to the full mesh. In a partially connected mesh, all the nodes aren’t necessary to be connected with one another during a network. Peripheral networks are connected using partial mesh and work with a full-mesh backbone in tandem.

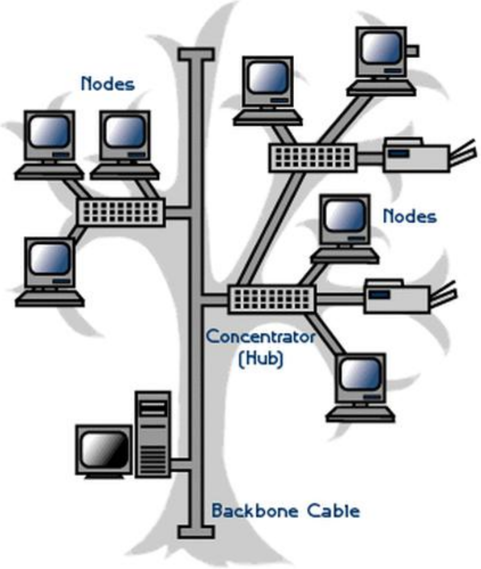
- **Advantages of Mesh Topology :**
  - Failure during a single device won’t break the network.
  - There is no traffic problem as there is a dedicated point to point links for every computer.
  - Fault identification is straightforward.
  - This topology provides multiple paths to succeed in the destination and tons of redundancy.
  - It provides high privacy and security.
  - Data transmission is more consistent because failure doesn’t disrupt its processes.
  - Adding new devices won’t disrupt data transmissions.
  - This topology has robust features to beat any situation.
  - A mesh doesn’t have a centralized authority.
- **Disadvantages of Mesh Topology :**
  - It’s costly as compared to the opposite network topologies i.e. star, bus, point to point topology.

- Installation is extremely difficult in the mesh.
- Power requirement is higher as all the nodes will need to remain active all the time and share the load.
- Complex process.
- The cost to implement mesh is above other selections.
- There is a high risk of redundant connections.
- Each node requires a further utility cost to think about.
- Maintenance needs are challenging with a mesh.

Example: connection of telephone regional office in which each regional office needs to be connected to every other regional office.

Tree Topology

The topology of a tree is similar to that of a star. Nodes in a tree, like those in a star, are connected to a central hub that manages network traffic. It has a root node, which is connected to all other nodes, producing a hierarchy. Hierarchical topology is another name for it. The number of Star networks is connected via Bus in Tree Topology.



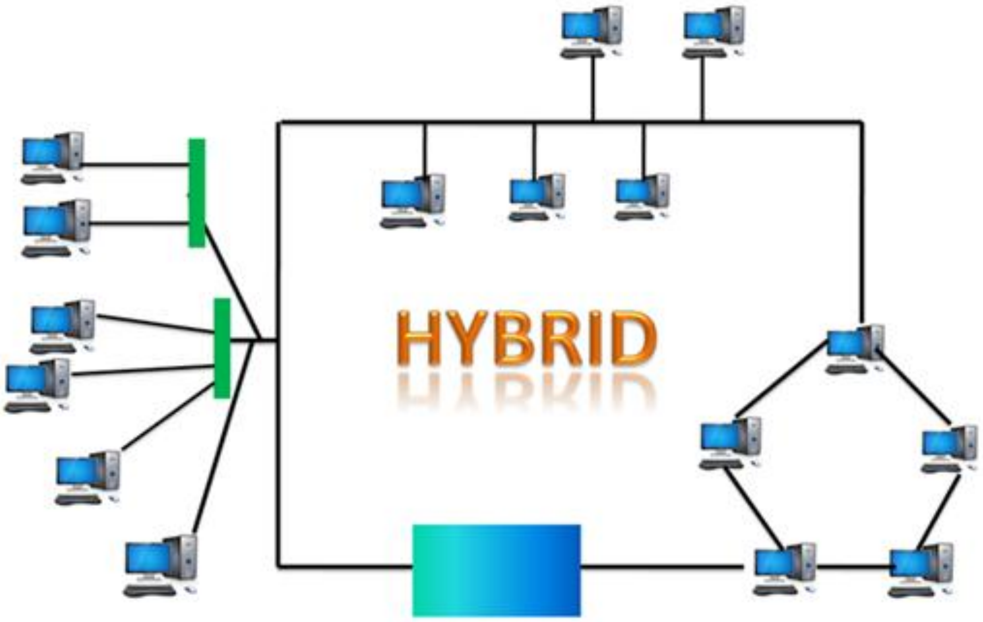
- **Advantages of Tree Topology** :
  - This topology is the combination of bus and star topology.
  - This topology provides a hierarchical as well as central data arrangement of the nodes.
  - As the leaf nodes can add one or more nodes in the hierarchical chain, this topology provides high scalability.
  - The other nodes in a network are not affected if one of their nodes gets damaged or does not work.
  - Tree topology provides easy maintenance and easy fault identification can be done.
  - A callable topology. Leaf nodes can hold more nodes.
  - Supported by several hardware and software vendors.
  - Point-to-point wiring for individual segments.
  - Tree Topology is highly secure.
  - It is used in WAN.
  - Tree Topology is reliable.
- **Disadvantages of Tree Topology** :

- This network is very difficult to configure as compared to the other network topologies.
- The length of a segment is limited & the limit of the segment depends on the type of cabling used.
- Due to the presence of a large number of nodes, the network performance of tree topology becomes a bit slow.
- If the computer on the first level is erroneous, the next-level computer will also go under problems.
- Requires a large number of cables compared to star and ring topology.
- As the data needs to travel from the central cable this creates dense network traffic.
- The Backbone appears as the failure point of the entire segment of the network.
- Treatment of the topology is pretty complex.
- The establishment cost increases as well.
- If the bulk of nodes is added to this network, then the maintenance will become complicated.

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.

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.



- **Advantages of Hybrid Topology**
  - This type of topology combines the benefits of different types of topologies in one topology.
  - Can be modified as per requirement.
  - It is extremely flexible.
  - It is very reliable.
  - It is easily scalable as Hybrid networks are built in a fashion which enables easy integration of new hardware components.
  - Error detecting and troubleshooting are easy.
  - Handles a large volume of traffic.
  - It is used to create large networks.
  - The speed of the topology becomes fast when two topologies are put together.
- **Disadvantages of Hybrid Topology**
  - It is a type of network expensive.
  - The design of a hybrid network is very complex.
  - There is a change in the hardware to connect one topology with another topology.
  - Usually, hybrid architectures are larger in scale so they require a lot of cables in the installation process.
  - Hubs which are used to connect two distinct networks are very costly. And hubs are different from usual hubs as they need to be intelligent enough to work with different architectures.
  - Installation is a difficult process.
- **Uses of Hybrid Topology**
  - Hybrid Topology helps in keeping the full diversity of the computer network.
  - Hybrid Topology is helpful when we require more than one topology in the system.
  - Hybrid Topology helps in reducing the cost of the overall system.
  - Hybrid Topology helps in easily running the system.
  - Hybrid Topology is widely used in educational institutes, research organizations, finance sectors, etc.

Physical Layering

Protocol Layering

A **protocol** is a set of rules and standards that primarily outline a language that devices will use to communicate. There are an excellent range of protocols in use extensively in networking, and that they are usually implemented in numerous layers.

It provides a communication service where the process is used to exchange the messages. When the communication is simple, we can use only one simple protocol.

When the communication is complex, we must divide the task between different layers, so, we need to follow a protocol at each layer, this technique we used to call protocol layering. This layering allows us to separate the services from the implementation.

Each layer needs to receive a set of services from the lower layer and to give the services to the upper layer. The modification done in any one layer will not affect the other layers.

Basic Elements of Layered Architecture

The basic elements of the layered architecture are as follows −

- **Service** − Set of actions or services provided from one layer to the higher layer.
- **Protocol** − It defines a set of rules where a layer uses to exchange the information with its peer entity. It is concerned about both the contents and order of the messages used.
- **Interface** − It is a way through that the message is transferred from one layer to another layer.

Reasons

The reasons for using layered protocols are explained below −

- Layering of protocols provides well-defined interfaces between the layers, so that a change in one layer does not affect an adjacent layer.
- The protocols of a network are extremely complicated and designing them in layers makes their implementation more feasible.

Advantages

The advantages of layered protocols are as follows −

- Assists in protocol style, as a result of protocols that operate at a particular layer have outlined information that they work and a defined interface to the layers on top of and below.
- Foster's competition because products from completely different vendors will work along.
- Prevents technology or capability changes in one layer from touching different layers above and below.
- Provides a typical language to explain networking functions and capabilities.

Disadvantages

The disadvantages of layered protocols are as follows −

- The main disadvantages of layered systems consist primarily of overhead each in computation and in message headers caused by the abstraction barriers between layers. Because a message typically should pass through several (10 or more) protocol layers the overhead of those boundaries is commonly more than the computation being done.

- The upper-level layers cannot see what is within the lower layers, implying that an application cannot correct where in an exceedingly connection a problem is or precisely what the matter is.
- The higher-level layers cannot control all aspects of the lower layers, so that they cannot modify the transfer system if helpful (like controlling windowing, header compression, CRC/parity checking, et cetera), nor specify routing, and should rely on the lower protocols operating, and cannot specify alternatives when there are issues.

TCP/IP Protocol Suit

The TCP/IP suite is a set of protocols used on computer networks today (most notably on the Internet). It provides an end-to-end connectivity by specifying how data should be packetized, addressed, transmitted, routed and received on a TCP/IP network. This functionality is organized into four abstraction layers and each protocol in the suite resides in a particular layer.

The TCP/IP suite is named after its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP). Some of the protocols included in the TCP/IP suite are:

- **ARP (Address Resolution Protocol)** – used to associate an IP address with a MAC address.
- **IP (Internet Protocol)** – used to deliver packets from the source host to the destination host based on the IP addresses.
- **ICMP (Internet Control Message Protocol)** – used to detects and reports network error conditions. Used in ping.
- **TCP (Transmission Control Protocol)** – a connection-oriented protocol that enables reliable data transfer between two computers.
- **UDP (User Datagram Protocol)** – a connectionless protocol for data transfer. Since a session is not created before the data transfer, there is no guarantee of data delivery.
- **FTP (File Transfer Protocol)** – used for file transfers from one host to another.
- **Telnet (Telecommunications Network)** – used to connect and issue commands on a remote computer.
- **DNS (Domain Name System)** – used for host names to the IP address resolution.
- **HTTP (Hypertext Transfer Protocol)** – used to transfer files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

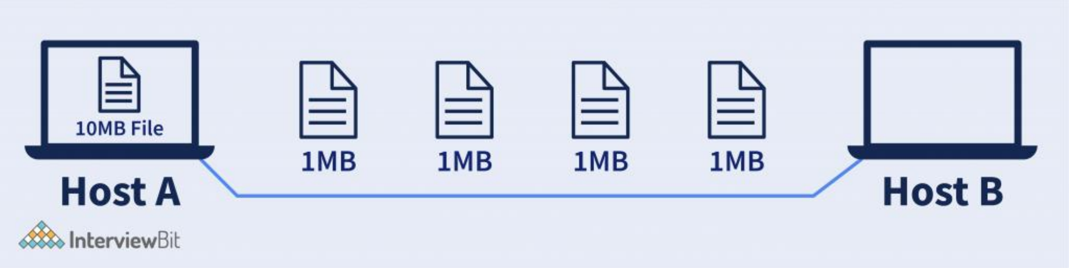
Introduction TCP/IP

TCP (Transmission Control Protocol), IP (Internet Protocol) is the collection of protocols that allows the computers to connect with the network and exchange data with other computers over the Network.The TCP/IP model is the foundation of the Internet that was introduced by the U.S. Department of Defence (DoD). At that time Internet was not so popular. After this, Internet slowly became popular.

TCP/IP protocols are based and implemented on the reference of the OSI Model (Open System Interconnection). OSI Model is the theoretical model that defines some set of protocols that need to be followed by every network for the successful transmission of data over the network. Most networking systems that we encounter today follow the TCP/IP model. TCP/IP Model much simplified practical model that is practically used in the real world.

Why TCP/IP

TCP/IP Model is a more optimized and practically implemented model. It has taken the reference from the OSI Model and put a lot of emphasis on accuracy. It includes several steps that ensure the data sent from one host to another host must reach on without any failures, or in the case, failure or loss of data happens then It doesn't need to retransmit the whole data. Instead, it only sends the incorrect data or the data And to achieve this, there are a lot of excellently designed algorithms that run behind to make this possible.

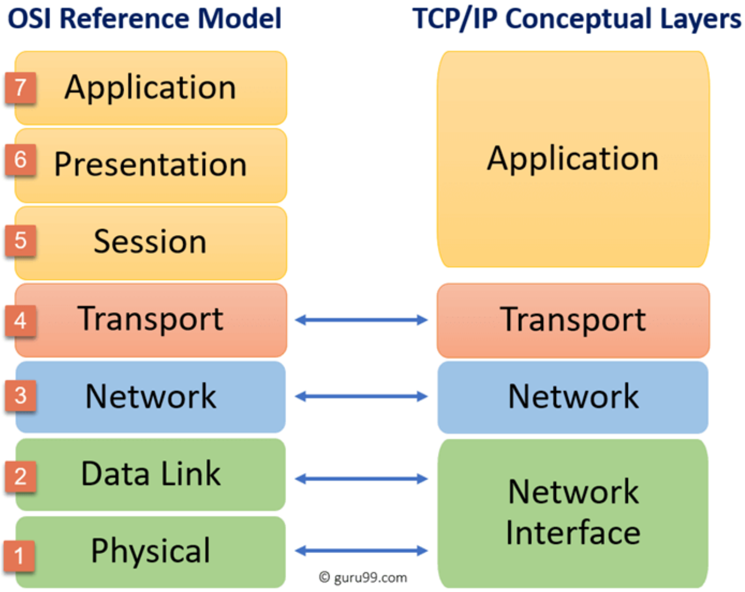


Explanation – Suppose, there are two hosts (computers) Host A and B. And Host A wants to send 10MB of data to Host B. For this, According to TCP/IP Model Protocols, the data is divided into small pieces and then it will be sent.

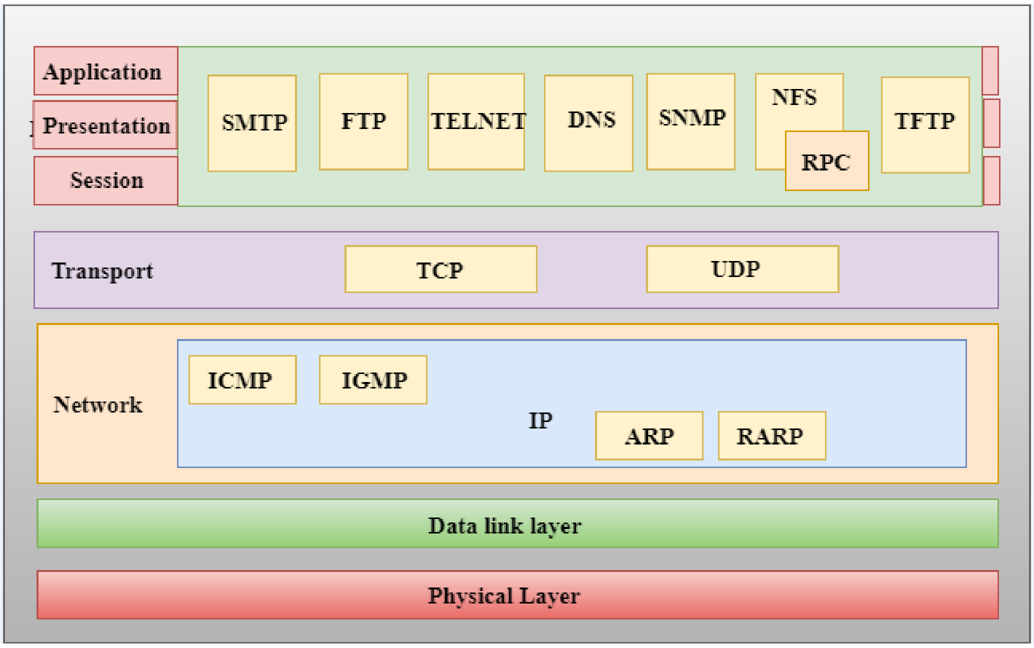
Layers in TCP/IP Model –

TCP/IP Model is a practically implemented version of the OSI Model. Although layers are different in TCP/IP Model in comparison with the OSI Model. The layers are grouped according to the task performed by each layer. It has commonly 4 layers. But somewhere it has been considered as 5 Layers. So the common 4 layers of the TCP/IP Model is –

1) Application Layer
2) Transport Layer
3) Network Layer
4) Network Interface Layer



Functions of TCP/IP layers:



- In the OSI Model, we have the first four layers that have the responsibility of the Host. And the rest 3 layers have the responsibility of the Network.

