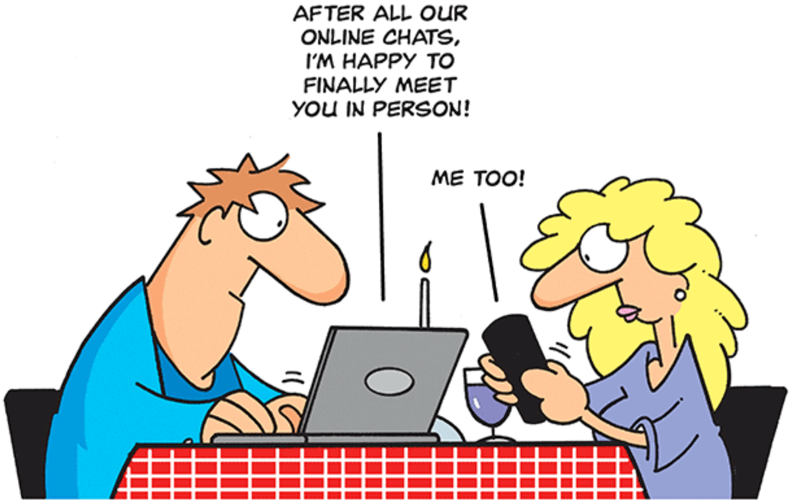
DATA COMMUNICATION AND NETWORKS


AFTER ALL OUR ONLINE CHATS, I'M HAPPY TO FINALLY MEET YOU IN PERSON!
ME TOO!

A/L Guide

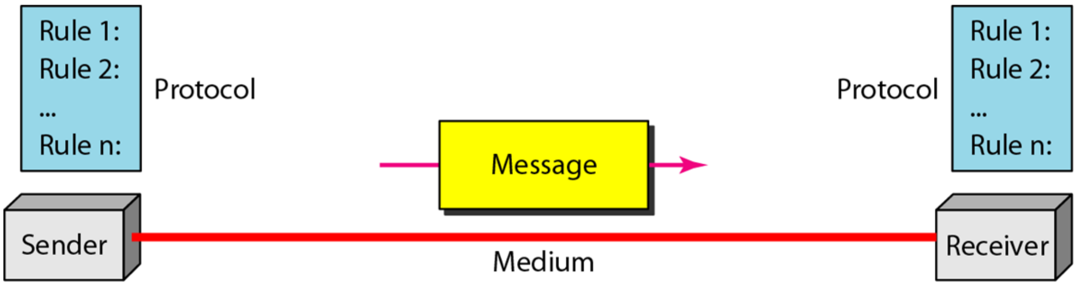
TERAN SUBASINGHE

Data Communication

What is data communication?

Data Communication is a process of exchanging data or information between two or more devices along a communication medium.

Components of a data communication



1. **Message** - Message is the information to be communicated by the sender to the receiver.

2. **Sender** (Transmitter) - The sender is any device that is capable of sending the data (message).

3. **Receiver** - The receiver is a device that the sender wants to communicate the data (message).

4. **Communication Medium** - It is the path by which the message travels from sender to receiver.

5. **Protocol** –

- It is an agreed upon set or rules used by the sender and receiver to communicate data.

- A protocol is a set of rules that governs data communication.

- A Protocol is a necessity in data communications without which the communicating entities are
like two persons trying to talk to each other in a different language without know the other language.

