**COMPUTER NETWORKS**

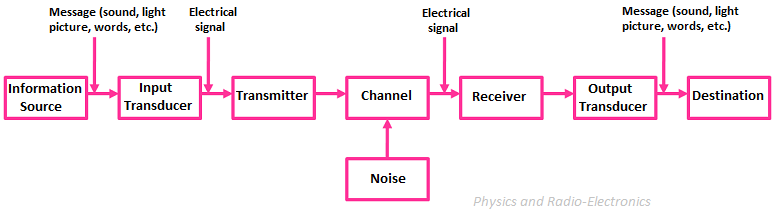
**UNIT-1**

**Elements of a Communication System**

Communication means sending, receiving and processing of information between two or more devices. A collection of elements (devices) which works together to establish a communication between the sender and receiver is called a communication system. Some examples of communication system include radio broadcasting, television broadcasting, radio telegraphy, mobile communication, computer communication etc. Two or more people communicating with each other by using sound signals is also known as the communication system.

Block Diagram of Communication system

The basic components of a communication system are information source, input transducer, transmitter, communication channel, receiver, output transducer, and destination.



**Information Source**

As we know that the communication system establishes the communication bridge between the sender (transmitter) and receiver. To establish this communication bridge between the sender and receiver, first, we need an information to send. This information originates in the information source.

For example, if you are talking with your friend on a phone, you are considered as the information source who generates information in the form of sound.

For beginners to analog communication, it’s important to understand the difference between message and information. The message is the part of a communication which involves sending information from source to destination. Information is a meaningful data that the receiver consumes.

**Input** **Transducer**

If you want to talk (communicate) with your friend who is sitting beside you, then you can directly talk with him by using voice signals (sound signals). But if the same friend is farther away from you, then you can’t directly communicate with him by using voice signals (sound signals) because sound signals cannot travel larger distances. So in order to overcome this problem and transmit information to larger distances, first we need to convert this sound signal into another form of signal (electrical signal or light signal) which travel larger distances. The device which is used to convert this sound signal into another form of signal is called **transducer.**

A transducer is a device which converts one form of energy or signal into another form of energy or signal. The transducer is present at the input side and output side of the communication system. The transducer that is present at the input side of the communication system is called input transducer. Generally, the input transducer converts the non-electrical signal (sound signal or light signal) into an electrical signal. The best example of an input transducer is the microphone which is placed between the information source and the transmitter section. A microphone is a device which converts your voice signals (sound signals) into electrical signals.

### Transmitter

The transmitter is a device which converts the signal produced by the source into a form that is suitable for transmission over a given channel or medium. Transmitters use a technique called modulation to convert the electrical signal into a form that is suitable for transmission over a given channel or medium. Modulation is the main function of a transmitter.

When we send the signal to larger distances, it undergoes various circumstances which makes the signal weak. In order to send the signals to larger distances, without the effect of any external interferences or noise addition and without getting faded away, it has to undergo a process called modulation. Modulation increases the strength of a signal without changing the parameters of the original signal. Thus the resulted signal overcomes the various effects which make it to become weak.

### Communication Channel

The communication channel is a medium through which the signal travels.

or

The communication channel is a wired or wireless medium through which the signal (information) travels from source (transmitter) to destination (receiver).

or

The communication channel is a wired or wireless medium that is used to send the signal from the source  (transmitter) to the destination (receiver).

The communication channel is a wired or wireless medium that connects the transmitter and receiver for sending the signal.

Communication channels are divided into two categories: wired and wireless. Some examples of wired channels include co-axial cables, fiber optic cables, and twisted pair telephone lines. Examples of wireless channels are air, water, and vacuum.

Although channel provides a way for communication, it has one drawback. The communication channel reduces the signal strength (attenuates the signal) that carries the information. This reduction in signal strength is mainly caused by the addition of external noise, physical surroundings, and travel distance. Thus the signal received by the receiver is very weak. To compensate this signal loss, amplifiers (the device that amplifies the signal strength) are used at both the transmitter and the receiver side.

### Noise

Noise is an unwanted signal that enters the communication system via the communication channel and interferes with the transmitted signal. The noise signal (unwanted signal) degrades the transmitted signal (signal containing information).

### Receiver

The receiver is a device that receives the signal (electrical signal) from the channel and converts the signal (electrical signal) back to its original form (light and sound) which is understandable by humans at the destination. TV set is a good example of a receiver. TV set receives the signals sent by the TV transmitting stations and converts the signal into a form which is easily understandable by the humans who are watching TV.

### Output Transducer

The transducer that is present at the output side of the communication system is called output transducer. Generally, the output transducer converts the electrical signal into a non-electrical signal (sound signal, light signal, or both sound and light signal). The best example of an output transducer is the loudspeaker which is placed between the receiver section and the destination. The loudspeaker converts the electrical signals into sound signals which are easily understandable by the humans at the destination.

### Destination

The destination is the final stage in the communication system. Generally, humans at some place are considered as the destination. A destination is a place where humans consume the information. For example, if you are watching TV, you are considered as the destination.

**DATA TRANSMISSION:-COMMUNTION MODES**

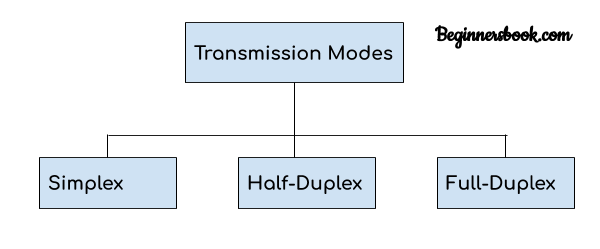
# Transmission Modes in Computer Networks (Simplex, Half-Duplex and Full-Duplex)

Transmission mode means transferring of data between two devices. It is also known as 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:-

 **Simplex Mode**

 **Half-Duplex Mode**

 **Full-Duplex Mode**

  
There are three modes of [transmission](https://teachcomputerscience.com/data-transmission/), namely: simplex, half duplex, and full duplex.  The transmission mode defines the direction of signal flow between two connected devices.

The primary difference between three modes of transmission is that in asimplex mode of transmission the communication is unidirectional, or one-way; whereas in the half duplex mode of transmission the communication is two-directional, but the channel is interchangeably used by both of the connected devices.  On the other hand, in the full duplex mode of transmission, the communication is bi-directional or two-way, and the channel is used by both of the connected devices simultaneously.

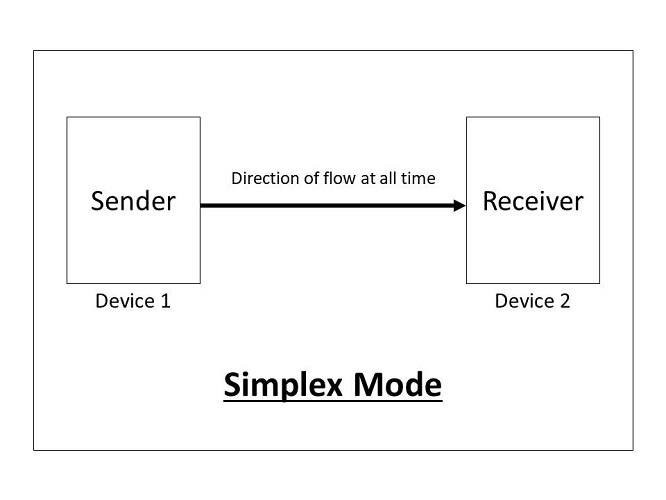
### Comparison Chart

### Simplex

In simplex transmission mode, the communication between sender and receiver occurs in only one direction.  The sender can only send the data, and the receiver can only receive the data.  The receiver cannot reply to the sender.

Simplex transmission can be thought of as a one-way road in which the traffic travels only in one direction—no vehicle coming from the opposite direction is allowed to drive through.

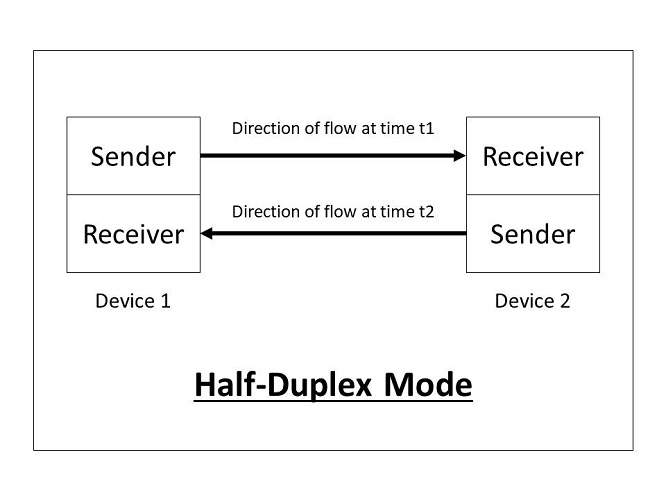
To take a keyboard / monitor relationship as an example, the keyboard can only send the input to the monitor, and the monitor can only receive the input and display it on the screen.  The monitor cannot reply, or send any feedback, to the keyboard.