  Similarly in TCP/IP Model we have the first half is the responsibility of the Host and another half is the responsibility of the Network.
- There is the logical combination of the first 3 layers of the OSI Model (Application, Presentation, and Session Layer) into the single layer in the TCP/IP Model called the **Application Layer**. It has combined because all the first three layers of the OSI Model have been performed by each application itself.

  Example – Browser does all the 3 work done by the Application, Presentation, and Session Layer. So why there can be a separate layer for each? So TCP/IP Model defines that the task related to individual applications are being performed in the application layer.
- In the OSI Model, we have the first four layers that have the responsibility of the Host. And the rest 3 layers have the responsibility of the Network.
- Similarly in TCP/IP Model we have the first half is the responsibility of the Host and another half is the responsibility of the Network.
- There is the logical combination of the first 3 layers of the OSI Model (Application, Presentation, and Session Layer) into the single layer in the TCP/IP Model called the Application Layer. It has combined because all the first three layers of the OSI Model have been performed by each application itself.
- Example – Browser does all the 3 work done by the Application, Presentation, and Session Layer. So why there can be a separate layer for each? So TCP/IP Model defines that the task related to individual applications are being performed in the application layer.
- Similarly, the last 2 Layer of the OSI model (Data-Link layer and the Physical Layer) is also logically combined into the single layer called Network-Interface Layer. This combined is also because these two layers deal with the mediums (wireless or wired). So logically this is combined into a single layer.

TCP/IP Model with 5 Layers

The last two layers of the OSI Model (Data-Link and Physical Layer) deals with the network medium. Which Data-Link Layer task is to convert the packets into Bits of Frames and other Physical layer Deals with BitStream Signals to the medium. So in TCP/IP Model with 5 layers have separated these 2. So TCP/IP Model with 5 layers are –

1) Application Layer
2) Transport layer
3) Network Layer
4) Data-link Layer
5) Physical Layer

1) Application Layer

This layer deals with the application part. Applications that require communication with the network, then the protocols defined in the application layer will be followed by the applications for transmission of data. There are a bunch of protocols that are followed by individual applications that need to transmit the data to the network or fetch data from the network.

At the front of the Applications, the data originated will be processed by the application layer. So some of the applications that interact with the internet follow protocols, like –

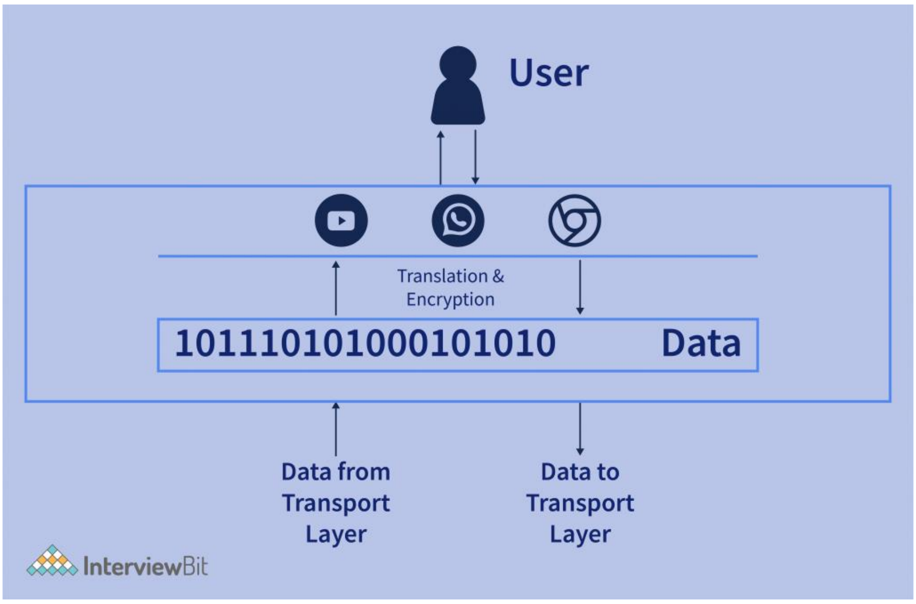
- Browser —- HTTP / HTTPS, FTP, DNS
- Outlook —- SMTP
- WhatsApp —- Customized (XMPP).
- Remote Desktop —- Telnet, RDP.

- **HTTP/HTTPS – (Hypertext Transfer Protocol).**
  - This is the most popular protocol used by webpage and whole (www) itself. Every time we browse for the webpage, this is the protocol that is used in the background to bring the web page from the server to our client machine. HTTP uses Port Number 80 to communicate between all clients and servers and HTTPS uses TCP port 443. There can be many applications that are using the network to send packets. So Port Number is the 16-bit number that is used by the application for the identification of packets that belongs to which application.
  - **Example–** Port 80 is used by the Browser so it will be identified that the packet with Port Number 80 must be sent to the browser.
  - HTTPS is the HTTP protocol with a secured connection. This is mostly used for transmitting secured files over the network. Like – Passwords, Financial details, etc. HTTPS has an SSL (Secure Socket Layer) Certificate, that states it is a secured connection.
- **DNS – (Domain Name Server)**
  - It is a TCP/IP Protocol that helps to get the IP Address of the particular domain. There are DNS servers that give the IP Address of the domain name. Mostly the ISP have their internal DNS server. DNS packets rely on Port Number 53.
  - Example – Domain Name – https://www.interviewbit.com/ requested then DNS Server will revert with IP Address – 13.227.166.23

- **FTP – (File Transfer Protocol)**
    - It is also a standard TCP/IP protocol, that is used to transmit a file from one host to another host in the network. It first establishes a connection to the host and after a successful connection, it is ready to transfer files. It uses two different ports, Port 21 for Command and Port 20 for Data transfer.
- **SMTP – (Simple Mail Transfer Protocol)**
    - It is used to send and receive emails over the internet. It has a mail server, mail exchanger, and mail delivery agent that helps to deliver mail to the user. Ports 25, 465, 587, or 2525 for SMTP have all been considered standard SMTP ports at some point, but only 587 or 2525 really should be considered for modern use.

Other than some of these basic protocols, the Application layer also does some the operations like –

- **Translation** – It translates the data received from the application layer into the form of ASCII (American Standard Code for Information Interchange) Codes, or UNICODE to the Binary Format.
    - Example – Data – Hello. So ASCII Code associated with it is 72 101 108 108 111. And the next to the Binary Code will be – 01001000 01100101 01101100 01101100 01101111.
    - So this is the first thing that the presentation layer will do post receiving data from the application layer.
- **Data Compression** – In this what exactly happens is, Suppose after translation we get 1MB of Data. So Data Compression tries to reduce the size of the data without much loss of data because the less the size is the faster transmission can happen over the network.
    - Example – Suppose we have an image of size 1MB, Now Data Compression tries to reduce this file size to less than 1MB.
    - So this is also done by the Presentation Layer for better communication.
- **Encryption** – The objective of encryption is to encrypt the data so that the data can't be understood by the hackers that might see the data and misuse it. Like HTTPS uses SSL (Secure Socket Layer) protocol to encrypt the data. Secure Sockets Layer is a cryptographic protocol designed to provide communications security over a computer network.
- **Establish, Manage and Terminate connections** – Establishment of Connection means making a connection in which both server and client have agreed to transfer the data.
    - Managing Connection means getting knowledge of the connections that were established and the data transfer can be done effectively.
    - In Terminating connection, after the data transfer completes then the connection must be terminated.
- **Authorization and Authentication** – Authorization states validation of user id and password. Authorization states after the authentication, whether the user has permission to access the particular file or not.



- In the above figure, the data that came from the end-user application is being converted to binary data for the next layer for further processing. And on another side, the data that came from the presentation layer is converted into user-readable application data.

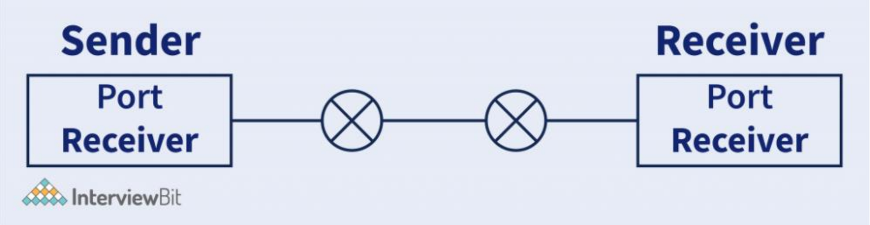
2) Transport layer

The transport layer enables communication between two processes. It ensures that the data to be sent to the destination must de be delivered to the same process that it has been

The transport layer enables communication between two processes. It ensures that the data to be sent to the destination must de be delivered to the same process that it has been meant for.

Processes are nothing but the application that is requesting or sending data. Each process communicates with the port number that helps the transport layer to identify the correct process meant for the data.

In transport Layer, It has majorly two protocols. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

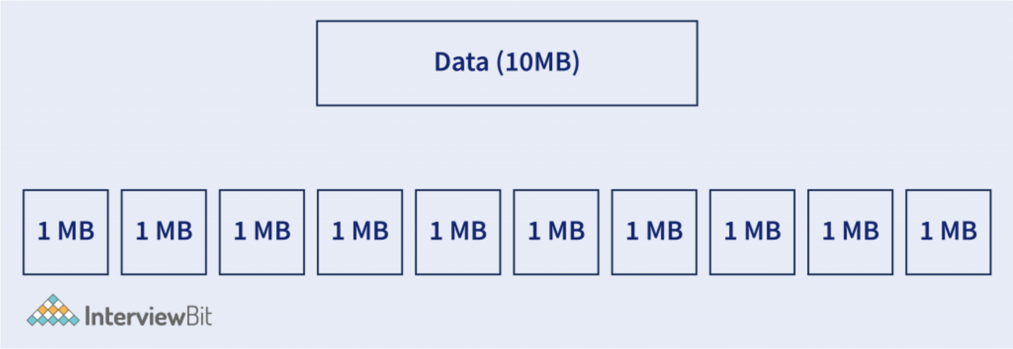


Explanation – In the image, we can see that Post Sender belongs to a process that is occupied by the Application in the sender system to send the data, And on the other side Port receiver belongs to the Application process. So transport layer ensures that the data must deliver to the correct application.

Transport Layer performs the following operation on the bits of data received from the Application layer. And those are –

a) **Segmentation** – Segments are the small groups of data that are divided from the large data. Suppose we have 10 MB of data then the whole 10MB data is divided into segments supposing 1MB each.

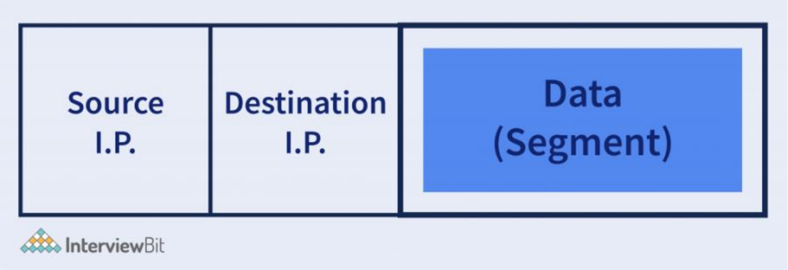
Here Data Can be considered as the sequence of bytes that is received from the above layer.



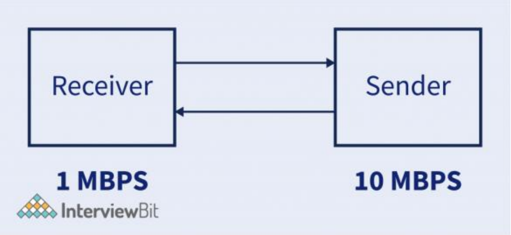
These segments are sent to the lower level for further process.

Why Segmentation? – The big question arrives is why the data is divided into segments? Why can't the whole lot is being sent on a go?

- It is because the packet size of (TCP or UDP) has some limitations with the size of packet defined by IEEE.
- Segmentation does that if the data is divided into pieces, then it is more manageable.
- Each segment must be given a number because, in transportation, It may not the situation that the segment arrives in the same sequence.
- On the other end in Transport Layer, If a segment has a number then it will be easy to send the data over the medium.
- Each Segment contains the port number that needs to identify the hat software did access this data that is sent to the network.
- A general segment looks like –

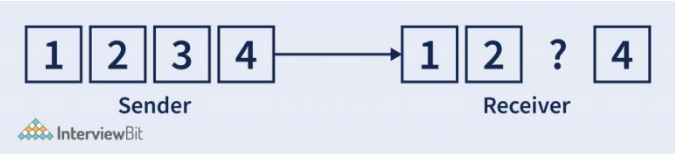


b) Flow Control – Flow control means managing the flow of data that is transmitted between one host to another host.



- Supposed Sender is sending data to Reciever **@10MBPS Transfer Rate**. But Reciever can't able to process the data **@10MBPS**. It can only process data @1MBPS.
- So receiver will ask the server for a 1MBPS Transfer rate, As it can't process the data. Then sender sends the data **@1MBPS** Rate.
- So this is called **Flow Control**.

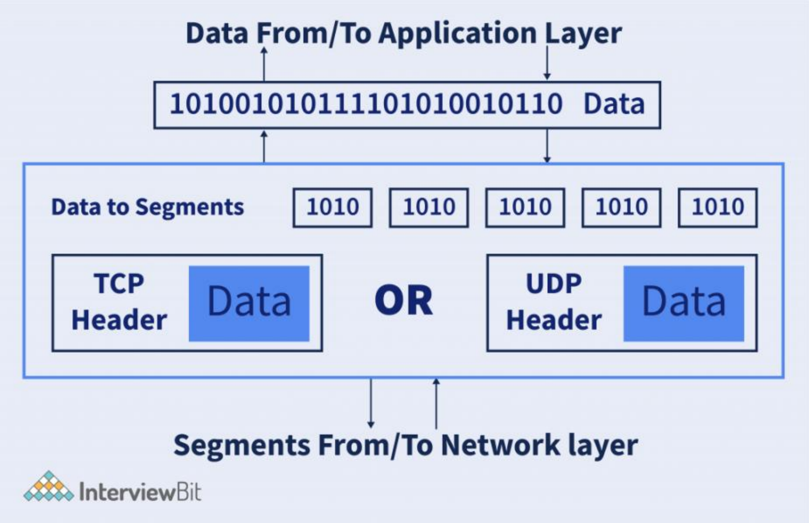
c) **Error Control** – It controls the error of data. This means in case there is any inconsistency happened on the data then it helps to correct that data.