Representation of Data in Signal Form

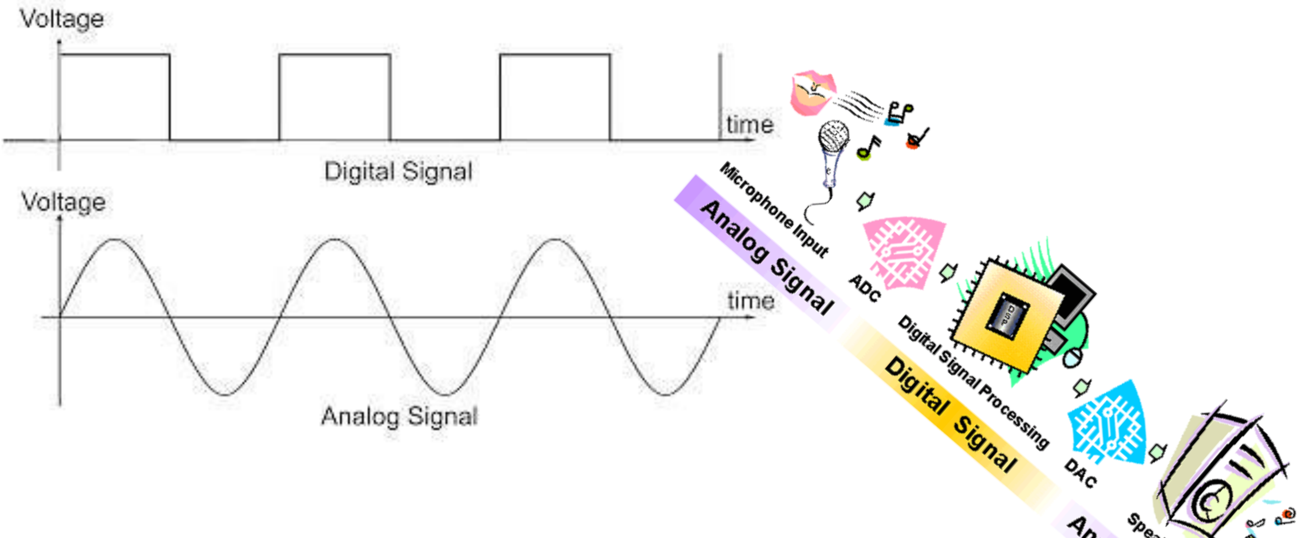
Computer networks are designed to transfer data from one point to another. During transit data is in the form of electromagnetic signals.

Analog data refers to information that is continuous; ex. sounds made by a human voice

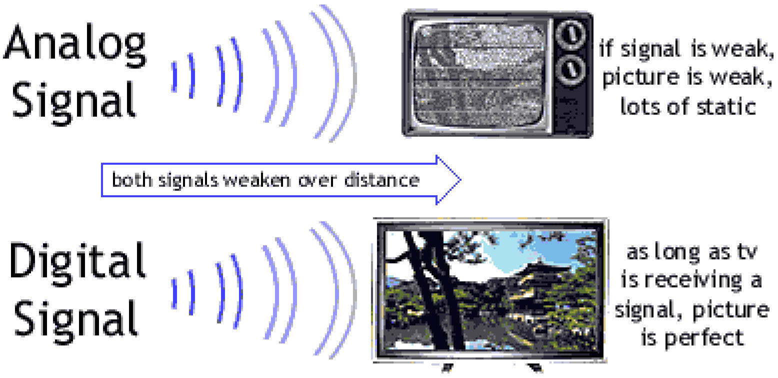
Digital data refers to information that has discrete states. Digital data take on discrete values.

Analog Signal: They have infinite values in a range.

Digital Signal: They have limited number of defined values



Description	Analog	Digital
Number of "Channels"	1 per coax (video) 100+ via RF modulation	Virtually Infinite using IP Multicasting
Video Sources	Analog cameras, tuners, satellite feeds	Analog cameras, tuners, satellite feeds
Reach	Anywhere there is a coax	Anywhere there is Ethernet
Quality	Variable	DVD-quality
Network Input	RF Modulators	MPEG Encoders
Network Output	Analog Set Top, TV monitor	Digital Set Top, PC Screens
Video On Demand	Limited: Requires RF Frequency Management (one VoD per RF channel)	Limited only by network bandwidth (one Ethernet Switch supports 20 to 200 VoD sessions)
Two Way Television (conferencing)	Difficult: each source requires its own RF modulator and dedicated RF TV "channel".	Unlimited, automatic setup. Very few network dependencies
Installation	Costly: Coax cable to every location	None: Uses existing Ethernet network
Live Television Channel Selection	IR Remote Control	IR Remote Control, mouse-click for PC
Management	Static channel assignment	Automatic – channels exist as needed
Channel Guide	Fixed or scheduled channel guide on dedicated RF channel	Dynamically generated digital display on TV and PC
Recording	Analog VCR's connected via coax spider	Digital recording scheduled or on demand
Viewer Statistics	Difficult	Automatic
Skills Required	Video, RF engineering	IP Networking
Cost	Low	Medium (low compared to installing new coax everywhere)


Analog Signal
if signal is weak, picture is weak, lots of static
both signals weaken over distance
Digital Signal
as long as tv is receiving a signal, picture is perfect

Common Data Communication Standards

DSL (Digital Subscriber Line) is a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines.

