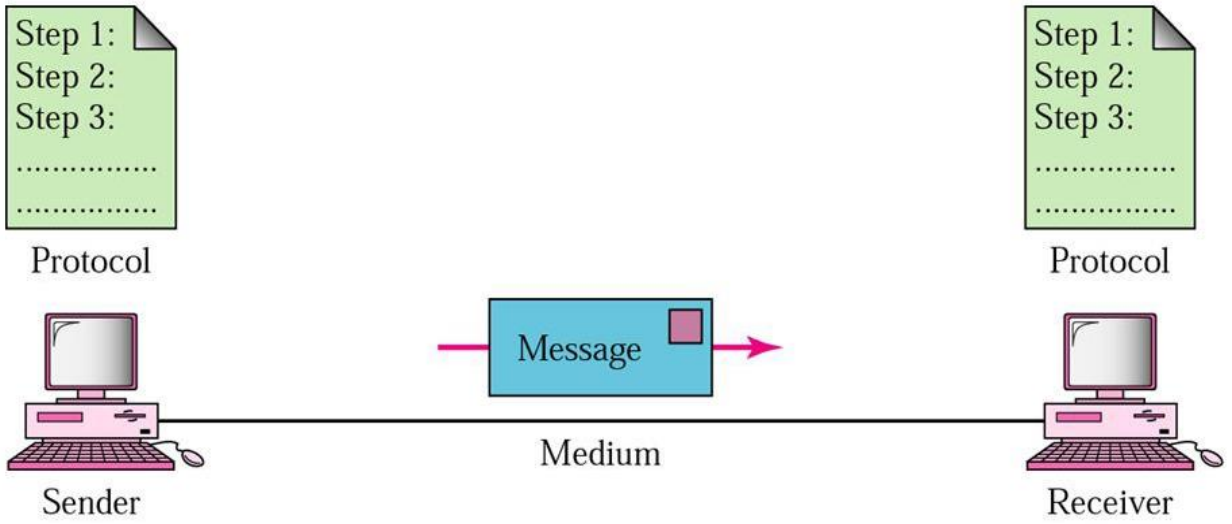
# Concept of network and data communication

Presented by Nimesh Shiwakoti

# What is data communication?

**Data communication** refers to the exchange of data between a source and a receiver via form of transmission media such as a wire cable or wirelessly.

The meanings of source and receiver are very simple. The device that transmits the data is known as source and the device that receives the transmitted data is known as receiver.



Data communications to occurs when the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. Delivery- The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. Accuracy- The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

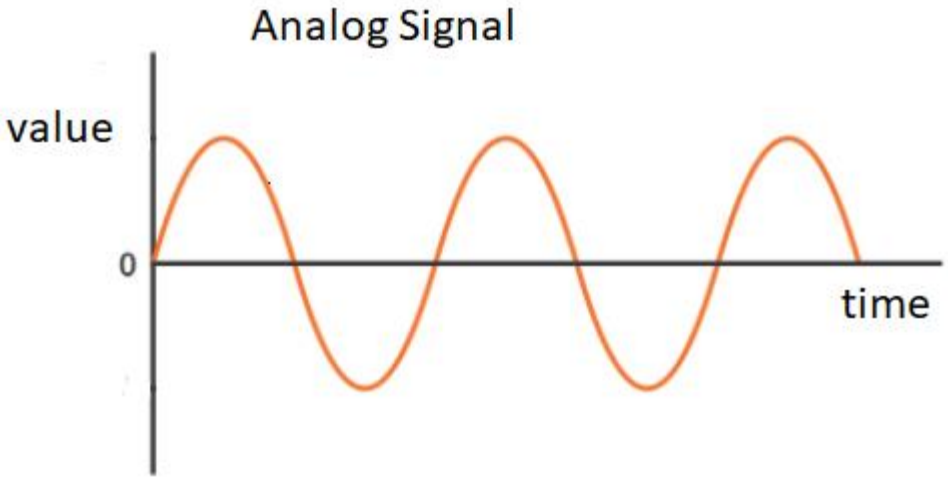
3. Timeliness- The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

4. Jitter- Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

# Signals

- S*ignals* are the electric or electromagnetic impulses used to encode and transmit data. Data is then transmitted through some medium, such as a cable or the airwaves. The receiving node then reverses the conversion and turns the electronic pulses or waveforms back into the 0’s and 1’s that represent the original data.
- Both the sending and receiving node have to understand the encoding technique, or language, that is applied during the conversions. Encoding can be proprietary, such as the language used by a DSL modem or a microwave satellite, or universal and based on a known open source standard.
- There are two type of signals they are analog and digital signal

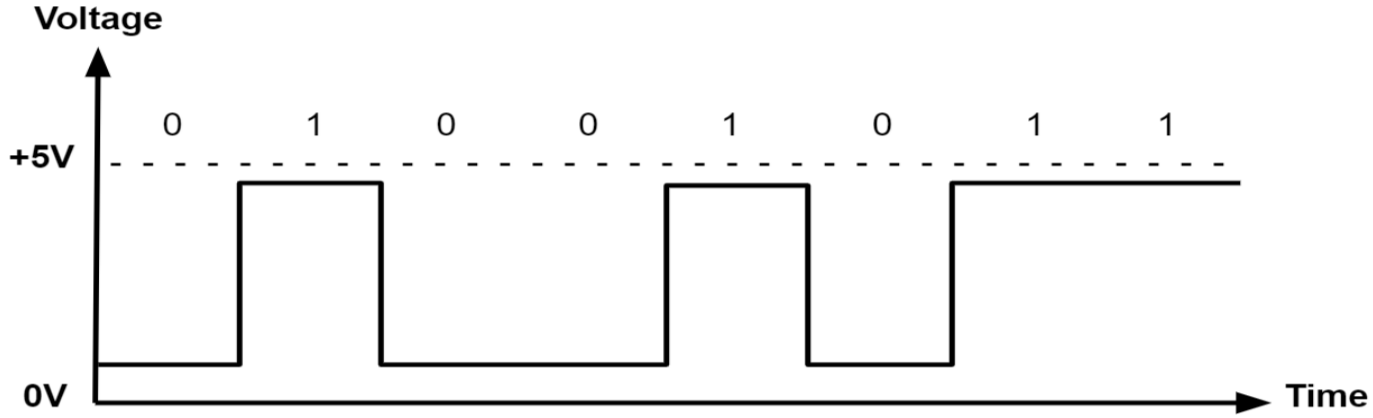
# Analog signal




Analog signal is **a continuous signal** which varies in amplitude, phase, or some other property in proportion to that of a variable.

Analog is best explained by the transmission of signal such as sound or human speech, over an electrified copper wire. In its native form, human speech is an oscillatory disturbance in the air. Which varies in terms of its volume or power (amplitude) and its pitch or tone (frequency)? Analogous variations in electrical or radio waves are created in order to transmit the analog information signal for video or audio or both over a network from a transmitter (TV station or CATV source) to a receiver (TV set, computer connected with antenna). At the receiving end an approximation (analog) of the original information is presented.

# Digital Signal




digital signal is a signal that represents data as a sequence of discrete values. A digital signal can only take on one value from a finite set of possible values at a given time.

Simple digital signals represent information in discrete bands. In most digital circuits, the signal can have two possible valid values; this is called a **binary signal** or **logic signal**. They are represented by two voltage bands: one near a reference value (typically termed as *ground* or zero volts), and the other a value near the supply voltage. These correspond to the two values "zero" and "one" (or "false" and "true") of the Boolean domain, so at any given time a binary signal represents one binary digit (bit). i.e. 0 or 1

# Transmission Impairments

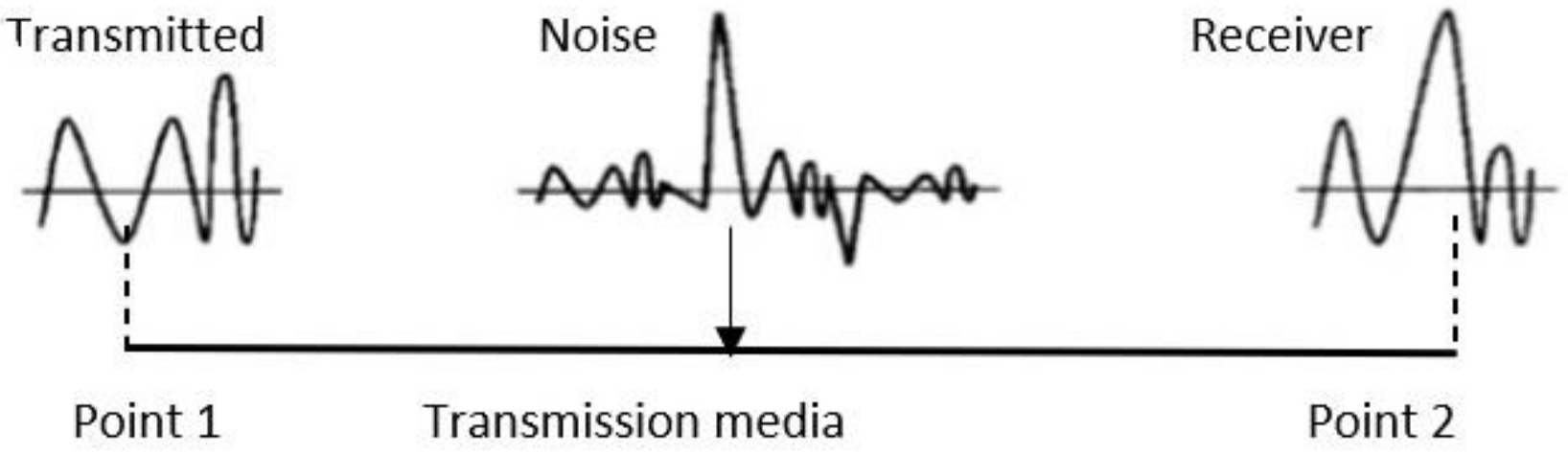
Transmission impairment occurs when the received signal is different from the transmitted signal. As we know, a signal can be transmitted as Analog signal or it can be transmitted as a digital signal.

In Analog signals due to transmission impairment the resulting received signal gets different amplitude or the shape. In the case of digitally transmitted signals at the receiver side we get changes in bits (0's or 1's).

# There are various causes of transmission impairments

**Noise**

Noise is the major factor for the transmission distortion as any unwanted signal gets added to the transmitted signal by which the resulting transmitted signal gets modified and at the receiver side it is difficult to remove the unwanted noise signal. These noises are various kinds like shot noise, impulse noise, thermal noise etc.

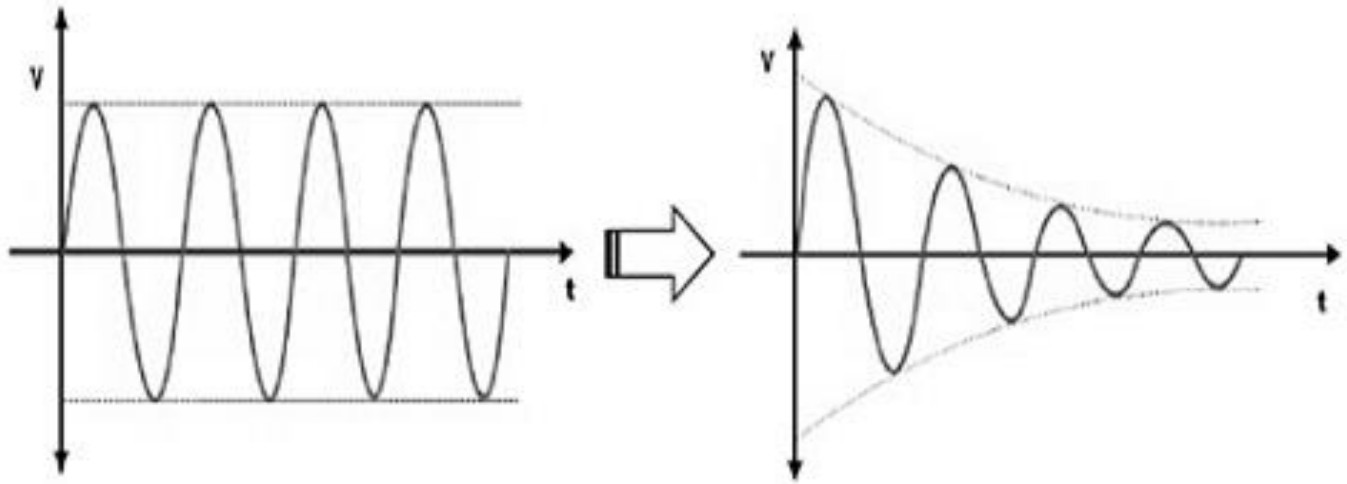


# Distortion

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies.

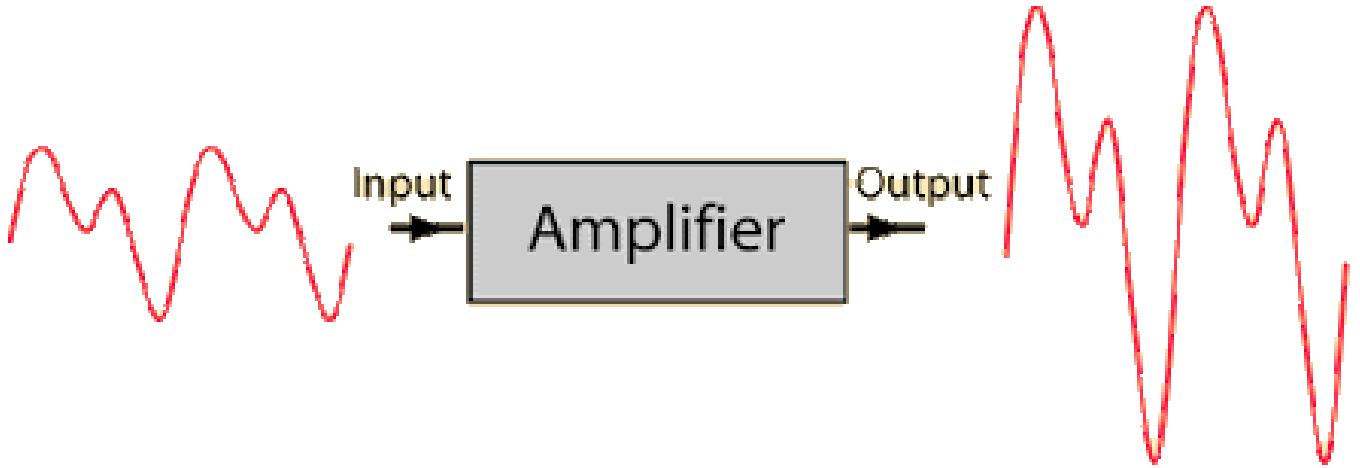
# Attenuation

Attenuation is generally decreased in signal strength, by which the received signal will be difficult to receive at the receiver end. This attenuation happens due to the majority factor by environment as environment imposes a lot of resistance and the signal strength decreases as it tries to overcome the resistance imposed.



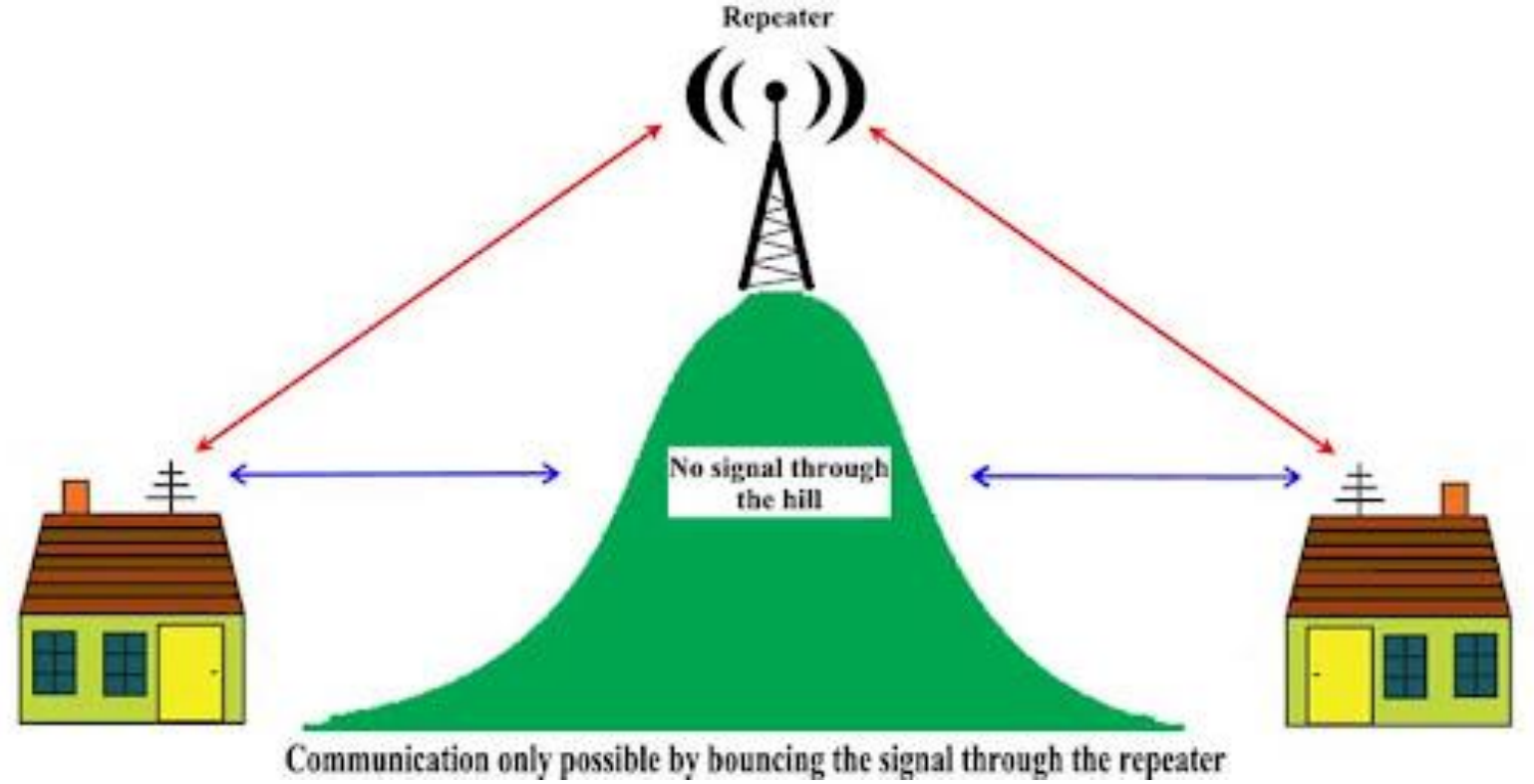
# Amplification

The amplification of signals is defined as **an increase in the intensity of a signal using an electronic circuit knows as amplifier.**



# Repeater

**Repeater** is an electronic device that receives a signal and retransmits it. Repeaters are used to extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction.