- Suppose Sender is sending some data considering 4 segments. Now in case, the 3rd segment got lost in the medium. So Error control helps to fix that.
- It has some algorithms that help to fix this data. Like Automatic Repeat Request. In which the segment which hasn't receiver to the receiver. Then it will ask to resend it.
- Data loss can happen in the physical network, So errors are recognized controlled by the transport layer.

We have encountered a word called TCP and UDP. These are the protocols that describe the type of packets that are generated by the transport layer for each segment it has been divided.

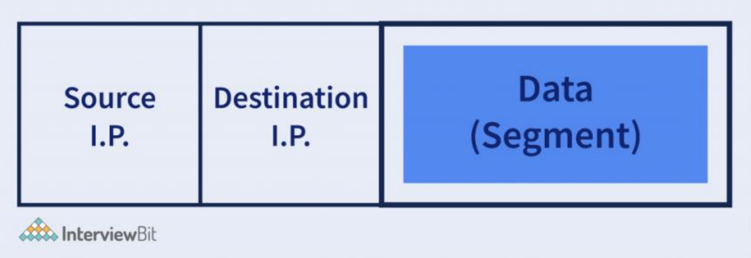
TCP	UDP
Transmission Control Protocol (TCP) is one of the main protocols of the Internet Protocol Suite. It is mostly used for webpage transmission.	User Datagram Protocol (UDP) is also one of the most used protocols on the Internet. UDP protocols are used in many where connection orientation is not the main priority and want faster data transmission. And some loss of data is acceptable.
The most essential feature of TCP is – 1. It is a connection-oriented protocol. 2. It provides feedback once the packet is successfully received on the other end and that makes TCP a slower protocol. 3. There can be no loss of data can happen in TCP.	The most essential feature of UDP is – 1. It is a connection-less protocol. 2. It transmits the data faster, but there can be a loss of data. 3. No Feedback mechanism is used in this.


Data From/To Application Layer
101001010111101010010110 Data
Data to Segments
1010
1010
1010
1010
1010
TCP Header
Data
OR
UDP Header
Data
Segments From/To Network layer
InterviewBit

The above figure describes a very high-level overview of what happens in the Transport Layer. The Header need not be each time TCP or UDP. It can be more like ICMP (Internet Control Message Protocol), DNS (Domain Name System), ARP (Address Resolution Protocol), etc. depending on the type of data or request.

3) Network Layer

Whatever data comes from the above layers in the form of segments that data are encapsulated with the Source and Destination I.P. Address that we call as packet, and these packets are sent to the network it belongs to.



IP Address helps to identify the network to which the packet has to be sent. There is a very famous protocol used in the Network layer, called IP (Internet Protocol). IP has two different versions that have been widely used nowadays.

a) IPv4 (Internet Protocol version 4).

b) IPv4 (Internet Protocol version 6).

IP Address -? It is the address that the network system has uniquely identified. It is the 32-bit or 4-byte address (in IPv4) and each byte has an address range of 0-255, called an octet. And in (IPv6) it is 128bit long with 16 octets in it.

In the real world, there are billions of devices are connected to the internet. And these devices are spread all across the globe. So the device is difficult so the IP Address provides that it groups the devices into a particular network with the unique IP Address, which helps to identify where the device is to whom the communication to happen.

IPv4 – It is the internet protocol version 4 address assigned to the device that connects to the network for identification. It is 32-bit long which means the number of devices it can connect is up to – $\mathbf{2^{32}-2}$.

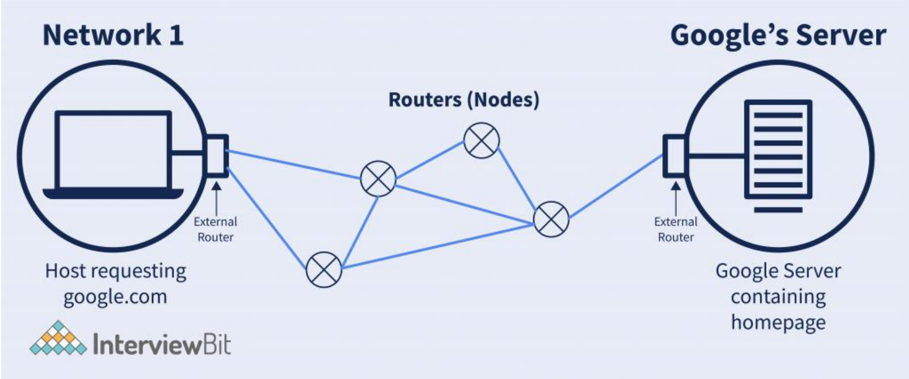
It has a header of 20 Octets (Bytes) in which the data from the transport layer is encapsulated. And this header helps to identify the packet and which network it belongs to.

IPv6 – It is the Internet Protocol version 6 address assigned to the device that connects to the network for identification. It is 128-bit long. So the number of devices it can connect to is $\mathbf{2^{128} – 2}$.

It also has a header of 40 Octets (Bytes) that contains that helps to identify the packet and the network it belongs to.

Modern Routers works on this network layer as the packets need to be routed from the source to the destination.

Routing - Routing means setting the path of the packet to reach from the sender to the receiver.

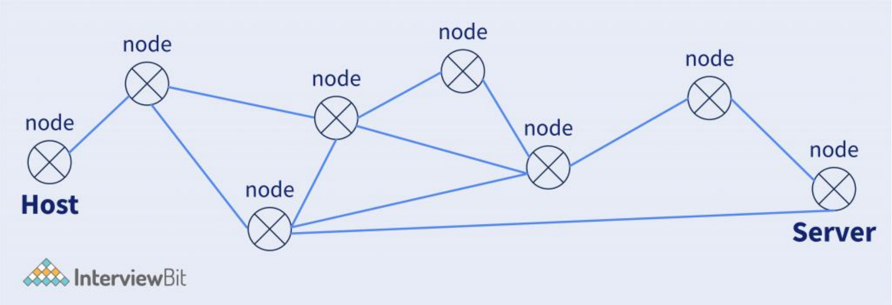


Explanation – Suppose we visit the website google. Then google's network has theirs in US California. So what will happen here is, the packet sent from the host to the google server will have to follow some path. Because there might be no direct connection from the host to google's server. And between paths, there can be many routers present. So setting, what will be the next router through which the packet needs to be transmitted, and the connection between these is called Routing. And the router handles these things.

There is an external router associated with the network that deals with sending the packet from the host network to the destination network using the next node. When a router gets the destination IP address then performs something called masking. **Masking** is a simple bitwise operation. The router sets some bits to 0 and performs a bitwise AND operation, and after masking on the destination IP address, it will get the network IP Address. Now with the help of the network IP address, it will decide the next router for the packet it has to send.

Network layer encapsulate the packet with the IP Address -There is something called DNS. Domain Name System, that provides the IP address corresponding to the domain name it has been requested for.

Path Determination – What it means is actually what, there could be multiple ways from which I can send one packet to the destination. The objective of path determination is to determine the best path so that I can send this packet very very efficiently in less time.



So here in the above figure, we have multiple nodes from the host to the server. So routers help to determine the path that needs to be followed so the packet reaches the destination efficiently.

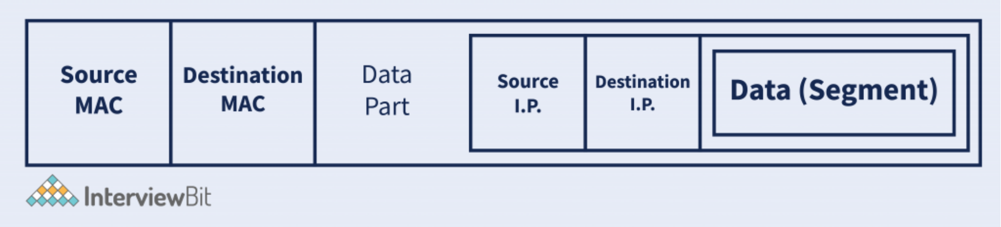
So routers use algorithms used in graph theory, like minimum spanning tree, shortest path, etc.

4) Data Link Layer

The packet is sent from the Network layer, And on that packet the headers are added along with the MAC Address of Source and Destination.

- **MAC Address** – (Media Access Control) also called physical address, is the 48-bit or 6-Bytes long containing the Hexadecimal code. It is the address assigned uniquely to each of the network devices. NIC(Network Interface Card) WiFi Card, USB WiFi Dongle, etc.

After encapsulating the packet from the network layer with the Source and Destination MAC Adress. Data-Link Layer generates a **Frame**. And that frame is sent to the next layer for data to send to the destination. A general frame looks like –



Why MAC Address? MAC address helps to uniquely identify the device. Suppose in the network, the packet is received, then which particular device belongs to. So the MAC address helps to identify this.

We have seen in the network layer that IP Address is used to uniquely identify the device and MAC Address also performs the same. **So why not only use either MAC Address or IP Address?**

MAC Address is uniquely assigned to every single device that is connected with the network. And there are even billions of devices on the internet actress the globe. So if any host wants to send the data from one location to another, then without knowing the location, how it can reach. So IP Address behaves the same, IP address is the logical address that defines a particular location of network it belongs to. And after breaching the location of the network the MAC Address helps to identify the device. And that is what happens in the Data-Link layer, which defines the end device that the packet belongs to.

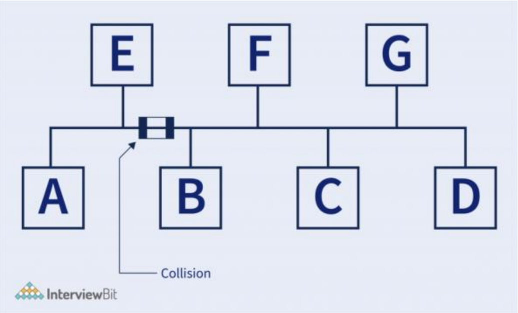
Example – 1 Letter needs to be sent From INDIA to the US. So The destination Address contains – **Country Name -> State -> City Name -> Pin Code -> Street -> Home Address**.

Here it is forming a hierarchy, That is exactly what IP Address helps to recognize the destination. (Up to the Street). And after reaching the street the Home Address is identified. And that MAC Adress helps to do.

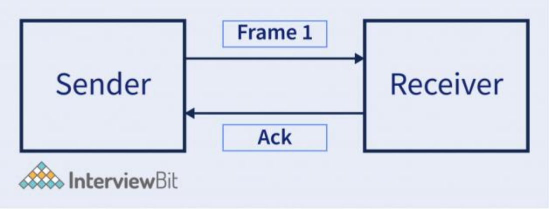
On the other hand, Data-Link Layer also has some broadcast –

- **Access to Media** – Media are like – (Copper Wire, Fiber Optical Cable, Wireless), etc. So the data link layer has access to these media on which medium the packet needs to transfer. Access to the media can help to detect congestion, Error, Collision, etc.
- **Media Access Control** – Data Link Layer has control over the data, which means when to transmit the data, Is there any error while transmitting? Is Data received is error-free? etc.
  - Example – Suppose there are several hosts connected in the same medium, Consider in (BUS TOPOLOGY).

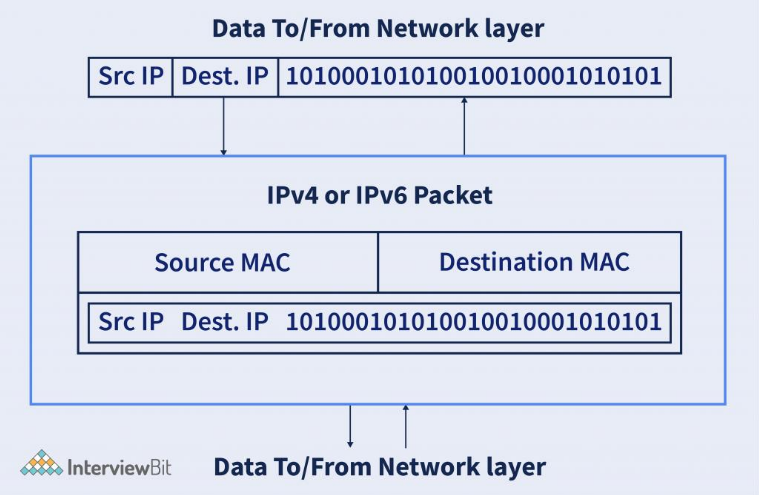
- In the below figure, Host B is sending data to Host A, and at the same time, Host E is also sending some data to Host C. So there is a collision. In the end, it is the electrical pulses that travel on the medium, and that will collide the whole data.
- So Data Link-Layer has access to the medium and there are a bunch of algorithms used for detecting avoiding the collision. Like CDMA, TDMA, CSMA – CD, etc.



- **Error Detection and Correction –** It is the mechanism to detect any error on the data. This means checking whether the data is correctly received or not.
  - Some algorithms help to check that. Like – **CRC (Cyclic redundancy check), Checksum, Bit Parity, etc.**
  - And these works like a function on which input is given and it returns some bits that are piggybacked with data and on the destination, that bit helps to detect the error.
- **Optional –** It also has some other operations like Flow Control & Acknowledgement. **Acknowledgment –** It means informing the sender that the frame it has sent is successfully received by the receiver.



- **Flow Control –** It is a set of procedures that explain to the sender how much data or frames it can transfer or transmit before data overwhelms the receiver. The receiving device also contains only a limited amount of speed and memory to store data. So, informing the sender that stops sending frame after some certain number of frames.
  - The below image is the high-level view of how data is encapsulated with the IP Address in the Data-Link layer.

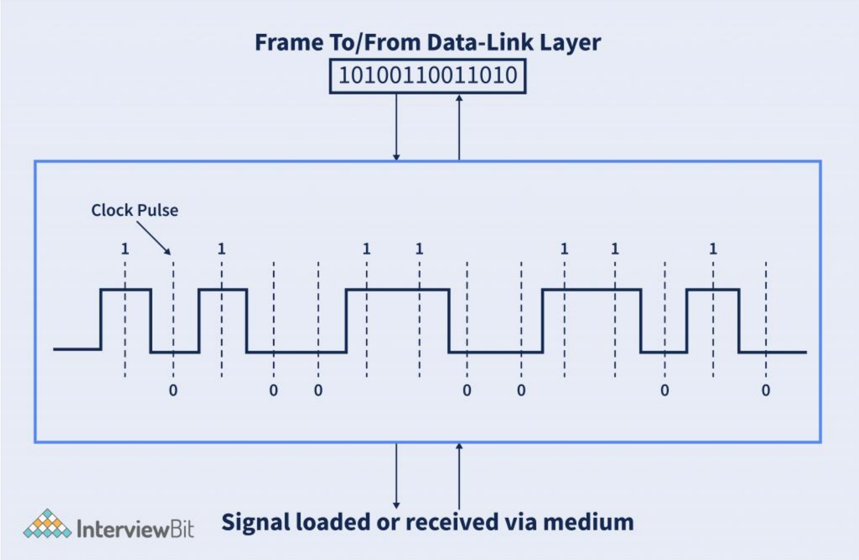


5) Physical Layer

Physical Layer deals with the signals, that how data to transmit to the medium. From the Data-Link layer, the frame of bits received then is sent converted into the actual electrical signals according to the type of medium is used. Like Light beam signal for Optical Fiber Cable, Radio Frequency for wireless. Etc.