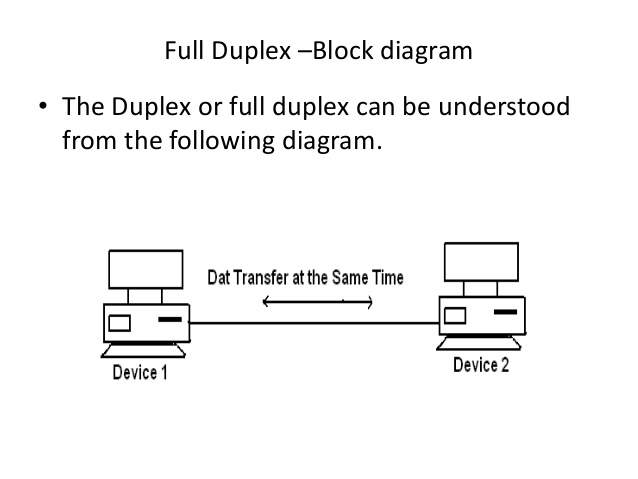
### Half Duplex

The communication between sender and receiver occurs in both directions in half duplex transmission, but only one at a time.  The sender and receiver can both send and receive the information, but only one is allowed to send at any given time.  Half duplex is still considered a one-way road, in which a vehicle traveling in the opposite direction of the traffic has to wait till the road is empty before it can pass through.

For example, in walkie-talkies, the speakers at both ends can speak, but they have to speak one by one.  They cannot speak simultaneously.

**Full Duplex**

In full duplex transmission mode, the communication between sender and receiver can occur simultaneously.  The sender and receiver can both transmit and receive at the same time. Full duplex transmission mode is like a two-way road, in which traffic can flow in both directions at the same time.

For example, in a telephone conversation, two people communicate, and both are free to speak and listen at the same time

# Simplex, Half-Duplex, Full-Duplex, Unicast, Broadcast & Multicast -HSC

# Transmission speed

Transmission speed is the rate at which [data](https://webopedia.com/TERM/D/data.html) [packets](https://webopedia.com/TERM/P/packet.html) cross a computer [network](https://webopedia.com/TERM/N/network.html) from one [server](https://webopedia.com/TERM/S/server.html) to another. Transmission speed is typically measured in [megabits per second](https://webopedia.com/TERM/M/Mbps.html) (Mbps), which equals one million bits per second, although [gigabit](https://webopedia.com/TERM/G/gigabit.html) and even [terabit](https://webopedia.com/TERM/T/terabyte.html) speeds are becoming common. The speed of light is considered the ideal rate of data transmission; transmission speed across cables or wires is a fraction or percent of that.

Transmission speed depends on:

* The wires or cables used in the network. They vary in Mbps.
* The distance between two servers, the sending and receiving points. Distance can severely affect transmission speed, to the point of great financial detriment if a company’s network connection is just a little too slow, for example.
* The number of packets being transmitted across a network. Many requests on a network can slow it.

**Transmission Media**

**Transmission media** refer to the media through which data can be carried from a source to a destination. Data is transmitted from one device to another through electromagnetic signals. Transmission media are located under and controlled by the physical layer .

The different categories of transmission media include guided (or wired) and unguided (or wireless) media. **Guided transmission media** use a cabling system that guides the data signals ...

**Types of Transmission Media**

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:

**1. Guided Media:**   
It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.   
Features:

* High Speed
* Secure
* Used for comparatively shorter distances

There are 3 major types of Guided Media:

**(i) Twisted Pair Cable –**   
It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

1. **Unshielded Twisted Pair (UTP):**   
   This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.

Advantages:

* + Least expensive
  + Easy to install
  + High-speed capacity
  + Susceptible to external interference
  + Lower capacity and performance in comparison to STP
  + Short distance transmission due to attenuation

1. **Shielded Twisted Pair (STP):**   
   This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

Advantages:

* + Better performance at a higher data rate in comparison to UTP
  + Eliminates crosstalk
  + Comparatively faster
  + Comparatively difficult to install and manufacture
  + More expensive
  + Bulky

**(ii) Coaxial Cable –**   
It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

Advantages:

* High Bandwidth
* Better noise Immunity
* Easy to install and expand
* Inexpensive

Disadvantages:

* Single cable failure can disrupt the entire network

**(iii) Optical Fibre Cable –**   
It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.

The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

Advantages:

* Increased capacity and bandwidth
* Lightweight
* Less signal attenuation
* Immunity to electromagnetic interference
* Resistance to corrosive materials

Disadvantages:

* Difficult to install and maintain
* High cost
* Fragile

**(iv) Stripline**

Stripline is a transverse electromagnetic (TEM) transmission line medium invented by Robert M. Barrett of the Air Force Cambridge Research Centre in the 1950s. Stripline is the earliest form of the planar transmission line. It uses a conducting material to transmit high-frequency waves it is also called a waveguide. This conducting material is sandwiched between two layers of the ground plane which are usually shorted to provide EMI immunity.

**(v) Microstripline**

In this, the conducting material is separated from the ground plane by a layer of dielectric.

**2. Unguided Media:**   
It is also referred to as Wireless or Unbounded transmission media.No physical medium is required for the transmission of electromagnetic signals.

Features:

* The signal is broadcasted through air
* Less Secure
* Used for larger distances

There are 3 types of Signals transmitted through unguided media:

**(i) Radiowaves –**   
These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radiowaves for transmission.

Further Categorized as (i) Terrestrial and (ii) Satellite.

**(ii) Microwaves –**   
It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

**(iii) Infrared –**   
Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

## Analog and Digital Transmission

There are a number of differences between analog and digital transmission, and it is important to understand how conversions between analog and digital occur. Let's look first at the older form of transmission, analog.

### Analog Transmission

An analog wave form (or signal) is characterized by being continuously variable along amplitude and frequency. In the case of telephony, for instance, when you speak into a handset, there are changes in the air pressure around your mouth. Those changes in air pressure fall onto the handset, where they are amplified and then converted into current, or voltage fluctuations.

### Digital Transmission

Digital transmission is quite different from analog transmission. For one thing, the signal is much simpler. Rather than being a continuously variable wave form, it is a series of discrete pulses, representing one bits and zero bits (see [Figure 2.10](javascript:popUp('/content/images/chap2_0201760320/elementLinks/02fig10.gif'))). Each computer uses a coding scheme that defines what combinations of ones and zeros constitute all the characters in a character set (that is, lowercase letters, uppercase letters, punctuation marks, digits, keyboard control functions).

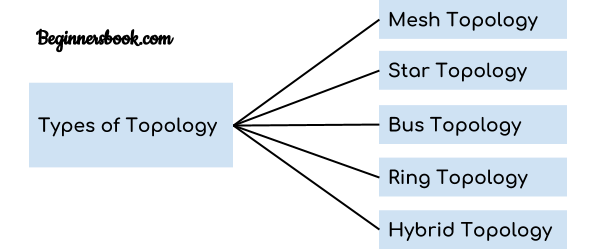
### Analog Versus Digital Transmission

| Feature | Analog Characteristics | Digital Characteristics |
| --- | --- | --- |
| Signal | Continuously variable, in both amplitude and frequency | Discrete signal, represented as either changes in voltage or changes in light levels |
| Traffic measurement | Hz (for example, a telephone channel is 4KHz) | Bits per second (for example, a T-1 line carries 1.544Mbps, and an E-1 line transports 2.048Mbps) |
| Bandwidth | Low bandwidth (4KHz), which means low data transmission rates (up to 33.6Kbps) because of limited channel bandwidth | High bandwidth that can support high-speed data and emerging applications that involve video and multimedia |
| Network capacity | Low; one conversation per telephone channel | High; multiplexers enable multiple conversations to share a communications channel and hence to achieve greater transmission efficiencies |
| Network manageability | Poor; a lot of labor is needed for network maintenance and control because dumb analog devices do not provide management information streams that allow the device to be remotely managed | Good; smart devices produce alerts, alarms, traffic statistics, and performance measurements, and technicians at a network control center (NCC) or network operations center (NOC) can remotely monitor and manage the various network elements |
| Power requirement | High because the signal contains a wide range of frequencies and amplitudes | Low because only two discrete signals—the one and the zero—need to be transmitted |
| Security | Poor; when you tap into an analog circuit, you hear the voice stream in its native form, and it is difficult to detect an intrusion | Good; encryption can be used |
| Error rates | High; 10–5 bits (that is, 1 in 100,000 bits) is guaranteed to have an error | Low; with twisted-pair, 10–7(that, is 1 in 10 million bits per second) will have an error, with satellite, 10–9 (that is, 1 in 1 billion per second) will have an error, and with fiber, 10–11 (that is only 1 in 10 trillion bits per second) will have an error |

### Topology (Network Design)

Computer networks can have different designs, with the two basic forms being client/server and peer-to-peer networks. [Client/server networks](https://www.fieldengineer.com/blogs/annual-maintenance-networks-servers) have centralized servers for storage, which are accessed by client computers and devices. Peer-to-peer networks tend to have devices that support the same functions. They are more common in homes, while client/server networks are more likely to be used by businesses.