# Modulation

Modulation is the process of encoding information from a message source in a way that is suitable for transmission. This is achieved by altering the characteristics of a wave. By superimposing a message on to a high frequency signal known as a carrier wave (or sinusoidal signal), video, voice and other data can be transmitted.

In the modulation process, a parameter of the carrier wave (such as amplitude, frequency or phase) is varied in accordance with the modulating signal. This variation acts as a code for data transmission.

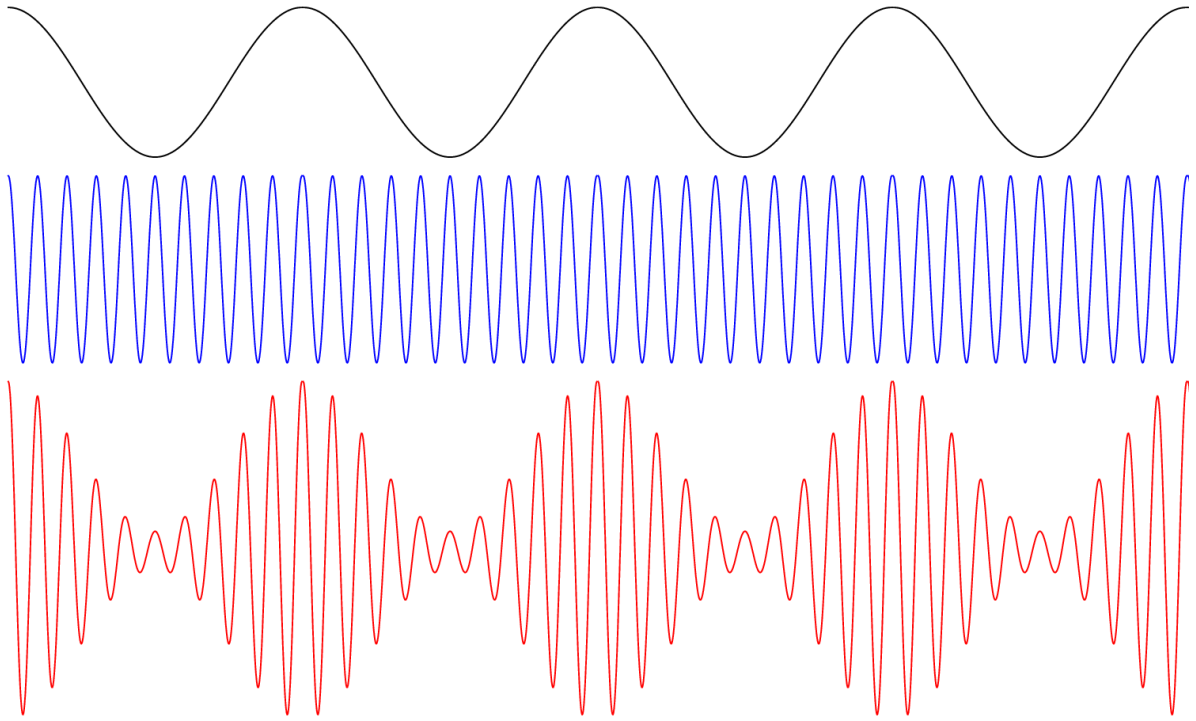
This modulated signal is then transmitted by the transmitter.

The receiver demodulates the received modulated signal and gets the original information signal back.

# Types of modulation

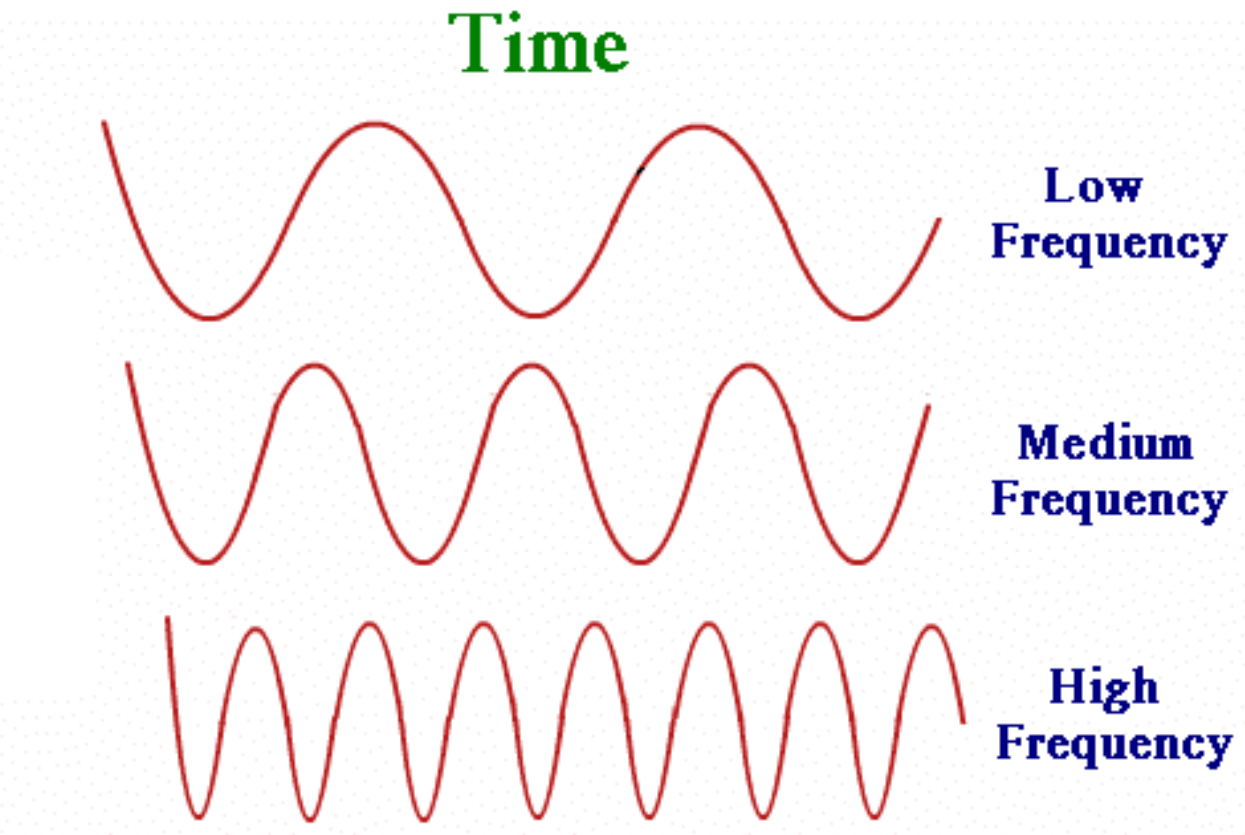
**Amplitude modulation (A.M.)**

Amplitude modulation or AM is the method of varying the instantaneous amplitude of carrier signal accordingly with instantaneous amplitude of message signal.



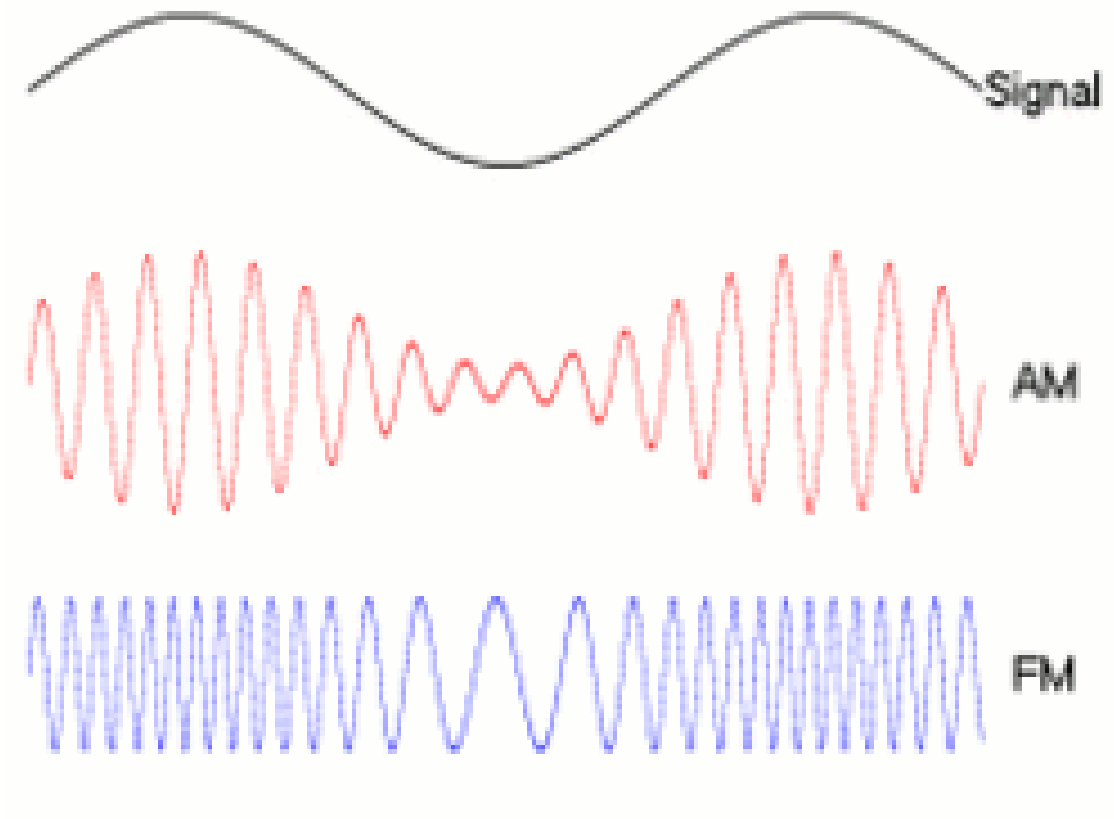
# Frequency

*The frequency of a wave is the number of waves passing a point in a certain time.*



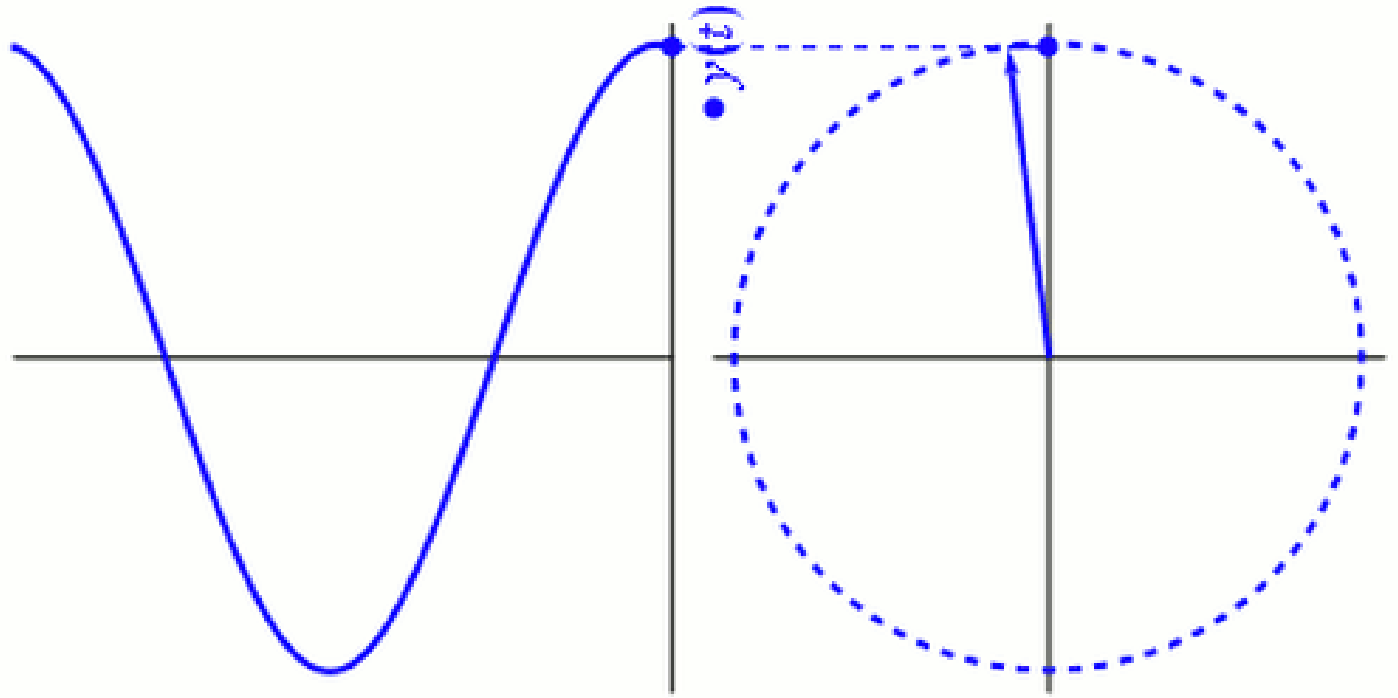
# Frequency Modulation(F.M.)

FM or Frequency modulation is the process of varying the in instantaneous frequency of Carrier signal accordingly with instantaneous amplitude of message signal.