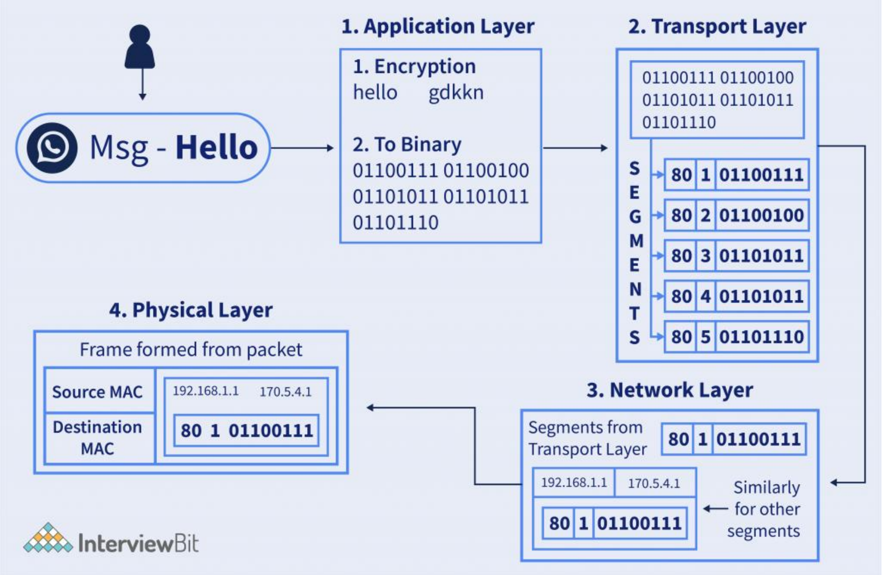
There are many encoding schemes in which the data is encoded. Like – Manchester Encoding (As per G.E. Thomson and also IEEE 802.3 Encoding Scheme), Differential Manchester Encoding Scheme. Etc

Other, on the receiver side, the physical layer accepts the electrical signal that is received, Decodes that signal and makes to a stream of bits, and sends it to the upper layer (Data Link Layer).


Frame To/From Data-Link Layer
10100110011010
Clock Pulse
1
0
1
0
0
1
1
0
0
1
1
0
1
0
InterviewBit
Signal loaded or received via medium

The above image shows the frame received from the data-link layer is converted into the electrical signals and loaded to the medium.

High-Level Diagramatic Overview of Data flow from the User application to the medium in TCP/IP Model –



Steps Explained –

a) Suppose users send messages on WhatsApp – "Hello". Then on the **Application Layer**, it is encrypted according to the algorithm and the ASCII or UNICODE text is converted to binary data and sent to the next layer.

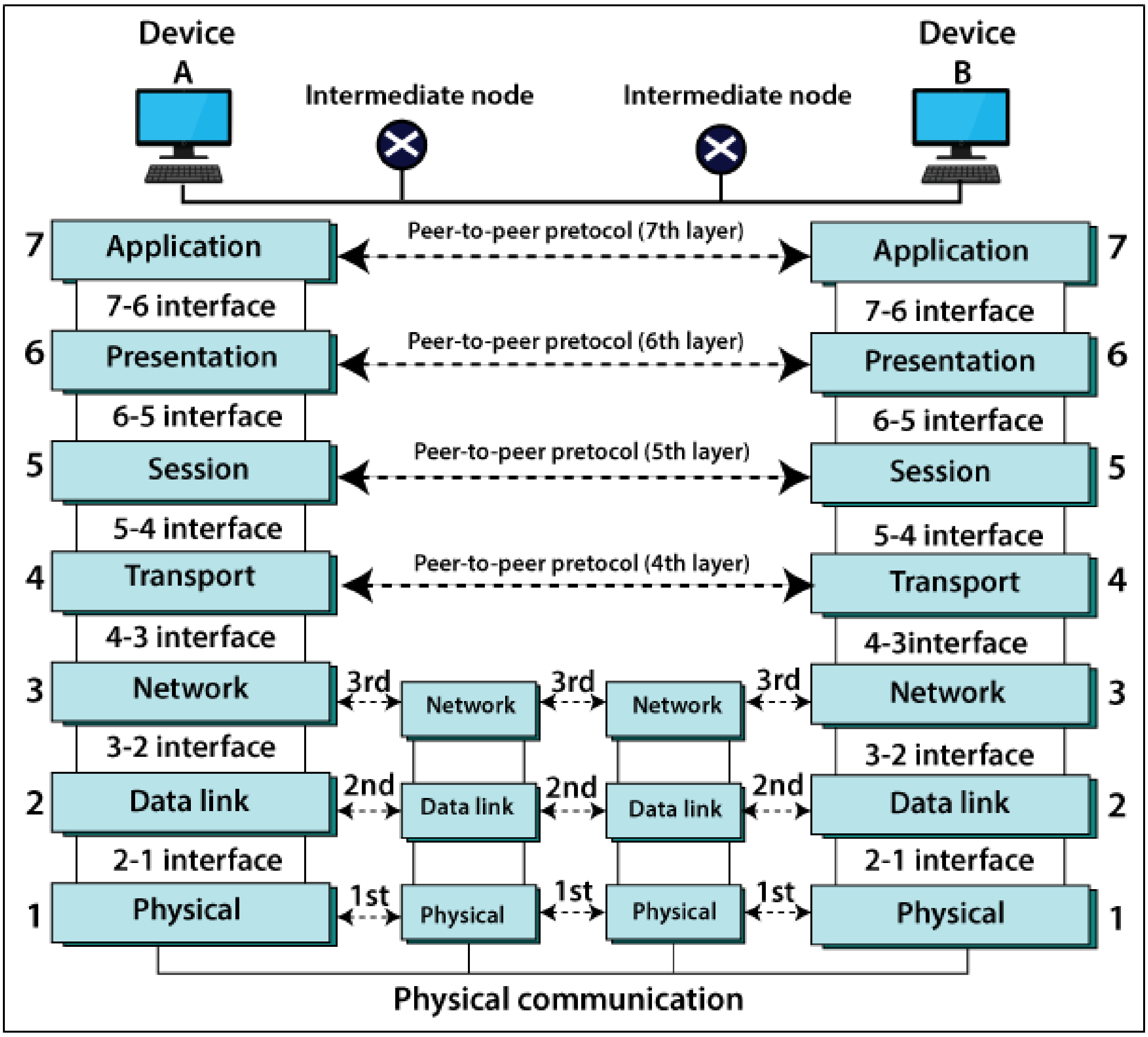
b) In the **Transport Layer**, the data is divided into segments and sent to the next layer for processing.

c) In the **Network Layer**, the source and destination IP Address is added and forms a packet of each segment, and sent for the next layer.

d) In the **Physical Layer**, the MAC address of the destination is added and the frame is converted into signals and the bitstream is loaded to the medium, and then it transmits to the network to reach the destination.

ISO 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.



7. The application layer - This is the only layer that directly interacts with data from the user. Software applications like web browsers and email clients rely on the application layer to initiate communications. But it should be made clear that client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user. Application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

6. **The presentation layer -** This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, encryption, and compression of data.

   Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.

   If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender's end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.

   Finally the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

5. **The session layer -** This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

   The session layer also synchronizes data transfer with checkpoints. For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

4. **The transport layer -** Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.

   The transport layer is also responsible for flow control and error control. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection doesn't overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete, and requesting a retransmission if it isn't.

3. **The network layer -** The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination; this is known as routing.

2. **The data link layer -** The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the SAME network. The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control

and error control in intra-network communication (The transport layer only does flow control and error control for inter-network communications).

1. **The physical layer -** This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

Advantages of OSI Model

The OSI model helps users and operators of computer networks:

- Determine the required hardware and software to build their network.
- Understand and communicate the process followed by components communicating across a network.
- Perform troubleshooting, by identifying which network layer is causing an issue and focusing efforts on that layer.

Bandwidth Utilization

Introduction to Bandwidth

Bandwidth, or precisely **network bandwidth**, is the maximum rate at which data transfer occurs across any particular path of the network. Bandwidth is basically a measure of the amount of data that can be sent and received at any instance of time.

The higher the bandwidth of a network, the larger the amount of data the network can be sending to and from across its path. The bandwidth with closely related terms such as the **data rate** and the **throughput**. Bandwidth is something that deals with the measurement of capacity and not the speed of data transfer.

Units of Measurement

Bandwidth is usually measured in bits transferred per second through a path or link. The common units of bandwidth we come across are as follows.

- bps (Bits per second)
- Mbps (Megabits per second)
- Gbps (Gigabits per second)

Example: Here, a bandwidth of 10 bps for a channel is just another way of saying that a maximum of 10 bits can be transferred using that link for any given time. It has no relation with the transfer speed of the channel.

Computer's Bandwidth

The bandwidth required by any user depends on the usage of that person, if he/she requires more bandwidth then that person requires more bandwidth.

Example, if someone is regularly using gaming, and streaming HD Videos, it requires a speed of around 100 Mbps maximum for surfing without lag, and for normal use like music, and web surfing. etc. 25 Mbps is the maximum. Sometimes it depends on the person, if the person is patient with buffering, then he/she requires less bandwidth for its usage.

Optimizing Network Bandwidth

Often we are concerned about network speed optimization but optimization of bandwidth is also a matter of importance when it comes to making the network suitable for fast and effective communication. This is because having poorly-optimized bandwidth in a network can surely have an adverse impact on the overall performance of the network and thus decline the efficiency and user experience severely.

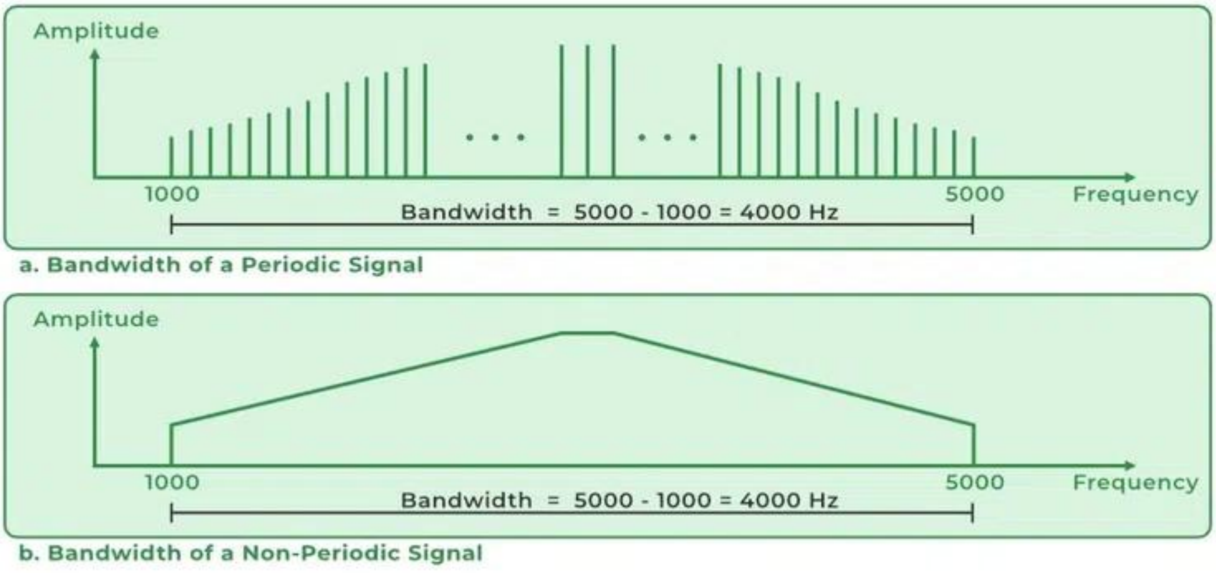
Methods of Optimizing Bandwidth

Here are a few methods used to optimize the bandwidth of a given network.

- Using the QoS Settings to set the network traffic policies and prioritize traffic based on its type such that high-maintenance applications are well equipped with the bandwidth needed by them to perform effectively.
- Deploying application public and private clouds that will offload the network as lesser maintenance of the traffic needs to be done in the particular network being optimized.
- Eliminating any kind of unproductive non-essential traffic wastes bandwidth on irrelevant operations.
- Scheduling Updates, installing software patches, or creating backups outside of Peak Hours can significantly reduce the strain on network bandwidth.

Importance of Bandwidth

It is the bandwidth of a web page that determines how quickly it will load in a browser. When choosing a web hosting platform, this is arguably the most important factor to consider. It is important to consider how the website and internet connection will impact bandwidth. The bandwidth requirement for a website with a lot of graphics can reach 10 gigabytes or more. The bandwidth usage of a simpler website will also be lower. A faster internet connection will allow you to download web pages and movies smoothly, just as a higher bandwidth will improve the user experience.


Amplitude
1000
5000
Frequency
Bandwidth = 5000 - 1000 = 4000 Hz
a. Bandwidth of a Periodic Signal
Amplitude
1000
5000
Frequency
Bandwidth = 5000 - 1000 = 4000 Hz
b. Bandwidth of a Non-Periodic Signal

Bandwidth

Difference between Bandwidth and Data Rate:

Bandwidth: Bandwidth is defined as the width of the spectrum. Spectrum is the range of frequencies contained in the signal. Since bandwidth is the width of the spectrum and spectrum is a range of frequencies, bandwidth is measured in Hertz or khz or mhz.

Data Rate: Data Rate is defined as the amount of data transmitted during a specified time period over a network. It is the speed at which data is transferred from one device to another or between a peripheral device and the computer. It is generally measured in Mega bits per second (Mbps) or Megabytes per second (MBps). For example, if bandwidth is 100 Mbps but the data rate is 50 Mbps, it means maximum 100 Mb of data can be transferred but the channel is transmitting only 50 Mb of data per second.

Difference between Bandwidth and Data Rate

Bandwidth	Data Rate
It is the potential of carrier channel that can carry data.	It is the amount of data transmitted during a specified time period over a network.
It is the difference between range of frequencies.	It is the speed of data transmission.
Normally it is measured in Hz or Khz or Mhz.	It is normally measured in Mbps or MBps.
It refers to maximum data transmission capacity of channel.	It refers to the actual data transmission speed.
It is physical layer property in OSI model.	While it is common in all layers.
It shows the capacity of the channel.	It shows the present speed of data transmission.
It does not depend on properties of sender or receiver.	While it gets affected by sender or receiver.

Difference between Bandwidth and Throughput

Bandwidth: It is defined as the potential of the data that is to be transferred in a specific period of time. It is the data carrying capacity of the network/transmission medium.

Throughput: It is the determination of the amount of data is transmitted during a specified time period via a network, interface or channel. Also called as effective data rate or payload rate.

Difference between Bandwidth and Throughput:

Comparison	Bandwidth	Throughput
Basic	Data capacity is travelled via a channel.	Practical measure of the amount of data actually transmitted through a channel.
Measured in	Bits / Second	Average rate is measured depending on bandwidth. It is measured in terms of bits transferred per second (bps).
Concerned with	Transfer of data by some means.	Communication between two entities

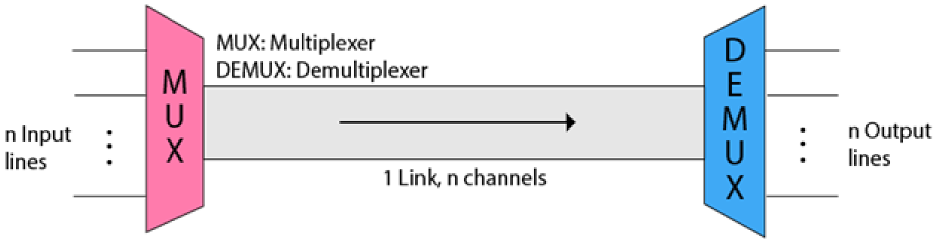
Relevance to layer	Physical layer property.	Work at any of the layers in the OSI model.
Dependence	Not depend on the latency.	It depends on the latency.
Definition	It refers to the maximum amount of the data that can be passed from one point to another.	It is considered as the actual measurement of the data that is being moved through the media at any particular time.
Effect	It is not affected by physical obstruction because it is a theoretical unit to some extent.	It can be easily affected by change in interference, traffic in network, network devices, transmission errors and the host of other type.
Real world Example (Water Tap Example).	It is the speed of tap at which water is coming out.	It is the total amount of water that comes out.