## Types of Topology

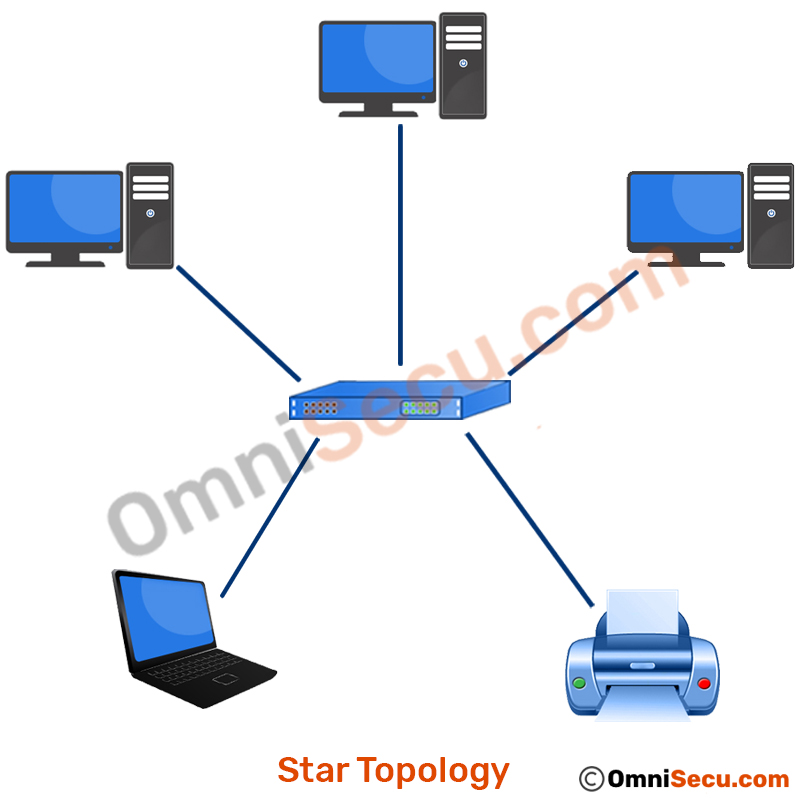
There are five types of topology in computer networks:  


‍

**Here are some of the topologies that are used to create networks:**

**Star Topology**

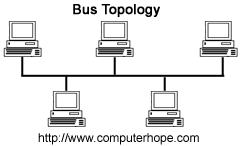
A central node connects a cable to each computer in the network in a star topology. Each computer in the network has an independent connection to the center of the network, and one connection breaking won't affect the rest of the network. However, one downside is that many cables are required to form this kind of network.



‍

‍**Bus Topology**

In a bus topology network connection, one cable connects the computer. The information for the last node on the network has to run through each connected computer. There is less cabling required, but if the cable breaks it means that none of the computers can reach the network.

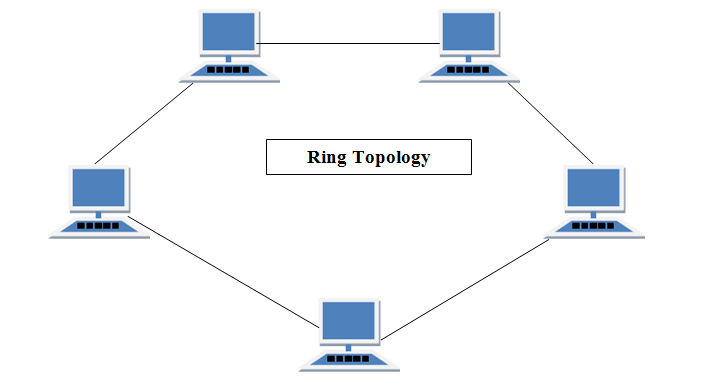


‍

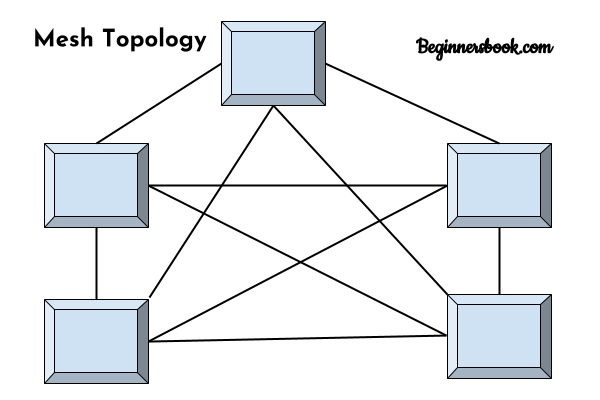
**Ring Topology**

A ring topology is similar to a bus topology. It uses a single cable with the end nodes connected to each other so the signal can circle through the network to find its recipient. The signal will try several times to find its destination even when the network node is not working properly. A collapsed ring has a central node which is a hub, router or switch. The device has an internal ring topology and has places for cable to plug in. Every computer in the network has its own cable to plug into the device. In an office, this probably means having a cabling closet, where all computers are connected to the closet and the switch.

‍

‍

## ‍Mesh Topology

  
In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it means that the link only carries data for the two connected devices only. Lets say we have n devices in the network then each device must be connected with (n-1) devices of the network. Number of links in a mesh topology of n devices would be n(n-1)/2.

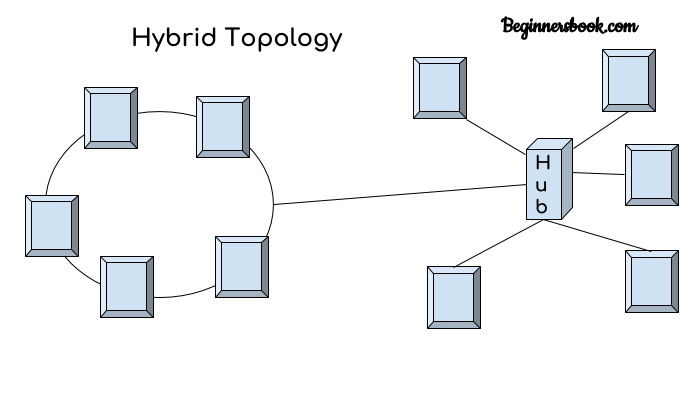
### Advantages of Mesh topology

1. No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.  
2. Mesh topology is reliable and robust as failure of one link doesn’t affect other links and the communication between other devices on the network.  
3. Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.  
4. Fault detection is easy.

### Disadvantages of Mesh topology

1. Amount of wires required to connected each system is tedious and headache.  
2. Since each device needs to be connected with other devices, number of I/O ports required must be huge.  
3. Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link.

## Hybrid topology

  
A combination of two or more topology is known as hybrid topology. For example a combination of star and mesh topology is known as hybrid topology.

### Advantages of Hybrid topology

1. We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.  
2. Scalable as we can further connect other computer networks with the existing networks with different topologies.

### Disadvantages of Hybrid topology

* 1. Fault detection is difficult.  
     2. Installation is difficult.  
     3. Design is complex so maintenance is high thus expensive.

**Tree Topology**:-

* All the computer are connected like the branches of a tree. In Computer Networking, tree topology is known as a combination of a Bus and Start network topology. The main advantages of this topology are better flexibility and scalability.
* Tree network topology is the simplest topology in which only one route exists between any two nodes on the network. The pattern of connection resembles a tree in which all branches spring from one root hence (Tree Topology).