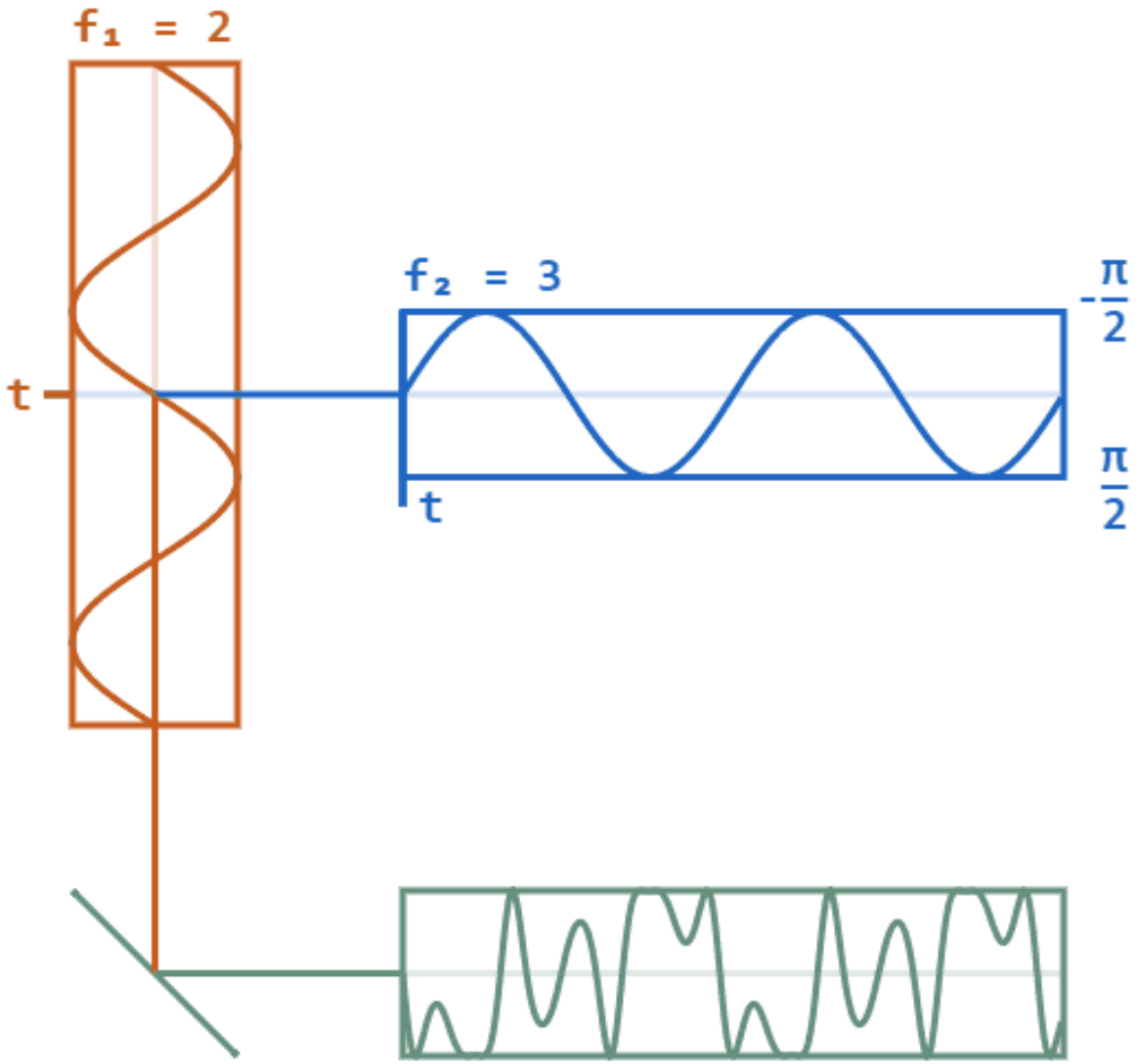
# *Phase*

*Phase is the position of a point in time (an instant) on a waveform cycle.*



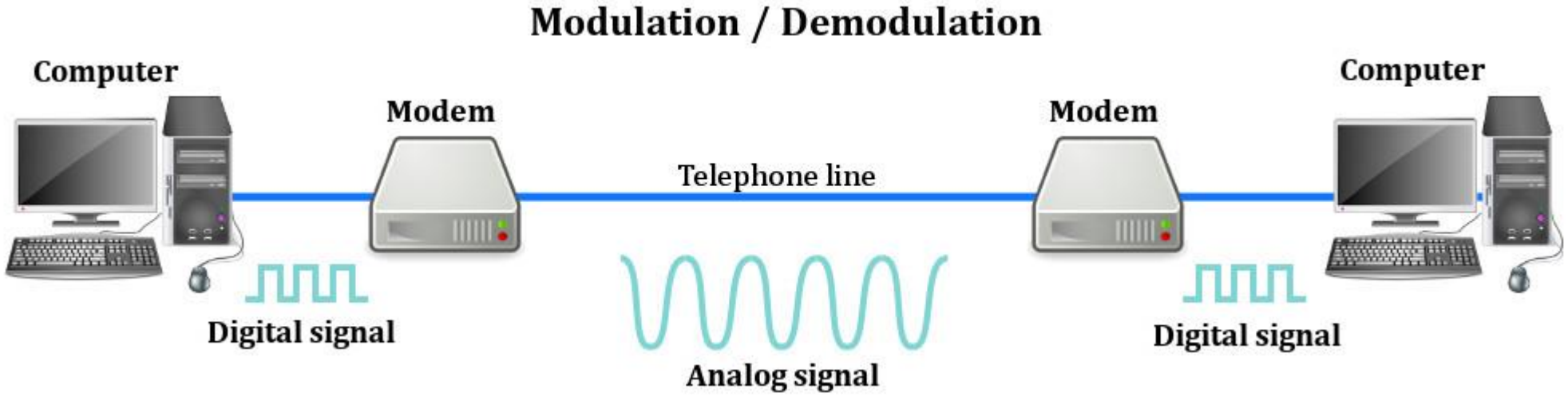
# Phase modulation

PM or Phase modulation is the process of varying the instantaneous phase of Carrier signal accordingly with instantaneous amplitude of message signal.



# Demodulation

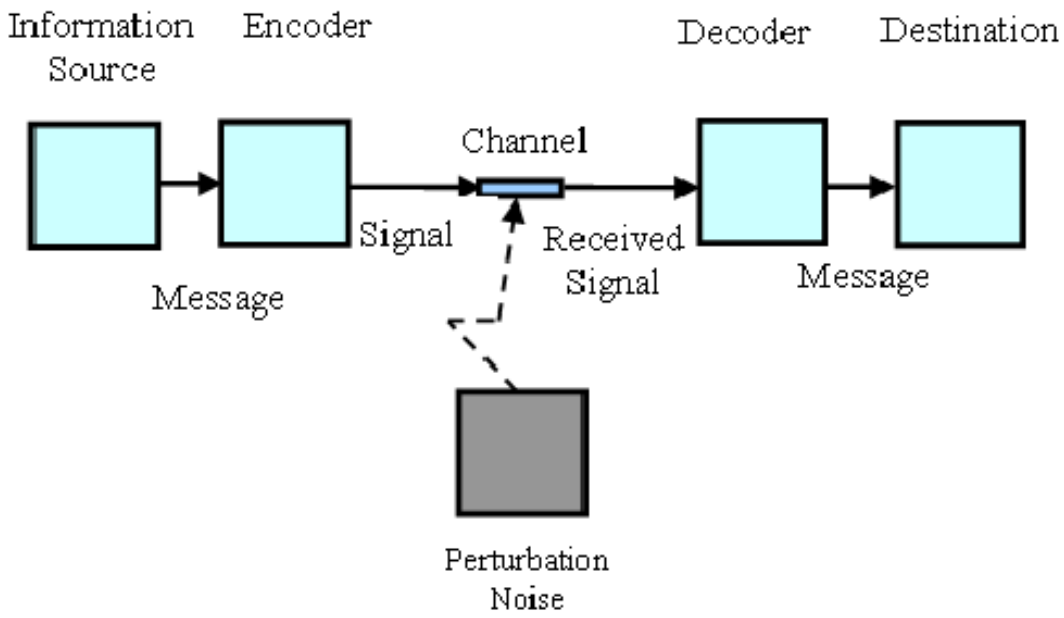
**Demodulation** is the act of extracting  data from this signal once it reaches its destination. A common example of a demodulating device is a modem. Modem can both modulate and demodulate the signal. it was generally used for internet access in circuit switching system. Demodulation are also called as detector



# Communication system

Communication system is a system model describes a communication exchanges between two stations, transmitter and receiver. Signals or information's passes from source to distention through what is called channel, which represents a way that signal use it to move from source toward destination.

To transmit signals in communication system, it must be first processed by several stages, beginning from signal representation, to signal shaping until encoding and modulation. After preparing the transmitted signal, it passed to the transmission line of channel and due signal crossing this media it faces many impairments such noise, attenuation and distortion.



# communication channel

A communication channel is **the medium used to transport information from one network device to another**. Wired channels transport data through wires and cables. Wireless channels transport data from one device to another without the use of cable or wires. Each channel has a frequency for communication which is measured in Hz.

# Elements of data communication

**Message**

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

**Sender**

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

**Receiver**

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

**Transmission Medium**

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

**Set of rules (Protocol)**

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

# Data Transmission mode / communication mode

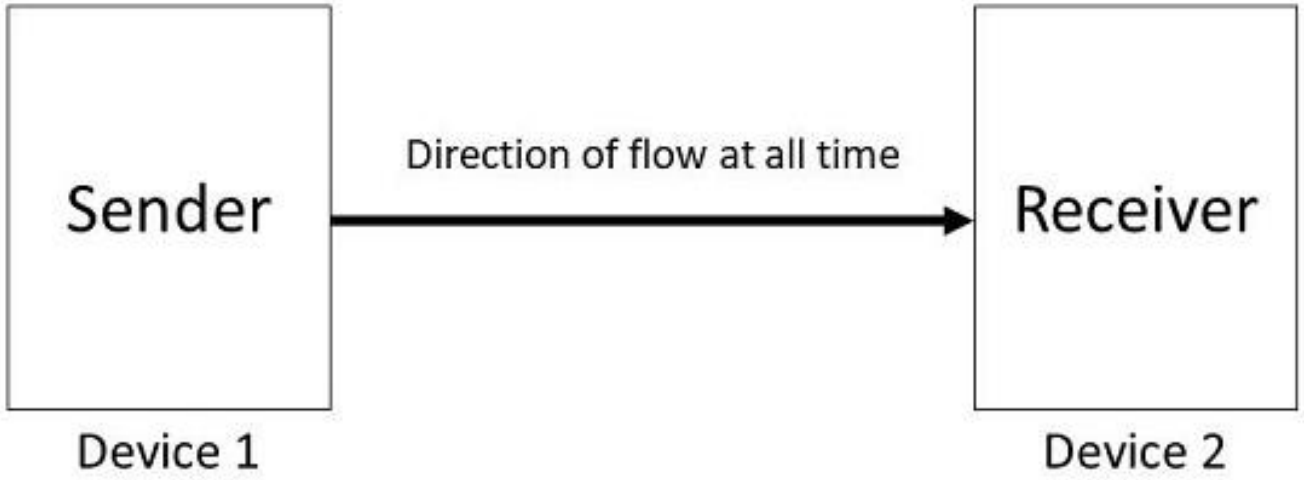
Data Transmission mode defines the direction of the flow of information between two communication devices. It is also called Data Communication or Directional Mode. It specifies the direction of the flow of information from one place to another in a computer network.

***The data transmission modes can be characterized in the following three types based on the direction of exchange of information:***

1. Simplex
2. Half-Duplex
3. Full Duplex

# 1. Simplex

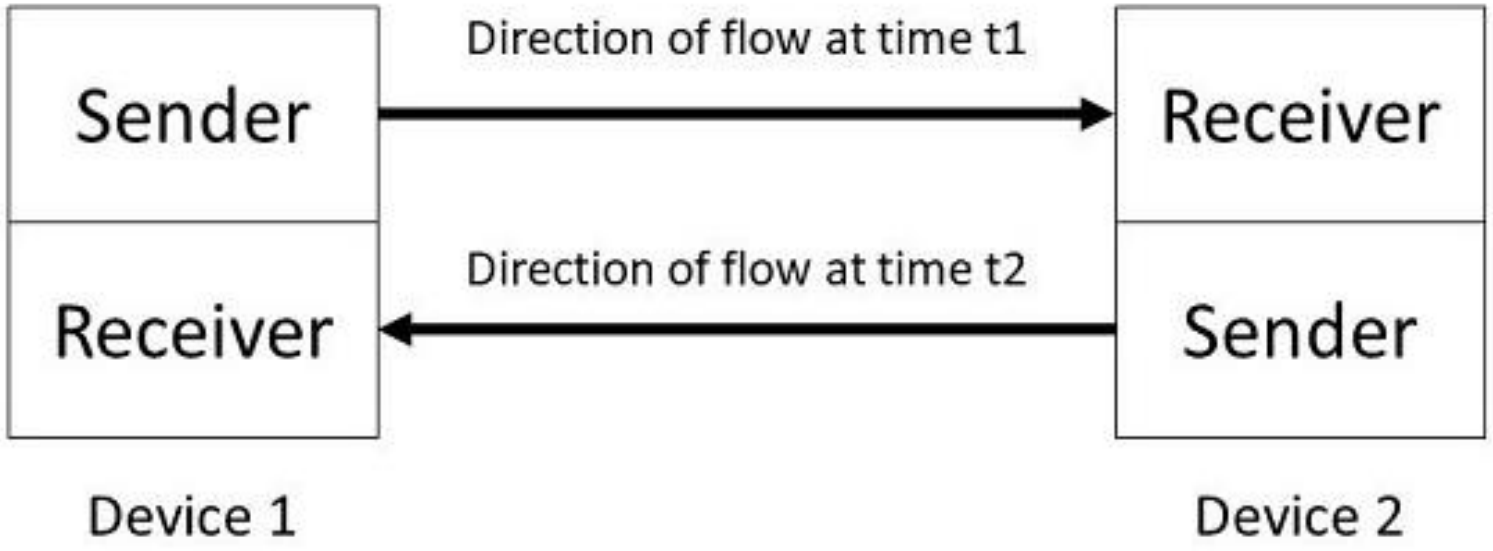
**Simplex is the data transmission mode in which the data can flow only in one direction, i.e., the communication is unidirectional.** In this mode, a sender can only send data but can not receive it. Similarly, a receiver can only receive data but can not send it.




**Simplex Mode**

# 2. Half-Duplex

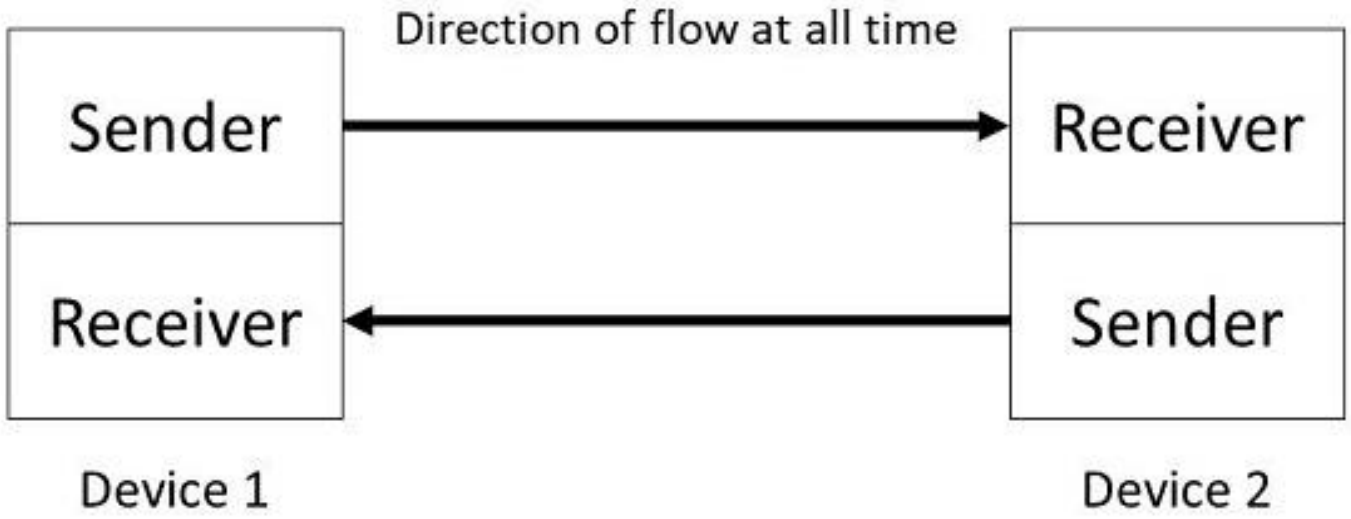
**Half-Duplex is the data transmission mode in which the data can flow in both directions but in one direction at a time. It is also referred to as Semi-Duplex.** In other words, each station can both transmit and receive the data but not at the same time. When one device is sending the other can only receive and vice-versa.




**Half-Duplex Mode**

# 3. Full-Duplex

**Full-Duplex is the data transmission mode in which the data can flow in both directions at the same time. It is bi-directional in nature.** It is two-way communication in which both the stations can transmit and receive the data simultaneously.




**Full-Duplex Mode**

# Distinguish between Analog and Digital signals.

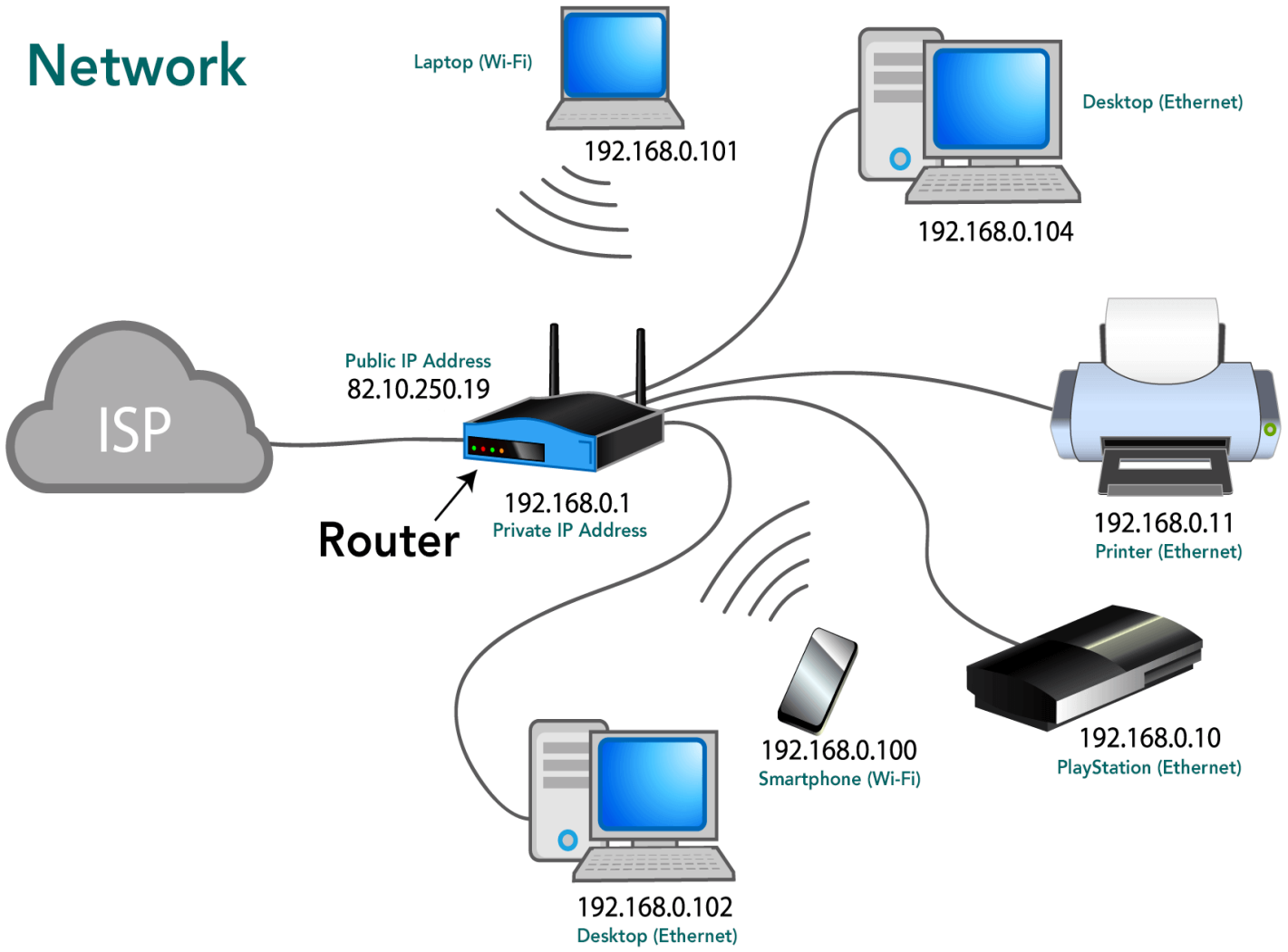
| **Analog signal** | **Digital signal** |
|---|---|
| Analog signals are continuous signals. | Digital signals are not continuous, they are discrete signals. |
| We can represent analog signals in the form of sign waves. | We can represent digital signals in the form of square waves. |
| The values of voltage will be in a continuous range | The values of voltage will be discontinuous. |
| Records the information as it is. | Converts the information into binary form. |
| These signals are used in analog devices. | Digital electronic devices like computers, smartphones, smartwatches, etc. use these signals |
| Examples: Any natural sound, human voice, data read by analog devices. | Electronic signals, computer signals, data read by digital devices. |

# Computer Network

A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to allow data sharing. An example of a network is **the Internet**, which connects millions of people all over the world.