Multiplexing

Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines **n** input lines to generate a single output line. Multiplexing follows **many-to-one**, i.e., **n** input lines and **one** output line.

Demultiplexing is achieved by using a device called Demultiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.



- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
- The composite signal is passed through a Demultiplexer and Demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Importance of Multiplexing

- The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.
- If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example:

If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.

- When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.
- Transmission services are very expensive.

History of Multiplexing

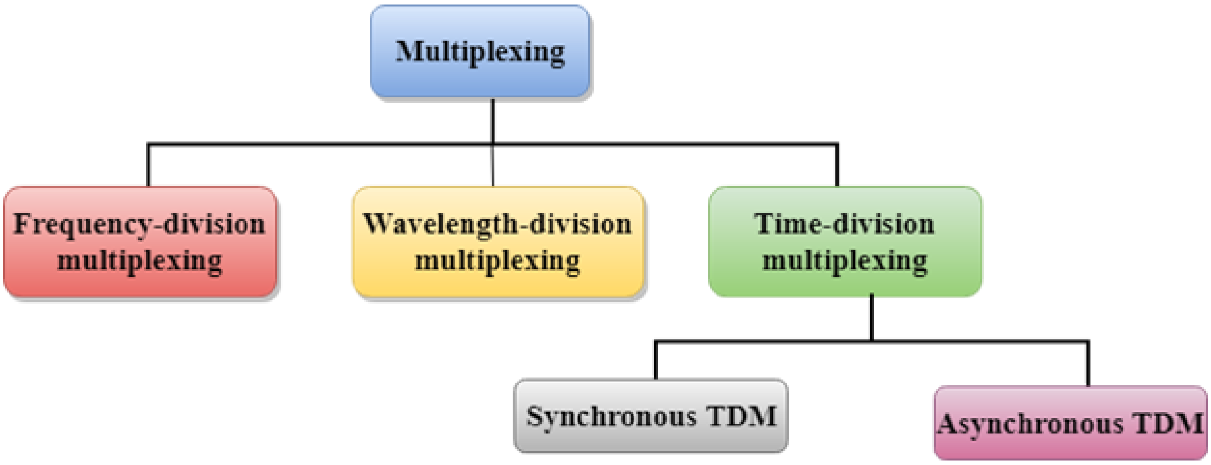
- Multiplexing technique is widely used in telecommunications in which several telephone calls are carried through a single wire.
- Multiplexing originated in telegraphy in the early 1870s and is now widely used in communication.
- George Owen Squier developed the **telephone carrier multiplexing** in 1910.

Advantages of Multiplexing:

- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.

Multiplexing Techniques

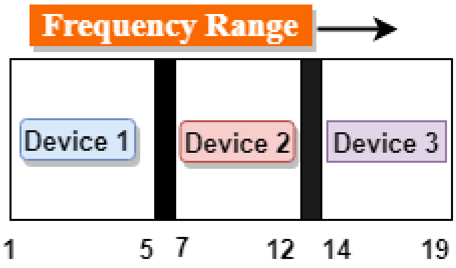
Multiplexing techniques can be classified as:


Multiplexing
Frequency-division multiplexing
Wavelength-division multiplexing
Time-division multiplexing
Synchronous TDM
Asynchronous TDM

Frequency-division Multiplexing (FDM)

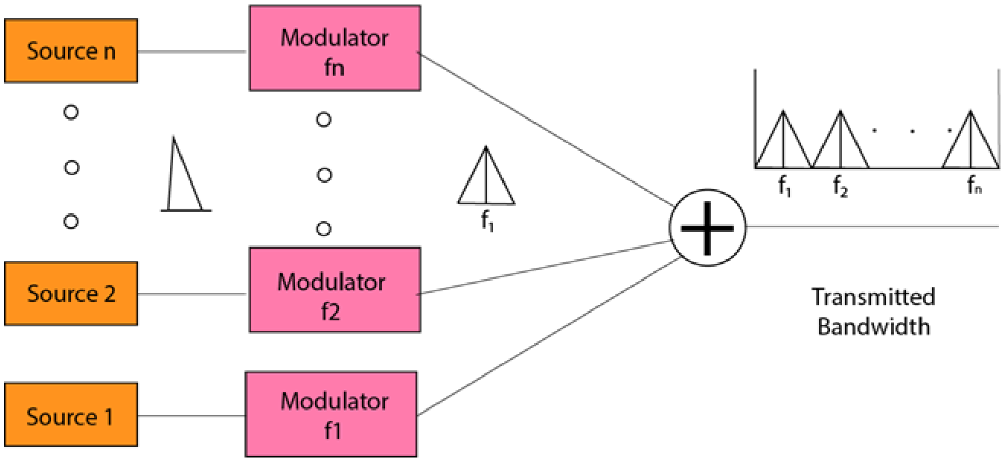
It is an analog technique.

Frequency Division Multiplexing is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.



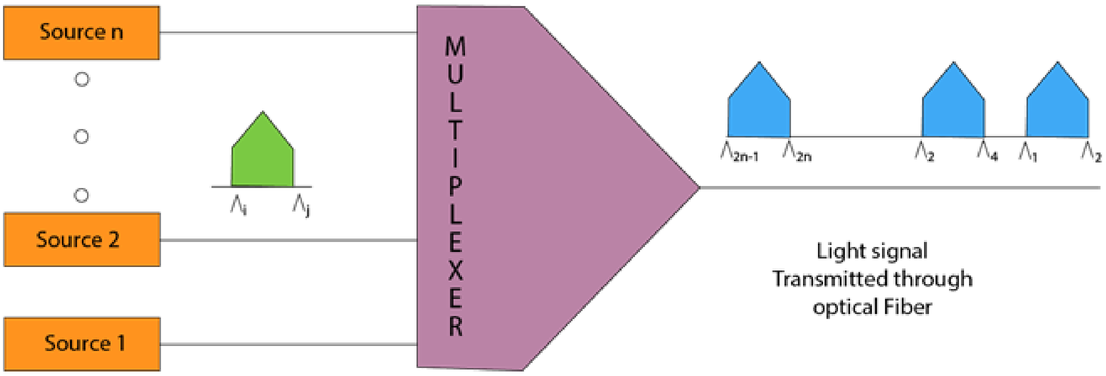
- In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.
- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.

- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.
- The carriers which are used for modulating the signals are known as **sub-carriers**. They are represented as f1,f2..fn.
- **FDM** is mainly used in radio broadcasts and TV networks.



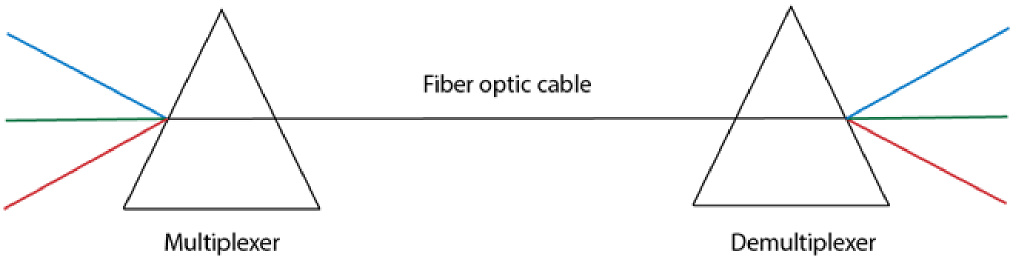
- **Advantages Of FDM:**
  - FDM is used for analog signals.
  - FDM process is very simple and easy modulation.
  - A Large number of signals can be sent through an FDM simultaneously.
  - It does not require any synchronization between sender and receiver.
- **Disadvantages Of FDM:**
  - FDM technique is used only when low-speed channels are required.
  - It suffers the problem of crosstalk.
  - A Large number of modulators are required.
  - It requires a high bandwidth channel.
- **Applications Of FDM:**
  - FDM is commonly used in TV networks.
  - It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Wavelength Division Multiplexing (WDM)



WDM Transmitter

- Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.
- WDM is used on fibre optics to increase the capacity of a single fibre.
- It is used to utilize the high data rate capability of fibre optic cable.
- It is an analog multiplexing technique.
- Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.
- Multiplexing and Demultiplexing can be achieved by using a prism.
- Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.
- Prism also performs a reverse operation, i.e., demultiplexing the signal.



Time Division Multiplexing

- It is a digital technique.
- In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
- In **Time Division Multiplexing technique**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.
- It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

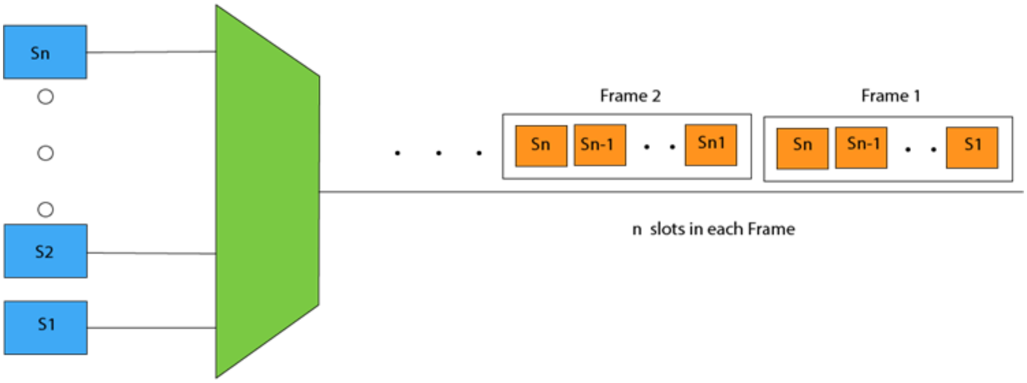
There are two types of TDM:

a) Synchronous TDM
b) Asynchronous TDM

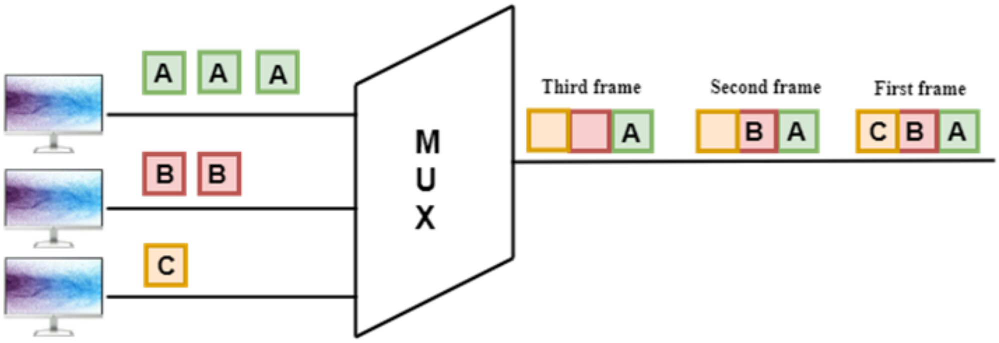
a) Synchronous TDM

- A Synchronous TDM is a technique in which time slot is preassigned to every device.
- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.

- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.
- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.
- If there are n devices, then there are n slots.



Concept of Synchronous TDM



In the above figure, the Synchronous TDM technique is implemented. Each device is allocated with some time slot. The time slots are transmitted irrespective of whether the sender has data to send or not.

Disadvantages of Synchronous TDM:

- The capacity of the channel is not fully utilized as the empty slots are also transmitted which is having no data. In the above figure, the first frame is completely filled, but in the last two frames, some slots are empty. Therefore, we can say that the capacity of the channel is not utilized efficiently.
- The speed of the transmission medium should be greater than the total speed of the input lines. An alternative approach to the Synchronous TDM is Asynchronous Time Division Multiplexing.

b) Asynchronous TDM

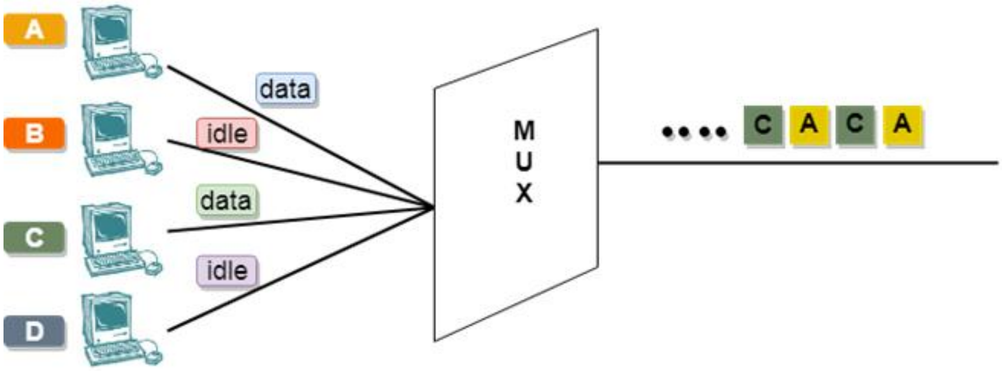
- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.
- An asynchronous TDM technique dynamically allocates the time slots to the devices.

- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

ADDRESS	DATA

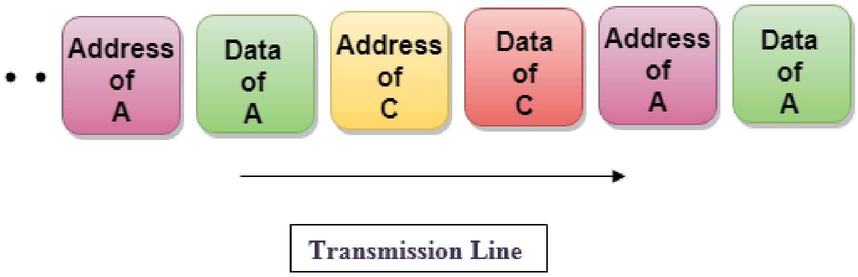
- The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.
- In Synchronous TDM, if there are n sending devices, then there are n time slots. In Asynchronous TDM, if there are n sending devices, then there are m time slots where m is less than n (**m<n**).
- The number of slots in a frame depends on the statistical analysis of the number of input lines.

Concept of Asynchronous TDM



In the above diagram, there are 4 devices, but only two devices are sending the data, i.e., A and C. Therefore, the data of A and C are only transmitted through the transmission line.

Frame of above diagram can be represented as:

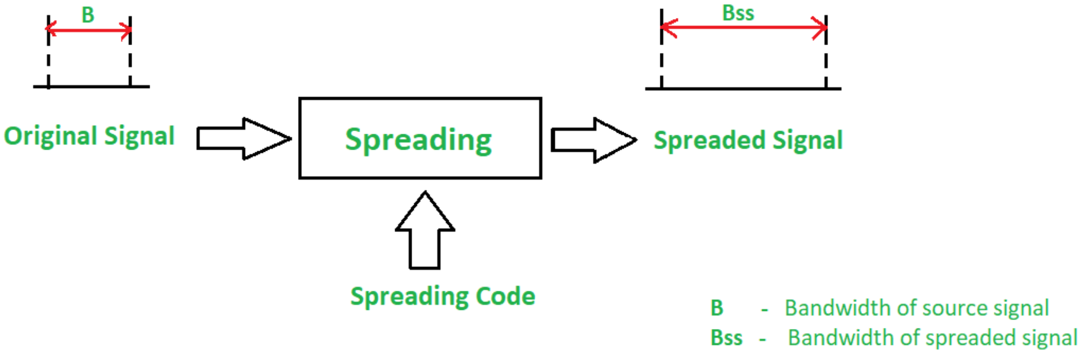


The above figure shows that the data part contains the address to determine the source of the data.

Spectrum Spreading

The increasing demand for wireless communications has problems due to limited spectrum efficiency and multipath propagation. The use of spread spectrum communication has simplified these problems. In the spread spectrum, signals from different sources are combined to fit into **larger bandwidth**.