### Tree Topology and Its Advantages and Disadvantages- Snabay Networking

### ****Advantages of Tree Topology****

1. It is a combination of bus and star topology
2. It provides high scalability, as leaf nodes can add more nodes in the hierarchical chain.
3. Other nodes in a network are not affected, if one of their nodes get damaged
4. It provides easy maintenance and fault identification.
5. Supported by several [hardware and software](https://tech.computernetworktopology.com/?p=28) vendors.
6. [Point-to-point](https://computernetworktopology.com/point-to-point-topology/) wiring for individual segments.

### ****Disadvantages of Tree Topology****

1. Large cabling is required as compared to star and bus topology.
2. On the failure of a hub, the entire network fails.
3. Tree network is very difficult to configure than other [network topologies](https://computernetworktopology.com/).

**Internet** :-The **Internet** (or **internet**) is the global system of interconnected computer networks that uses the **Internet** protocol suite (TCP/IP) to communicate between networks and devices.

**How Does the Internet Work?**

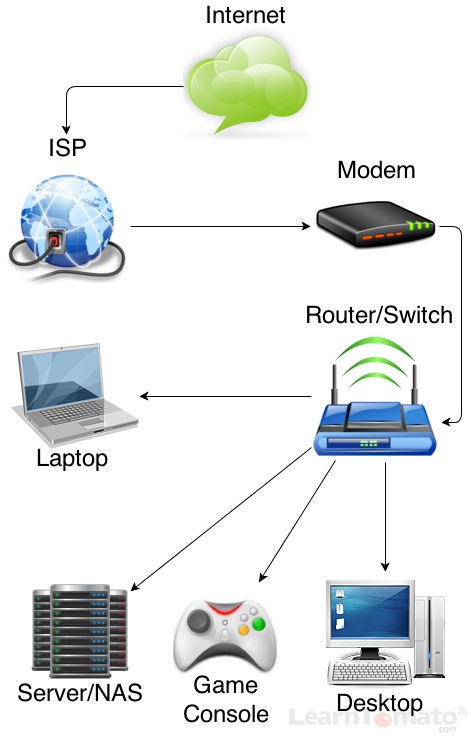
When you opened your email, your email application sent a request to your email provider (for example, Gmail) through your laptop’s Network Interface Card to your Wireless Access Point (WAP) using your local WiFi. The WAP then sent the request through a wire to the local router.

The local router took that request and sent it to another router, which then sent to another router, and another router, all the way through a chain of routers until the data was transferred over one of the transatlantic communication cables to the United States.

There, it ended up at a Google data center (because you use Gmail). Google then processed your request to get any new emails that had come in since you last loaded your email. They packaged up your new, unread emails in a digital package called a “response,” and sent that package back to the same address (your laptop) that requested the updates. The response probably took different routes on the way back, but it went through the same mechanisms.

The data was transferred from the Google data center through multiple lines and reached your home router/modem, which made the data available over your home WiFi. Your laptop’s Network Interface Card received the response, sent it to your email application, and then voilà—your new emails fill up your inbox!

And that all happened in the blink of an eye. It’s pretty amazing how the internet works, isn’t it? So the next time someone asks, “what is the internet” or “how does the internet work?” hopefully you can use this simple explanation to help them understand how this technology that’s so important to our modern daily life actually works.



# WWW Overview

**Client-Server Definition**

Client-server denotes a relationship between cooperating programs in an application, composed of clients initiating requests for services and servers providing that function or service.

# ‍ Client-Server Model

The Client-server model is a distributed application structure that partitions task or workload between the providers of a resource or service, called servers, and service requesters called clients. In the client-server architecture, when the client computer sends a request for data to the server through the internet, the server accepts the requested process and deliver the data packets requested back to the client. Clients do not share any of their resources. Examples of Client-Server Model are Email, World Wide Web, etc.

**How the Client-Server Model works ?**  
In this article we are going to take a dive into the **Client-Server** model and have a look at how the **Internet** works via, web browsers. This article will help us in having a solid foundation of the WEB and help in working with WEB technologies with ease.

* **Client:** When we talk the word **Client**, it mean to talk of a person or an organization using a particular service. Similarly in the digital world a **Client** is a computer (**Host**) i.e. capable of receiving information or using a particular service from the service providers (**Servers**).
* **Servers:** Similarly, when we talk the word **Servers**, It mean a person or medium that serves something. Similarly in this digital world a **Server** is a remote computer which provides information (data) or access to particular services.

So, its basically the **Client** requesting something and the **Server** serving it as long as its present in the database.



A host is a computer that is accessible over a [network](https://techterms.com/definition/network). It can be a [client](https://techterms.com/definition/client), [server](https://techterms.com/definition/server), or any other type of computer. Each host has a unique identifier called a hostname that allows other computers to access it.

Depending on the network [protocol](https://techterms.com/definition/protocol), a computer's hostname may be a [domain name](https://techterms.com/definition/domain_name), [IP address](https://techterms.com/definition/ip_address), or simply a unique text [string](https://techterms.com/definition/string). For example, the hostname of a computer on a local network might be Tech-Terms.local, while an Internet hostname might be techterms.com. A host can access its own data over a network protocol using the hostname "[localhost](https://techterms.com/definition/localhost)."

**What Do Networks Do?**

Computer networks are used to carry out a large number of tasks through the sharing of information.

**Some of the things that networks are used for include:**

* Communicating using email, video, instant messaging and other methods
* Sharing devices such as printers, scanners and photocopiers
* Sharing files
* Sharing software and operating programs on [remote systems](https://www.fieldengineer.com/blogs/benefits-of-remote-network-engineer)
* Allowing network users to easily access and maintain information

# Advantages and disadvantages of networks

## Advantages

* Sharing devices such as printers saves money.
* Site (software) licences are likely to be cheaper than buying several standalone licences.
* Files can easily be shared between users.
* Network users can communicate by email and instant messenger.
* Security is good - users cannot see other users' files unlike on stand-alone machines.
* Data is easy to backup as all the data is stored on the file server.

## Disadvantages

* Purchasing the network cabling and file servers can be expensive.
* Managing a large network is complicated, requires training and a network manager usually needs to be employed.
* If the file server breaks down the files on the file server become inaccessible. Email might still work if it is on a separate server. The computers can still be used but are isolated.
* Viruses can spread to other computers throughout a computer network.
* There is a danger of hacking, particularly with wide area networks. Security procedures are needed to prevent such abuse, eg a firewall.

**Types of Network**

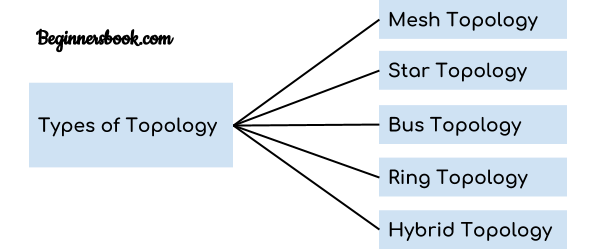
There are many different types of network, which can be used for different purposes and by different types of people and organization. Here are some of the network types that you might come across:

* **Local Area Networks (LAN)**  
  A local area network or [LAN](https://www.fieldengineer.com/skills/lan-technician) is a network that connects computers within a limited area. This might be in a school, an office or even a home.
* **Personal Area Networks (PAN)**‍  
  A personal area network is a network that is based on an individual's workspace. The individual's device is the center of the network, with other devices connected to it. There are also wireless personal area networks.
* **Home Area Networks (HAN)  
  ‍**A home area network connects devices within a home environment. It might include personal computers, tablets, smartphones, printers, TVs and other devices.
* **Wide Area Networks (WAN)  
  ‍**A [wide area network](https://www.fieldengineer.com/skills/wan-engineer) is a network that covers a larger geographical area, usually with a radius of more than a kilometer.
* **Campus Networks  
  ‍**A campus network is a [LAN](https://www.fieldengineer.com/skills/lan-engineer) or set of connected LANs which is used by a government agency, university, corporation or similar organization and is typically a network across a set of buildings that are close together.
* **Metropolitan Area Networks (MAN)  
  ‍**Metropolitan area networks are networks that stretch across a region the size of a metropolitan area. A MAN is a series of connected LANs in a city, which might also connect to a WAN.
* **Enterprise Private Networks  
  ‍**An enterprise private network is used by a company to connect its various sites so that the different locations can share resources.
* **Internetworks  
  ‍**Internetworks connect different networks together to build a larger network. Internetworking is often used to describe building a large, global network.
* **Backbone Networks (BBN)  
  ‍**A backbone is a part of a network that connects different pieces and provides a path for information to be exchanged.
* **Global Area Networks (GAN)  
  ‍**A global area network is a worldwide network that connects networks all over the globe, such as the internet.