There are two types of Network

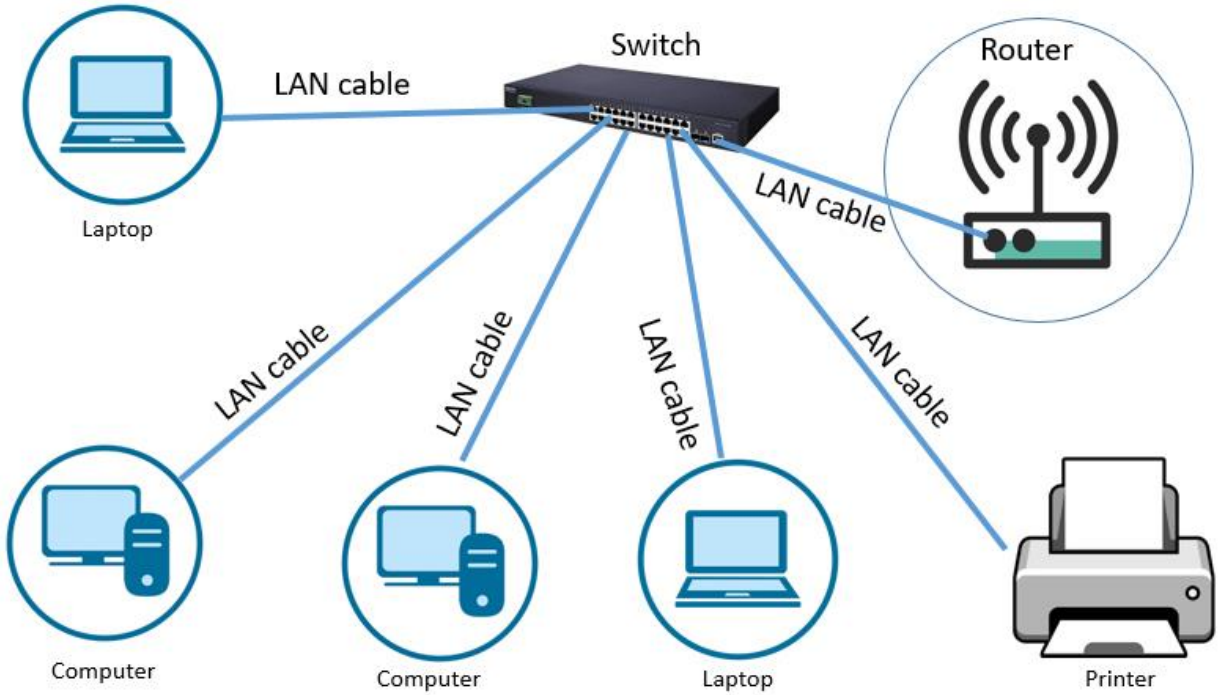
1. LAN (Local area Network)
2. Metropolitan Area Network (MAN)
3. WAN (Wide Area Network)



# Local Area Network (LAN)

A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link to a server. Typically, a LAN encompasses computers and peripherals connected to a server within a distinct geographic area such as an office or a commercial establishment.

Ethernet and Wi-Fi are the two most common technologies in use for local area networks. Speed of LAN are 100 to 1000 Mbps




Local Area Network

# Advantages of LAN

1. **Resource Sharing**

Sharing of resources such as hard disk drives, DVD drives and Printers are made easy in Local Area Network. For an example all the resources can be connected to one single computer with a network so that whenever there is a need of resources it can be shared with the connected computers.

**2. Software Sharing**

Another type of sharing made easy here is the Software sharing. A single computer with the licensed software can be shared among other users in the network. There is no need to purchase individual license for each and every computer in the network. All can be worked under one single license.

**3. Convenient Communication**

Using LAN users can exchange messages and data in a convenient way. Since the data is placed on the server it can be accessed anytime by the LAN users. Every single LAN user can do this with others on the network. Hence, this not only saves lots of time, it ensures that messages get delivered to the right people.

**4. Centralized Data**

As mentioned earlier data of the users are located at the centralized server. Any workstation in a particular network can be used to access this information. Moreover users can access their own set of data by logging into their respective accounts.

**5. Improved Security**

Since data is stored on a local server, it can be guaranteed to be secure. If the data on the server is updated then simply all the LAN users can access them. In addition to that, the host has the capability to deny or allow users in a particular network so that additional security measurements can be imposed.

**6. Internet Sharing**

LAN has the capability to share internet connection among all the LAN users. One single computer with an internet connection shares internet with all the connected computers. This type of infrastructure can be seen in Offices and Netcafes.

# Disadvantages of LAN

**1. Implementation Cost**

Even though LAN saves lots of money in terms of resource sharing, the initial cost involved in setting up the network is quite high. This is mainly due to the requirement of a special software that is needed to make a server. In addition to that purchasing of hardware equipments such as routers, hubs, switches and cables are required for the first time setup.

**2. Security**

Since it is rather easy to gain access to programs and other types of data, security concerns are a big issue in LAN. The sole responsibility to stop unauthorized access is in the hands of LAN administrators. The LAN administrator has to make sure that the centralized data is properly secured by implementing correct set of rules and privacy policies on the server.

## 4. Maintenance

LAN often faces hardware problems and system failure. Hence, it requires a special administrator to look after these issues. The administrator needs to be well knowledgeable in the field of networking and needed at its full time job.

## 5. Area Coverage

LAN is usually made to cover up a limited distance (up to 10km). Most probably it is operated in small areas such as in offices, banks and schools. This is because its cabling system cannot be extended more than a certain range.

## 6. Server Crashes

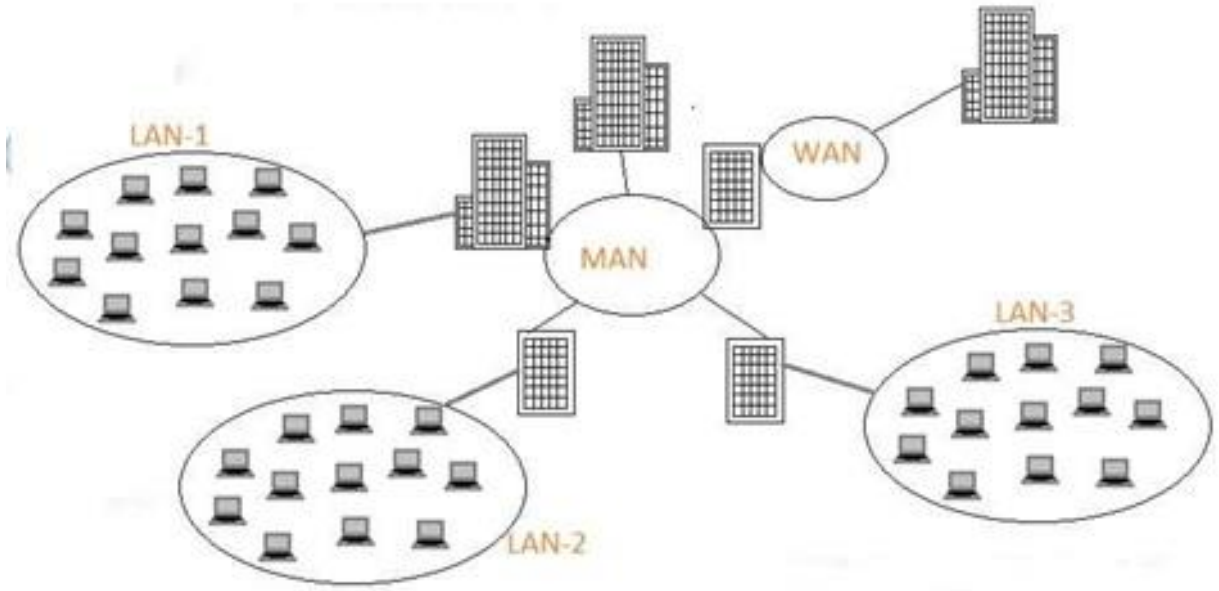
Central server which is present on the LAN architecture manages all the attached computers. If in case the server encounters any faults all the connected computers are affected too. For an example if the files on the server gets corrupted, no more data on the attached computers can be accessible.

## 7. Malware Spreading

Appearance of virus in a LAN based infrastructure is highly dangerous. If one the attached computers are affected with a virus, it can easily spread to the remaining computers present on the network.

# Metropolitan Area Network (MAN)

A metropolitan area network (MAN) is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings. A MAN is larger than a local area network (LAN) but smaller than a wide area network (WAN). MANs do not have to be in urban areas; the term "metropolitan" implies the size of the network, not the demographics of the area that it serves.



# Advantages of a MAN Network

**1: Less Expensive:**
It is less expensive to attach MAN with WAN Network. MAN gives you good efficiency of data. All data on MAN is easily manageable in a centralized way.
**2: Sending Local Emails:**
You can send local emails fast and free on MAN.
**3: High Speed than WAN:**
The speed of data can easily reach 1000 Mbps, as MAN uses fiber optics. Files and database transfer rates are fast.
**4: Sharing of the Internet:**
With the installation of MANs, users can share their internet connection. In this way, multiple users can get the same high-speed internet.
**5: Conversion of LAN to MAN is Easy:**
MAN is a combination of two or more LAN network. So it is a faster way to connect two LAN networks together. It is possible by the fast configuration of links.
**6: High Security:**
MAN’s has a high-security level than WAN.

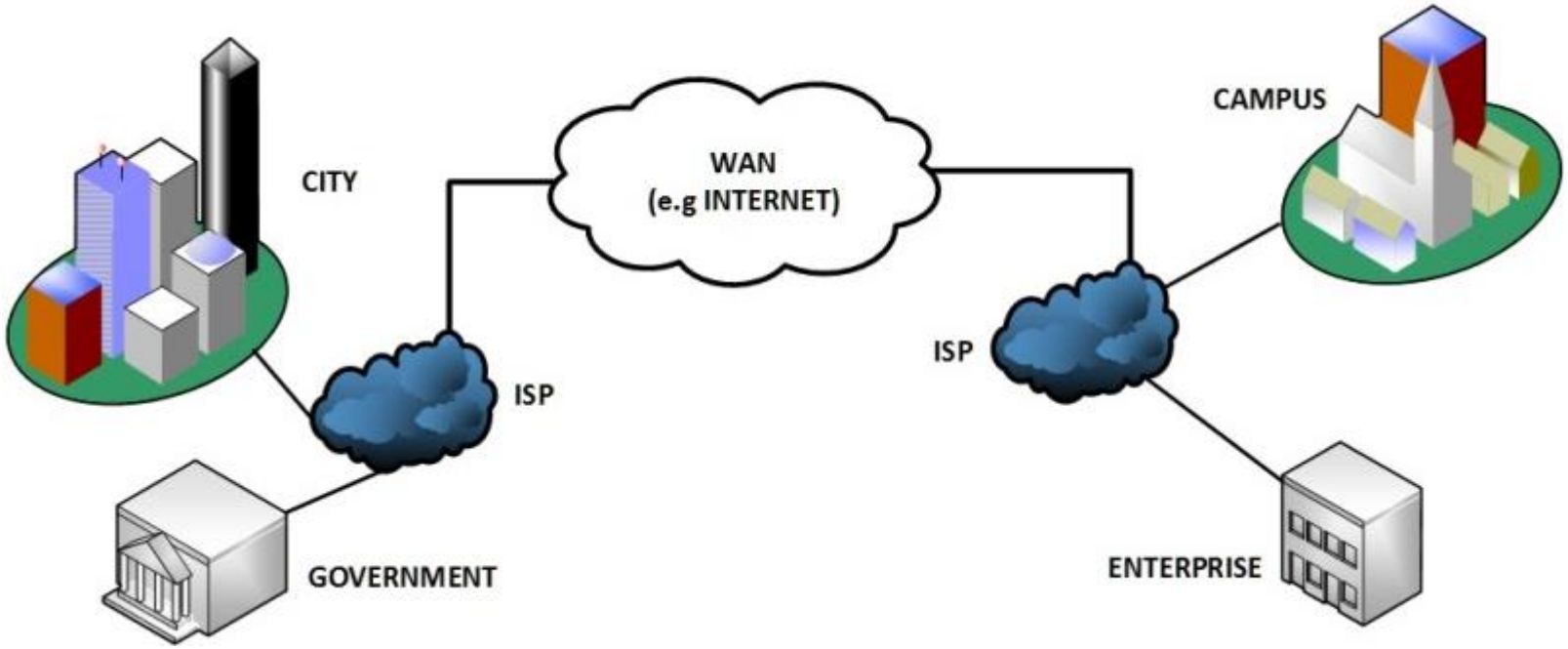
# Disadvantages of MAN Network

**1: Difficult To Manage:**
It is very difficult to manage if the size and number of LANs network increase. This is due to security and extra configuration problems.
**2: Internet Speed Difference:**
As it cannot work on phone copper wires. Copper wires affect the speed of MAN. So high cost is needed for fiber optics.
**3: Hackers Attack:**
In this network, there is a high risk of attacking hackers as compared to LAN. So data may be a leak. Highly security staff is the need in MAN.
**4: Technical Staff Requires to Set up**:
Highly technical people require to setup MAN. The technical people are network administrators and troubleshooters.
**5: Need More wires:**
In MAN more than LAN network, cables require. As you know, it is a combination of two LANs.

# Wide Area Networks(WAN)

In its simplest form, a wide-area network (WAN) is a collection of local-area networks (LANs) or other networks that communicate with one another. A WAN is essentially a network of networks, with the Internet the world's largest WAN. It is larger Network Than MAN.

Today, there are several types of WANs, built for a variety of use cases that touch virtually every aspect of modern life.



# Advantages of Wide Area Network

**1. Area Coverage**

WAN generally covers geographical areas of large proportions (1000kms or more than that). Probably if your business offices are located at different locations, then without an effort all the branches can be communicated through WAN. For this purpose Internet Service Providers (ISPs) can provide leased lines.

**2. Centralized Data**

Using WAN means that you can share the data connected to all the devices in the respective network. For an example you can setup head office server and share the data among all the office branches. Hence, there is no need to purchase separate emails, files and backup servers. Instead you can get all the backup and support from the head office server.

**3. Updated Files**

From WAN users can get updated files and data from the servers. Companies can work to update files from the servers so that all the connected devices can receive them. That too in a fraction of seconds.

**4. Message Exchange**

With the advancement of Internet of Things (IoT) and LAN, a sudden growth of WAN based devices can be seen. From this communication through messages can be done fast with the help of popular applications such as messenger and whatsapp.

**5. Increased Bandwidth**

In order for forming a backbone of a respective network, corporate LAN often uses leased lines. Using leased lines means that there are more bandwidths compared to a standard broadband connection. Ultimately business improvement in productivity can be seen.

**6. Assured Uptime**

Another biggest plus of WAN is that they offer guaranteed uptime. WAN providers offer uptime weekly, quarterly or annually. It is a part of the SLA (service-level agreement). It doesn't matter what the industry is the uptime can be assured.

# Disadvantages of Wide Area Network

**1. Security**

Since WAN has more technologies combined to each other, it faces more security issues comparing to LAN and MAN. This can open a security gap which paves the way for malicious attacks and identity thefts. Besides that WAN posses wide coverage which can be used negatively by people of different computers.

**2. Need of Security Solutions**

As mentioned earlier WAN frequently faces security issues. Probably as a result of the data transfer that can be easily accessed by the hackers. Hence, in every PCs, firewall needs to be enabled. And there are chances where malicious attacks can take place. Therefore, Antivirus software also needs to be installed.

**3. Installation Costs**

WANs are on default complicated and complex basically because of their geographical coverage. Hence, they are expensive to setup. Setting up a WAN requires purchasing of routers, switches and security solutions.

## 4. Disconnection Problems

In some areas especially in remote locations, there is no proper electricity supply or line structure. Due to this customers often face disconnection issues more frequently. For getting rid of this customers are required to purchase a dedicated line from the ISP.

## 5. Troubleshooting Issues

Troubleshooting WAN issues is a difficult task and requires more time. If there are issues in the network, it is difficult to pinpoint the exact cause due to their broad coverage of geographical areas. Moreover wires of the WAN goes under the sea. In case if those wires gets broken, it can be challenging to fix them since it involves lots of resources.