Most stations use air as the medium for communication, stations must be able to share the medium without an interception and without being subject to jamming from a malicious intruder. To achieve this, spread-spectrum techniques add redundancy means it uses **extended bandwidth** to accommodate signals in a protective envelope so that more secure transmission is possible. The spread code is a series of numbers that looks random but are actually a pattern. The original bandwidth of the signal gets **enlarged** (spread) through the spread code as shown in the figure.


B
Bss
Original Signal
Spreading
Spreaded Signal
Spreading Code
B - Bandwidth of source signal
Bss - Bandwidth of spreaded signal

Spread Spectrum

Principles of Spread Spectrum process:

- To allow redundancy, it is necessary that the bandwidth allocated to each station should be much larger than needed.
- The spreading process occurs after the signal is created by the source.

Conditions of Spread Spectrum are:

- The spread spectrum is a type of modulation where modulated signal BW is much larger than the baseband signal BW i.e. spread spectrum is a wide band scheme.
- A special code (pseudo noise) is used for spectrum spreading and the same code is to be used to despread the signal at the receiver.

Characteristics of the Spread Spectrum are:

a) Higher channel capacity.
b) Ability to resist multipath propagation.
c) They cannot easily intercept any unauthorized person.
d) They are resistant to jamming.
e) The spread spectrum provides immunity to distortion due to multipath propagation.
f) The spread spectrum offers multiple access capabilities.

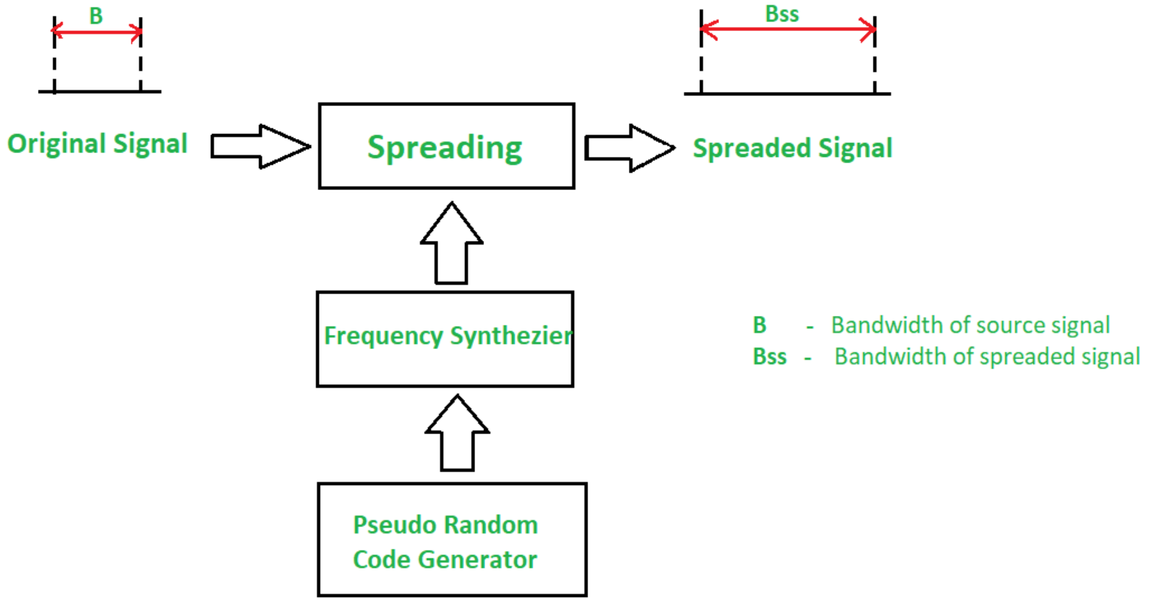
Types of techniques for Spread Spectrum

a) Frequency Hopping Spread Spectrum (FHSS)

b) Direct Sequence Spread Spectrum (DSSS)

a) Frequency Hopping Spread Spectrum (FHSS):

In Frequency Hopping Spread Spectrum (FHSS), different carrier frequencies are modulated by the source signal i.e. M carrier frequencies are modulated by the signal. At one moment signal modulates one carrier frequency and at the subsequent moments, it modulates other carrier frequencies. The general block diagram of FHSS is shown in the below figure.


B
Bss
Original Signal
Spreading
Spreaded Signal
Frequency Synthezier
Pseudo Random Code Generator
B - Bandwidth of source signal
Bss - Bandwidth of spreaded signal

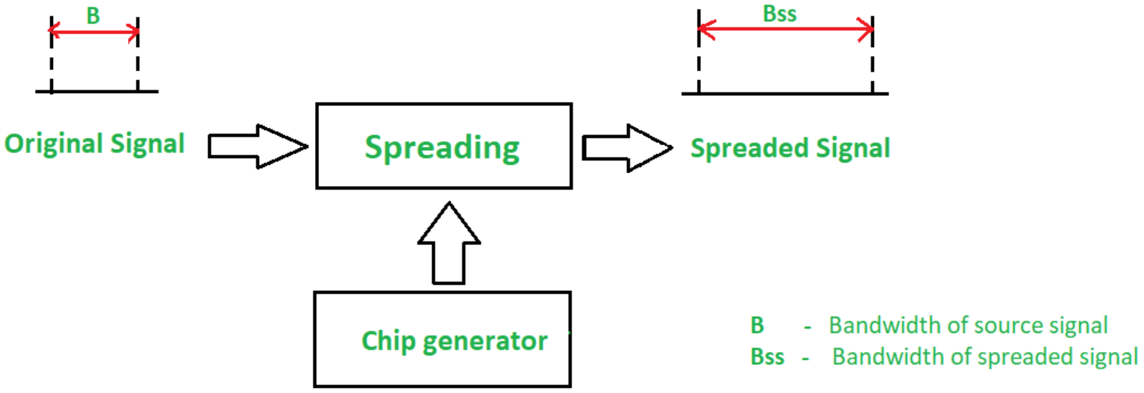
Frequency Hopping Spread Spectrum

A pseudorandom code generator generates Pseudo-random Noise of some pattern for each hopping period **T_h**. The frequency corresponding to the pattern is used for the hopping period and is passed to the frequency synthesizer. The synthesizer generates a carrier signal of that frequency. The figure above shows the spread signal via FHSS.

- **Advantages of FHSS:**
  - Synchronization is not greatly dependent on distance.
  - Processing Gain is higher than DSSS.
- **Disadvantages of FHSS:**
  - The bandwidth of the FHSS system is too large (in GHz).
  - Complex and expensive Digital frequency synthesizers are required.

b) Direct Sequence Spread Spectrum (DSSS):

In DSSS, the bandwidth of the original signal is also expanded by a different technique. Here, each data bit is replaced with n bits using a spreading code called **chips,** and the bit rate of the chip is called as **chip-rate**. The chip rate is n times the bit rate of the original signal. The below Figure shows the DSSS block diagram.


B
Bss
Original Signal
Spreading
Spreaded Signal
Chip generator
B - Bandwidth of source signal
Bss - Bandwidth of spreaded signal

Direct Sequence Spread Spectrum

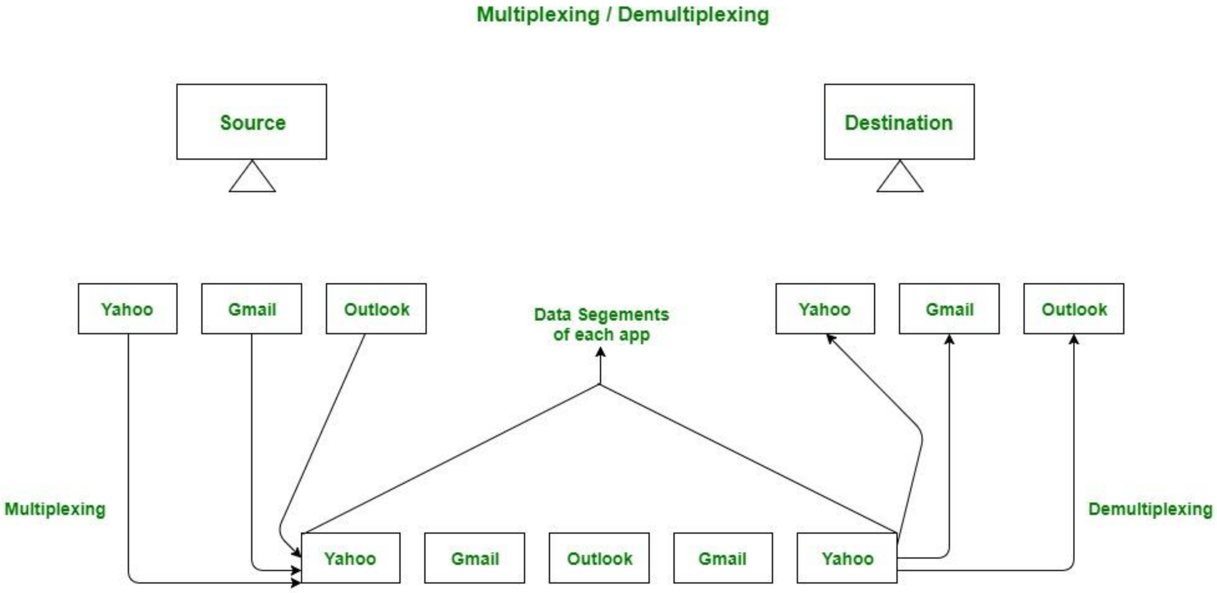
In wireless LAN, the sequence with n = 11 is used. The original data is multiplied by **chips** (spreading code) to get the spread signal. The required bandwidth of the spread signal is 11 times larger than the bandwidth of the original signal.

- **Advantages of DSSS:**
  - The DSSS System combats the jamming most effectively.
  - The performance of DSSS in presence of noise is superior to FHSS.
  - Interference is minimized against the signals.
- **Disadvantages of DSSS:**
  - Processing Gain is lower than DSSS.
  - Channel Bandwidth is less than FHSS.
  - Synchronization is affected by the variable distance between the transmitter and receiver.

Multiplexing and Demultiplexing in Transport Layer

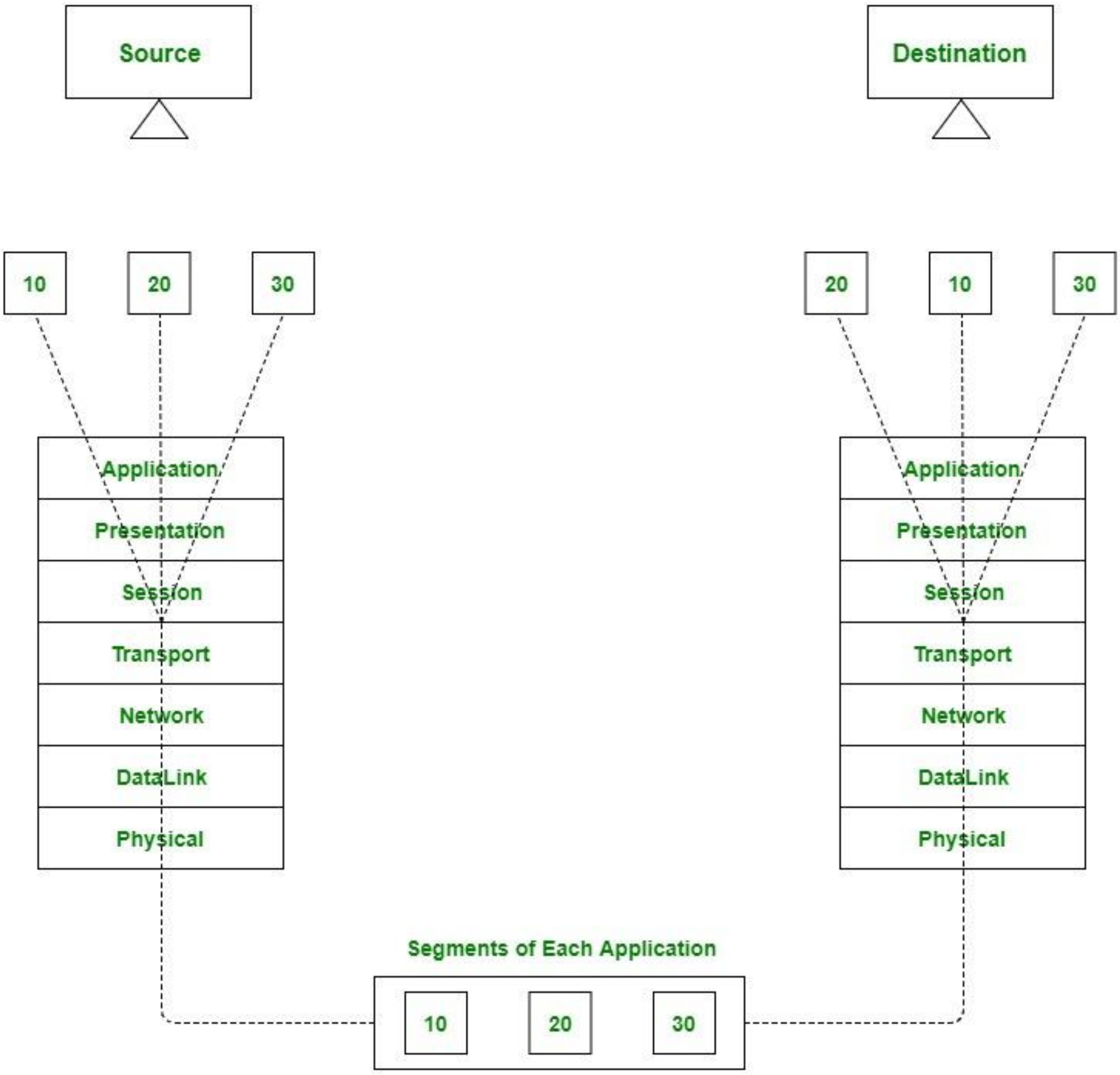
Multiplexing - – Gathering data from multiple application processes of the sender, enveloping that data with a header, and sending them as a whole to the intended receiver is called multiplexing.

Demultiplexing - Delivering received segments at the receiver side to the correct app layer processes is called demultiplexing.



Abstract view of multiplexing and demultiplexing

Multiplexing and demultiplexing are the services facilitated by the transport layer of the OSI model.