### Network Design

Computer networks can have different designs, with the two basic forms being client/server and peer-to-peer networks. [Client/server networks](https://www.fieldengineer.com/blogs/annual-maintenance-networks-servers) have centralized servers for storage, which are accessed by client computers and devices. Peer-to-peer networks tend to have devices that support the same functions. They are more common in homes, while client/server networks are more likely to be used by businesses.

## Types of Topology

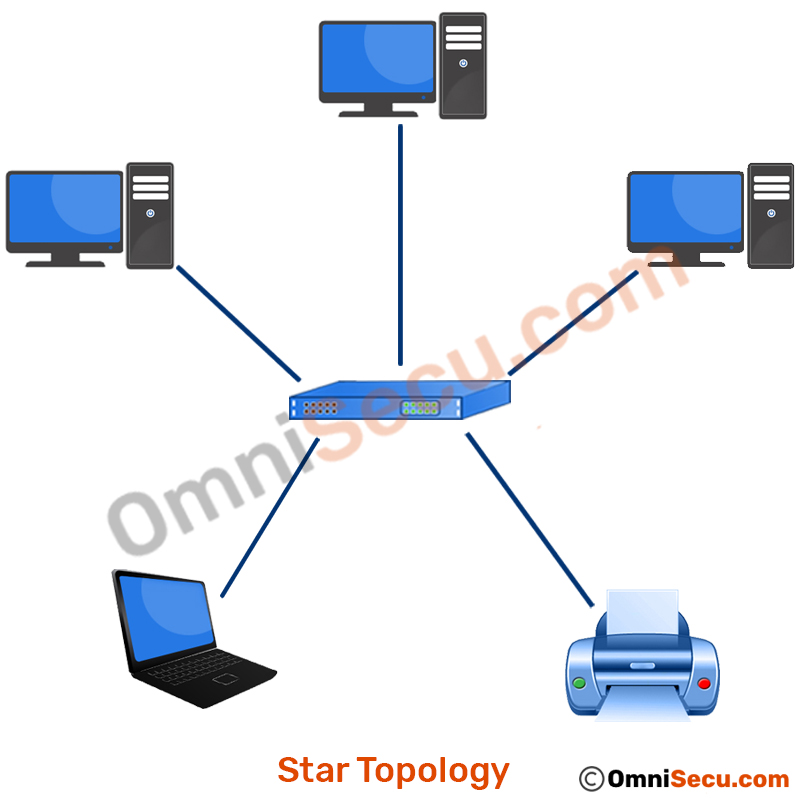
There are five types of topology in computer networks:  


‍

**Here are some of the topologies that are used to create networks:**

**Star Topology**

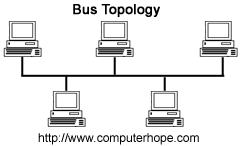
A central node connects a cable to each computer in the network in a star topology. Each computer in the network has an independent connection to the center of the network, and one connection breaking won't affect the rest of the network. However, one downside is that many cables are required to form this kind of network.



‍

‍**Bus Topology**

In a bus topology network connection, one cable connects the computer. The information for the last node on the network has to run through each connected computer. There is less cabling required, but if the cable breaks it means that none of the computers can reach the network.

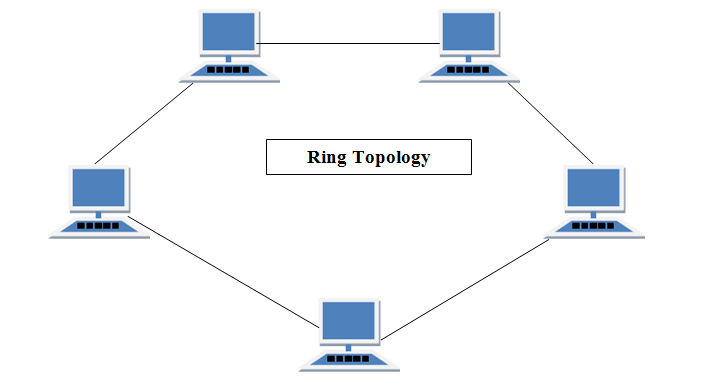


‍

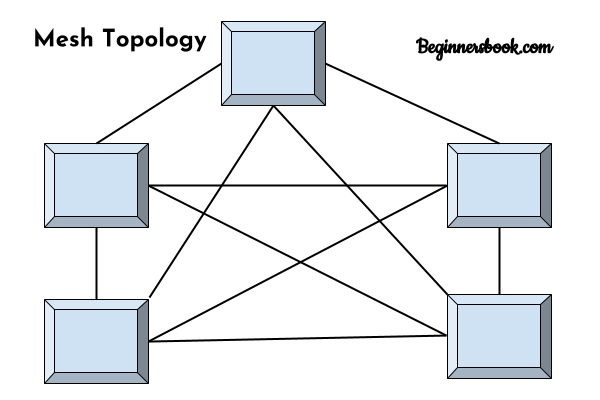
**Ring Topology**

A ring topology is similar to a bus topology. It uses a single cable with the end nodes connected to each other so the signal can circle through the network to find its recipient. The signal will try several times to find its destination even when the network node is not working properly. A collapsed ring has a central node which is a hub, router or switch. The device has an internal ring topology and has places for cable to plug in. Every computer in the network has its own cable to plug into the device. In an office, this probably means having a cabling closet, where all computers are connected to the closet and the switch.

‍

‍

## ‍Mesh Topology

  
In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it means that the link only carries data for the two connected devices only. Lets say we have n devices in the network then each device must be connected with (n-1) devices of the network. Number of links in a mesh topology of n devices would be n(n-1)/2.

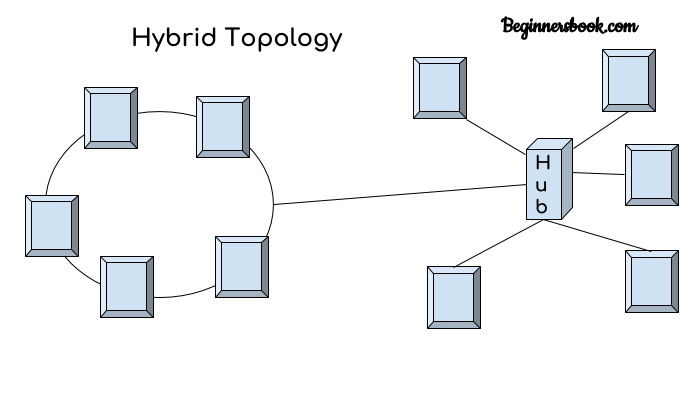
### Advantages of Mesh topology

1. No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.  
2. Mesh topology is reliable and robust as failure of one link doesn’t affect other links and the communication between other devices on the network.  
3. Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.  
4. Fault detection is easy.

### Disadvantages of Mesh topology

1. Amount of wires required to connected each system is tedious and headache.  
2. Since each device needs to be connected with other devices, number of I/O ports required must be huge.  
3. Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link.

## Hybrid topology

  
A combination of two or more topology is known as hybrid topology. For example a combination of star and mesh topology is known as hybrid topology.

### Advantages of Hybrid topology

1. We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.  
2. Scalable as we can further connect other computer networks with the existing networks with different topologies.

### Disadvantages of Hybrid topology

* 1. Fault detection is difficult.  
     2. Installation is difficult.  
     3. Design is complex so maintenance is high thus expensive.

**Tree Topology**:-

* All the computer are connected like the branches of a tree. In Computer Networking, tree topology is known as a combination of a Bus and Start network topology. The main advantages of this topology are better flexibility and scalability.
* Tree network topology is the simplest topology in which only one route exists between any two nodes on the network. The pattern of connection resembles a tree in which all branches spring from one root hence (Tree Topology).

### Tree Topology and Its Advantages and Disadvantages- Snabay Networking

### ****Advantages of Tree Topology****

1. It is a combination of bus and star topology
2. It provides high scalability, as leaf nodes can add more nodes in the hierarchical chain.
3. Other nodes in a network are not affected, if one of their nodes get damaged
4. It provides easy maintenance and fault identification.
5. Supported by several [hardware and software](https://tech.computernetworktopology.com/?p=28) vendors.
6. [Point-to-point](https://computernetworktopology.com/point-to-point-topology/) wiring for individual segments.