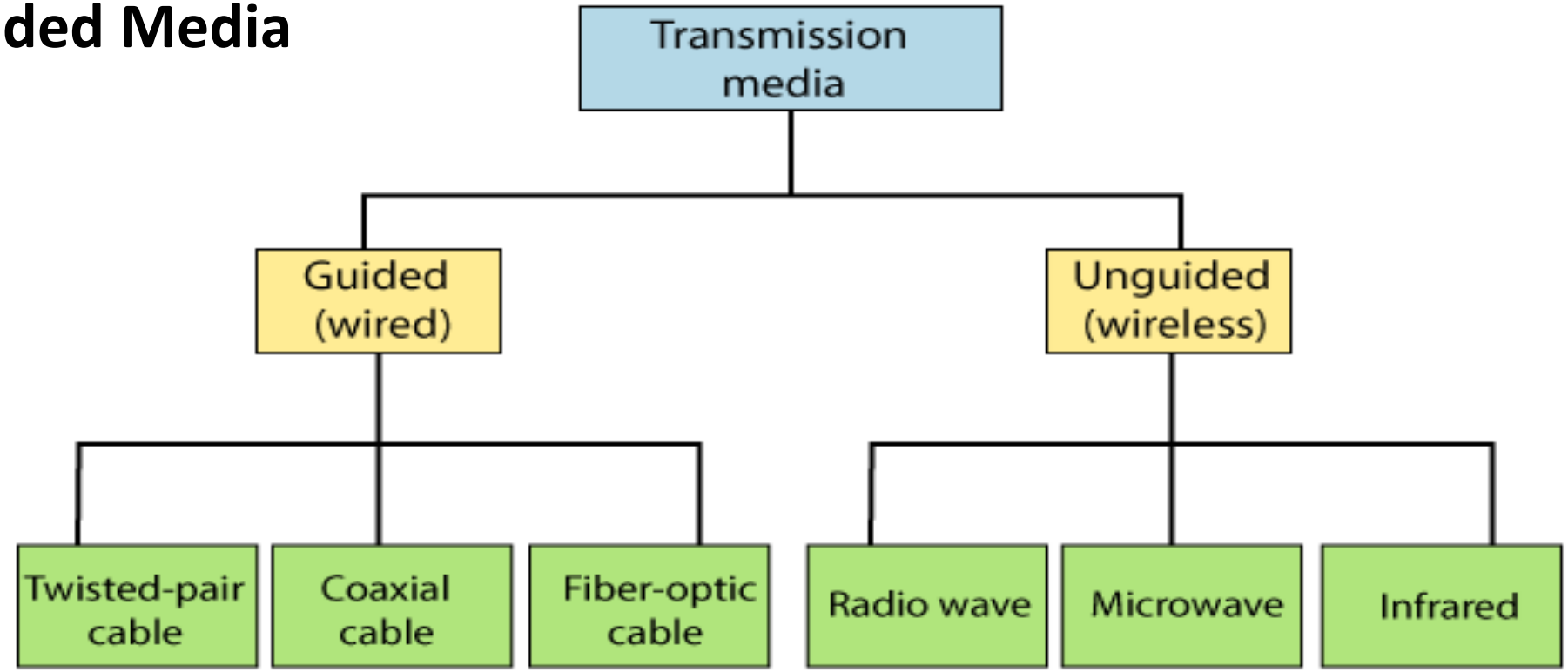
## 6. Maintenance Issues

Maintaining WAN is a difficult task to carry out. Especially maintaining a data center that operates 24/7 is the biggest challenge out of all. It is full time job that needs assistance from network administrators and technicians.

# Transmission Medium

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**
2. **Unguided Media**



# Guided Media

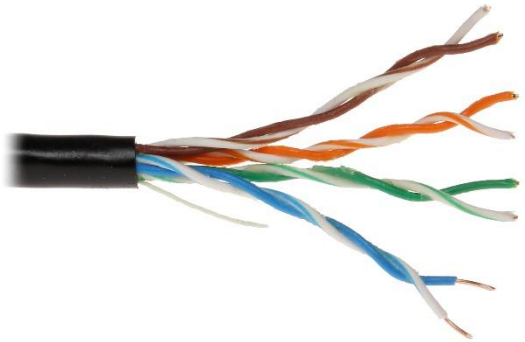
It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

**Features:**

- High Speed
- Secure
- Used for comparatively shorter distances

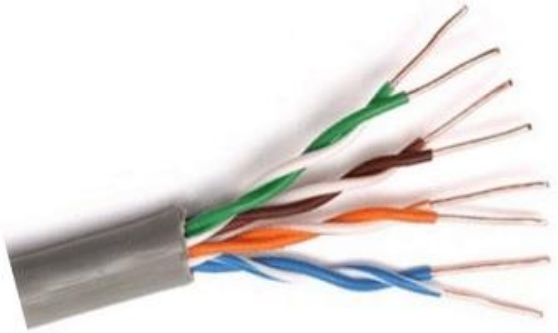
# There are 3 major types of Guided Media:

## (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:

**Unshielded Twisted Pair (UTP):**



UTP consists of two insulated copper wires twisted around one another. 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.

**Shielded Twisted Pair (STP):**

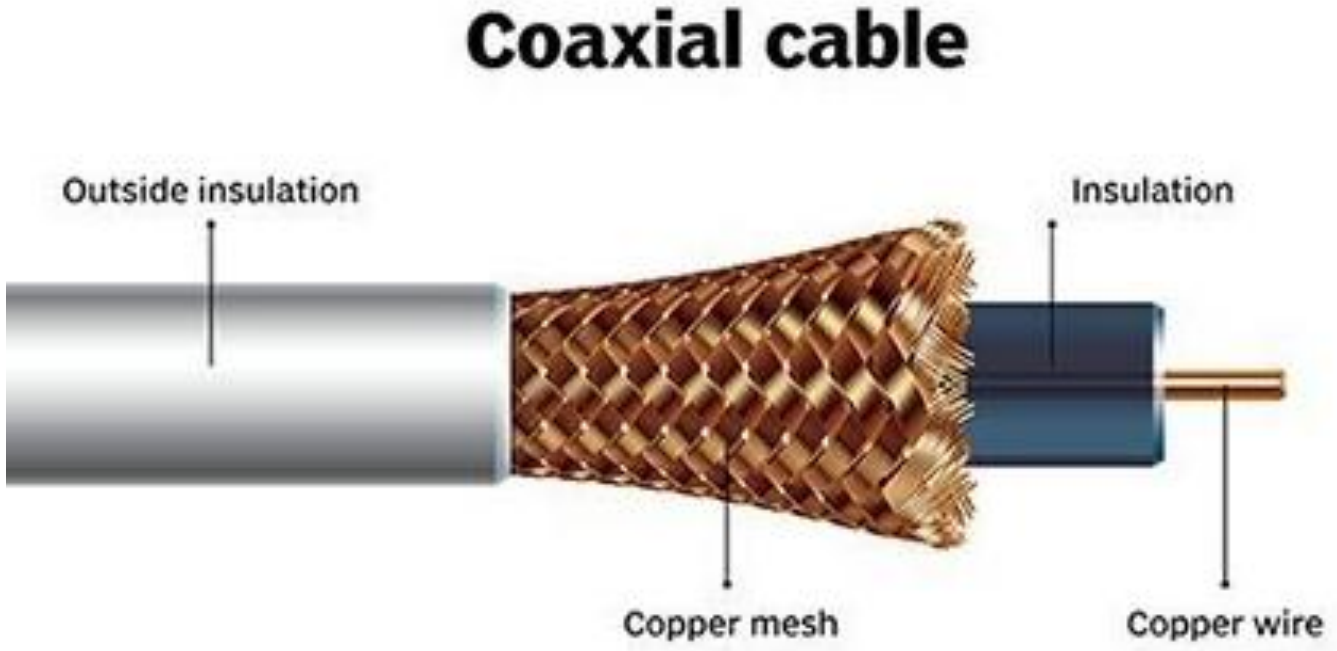
This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

# differences of the UTP and STP

| UTP | STP |
| --- | --- |
| It is an unshielded twisted pair. | It is a shielded twisted pair. |
| UTP cable is a twisted pair cable with wires that are twisted together. | It is enclosed within a foil or mesh shield. |
| The price of UTP is lower as compared to the STP. | The price of STP is much costlier than UTP. |
| It does not require a grounding cable. | It requires a grounding cable. |
| In UTP, the electromagnetic interference is more than the STP while transferring the signal to the transmission media. | It reduces electromagnetic interference while transferring the signal to the transmission media. |
| UTP has high crosstalk. | STP has low crosstalk. |
| Transferring speed of the data signal is slow as compared to the STP. | Transferring speed of the data signal is high as compared to the UTP. |
| Installation of UTP cables is easy as they are lighter, small in size, and flexible. | Installation of STP cable is quite difficult as compared to the UTP. Its size is heavy, bigger, and stiffer. |
| It does not require much maintenance. | It requires more maintenance. |
| UTP cables are noisier. | STP cables are less noisy. |
| However, the UTP cable is used to establish the connection within a short distance, like a home or small industry. | Generally, it is used to establish the connection for enterprises over a long distance. |

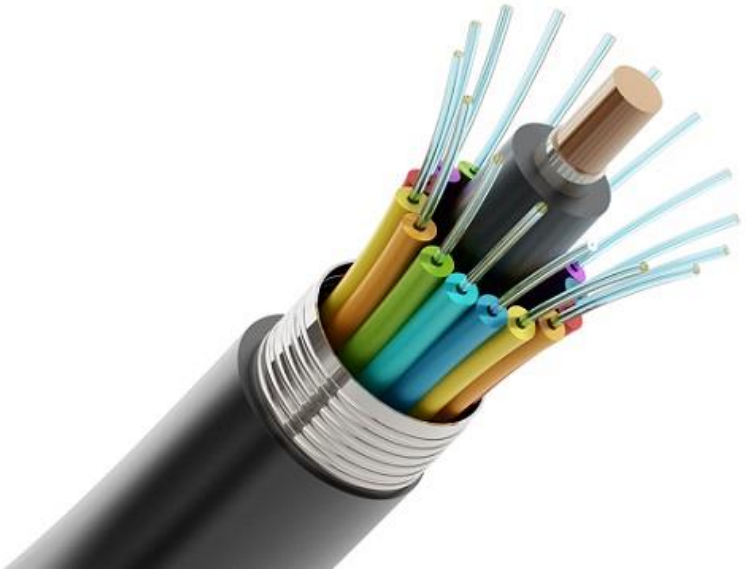
## (ii) Coaxial Cable

It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 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.



## (iii) Optical Fiber 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.



# 2. Unguided Media:

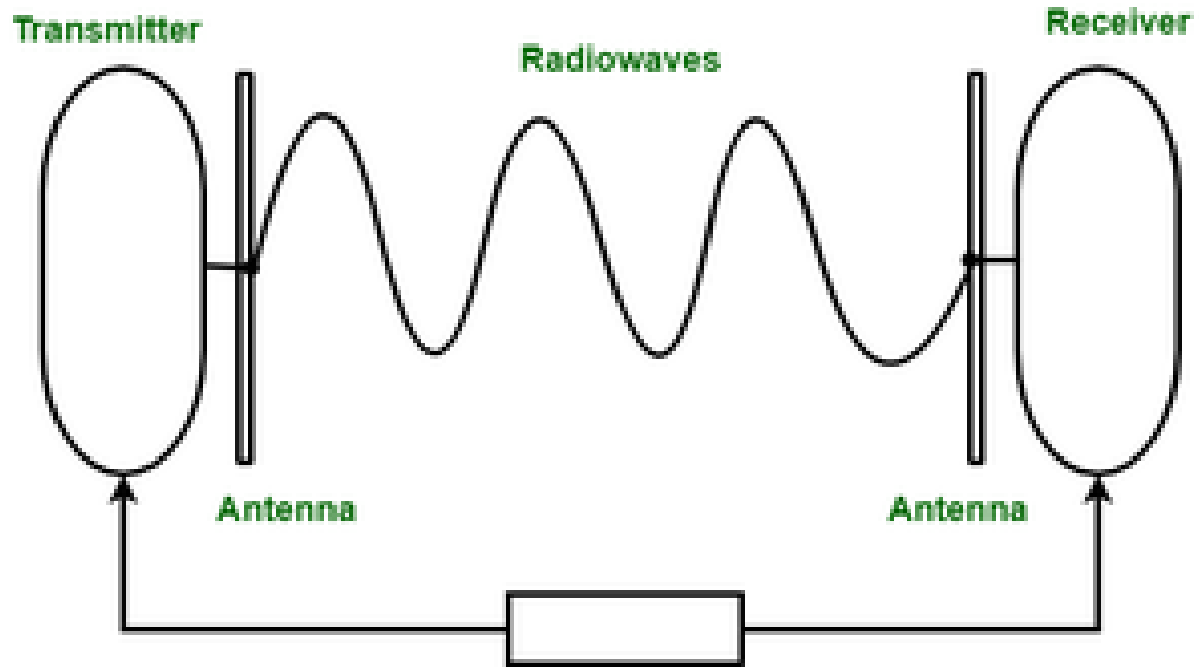
It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

Features:

- The signal is broadcasted through air
- Less Secure
- Used for larger distances
- There are 3 types of Signals transmitted through unguided media:

## (i) Radio waves

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 Radio waves for transmission.

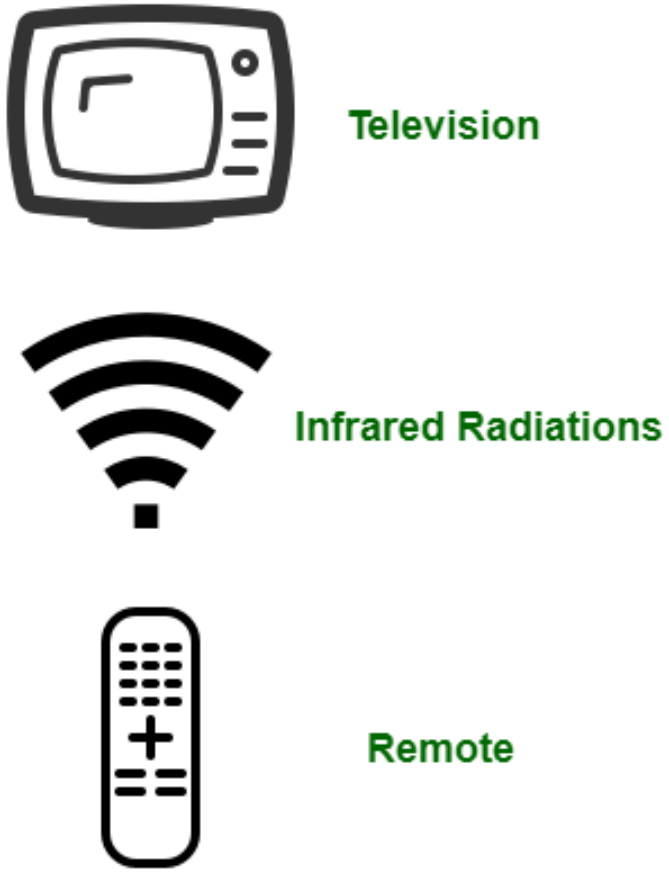


## (ii) Microwaves

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.



# difference between the Guided Media and Unguided Media

| S.No. | Guided Media | Unguided Media |
|---|---|---|
| 1. | The signal energy propagates through wires in guided media. | The signal energy propagates through air in unguided media. |
| 2. | Guided media is used for point to point communication. | Unguided media is generally suited for radio broadcasting in all directions. |
| 3. | Discrete network topologies are formed by the guided media. | Continuous network topologies are formed by the unguided media. |
| 4. | Signals are in the form of voltage, current or photons in the guided media. | Signals are in the form of electromagnetic waves in unguided media. |
| 5. | Examples of guided media are twisted pair wires, coaxial cables, optical fiber cables. | Examples of unguided media are microwave or radio links and infrared light. |
| 6. | By adding more wires, the transmission capacity can be increased in guided media. | It is not possible to obtain additional capacity in unguided media. |

# Transmission impairments terminology

**Distortion**

If a signal changes its form or shape, it is referred to as distortion. Signals made up of different frequencies are composite signals. Distortion occurs in these composite signals.

**Noise**

Noise is another problem. There are some random or unwanted signals mix up with the original signal is called noise. Noises can corrupt the signals in many ways along with the distortion introduced by the transmission media.

**Cross talk**

Cross talk is an effect a wire on the another. One wire acts as a sending antenna and the transmission medium acts as the receiving antenna.

Just like in telephone system, it is a common experience to hear conversation of other people in the background. This is known as cross talk.

**Jitter**

Jitter is when there is a time delay in the sending of data packets over your network connection. This is often caused by network congestion, and sometimes route changes.

**Echo**

It is occurred when sent signal is returned back with some time delay i.e. more than 30ms.

**Singing**

It occurs when the transmitted signal is coupled into a return path and fed back to the source.

**Bandwidth**

he maximum amount of data transmitted over a communication channel in a given amount of time.

**Number of receiver**

more the number of receiver are, lesser is the data transfor rate.