Ethernet is the most widely-installed local area network (LAN) technology. Specified in a standard, IEEE 802.3.

FDDI (Fiber-Distributed Data Interface) is a standard for data transmission on fiber optic lines in a that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol.

PCM (pulse code modulation) is a digital scheme for transmitting analog data. The signals in PCM are binary; that is, there are only two possible states, represented by logic 1 (high) and logic 0 (low). This is true no matter how complex the analog waveform happens to be. Using PCM, it is possible to digitize all forms of analog data, including full-motion video, voices, music, telemetry, and virtual reality (VR).

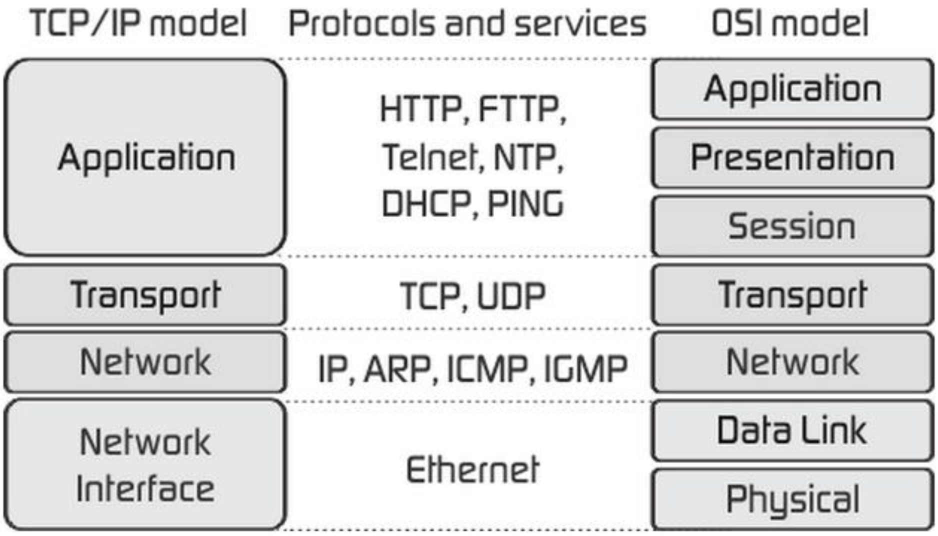
GSM (Global System for Mobile communication) is a digital mobile telephone system that is widely used in Europe and other parts of the world. GSM uses a variation of time division multiple access (Time Division Multiple Access) and is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data.

GPRS (General Packet Radio Services) is a packet-based wireless communication service that, when available in 2000, promises data rates from 56 up to 114 Kbps and continuous connection to the Internet for mobile phone and computer users.

Integrated Services Digital Network (ISDN) is a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media. Home and business users who install an ISDN adapter (in place of a modem) can see highly-graphic Web pages arriving very quickly (up to 128 Kbps).

EDGE (Enhanced Data GSM Environment), a faster version of the Global System for Mobile (GSM) wireless service, is designed to deliver data at rates up to 384 Kbps and enable the delivery of multimedia and other broadband applications to mobile phone and computer users.

TCP/IP Model



TCP/IP model	Protocols and services	OSI model
Application	HTTP, FTTP, Telnet, NTP, DHCP, PING	Application
		Presentation
		Session
Transport	TCP, UDP	Transport
Network	IP, ARP, ICMP, IGMP	Network
Network Interface	Ethernet	Data Link
		Physical

A. Host to Network Layer

This layer is a combination of protocols at the physical and data link layers. It supports all standard protocols used at these layers.

B. Network Layer or IP

Also called as the Internetwork Layer (IP). It holds the IP protocol which is a network layer protocol and is responsible for source to destination transmission of data. The Internetworking Protocol (IP) is an connection-less & unreliable protocol.

It is a best effort delivery service. I.e. there is no error checking in IP, it simply sends the data and relies on its underlying layers to get the data transmitted to the destination.

IP transports data by dividing it into packets or datagrams of same size. Each packet is independent of the other and can be transported across different routes and can arrive out of order at the receiver.

In other words, since there is no connection set up between the sender and the receiver the packets find the best possible path and reach the destination.

The packets may get dropped during transmission along various routes. Since IP does not make any guarantee about the delivery of the data its call an unreliable protocol.