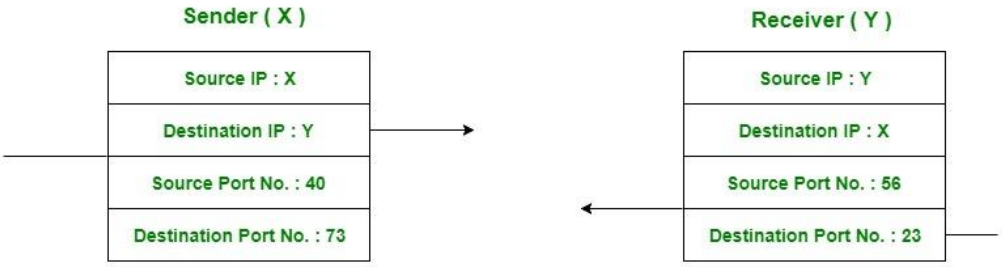
Transport layer- junction for multiplexing and demultiplexing

There are two types of multiplexing and Demultiplexing:

a) Connectionless Multiplexing and Demultiplexing

b) Connection-Oriented Multiplexing and Demultiplexing

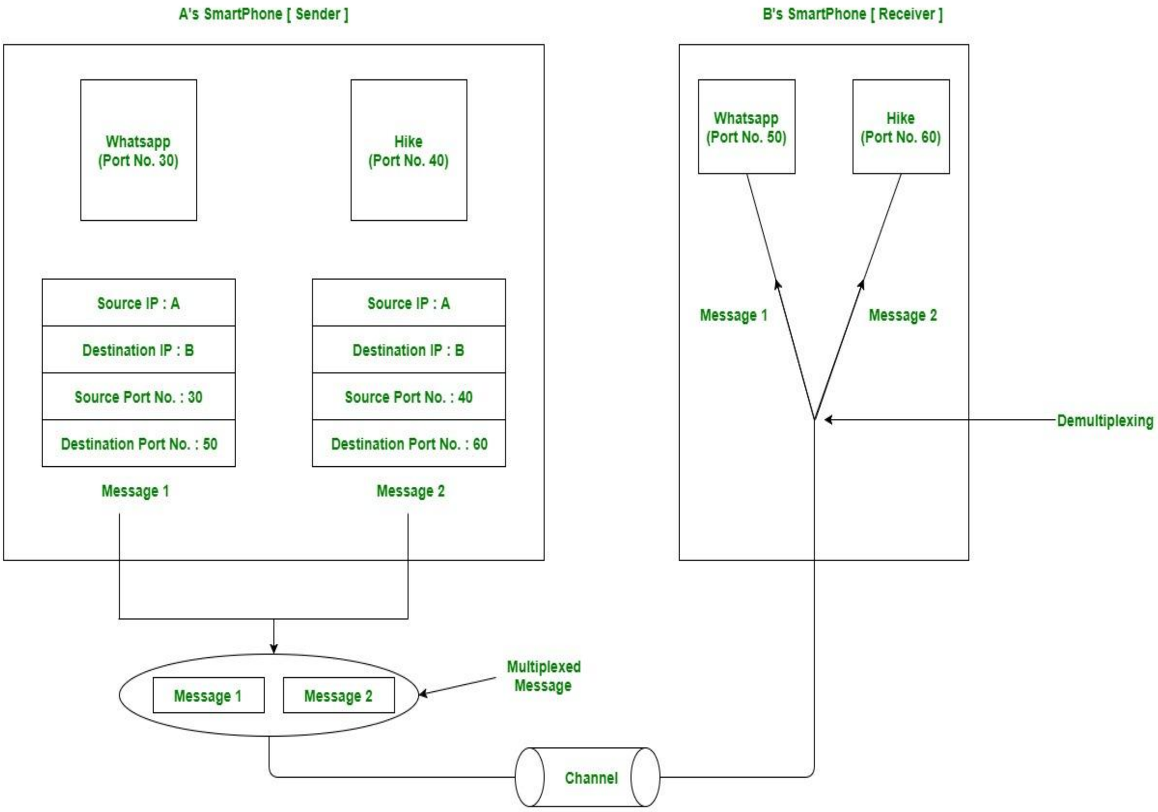
How Multiplexing and Demultiplexing is done – For sending data from an application on the sender side to an application at the destination side, the sender must know the IP address of the destination and port number of the application (at the destination side) to which he wants to transfer the data. Block diagram is shown below:



Transfer of packet between applications of sender and receiver

Let us consider two messaging apps that are widely used nowadays viz. Hike and WhatsApp. Suppose A is the sender and B is the receiver. Both sender and receiver have these applications installed in their system (say smartphone). Suppose A wants to send messages to B in WhatsApp and hike both. In order to do so, A must mention the IP address of B and destination port number of the WhatsApp while sending the message through the WhatsApp application. Similarly, for the latter case, A must mention the IP address of B and the destination port number of the hike while sending the message.

Now the messages from both the apps will be wrapped up along with appropriate headers (viz. source IP address, destination IP address, source port no, destination port number) and sent as a single message to the receiver. This process is called multiplexing. At the destination, the received message is unwrapped and constituent messages (viz messages from a hike and WhatsApp application) are sent to the appropriate application by looking to the destination the port number. This process is called demultiplexing. Similarly, B can also transfer the messages to A.



Message transfer using WhatsApp and hike messaging application

Transmission Media

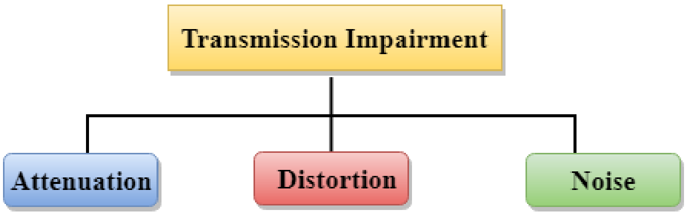
Introduction - Transmission Media

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through **LAN** (Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre based network, the bits in the form of light pulses.
- In **OSI** (Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
- The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

Some factors need to be considered for designing the transmission media:

- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

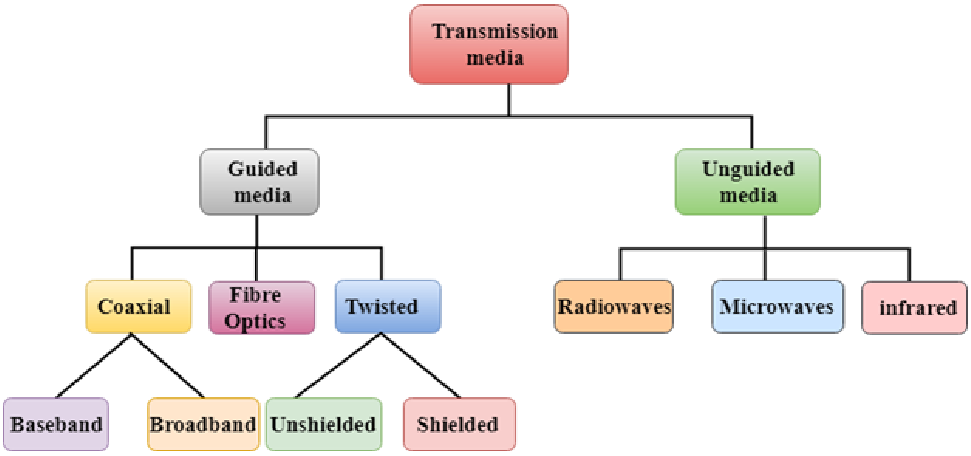
Causes of Transmission Impairment:



- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.

- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Classification of Transmission Media:



1) Guided Transmission Media
2) Un Guided Transmission Media

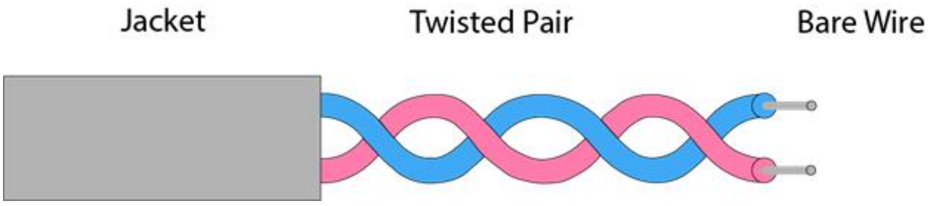
Guided Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

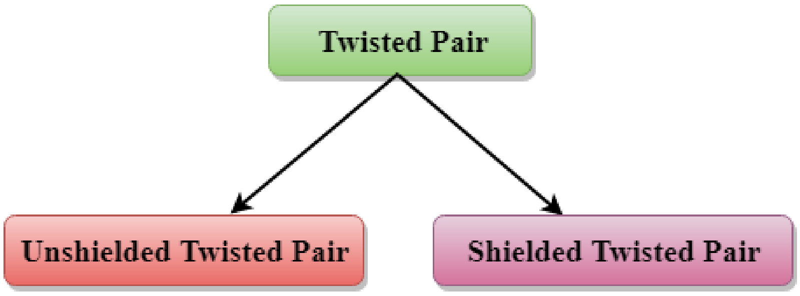
Types of Guided media:

Twisted pair: Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern. The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Types of Twisted pair:



Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- Category 1: Category 1 is used for telephone lines that have low-speed data.
- Category 2: It can support upto 4Mbps.
- Category 3: It can support upto 16Mbps.
- Category 4: It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- Category 5: It can support upto 200Mbps.

Advantages of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage of Unshielded Twisted Pair::

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics of Shielded Twisted Pair:

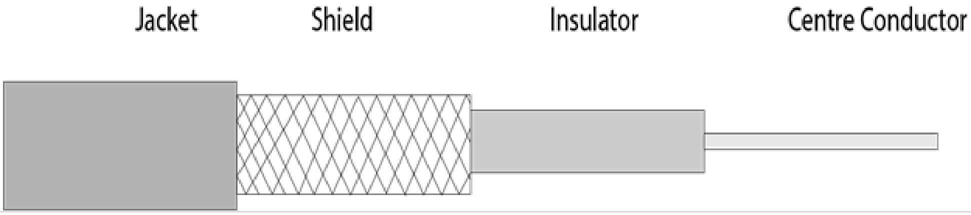
- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

Coaxial Cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the EMI(Electromagnetic interference).



Advantages:

- **Better bandwidth**: Co-axial cables offer better bandwidth than twisted pair cables, allowing for faster data transfer rates and improved performance.
- **Longer distance transmission**: Co-axial cables can transmit data over longer distances than twisted pair cables.
- **Resistance to interference**: Co-axial cables are resistant to electromagnetic interference, improving signal quality and reducing data loss.

Disadvantages:

- **More expensive:** Co-axial cables are more expensive than twisted pair cables, making them less cost-effective for some applications.
- **Difficult to install**: Co-axial cables are more difficult to install than twisted pair cables, requiring specialized equipment and expertise.
- **Limited flexibility**: Co-axial cables are less flexible than twisted pair cables, limiting their use in some applications.

Types of Coaxial cable

1) **Baseband Transmission:** It is defined as the process of transmitting a single signal at high speed.
   It is a method of transmission where a single signal is either transmitted or received in the type of discrete pulses of a single frequency across a communication medium like a cable. The baseband signal's frequency is not changed, and the signal's bandwidth is almost 0. Baseband systems do not use frequency shifting, so only one signal uses the entire bandwidth of the system at once. Therefore, any remaining bandwidth is wasted.

   In this technology, several devices in a network interact with one another by sending and receiving data on a single communication channel that is shared by all connected devices and utilizing the channel's full bandwidth. The data is either transmitted or received at any time. All the devices in the network must be able to understand the same type of signal. However, Time Division Multiplexing (TDM) enables sharing of the same media. The baseband signal is frequently utilized in wired Local Area Networks (LANs) that are based on Ethernet.

   There are various advantages and disadvantages of baseband transmission. Some advantages and disadvantages of baseband transmission are as follows:

   Advantages

   - It has a simple structure.
   - It is easy to install.
   - Its maintenance is simple and easy.
   - It has low-cost installation.

   Disadvantages

   - It may be only utilized for voice and data.
   - It has a short coverage and a limited range.
   - It works only on a limited distance.

2) **Broadband Transmission**: It is defined as the process of transmitting multiple signals simultaneously.

Broadband Transmission sends data in the form of analog signals, allowing signals to be sent at multiple frequencies simultaneously. This broadband transmission is unidirectional. In other words, the data is only transmitted in one direction at the same time. As a result, it may send or receive data but not perform both operations at the same time.

Broadband transmission utilizes ***Frequency Division Multiplexing (FDM)***. The bandwidth in FDM is split into a number of frequency bands, each of which transmits a different signal. A multiplexer separates the numerous signals at the receiving end. It is typically more expensive to maintain and install due to the extra hardware involved. However, they cover more distance than baseband transmission. Broadband transmission is typically utilized via cable TV, several types of ***Digital Subscriber Lines (DSL), Asynchronous Transfer Mode (ATM)***, and ***Power Line communication***.

Advantages and Disadvantages of Broadband Transmission

There are various advantages and disadvantages of broadband transmission. Some advantages and disadvantages of broadband transmission are as follows:

Advantages

- The main advantage of broadband transmission is its speed. It offers a fast speed for data transmission.
- It has a large bandwidth provision for data transmission.
- The data transmission may take place for a large distance.

Disadvantages

- It needs some extra hardware for data transmissions like Multiplexers and De-multiplexers.
- The broadband transmission maintenance and cost are high.

Baseband Vs Broadband Transmission

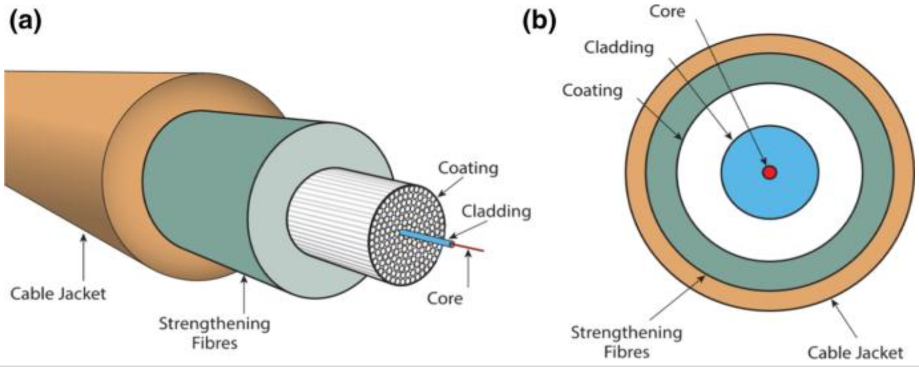
Features	Baseband Transmission	Broadband Transmission
Definition	It is a data transmission technique in which one signal needs the whole bandwidth of the channel to transfer the data.	It is a transmission technology in which many signals with different frequencies send data across a single channel at the same time.
Signal Type	It utilizes digital signals.	It utilizes analog signals.
Signal transmission	The signals may be transmitted in both directions.	The signal may transmit only one direction.
Direction Type	It is bidirectional in nature.	It is unidirectional in nature.
Multiplexing	It uses Time Division Multiplexing (TDM).	It uses Frequency Division Multiplexing (FDM).

Topology	It operates with bus topology.	It operates with both bus and tree topology.
Number of Channels	It utilizes the same channel for sending and receiving data.	It utilizes two channels, one for transmission and the second for data reception.
Distance Covered	Signals are only capable of travelling limited distances. Attenuation is needed for long distances.	Signals may be transmitted across long distances without attenuation.
Installation and Maintenance	It is simple and easy to install and maintain.	It is complex to install and maintain.
Cost	It is less expensive to design.	It is costly to design.
Encoding Technique	Manchester and differential Manchester encoding are used in baseband.	It doesn't utilize any digital encoding, but it utilizes the PSK (Phase shift keying) encoding.
Impedance	It contains a 50-ohm impedance.	It contains a 70-ohm impedance.
Transfer medium	It utilizes coaxial cables, wires, and twisted-pair cables as the transfer medium for digital signals.	It sends digital signals via coaxial cable, optical fibre cables, and radio waves.
Application	It is usually found in Ethernet.	It is usually found in telephone networks and cables.

Fibre Optic

- Fibre optic cable is a cable that uses electrical signals for communication.
- Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provides faster data transmission than copper wires.

Diagrammatic representation of fibre optic cable:



Basic elements of Fibre optic cable:

- **Core**: The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be **transmitted** into the fibre.
- Cladding: The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
- **Jacket**: The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Advantages of fibre optic cable over copper:

- **Greater Bandwidth**: The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- **Faster speed**: Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
- **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier**: Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

Disadvantages of fibre optic cable over copper::

- Cost: Optical fiber cables are more expensive to install than traditional copper cables. This can make them less attractive to companies and organizations that are looking for cost-effective solutions.
- Fragility: Optical fiber cables are fragile and can be damaged easily if they are bent or twisted too much. This makes them less suitable for applications that require cables to be frequently moved or repositioned.
- Difficult to splice: Optical fiber cables are more difficult to splice than traditional copper cables, which can make them more challenging to install and maintain.