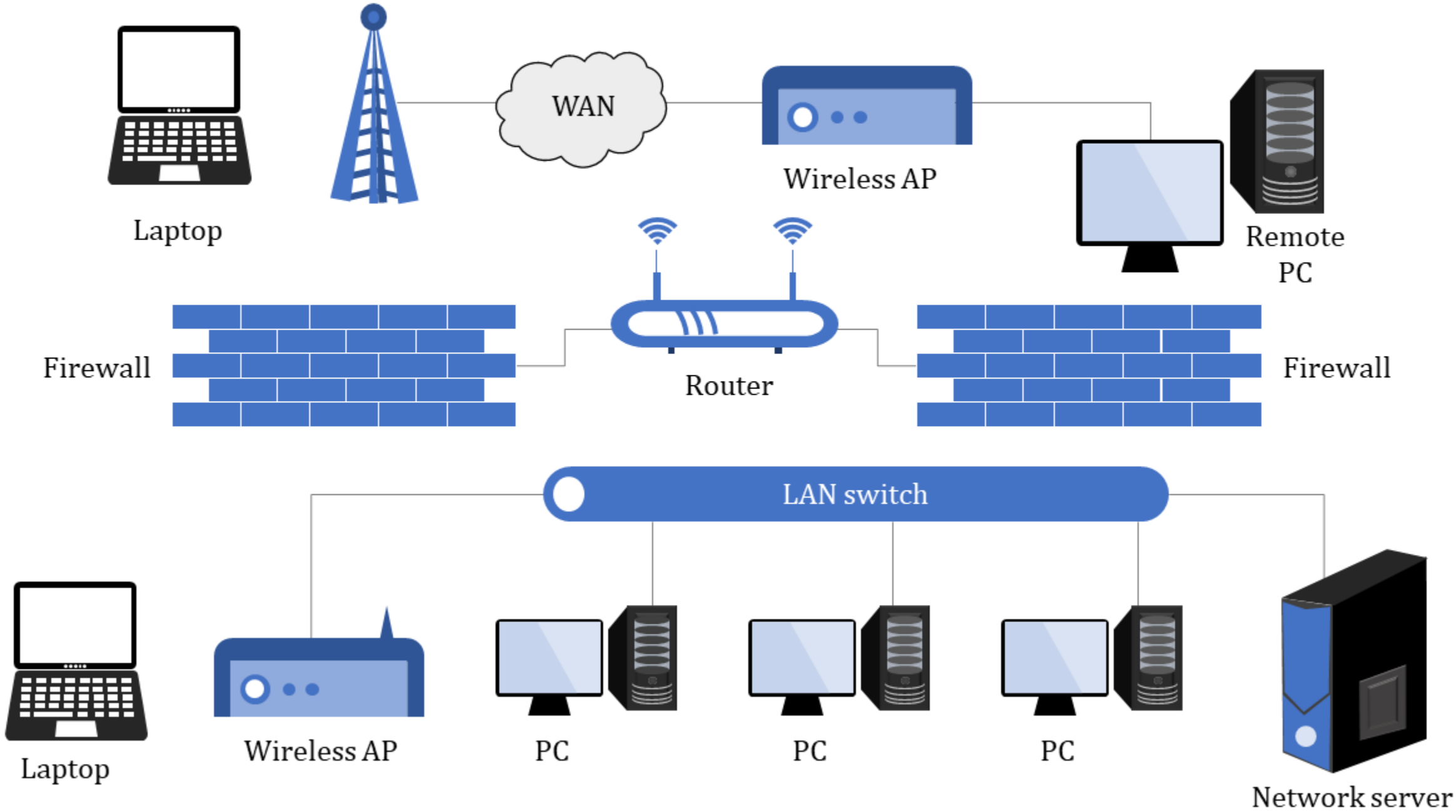
# Network architecture

Network architecture refers **to the way network devices and services are structured to serve the connectivity needs of client devices**. Network devices typically include switches and routers. Types of services include DHCP and DNS. Client devices comprise end-user devices, servers, and. smart things.

the two types of widely used network architectures are

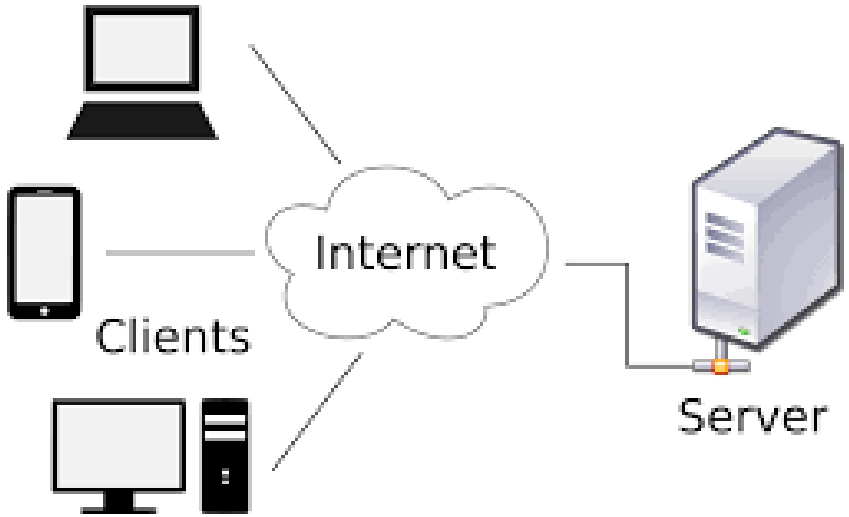
- **Client-server**
- **peer-to-peer (P2P)**

# Computer network architecture



# Client-server architecture

architecture of a computer network in which many clients (remote processors) request and receive service from a centralized server (host computer). Client computers provide an interface to allow a computer user to request services of the server and to display the results the server returns. Servers wait for requests to arrive from clients and then respond to them. Ideally, a server provides a standardized transparent interface to clients so that clients need not be aware of the specifics of the system (i.e., the hardware and software) that is providing the service. Clients are often situated at workstations or on personal computers, while servers are located elsewhere on the network, usually on more powerful machines. Examples of Client-Server Model are Email, World Wide Web, etc.



# Advantages of Client-Server model:

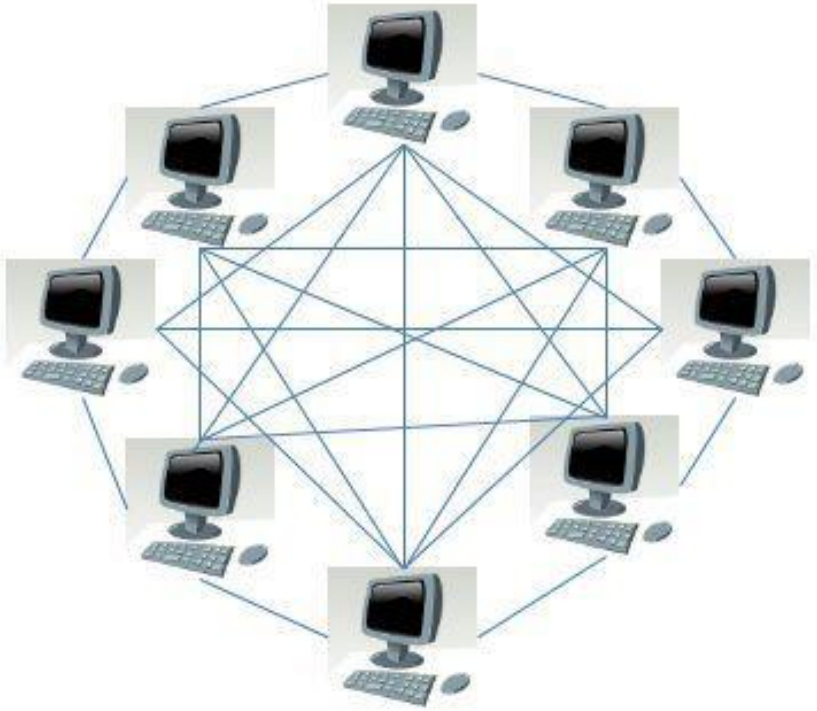
- Centralized system with all data in a single place.
- Cost efficient requires less maintenance cost and Data recovery is possible.
- The capacity of the Client and Servers can be changed separately.
- Service can be accessed any where and across any platform

# Disadvantages of Client-Server model:

- Clients are prone to viruses, Trojans and worms if present in the Server or uploaded into the Server.
- Server are prone to Denial of Service (DOS) attacks.
- Data packets may be spoofed or modified during transmission.
- Phishing or capturing login credentials or other useful information of the user are common and MITM(Man in the Middle) attacks are common.

# peer to peer model:

In the **peer to peer network**, all “Peers” means all computers which are linked with each other through network or internet. P2P  has not any central server, so each user is capable to share any types of files on any peer over this model.  On other words, you can say that every peer on this P2P model plays role as server as well as client. 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 Model

# Advantages of peer to peer model

- It does not require any network operating system.
- All workstations are capable to access any types of files, so does not require any costly server.
- All users have own permission that they can share any file over the network. So, does not need any well trained staff for operating this Peer to Peer network.
- Peer to peer network does not need any full time system administrator for managing entire network.
- Without any high level knowledge of this network, you can easily configure this P2P network.
- P2P network is more protective.
- If, any one peer of this network is getting to halt then entire network will not effected instead of those parts.

# Disadvantages of Peer to Peer Network

- Peer to Peer network is a decentralized so it is big challenge to administrator. Entire accessibility of fully network cannot be controlled by one person.
- All computer system can be used anytime duration.
- Every computer system contains unique password over the whole network.
- It does not contain any center medium of data storage for file archiving.
- Slow performance because every computer is accessed by other users.
- To get backup of data is harder task because it’s all data is saved on different **types of computer** system as well as it has not any centralized server.

# Difference between Client-Server and Peer-to-Peer

| S.NO | Client-Server Network | Peer-to-Peer Network |
|---|---|---|
| 1. | In Client-Server Network, Clients and server are differentiated, Specific server and clients are present. | In Peer-to-Peer Network, Clients and server are not differentiated. |
| 2. | Client-Server Network focuses on information sharing. | While Peer-to-Peer Network focuses on connectivity. |
| 3. | In Client-Server Network, Centralized server is used to store the data. | While in Peer-to-Peer Network, Each peer has its own data. |
| 4. | In Client-Server Network, Server respond the services which is request by Client. | While in Peer-to-Peer Network, Each and every node can do both request and respond for the services. |
| 5. | Client-Server Network are costlier than Peer-to-Peer Network. | While Peer-to-Peer Network are less costlier than Client-Server Network. |
| 6. | Client-Server Network are more stable than Peer-to-Peer Network. | While Peer-to-Peer Network are less stable if number of peer is increase. |
| 7. | Client-Server Network is used for both small and large networks. | While Peer-to-Peer Network is generally suited for small networks with fewer than 10 computers. |

# IP Address

An **IP address** represents an Internet Protocol address. A unique address that identifies the device over the network. It is almost like a set of rules governing the structure of data sent over the Internet or through a local network. An IP address helps the Internet to distinguish between different routers, computers, and websites. It serves as a specific machine identifier in a specific network and helps to improve visual communication between source and destination.

**IP address structure:**
IP addresses are displayed as a set of four digits- the default address maybe 192.158.1.38. Each number on the set may range from 0 to 255. Therefore, the total IP address range ranges from 0.0.0.0 to 255.255.255.255. There are two versions of IP address i.e. IPv4 (version 4) and IPv6 (version 6)

## IPv4

IP version four addresses are 32-bit integers which will be expressed in decimal notation. Example- 192.0.2.126 could be an IPv4 address.

## IPv6

IPv6 is the latest version of the Internet Protocol, which identifies devices across the internet so they can be located. The previous version, IPv4, uses a 32-bit addressing scheme to support 4.3 billion devices, which was thought to be enough. However, the growth of the internet, personal computers, smartphones and now Internet of Things devices proves that the world needed more addresses. Fortunately, the Internet Engineering Task Force (IETF) recognized this 20 years ago. In 1998 it created IPv6, which instead uses 128-bit addressing to support approximately 340 trillion trillion devices. IPv6 has a 128-bit address length. An example of an IPv6 address is**: 2001:0db8:85a3:0000:0000:8a2e:0370:7334**.

# Subnet Mask

subnets are a logical partition of an IP network into multiple, smaller network segments.

**Subnetting** is the practice of dividing a network into two or smaller networks. It increases routing efficiency, which helps to enhance the security of the network and reduces the size of the broadcast domain. A **broadcast domain** is a logical division of a computer network.

We can show Subnet Masks with four octets like **IP addresses** (255.255.255.0). Here, for the 255.255.255.0 Subnet Mask, we can use /24. This means that the first 24 bit is full of 1s and it is network part.

# Gateway

A gateway is a hardware device that acts as a "gate" between two networks. It may be a router, firewall, server, or another device that enables traffic to flow in and out of the network.

The gateway node is considered to be on the "edge" of the network as all data must flow through it before coming in or going out of the network. It may also translate data received from outside networks into a format or protocol recognized by devices within the internal network.

A router is a common type of gateway used in home networks. It allows computers within the local network to send and receive data over the Internet.

# MAC address

MAC address is the physical address, which uniquely identifies each device on a given network. To make communication between two networked devices, we need two addresses: **IP address and MAC address.** It is assigned to the NIC (Network Interface card) of each device that can be connected to the internet.

It stands for **Media Access Control**, and also known as **Physical address, hardware address, or BIA (Burned In Address).**

It is globally unique; it means two devices cannot have the same MAC address. It is represented in a hexadecimal format on each device, such as **00:0a:95:9d:67:16.**

# Internet

Internet is a world-wide global system of interconnected computer networks. Internet uses the standard Internet Protocol (TCP/IP).Every computer in internet is identified by a unique IP address. IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.

A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.

For example, a DNS server will resolve a name **http://www.tutorialspoint.com** to a particular IP address to uniquely identify the computer on which this website is hosted.

Internet is accessible to every user all over the world.

# Intranet

An Intranet is a part of the Internet and is owned and used privately by an organization. It is mainly used to connect all the computers and establish a private network of an organization to provide employees the ability to collaborate on projects, manage or update information, share calendars, and to-do list, etc. Organizations prefer using Intranet to keep their data inaccessible from outsiders, making their suspicious data and project information secure. Intranet includes a firewall to prevent unauthorized users from accessing the network.

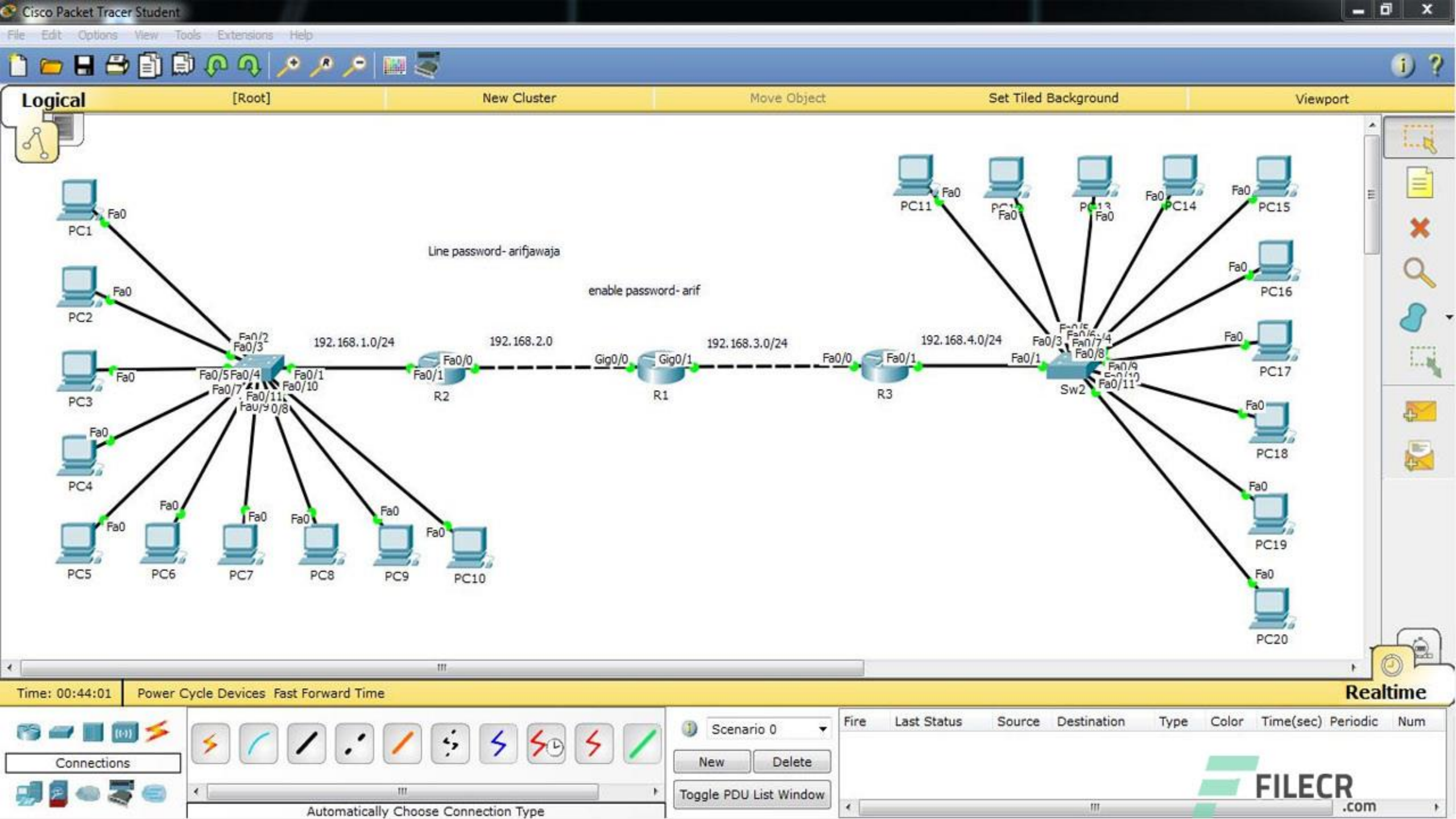
# Extranet

An extranet is a private network that only authorized users can access. These authorized users may include business partners, suppliers, and even some customers. They can use the extranet to exchange information with each other without having to enter the host company's main network.

An extranet is like a secure file room located somewhere off the company premises. Only those issued a key can enter and browse through the filing cabinets.