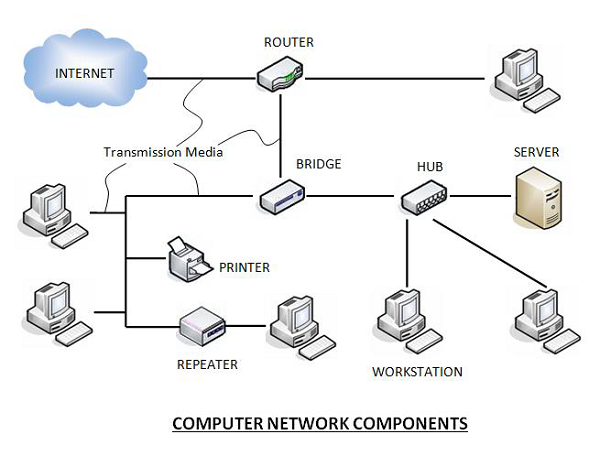
### ****Disadvantages of Tree Topology****

1. Large cabling is required as compared to star and bus topology.
2. On the failure of a hub, the entire network fails.
3. Tree network is very difficult to configure than other [network topologies](https://computernetworktopology.com/).

**Computer Network Components:-**

Computer networks components comprise both physical parts as well as the software required for installing computer networks, both at organizations and at home. The hardware components are the server, client, peer, transmission medium, and connecting devices. The software components are operating system and protocols.

The following figure shows a network along with its components

‍

## ‍Hardware Components

* **Servers** −Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources. Servers can be of various kinds: file servers, database servers, print servers etc.
* **Clients** − Clients are computers that request and receive service from the servers to access and use the network resources.
* **Peers**− Peers are computers that provide as well as receive services from other peers in a workgroup network.
* **Transmission Media** − Transmission media are the channels through which data is transferred from one device to another in a network. Transmission media may be guided media like coaxial cable, fibre optic cables etc; or maybe unguided media like microwaves, infra-red waves etc.
* **Connecting Devices** − Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:

             a. Routers

             b. Bridges

             c. Hubs

             d. Repeaters

             e. Gateways

              f. Switches

## Software Components

* **Networking Operating System** − Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.
* **Protocol Suite** − A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks. The two popular protocol suites are −
  + a. OSI Model ( Open System Interconnections)
  + b. TCP / IP Model

# ‍Computer Network Architecture

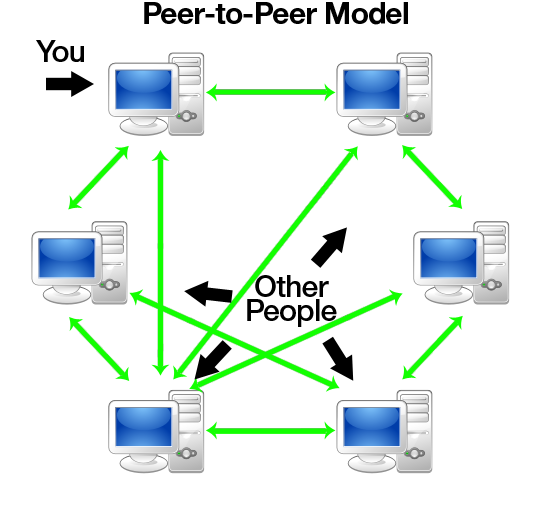
Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

**The two types of network architectures are used:**

* Peer-To-Peer network
* Client/Server network

Peer-To-Peer network

* Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
* Peer-To-Peer network is useful for small environments, usually up to 10 computers.
* Peer-To-Peer network has no dedicated server.
* Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



### Advantages Of Peer-To-Peer Network:

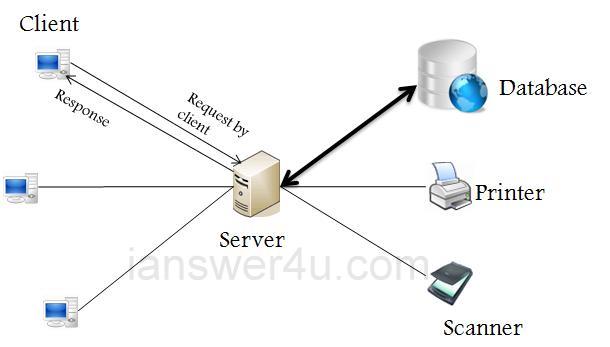
* It is less costly as it does not contain any dedicated server.
* If one computer stops working but, other computers will not stop working.
* It is easy to set up and maintain as each computer manages itself.

### Disadvantages Of Peer-To-Peer Network:

* In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
* It has a security issue as the device is managed itself.

## Client/Server Network

* Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
* The central controller is known as a **server** while all other computers in the network are called **clients**.
* A server performs all the major operations such as security and network management.
* A server is responsible for managing all the resources such as files, directories, printer, etc.
* All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



### Advantages Of Client/Server network:

* A Client/Server network contains the centralized system. Therefore we can back up the data easily.
* A Client/Server network has a dedicated server that improves the overall performance of the whole system.
* Security is better in Client/Server network as a single server administers the shared resources.
* It also increases the speed of the sharing resources.

### Disadvantages Of Client/Server network:

* Client/Server network is expensive as it requires the server with large memory.
* A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
* It requires a dedicated network administrator to manage all the resources.

**Introduction to the OSI Model :-**

• OSI stands for Open Systems Interconnection

• Created by International Standards Organization

• Was created as a framework and reference model to explain how different networking technologies work together and interact

• Is not a standard that networking protocols must follow

‍What the OSI Model Looks Like

• Each layer has specific functions it is responsible for

• All layers work together in the correct order to move data around a network

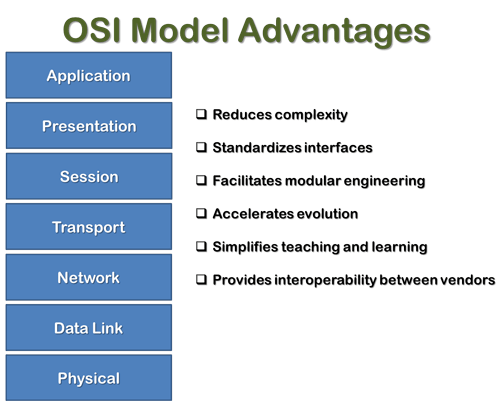
OSI Model Layer Mnemonics

• Top to bottom – All People Seem To Need Data Processing

• Bottom to top – Please Do Not Throw Sausage Pizza Away‍

# OSI Model

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

\*

## Characteristics of OSI Model:

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

**Functions of the OSI Layers**

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

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

**Physical layer**

* The main functionality of the physical layer is to transmit the individual bits from one node to another node.
* It is the lowest layer of the OSI model.
* It establishes, maintains and deactivates the physical connection.
* It specifies the mechanical, electrical and procedural network interface specifications.

## Functions of a Physical layer:

* **Line Configuration:** It defines the way how two or more devices can be connected physically.
* [**Data Transmission**](https://www.javatpoint.com/computer-network-transmission-modes)**:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
* [**Topology**](https://www.javatpoint.com/computer-network-topologies)**:** It defines the way how network devices are arranged.
* **Signals:** It determines the type of the signal used for transmitting the information.

### Data-Link Layer

* This layer is responsible for the error-free transfer of data frames.
* It defines the format of the data on the network.
* It provides a reliable and efficient communication between two or more devices.
* It is mainly responsible for the unique identification of each device that resides on a local network.
* It contains two sub-layers:
  + **Logical Link Control Layer**
    - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
    - It identifies the address of the network layer protocol from the header.
    - It also provides flow control.
  + **Media Access Control Layer**
    - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
    - It is used for transferring the packets over the network.