Domain Name System (DNS) in Application Layer

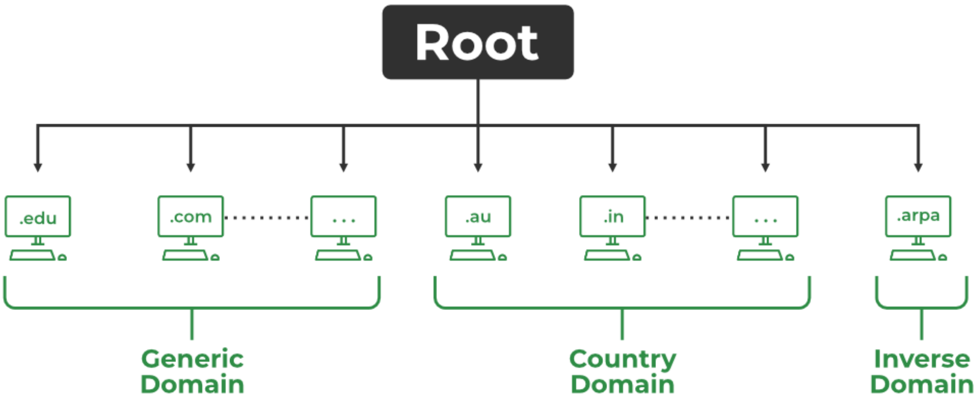
Domain Name System (DNS) is a hostname for **IP address** translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers. It is required for the functioning of the Internet.

Every host is identified by the IP address but remembering numbers is very difficult for people also the IP addresses are not static therefore a mapping is required to change the domain name to the IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

Types of Domain

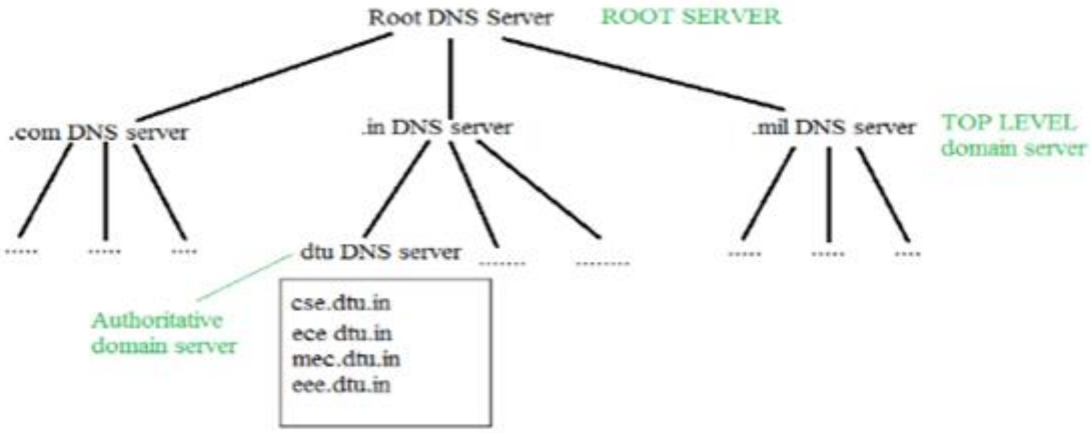
There are various kinds of domain:

1) **Generic domains:** .com(commercial), .edu(educational), .mil(military), .org(nonprofit organization), .net(similar to commercial) all these are generic domains.
2) **Country domain:** .in (India) .us .uk
3) **Inverse domain:** if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the IP addresses of geeksforgeeks.org then we have to type



Organization of Domain

It is very difficult to find out the IP address associated with a website because there are millions of websites and with all those websites we should be able to generate the IP address immediately, there should not be a lot of delays for that to happen organization of the database is very important.



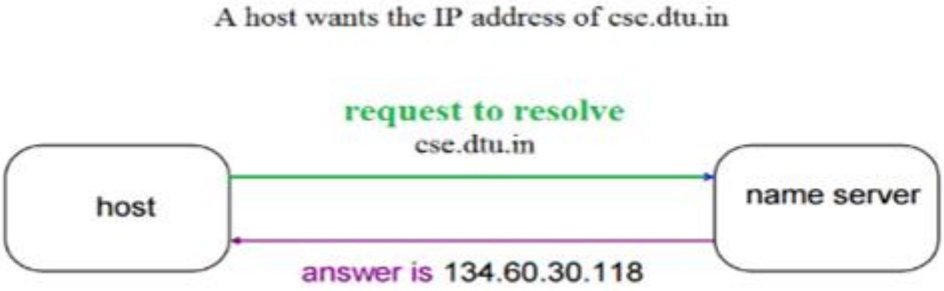
Root DNS Server

- **DNS record:** Domain name, IP address what is the validity? what is the time to live? and all the information related to that domain name. These records are stored in a tree-like structure.
- **Namespace:** Set of possible names, flat or hierarchical. The naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value.
- **Name server:** It is an implementation of the resolution mechanism.

DNS = Name service in Internet – A zone is an administrative unit, and a domain is a subtree.

Name-to-Address Resolution

The host requests the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.

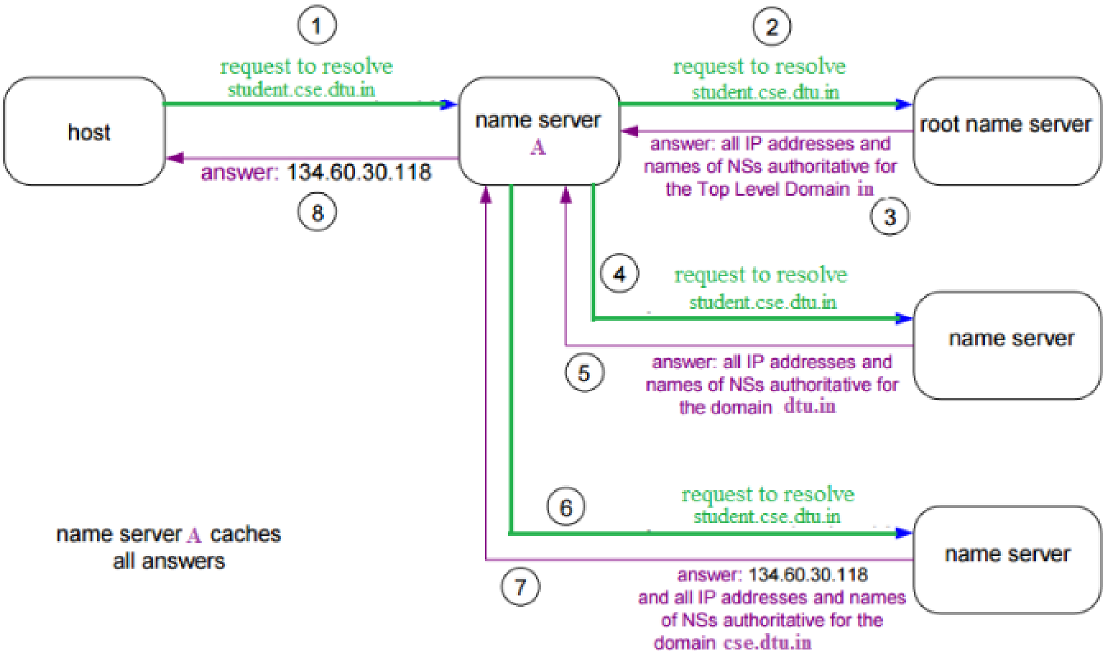


Name-to-Address Resolution

- **Hierarchy of Name Servers Root name servers:** It is contacted by name servers that cannot resolve the name. It contacts the authoritative name server if name mapping is not known. It then gets the mapping and returns the IP address to the host.
- **Top-level domain (TLD) server:** It is responsible for com, org, edu, etc, and all top-level country domains like uk, fr, ca, in, etc. They have info about authoritative domain servers and know the names and IP addresses of each authoritative name server for the second-level domains.
- **Authoritative name servers** are the organization's DNS servers, providing authoritative hostnames to IP mapping for organization servers. It can be maintained by an organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top-level domain server and then to the authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative IP address.

Domain Name Server

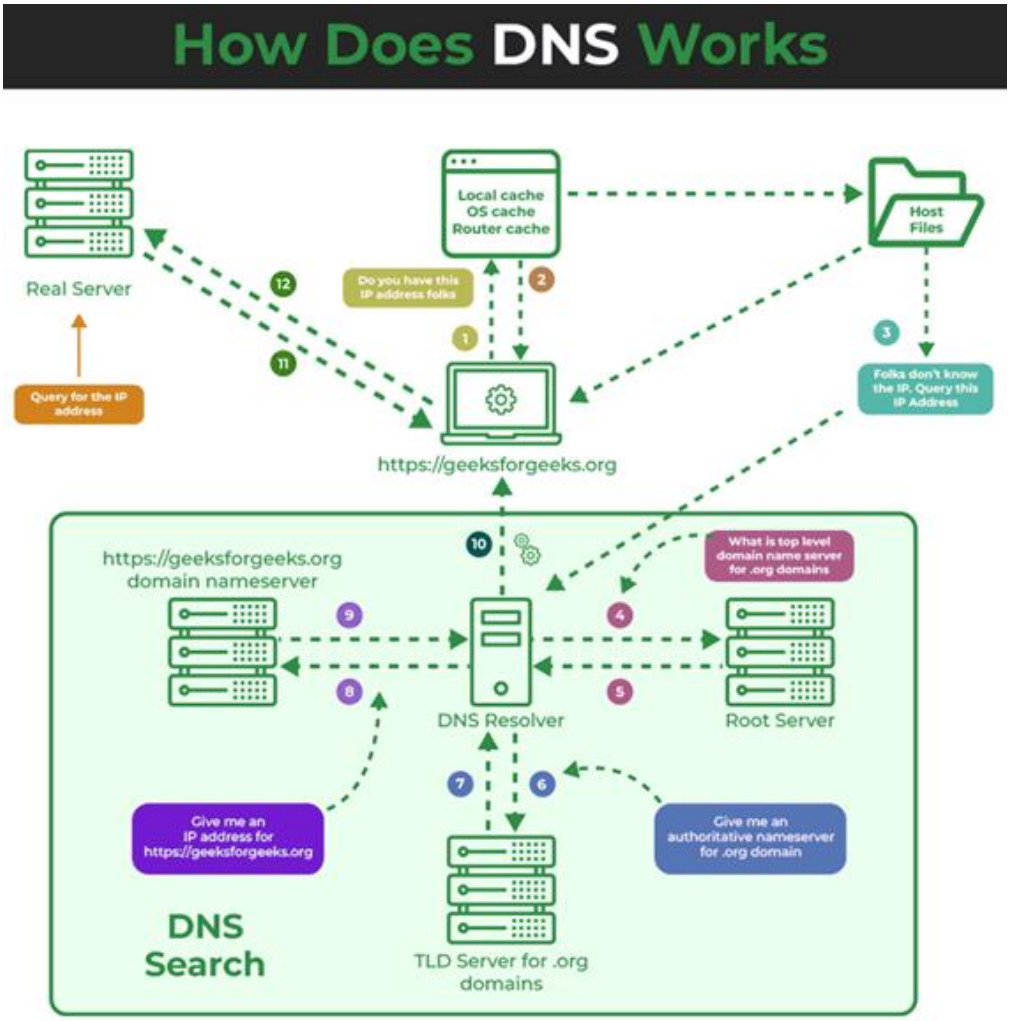
The client machine sends a request to the local name server, which, if the root does not find the address in its database, sends a request to the root name server, which in turn, will route the query to a top-level domain (TLD) or authoritative name server. The root name server can also contain some hostName to IP address mappings. The Top-level domain (TLD) server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.


1
request to resolve student.cse.dtu.in
host
name server A
answer: 134.60.30.118
8
2
request to resolve student.cse.dtu.in
root name server
answer: all IP addresses and names of NSs authoritative for the Top Level Domain in
3
4
request to resolve student.cse.dtu.in
name server
5
answer: all IP addresses and names of NSs authoritative for the domain dtu.in
6
request to resolve student.cse.dtu.in
name server
7
answer: 134.60.30.118 and all IP addresses and names of NSs authoritative for the domain cse.dtu.in
name server A caches all answers

Domain Name Server

DNS Work

The working of DNS starts with converting a hostname into an IP Address. A domain name serves as a distinctive identification for a website. It is used in place of an IP address to make it simpler for consumers to visit websites. Domain Name System works by executing the database whose work is to store the name of hosts which are available on the Internet. The top-level domain server stores address information for top-level domains such as .com and .net, .org, and so on. If the Client sends the request, then the DNS resolver sends a request to DNS Server to fetch the IP Address. In case, when it does not contain that particular IP Address with a hostname, it forwards the request to another DNS Server. When IP Address has arrived at the resolver, it completes the request over Internet Protocol.


How Does DNS Works
Real Server
Local cache
OS cache
Router cache
Host
Files
12
Do you have this IP address folks
2
1
3
11
Query for the IP address
Folks don't know the IP. Query this IP Address
https://geeksforgeeks.org
10
What is top level domain name server for .org domains
https://geeksforgeeks.org
domain nameserver
9
4
8
5
DNS Resolver
Root Server
7
6
Give me an IP address for https://geeksforgeeks.org
Give me an authoritative nameserver for .org domain
DNS
Search
TLD Server for .org domains

Authoritative DNS Server Vs Recursive DNS Resolver

Parameters	Authoritative DNS Server	Recursive DNS Resolver
Function	Holds the official DNS records for a domain	Resolves DNS queries on behalf of clients
Role	Provides answers to specific DNS queries	Actively looks up information for clients
Query Handling	Responds with authoritative DNS data	Queries other DNS servers for DNS data
Client Interaction	Doesn't directly interact with end-users	Serves end-users or client applications
Data Source	Stores the DNS records for specific domains	Looks up data from other DNS servers
Caching	Generally, doesn't perform caching	Caches DNS responses for faster lookups
Hierarchical Resolution	Does not participate in the recursive resolution	Actively performs recursive name resolution
IP Address	Has a fixed, known IP address	IP address may vary depending on ISP
Zone Authority	Manages a specific DNS zone (domain)	Does not manage any specific DNS zone

DNS Lookup - DNS Lookup or DNS Resolution can be simply termed as the process that helps in allowing devices and applications that translate readable domain names to the corresponding IP Addresses used by the computers for communicating over the web.

DNS Servers Involved in Loading a Webpage

Upon loading the webpage, several DNS Servers are responsible for translating the domain name into the corresponding IP Address of the web server hosting the website. Here is the list of main DNS servers involved in loading a Webpage.

- Local DNS Resolver
- Root DNS Servers
- Top-Level Domain (TLD) DNS Servers
- Authoritative DNS Servers
- Web Server

This hierarchical system of DNS servers ensures that when you type a domain name into your web browser, it can be translated into the correct IP address, allowing you to access the desired webpage on the internet.

DNS Resolver

DNS Resolver is simply called a DNS Client and has the functionality for initiating the process of DNS Lookup which is also called DNS Resolution. By using the DNS Resolver, applications can easily access different websites and services present on the Internet by using domain names that are very much friendly to the user and that also resolves the problem of remembering IP Address.

Types of DNS Queries

There are basically three types of DNS Queries that occur in DNS Lookup. These are stated below.

- **Recursive Query:** In this query, if the resolver is unable to find the record, in that case, DNS client wants the DNS Server will respond to the client in any way like with the requested source record or an error message.
- **Iterative Query:** Iterative Query is the query in which DNS Client wants the best answer possible from the DNS Server.
- **Non-Recursive Query:** Non-Recursive Query is the query that occurs when a DNS Resolver queries a DNS Server for some record that has access to it because of the record that exists in its cache.

DNS Caching - DNS Caching can be simply termed as the process used by DNS Resolvers for storing the previously resolved information of DNS that contains domain names, and IP Addresses for some time. The main principle of DNS Caching is to speed up the process of future DNS lookup and also help in reducing the overall time of DNS Resolution.