# Packet Tracer

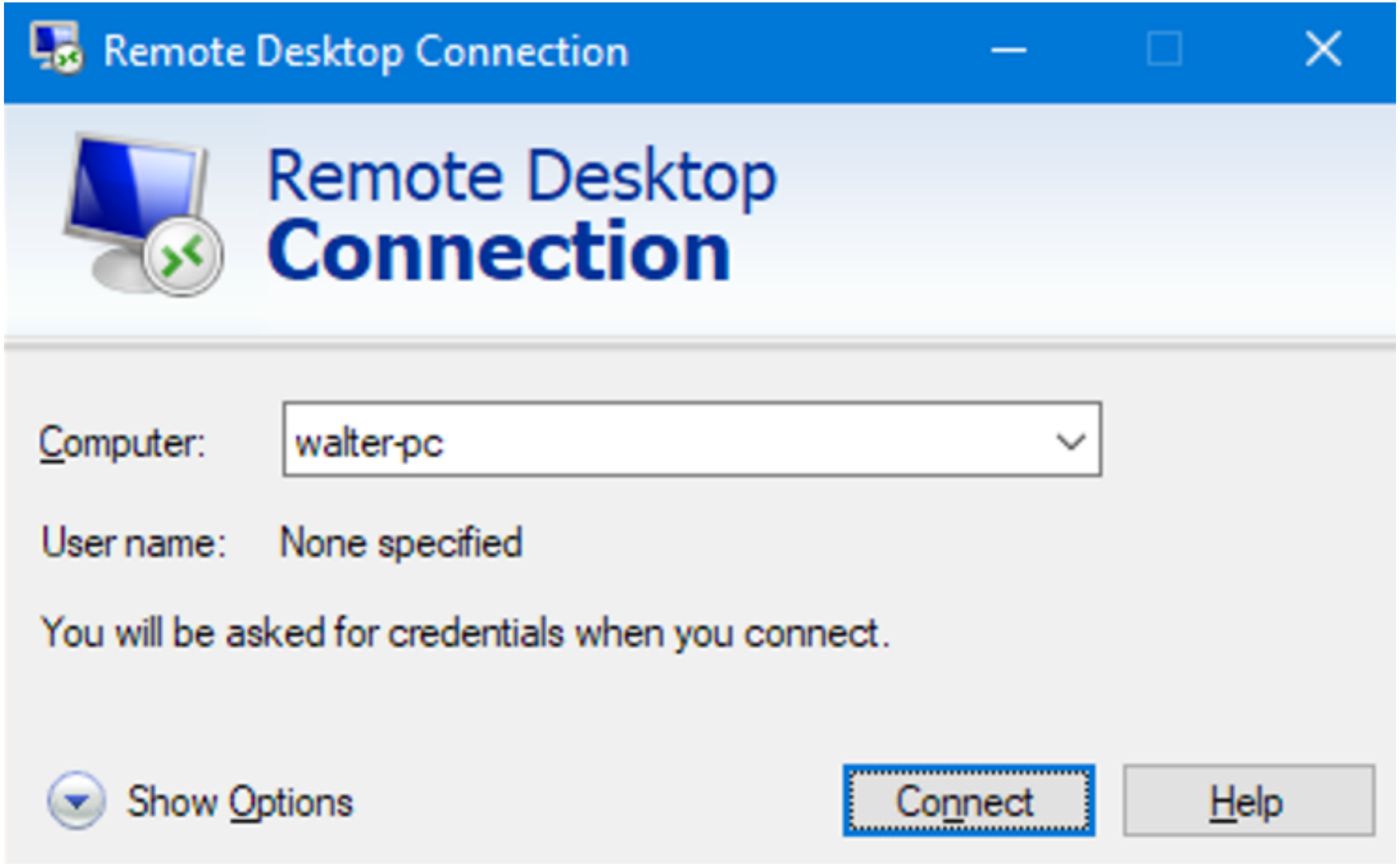
Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Line password- arifjawaja
enable password- arif
192.168.1.0/24
192.168.2.0
192.168.3.0/24
192.168.4.0/24
PC1
PC2
PC3
PC4
PC5
PC6
PC7
PC8
PC9
PC10
PC11
PC14
PC15
PC16
PC17
PC18
PC19
PC20
R1
R2
R3
Sw2
Time: 00:44:01
Power Cycle Devices Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num

# remote login

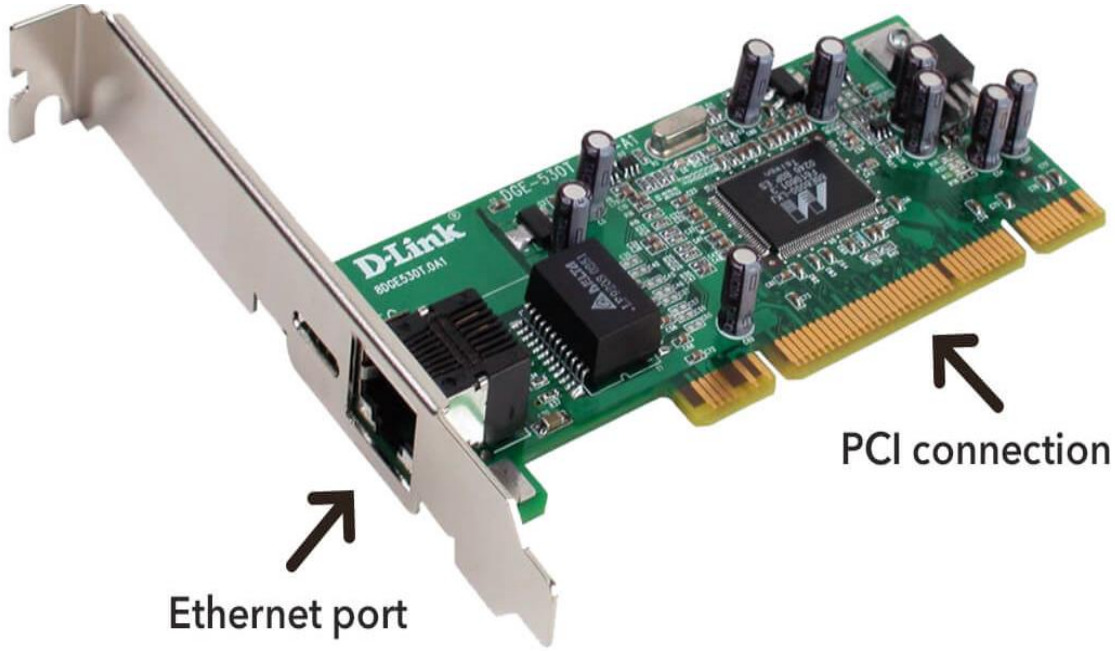
Remote access, also known as remote login, is the ability to access the data stored on a computer from a remote location. It enables you to open, edit, and save files located on your device from anywhere in the world. This ability is handy for offsite workers, travelers, and those who work out of office.

- There are several ways to set up remote access:
- With LAN (local area network)
- WAN (wide area network)
- VPN (virtual private network)
- Internet


Remote Desktop Connection
Remote Desktop
Connection
Computer:
walter-pc
User name:
None specified
You will be asked for credentials when you connect.
Show Options
Connect
Help

# NIC

A network interface controller is a computer hardware component that connects a computer to a computer network. A NIC allows a device to connect with other devices on a network. NICs are often used with Ethernet cables to physically connect different devices on a network. For instance, a server will have a NIC which allows it to connect to a router. You could connect your PC to a router using a NIC.



# MODEM

Modem is short for "**Modulator-Demodulator**." It is a hardware component that allows a computer or another device, such as a router or switch, to connect to the Internet. ... Similarly, it converts digital data from a computer or other device into an analog signal that can be sent over standard telephone lines.

# Router


A router[a] is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node.

# Switch

A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer of the OSI model.

# Network Topology

A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

## Star Topology :

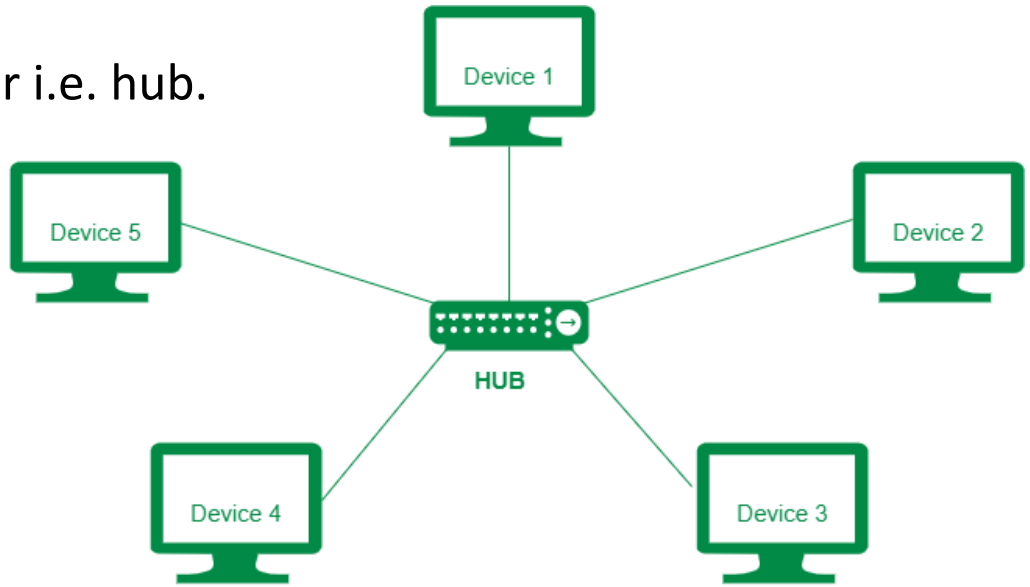
In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them.

**Advantages of this topology :**

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.

**Problems with this topology :**

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




Star Topology

## Bus Topology :

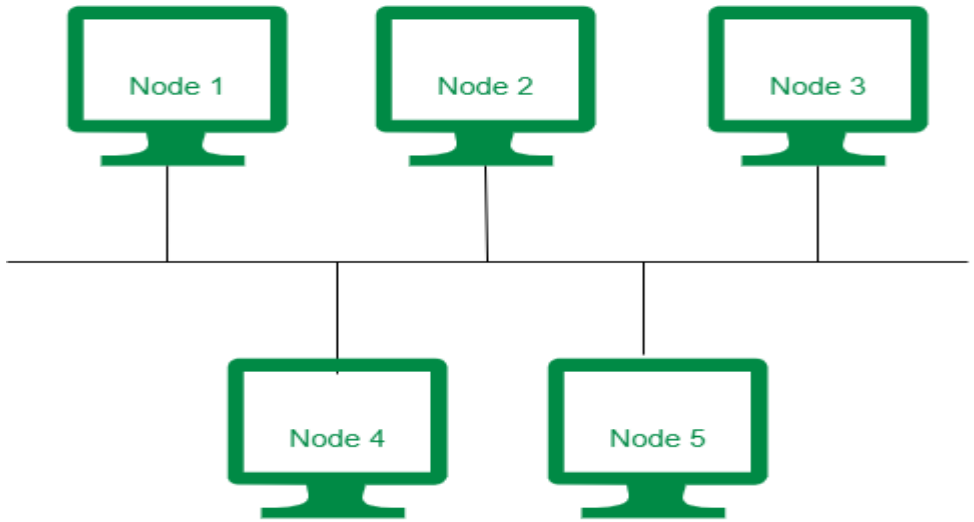
Bus topology is a network type in which every computer and network device is connected to a single cable. It transmits the data from one end to another in a single direction. No bi-directional feature is in bus topology. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

## Advantages of this topology :

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, which is known as backbone cable, and N drop lines are required.
- The cost of the cable is less as compared to other topologies, but it is used to build small networks.

## Problems with this topology :

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




Bus Topology

## Ring Topology :

In this topology, it forms a ring connecting devices with its exactly two neighboring devices.

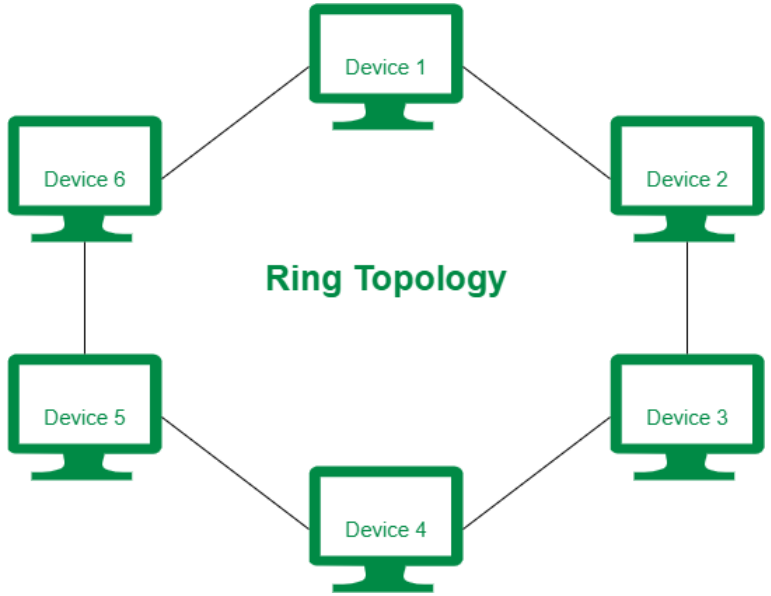
A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.

**Advantages of this topology :**

- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

**Problems with this topology :**

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

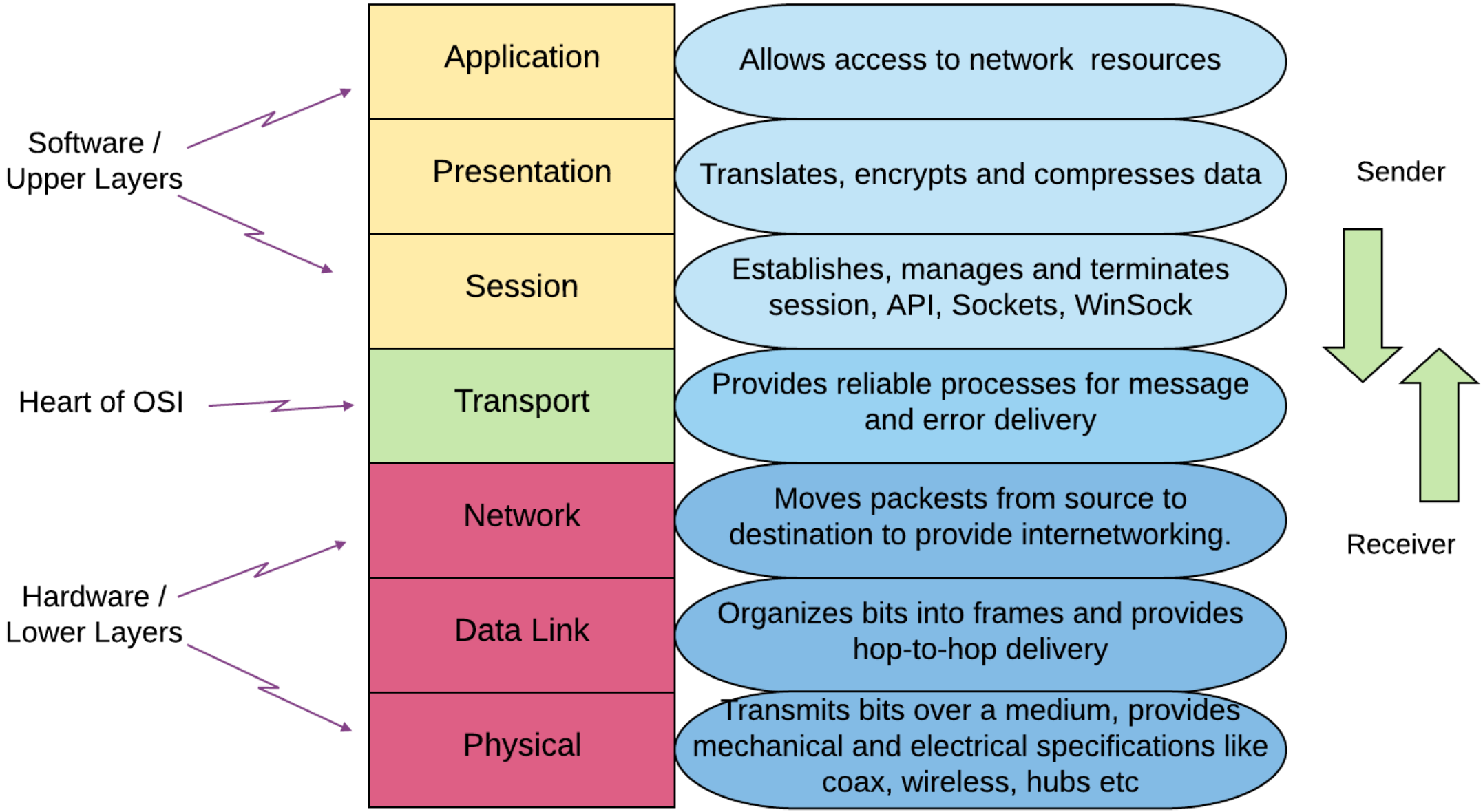


# OSI Model

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s

The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.