## Functions of the Data-link layer

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

### Network Layer

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

## Functions of Network Layer:

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

### Transport Layer

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

**The two protocols used in this layer are:**

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

## Functions of Transport Layer:

* **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
* **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
* **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
* **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
* **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

### Session Layer

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

## Functions of Session layer:

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

### Presentation Layer

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

## Functions of Presentation layer:

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

### Application Layer

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

## Functions of Application layer:

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

# TCP/IP model

* The TCP/IP model was developed prior to the OSI model.
* The TCP/IP model is not exactly similar to the OSI model.
* The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
* The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
* TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

## Functions of TCP/IP layers:

## Network Access Layer

* A network layer is the lowest layer of the TCP/IP model.
* A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
* It defines how the data should be sent physically through the network.
* This layer is mainly responsible for the transmission of the data between two devices on the same network.
* The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
* The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

## Internet Layer

* An internet layer is the second layer of the TCP/IP model.
* An internet layer is also known as the network layer.
* The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

### Following are the protocols used in this layer are:

**IP Protocol:** IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

* **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
* **Host-to-host communication:** It determines the path through which the data is to be transmitted.
* **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
* **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
* **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

**ARP Protocol**

* ARP stands for **Address Resolution Protocol**.
* ARP is a network layer protocol which is used to find the physical address from the IP address.
* **The two terms are mainly associated with the ARP Protocol:**
  + **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  + **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

**ICMP Protocol**

* **ICMP** stands for Internet Control Message Protocol.
* It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
* A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
* An ICMP protocol mainly uses two terms:
  + **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
  + **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
* The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
* ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

## Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

* **User Datagram Protocol (UDP)**
  + It provides connectionless service and end-to-end delivery of transmission.
  + It is an unreliable protocol as it discovers the errors but not specify the error.
  + User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
  + **UDP consists of the following fields:**  
    **Source port address:** The source port address is the address of the application program that has created the message.  
    **Destination port address:** The destination port address is the address of the application program that receives the message.  
    **Total length:** It defines the total number of bytes of the user datagram in bytes.  
    **Checksum:** The checksum is a 16-bit field used in error detection.
  + UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.
* **Transmission Control Protocol (TCP)**
  + It provides a full transport layer services to applications.
  + It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
  + TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
  + At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
  + At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

## Application Layer

* An application layer is the topmost layer in the TCP/IP model.
* It is responsible for handling high-level protocols, issues of representation.
* This layer allows the user to interact with the application.
* When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
* There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

### Following are the main protocols used in the application layer:

* **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
* **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
* **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
* **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
* **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
* **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

**Difference between TCP/IP and OSI Model:**

|  |  |
| --- | --- |
| **TCP/IP** | **OSI** |
| TCP refers to Transmission Control Protocol. | OSI refers to Open Systems Interconnection. |
| TCP/IP has 4 layers. | OSI has 7 layers. |
| TCP/IP is more reliable | OSI is less reliable |
| TCP/IP does not have very strict boundaries. | OSI has strict boundaries |
| TCP/IP follow a horizontal approach. | OSI follows a vertical approach. |
| TCP/IP uses both session and presentation layer in the application layer itself. | OSI uses different session and presentation layers. |
| TCP/IP developed protocols then model. | OSI developed model then protocol. |
| Transport layer in TCP/IP does not provide assurance delivery of packets. | In OSI model, transport layer provides assurance delivery of packets. |
| TCP/IP model network layer only provides connection less services. | Connection less and connection oriented both services are provided by network layer in OSI model. |
| Protocols cannot be replaced easily in TCP/IP model. | While in OSI model, Protocols are better covered and is easy to replace with the change in technology. |

**Transmission Impairment**

n communication system, analog signals travel through transmission media, which tends to deteriorate the quality of analog signal, which means that the signal at the beginning of the medium is not the same as the signal  at the end of the medium. The imperfection causes signal impairment. Below are the causes of the impairment.

**Causes of impairment –**

* **Attenuation –** It means loss of energy. The strength of signal decreases with increasing distance which causes loss of energy in overcoming resistance of medium. This is also known as attenuated signal. Amplifiers are used to amplify the attenuated signal which gives the original signal back and compensate for this loss.
* Image Source –

Attenuation is measured in **decibels(dB)**. It measures the relative strengths of two signals or one signal at two different point. 

* **Distortion –** It means changes in the form or shape of the signal. This is generally seen in composite signals made up with different frequencies. Each frequency component has its own propagation speed travelling through a medium. And thats why it delay in arriving at the final destination Every component arrive at different time which leads to distortion. Therefore, they have different phases at receiver end from what they had at senders end.
* **Noise –** The random or unwanted signal that mixes up with the original signal is called noise. There are several types of noise such as induced noise, crosstalk noise, thermal noise and impulse noise which may corrupt the signal.

**Induced** noise comes from sources such as motors and appliances. These devices act as sending antenna and transmission medium act as receiving antenna. **Thermal** noise is movement of electrons in wire which creates an extra signal. **Crosstalk** noise is when one wire affects the other wire. **Impulse** noise is a signal with high energy that comes from lightning or power lines 

* To find the theoretical bit rate limit, we need to know the ration .The signal-to-noise ratio is defined as

**SNR = AVG SIGNAL POWER / AVG NOISE POWER**

**SNRdB = 10Log10SNR**

**What is 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.

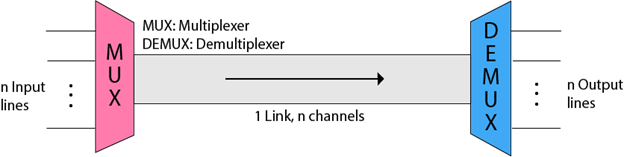
Why Multiplexing?

* 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.

Concept of Multiplexing



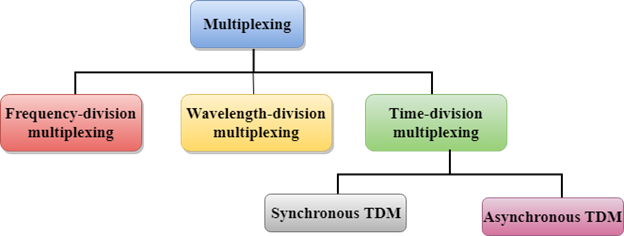
* The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
* The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

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

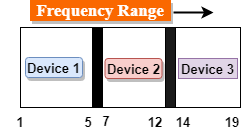
Multiplexing Techniques

Multiplexing techniques can be classified as:

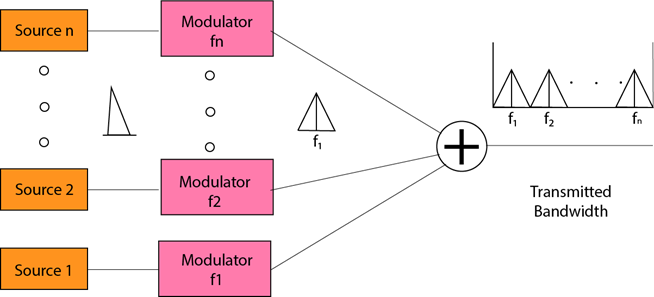


Frequency-division Multiplexing (FDM)

* 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.

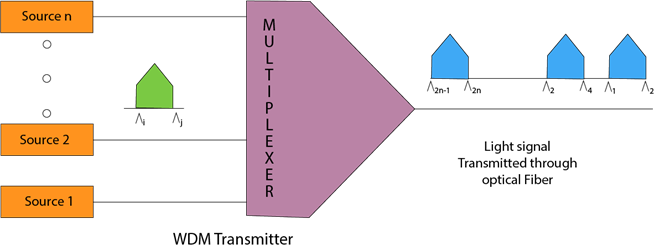
**Disadvantages Of FDM:**

* 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.

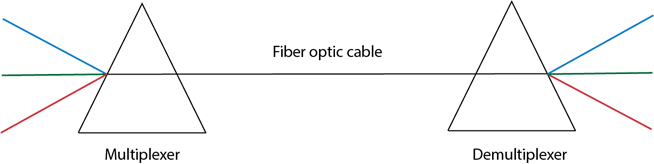
**Applications Of FDM:**

* 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)**



* 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

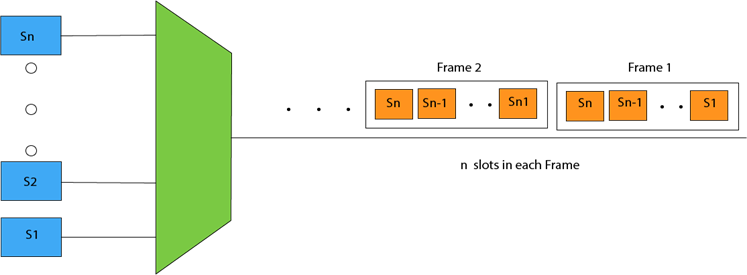
* It is a digital technique.
* In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
* In **Time Division Multiplexing technique**, 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:**

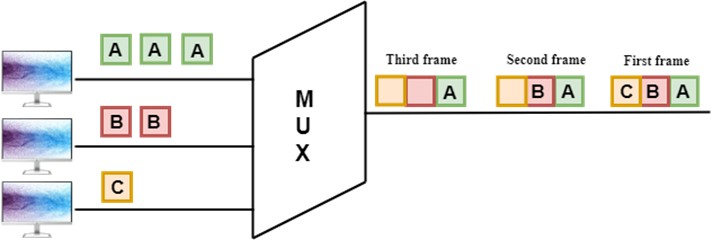
* Synchronous TDM
* Asynchronous TDM

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.

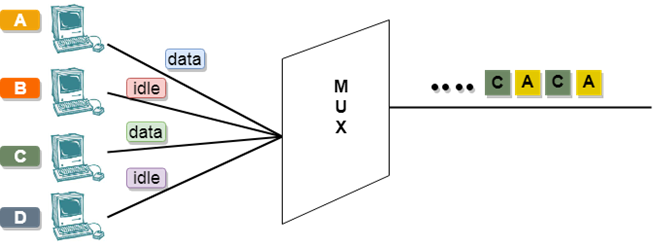
Asynchronous TDM

* 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.

Multiplexing Techniques

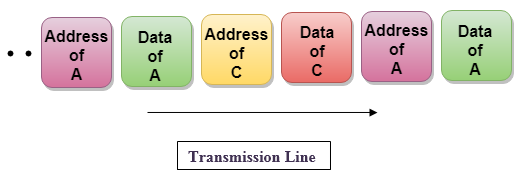
* The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.
* In Synchronous TDM, if there are 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.

# What is Switching?

orking, **Switching** is the process of transferring data packets from one device to another in a network, or from one network to another, using specific devices called **switches**. A computer user experiences switching all the time for example, accessing the Internet from your computer device, whenever a user requests a webpage to open, the request is processed through switching of data packets only.Switching takes place at the Data Link layer of the OSI Model. This means that after the generation of data packets in the Physical Layer, switching is the immediate next process in data communication. In this article, we shall discuss different processes involved in switching, what kind of hardware is used in switching, etcA switch is a dedicated piece of computer hardware that facilitates the process of switching i.e., incoming data packets and transferring them to their destination. A switch works at the [Data Link layer](https://www.geeksforgeeks.org/data-link-layer/) of the [OSI Model](https://www.geeksforgeeks.org/layers-of-osi-model/). A switch primarily handles the incoming data packets from a source computer or network and decides the appropriate port through which the data packets will reach their target computer or networkA switch decides the port through which a data packet shall pass with the help of its destination [MAC](https://www.geeksforgeeks.org/introduction-of-mac-address-in-computer-network/)(Media Access Control) Address. A switch does this effectively by maintaining a switching table, (also known as forwarding table).

A network switch is more efficient than a network Hub or repeater because it maintains a switching table, which simplifies its task and reduces congestion on a network, which effectively improves the performance of the network.

Process of Switching

The switching process involves the following steps:

**Frame Reception:** The switch receives a data frame or [packet](https://www.geeksforgeeks.org/what-is-packet-sniffing/) from a computer connected to its ports.

* **MAC Address Extraction:** The switch reads the header of the [data frame](https://www.geeksforgeeks.org/python-pandas-dataframe/) and collects the destination [MAC Address](https://www.geeksforgeeks.org/introduction-of-mac-address-in-computer-network/) from it.
* **MAC Address Table Lookup:** Once the switch has retrieved the MAC Address, it performs a lookup in its [Switching](https://www.geeksforgeeks.org/what-is-cut-through-switching/) table to find a port that leads to the MAC Address of the data frame.
* **Forwarding Decision and Switching Table Update:** If the switch matches the destination MAC Address of the frame to the MAC address in its switching table, it forwards the data frame to the respective port. However, if the destination MAC Address does not exist in its forwarding table, it follows the [flooding process](https://www.geeksforgeeks.org/how-to-prevent-mac-flooding/), in which it sends the data frame to all its ports except the one it came from and records all the MAC Addresses to which the frame was delivered. This way, the switch finds the new MAC Address and updates its [forwarding table](https://www.geeksforgeeks.org/program-for-ip-forwarding-table-lookup/).
* **Frame Transition:** Once the destination port is found, the switch sends the data frame to that port and forwards it to its target computer/network.

## Types of Switching

There are three types of switching methods:

* [Message Switching](https://www.geeksforgeeks.org/message-switching-techniques/)
* [Circuit Switching](https://www.geeksforgeeks.org/circuit-switching-in-computer-network/)
* [Packet Switching](https://www.geeksforgeeks.org/difference-between-message-and-packet-switching/)
  + Datagram Packet Switching
  + Virtual Circuit Packet Switching

Let us now discuss them individually:

**Message Switching:** This is an older switching technique that has become obsolete. In message switching technique, the entire data block/message is forwarded across the entire [network](https://www.geeksforgeeks.org/network-address-translation-nat/) thus, making it highly inefficient.

**Circuit Switching:** In this type of switching, a connection is established between the source and destination beforehand. This connection receives the complete bandwidth of the network until the data is transferred completely.  
This approach is better than [message switching](https://www.geeksforgeeks.org/message-switching-techniques/) as it does not involve sending data to the entire network, instead of its destination only.

**Packet Switching:** This technique requires the data to be broken down into smaller components, data frames, or [packets](https://www.geeksforgeeks.org/steps-of-finding-packets-in-wireshark/). These [data frames](https://www.geeksforgeeks.org/r-data-frames/) are then transferred to their destinations according to the available resources in the network at a particular time.  
This switching type is used in modern computers and even the Internet. Here, each data frame contains additional information about the destination and other information required for proper transfer through network components.

**Datagram Packet Switching:** In Datagram [Packet switching](https://www.geeksforgeeks.org/packet-switching-and-delays-in-computer-network/), each data frame is taken as an individual entity and thus, they are processed separately. Here, no connection is established before data transmission occurs. Although this approach provides flexibility in data transfer, it may cause a loss of data frames or late delivery of the data frames.

**Virtual-Circuit Packet Switching:** In [Virtual-Circuit](https://www.geeksforgeeks.org/virtual-circuit-in-computer-network/) Packet switching, a logical connection between the source and destination is made before transmitting any data. These logical connections are called virtual circuits. Each data frame follows these logical paths and provides a reliable way of transmitting data with less chance of data loss.

**What is the difference between narrowband ISDN and broadband ISDN?**



A narrow set of frequencies is considered in the Narrowband, and communication happens only in those frequencies. Less number of frequency sets are used as it is designed to work only with less frequencies. Broadband covers a wide bandwidth and uses different signals and frequencies in its spectrum.04-Jul-2023

**Broadband vs. Narrowband**

In communications, band is referred to as the range of frequencies (bandwidth) used in the channel. Depending on the size of the band (in terms of kHz, MHz or GHz), and some other properties of the communication channel, they can be categorized as narrowband, broadband and wideband etc. In data communication, bandwidth is measured in terms of bit rate (kbps, Mbps etc).

**Narrowband**

In radio, narrowband communication happens in a frequency range, where the frequency response of the channel is flat (the gain is constant for all the frequencies in the range). Therefore, the band should be smaller than the coherence bandwidth (maximum range of frequencies where channel response is flat), and relatively smaller than broadband range (or wideband), where channel response is not necessarily flat.

In data communication (or internet connections), narrowband is referred to the amount of data being transferred within a second (or bits per second). Dial-up internet connections (where data rate is less than 56 kbps) belong to the narrowband internet category. In dial up connections, computers are connected to internet through a modem and telephone cables.

**Broadband**

In radio communications, broadband has the similar meaning to wideband, which has a wider frequency range compared to narrowband. Usually, broadband range exceeds the coherence bandwidth, and therefore doesn’t possess a flat frequency response. Broadband is a relative term, and the size of the band may be in kHz, MHz or GHz depending on the application.

For internet connections, the term ‘broadband’ describes the data rate of the connection. Usually, a broadband connection has a higher bandwidth, in Mbps range, compared to narrowband. DSL (Digital Subscriber Line) technologies (such as ADSL and SDSL), HSDPA (High Speed Download Packet Access), WiMAX (Worldwide Interoperability for Microwave Access) are examples for broadband internet technologies.

|  |
| --- |
| **What is the difference between Broadband and Narrowband?**  1. Narrowband communications use a smaller frequency range (bandwidth) compared to broadband communications.  2. In internet access, broadband technologies provide higher data rate in terms of Mbps, whereas narrowband connections provide slower data rate such as 56 kbps.  3. In radio communications, bandwidth is smaller than the coherence bandwidth of the channel for narrowband, and wider for broadband. |

### 