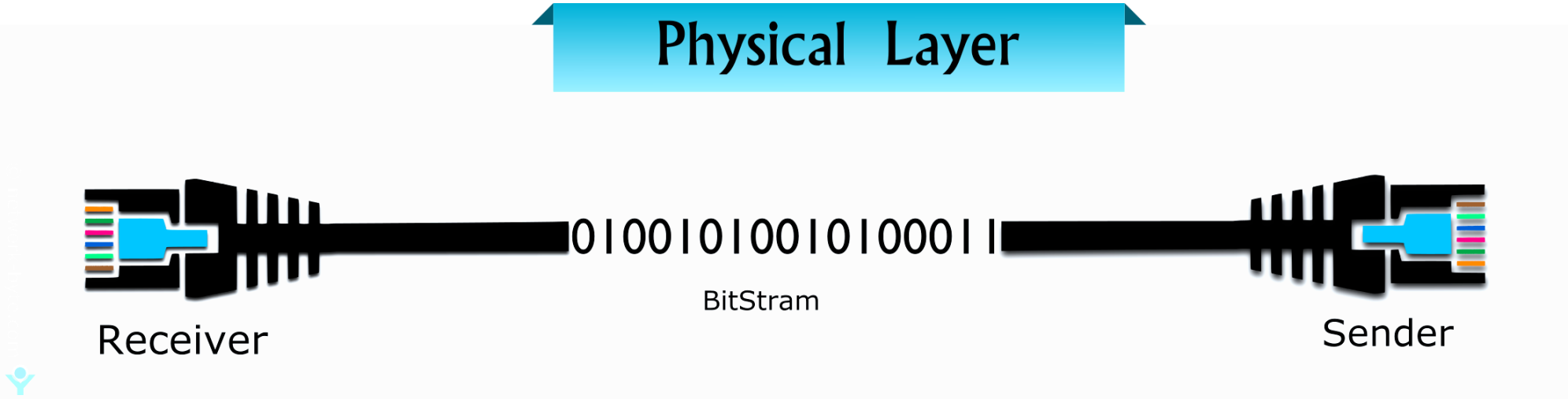
OSI was introduced in 1983 by representatives of the major computer and telecom companies, and was adopted by ISO as an international standard in 1984.


Application
Presentation
Session
Transport
Network
Data Link
Physical
Allows access to network resources
Translates, encrypts and compresses data
Establishes, manages and terminates session, API, Sockets, WinSock
Provides reliable processes for message and error delivery
Moves packests from source to destination to provide internetworking.
Organizes bits into frames and provides hop-to-hop delivery
Transmits bits over a medium, provides mechanical and electrical specifications like coax, wireless, hubs etc
Software / Upper Layers
Heart of OSI
Hardware / Lower Layers
Sender
Receiver

# OSI 7 Layers

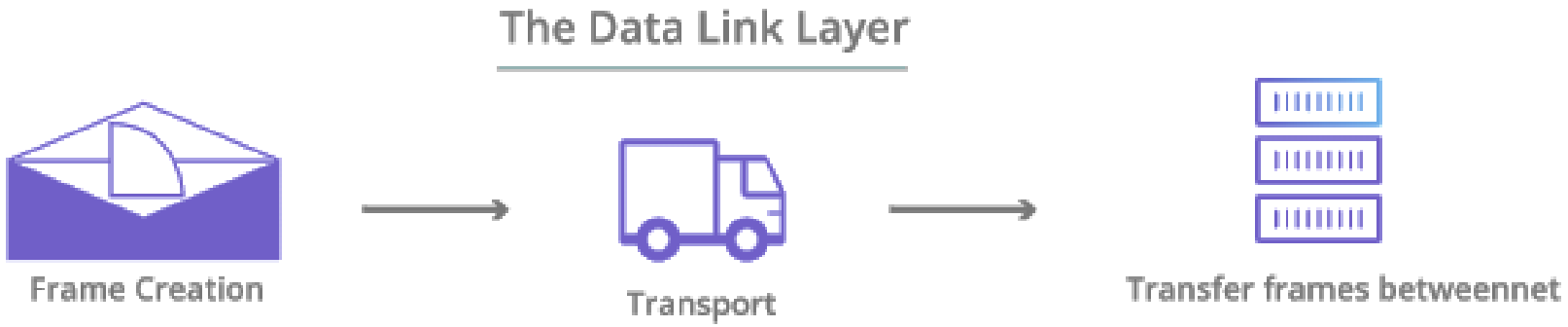
## 1. Physical Layer

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.



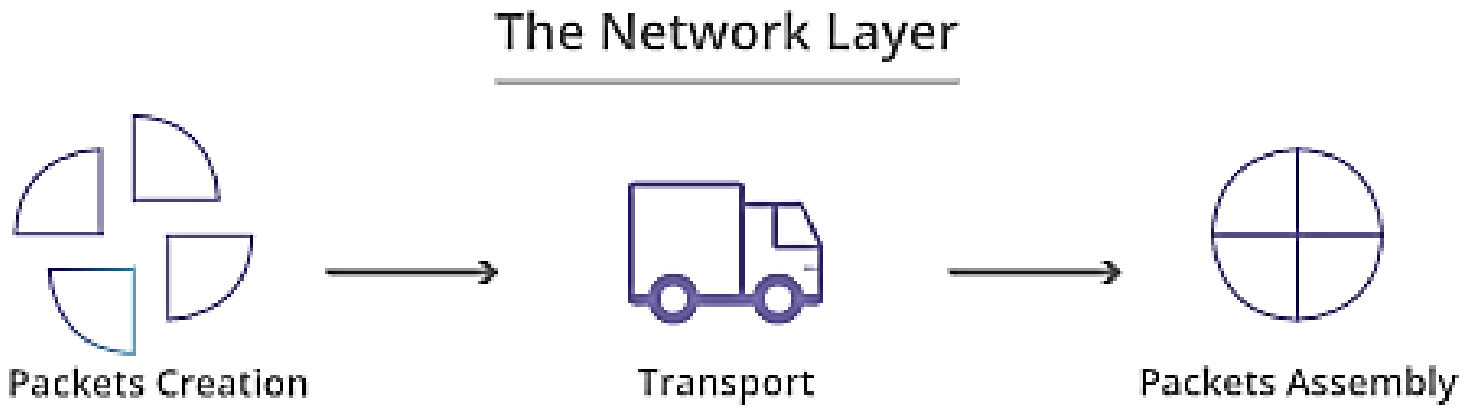
## 2. Data Link Layer

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data



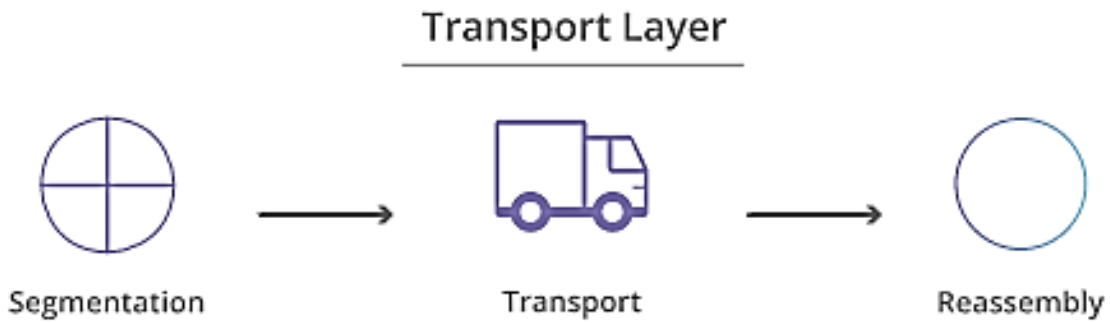
## 3. Network Layer

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node. The primary function of the network layer is **to enable different networks to be interconnected**. It does this by forwarding packets to network routers, which rely on algorithms to determine the best paths for the data to travel.



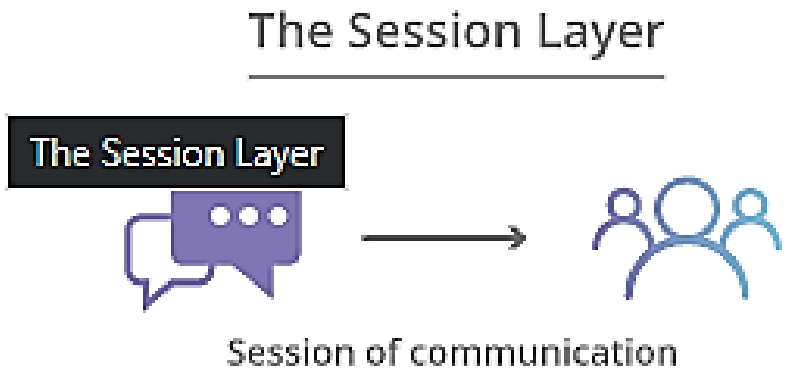
## 4. Transport Layer

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.



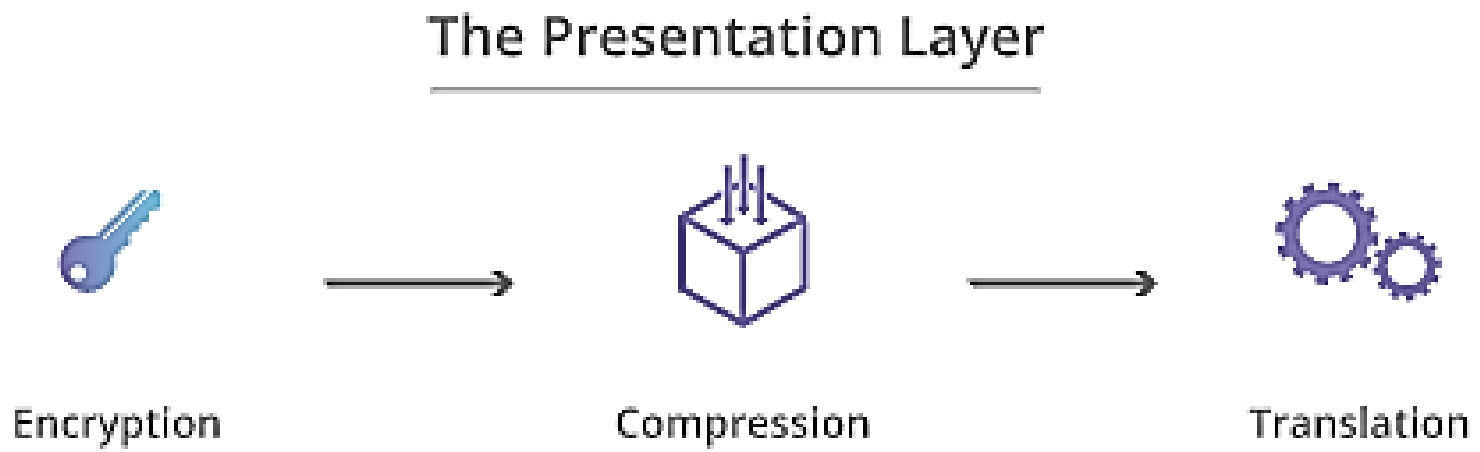
## 5. Session Layer

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.



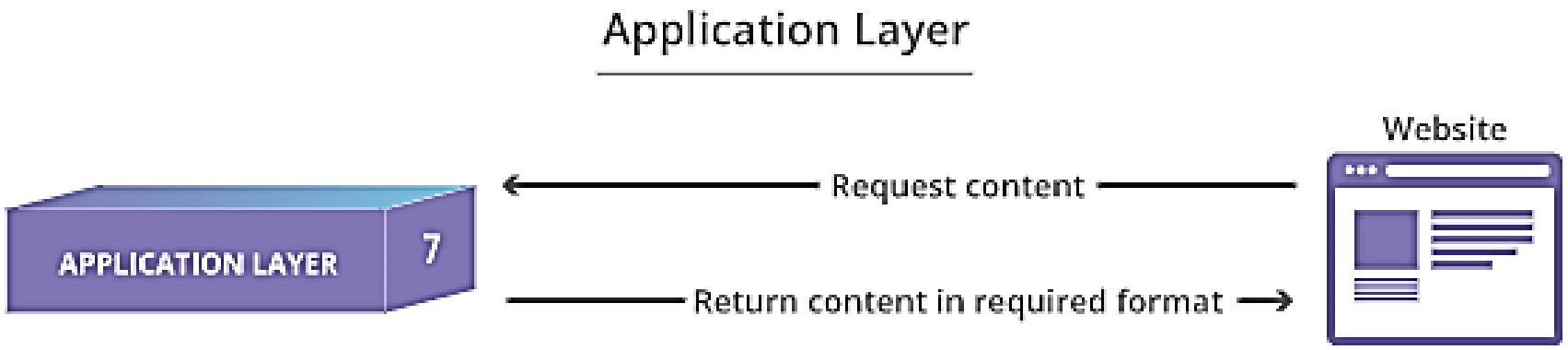
## 6. Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.



## 7. Application Layer

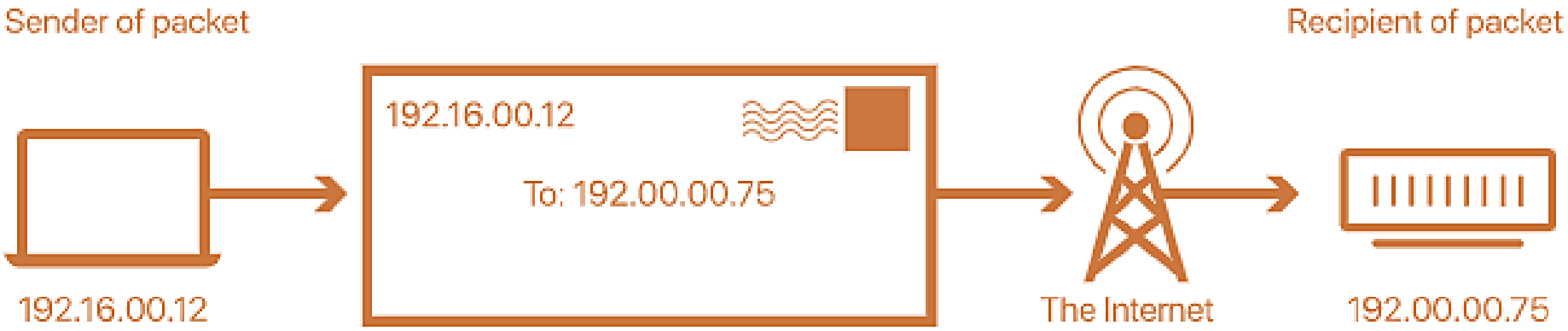
The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).



| Layer | Function | Example of protocols and/or equipment |
|---|---|---|
| Application - 7 | Services affecting end user applications | SMTP |
| Presentation - 6 | Presentation Layer | JPEG - MIDI - MPEG - PICT - TIFF - GIF - HTTPS - SSL - TLS |
| Session - 5 | Session Layer | NetBIOS - NFS - PAP - SCP - SQL - ZIP |
| Transport - 4 | Transport Layer | TCP - UDP |
| Network - 3 | Network Layer | Routers - Layer 3 Switches - IPsec - IPv4 - IPv6 - IPX - RIP |
| Data Link - 2 | Data Link Layer | Switches - ARP - ATM - CDP - FDDI - Frame Relay - HDLC - MPLS - PPP - STP - Token Ring |
| Physical - 1 | Physical Layer | Hubs - Bluetooth - Ethernet - DSL - ISDN - 802.11 - WiFi |

# How does IP addressing work?

An IP address is a unique identifier assigned to a device or domain that connects to the Internet. Each IP address is a series of characters, such as '192.168.1.1'. Via DNS resolvers, which translate human-readable domain names into IP addresses, users are able to access websites without memorizing this complex series of characters. Each IP packet will contain both the IP address of the device or domain sending the packet and the IP address of the intended recipient, much like how both the destination address and the return address are included on a piece of mail.



1100 0000 - 1010 1000 - 0000 0000 - 0000 0101

IPv4 addresses are 32-bit addresses. Each byte, or 8-bit segment of the address, is divided by a period and typically expressed as a number 0–255. Even though these numbers are typically expressed in decimal to aid in human comprehension, each segment is usually referred to as an **octet** to express the fact that it is a representation of 8 bits.

A typical IPv4 address looks something like this:192.168.0.5

The lowest value in each octet is a 0, and the highest value is 255.

we can also express this in binary to get a better idea of how the four octets will look. We will separate each 4 bits by a space for readability and replace the dots with dashes: 1100 0000-1010 1000-0000 0000 0000 0101. This is a 32 bit IP address. We can assign $2^{32}$=**4,294,967,296** to the devices connected.

IPv4 and IPv6, the most noticeable difference is the address space. IPv6 expresses addresses as an 128-bit number. To put that into perspective, this means that IPv6 has space for more than 7.9×1028 times the amount of addresses as IPv4.

To express this extended address range, IPv6 is generally written out as eight segments of four hexadecimal digits. Hexadecimal numbers represent the numbers 0–15 by using the digits 0–9, as well as the numbers a–f to express the higher values. A typical IPv6 address might look something like this:

1203:8fe0:fe80:b897:8990:8a7c:99bf:323d

# Assignments

1. what is communication? Explain four fundamentals characterstics for effective data communication
2. what is signal? write differences between analog and digital signal.
3. Explain all transmission Impairments
4. Describe Amplification and Repeiter.
5. what is Modulation? explain A.M. F.M. and P.M.
6. what is demodulation
7. what is communication system and communication channel?
8. what are elements of data communication.
9. Describe simple half-duplex and full-duplex
10. what is computer network? explai LAN, MAN and WAN.
11. write advantages and disadvantages of LAN and WAN.
12. explain guided and unguided transmissin medium
13. write differences between UTP and STP
14. Explain coaxial cable and optical fiber cable.
15. write differences between guided and unguided media
16. what is network architecture ? differenciate client server and peer to peer architecture
17. what is IP address? explain IPv4 and IPv6
18. waht is subnet mask?
19. Explain getway, MAC address, internet, intranet and extranet
20. what are NIC,router,switch and modem?
21. explain star bus and ring topology.
22. explain seven layers of OSI model in details