Even if it is unreliable IP cannot be considered weak and useless; since it provides only the functionality that is required for transmitting data thereby giving maximum efficiency. Since there is no mechanism of error detection or correction in IP, there will be no delay introduced on a medium where there is no error at all.

IP is a combination of four protocols:
1. ARP
2. RARP
3. ICMP
4. IGMP

1. **ARP** – Address Resolution Protocol
It is used to resolve the physical address of a device on a network, where its logical address is known. Physical address is the 48 bit address that is imprinted on the NIC or LAN card, Logical address is the Internet Address or commonly known as IP address that is used to uniquely & universally identify a device.

2. **RARP**– Reverse Address Resolution Protocol
It is used by a device on the network to find its Internet address when it knows its physical address.

3. **ICMP**- Internet Control Message Protocol
It is a signaling mechanism used to inform the sender about datagram problems that occur during transit. It is used by intermediate devices. In case and intermediate device like a gateway encounters any problem like a corrupt datagram it may use ICMP to send a message to the sender of the datagram.

4. **IGMP**- Internet Group Message Protocol
It is a mechanism that allows to send the same message to a group of recipients.

C. Transport Layer

Transport layer protocols are responsible for transmission of data running on a process of one machine to the correct process running on another machine. The transport layer contains three protocols:

1. **TCP** – Transmission Control Protocol
TCP is a reliable connection-oriented, reliable protocol. I.e. a connection is established between the sender and receiver before the data can be transmitted. It divides the data it receives from the upper layer into segments and tags a sequence number to each segment which is used at the receiving end for reordering of data.

2. **UDP** – User Datagram Protocol
UDP is a simple protocol used for process to process transmission. It is an unreliable, connectionless protocol for applications that do not require flow control or error control. It simply adds port address, checksum and length information to the data it receives from the upper layer.

3. **SCTP** – Stream Control Transmission Protocol
SCTP is a relatively new protocol added to the transport layer of TCP/IP protocol suite. It combines the features of TCP and UDP. It is used in applications like voice over Internet and has a much broader range of applications

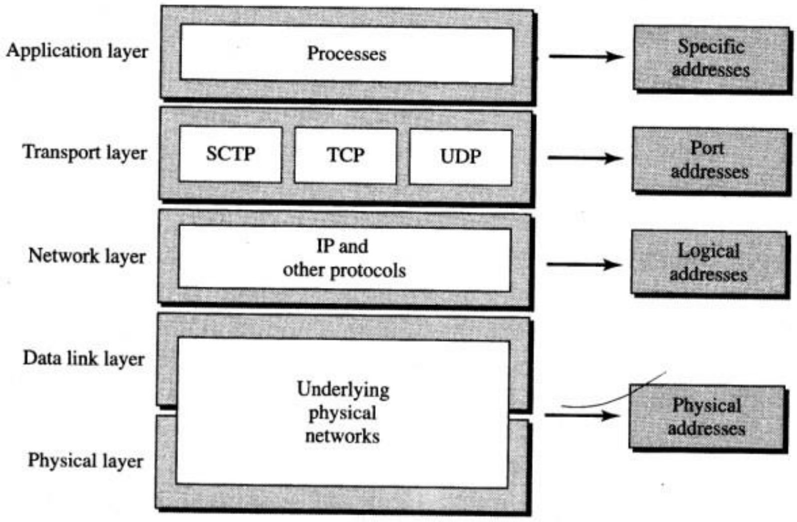
D. Application Layer

The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and define high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

Addressing in TCP/IP

The TCP/IP protocol suited involves 4 different types of addressing:

1. Physical Address
2. Logical Address
3. Port Address
4. Specific Address



1. Physical Address

- Physical Address is the lowest level of addressing, also known as link address.
- It is local to the network to which the device is connected and unique inside it.
- The physical address is usually included in the frame and is used at the data link layer.
- MAC is a type of physical address that is 6 byte (48 bit) in size and is imprinted on the Network Interface Card (NIC) of the device.
- The size of physical address may change depending on the type of network. Ex. An Ethernet network uses a 6 byte MAC address.

2. Logical Address

- Logical Addresses are used for universal communication.
- Most of the times the data has to pass through different networks; since physical addresses are local to the network there is a possibility that they may be duplicated across multiples networks also the type of physical address being used may change with the type of network encountered. For ex: Ethernet to wireless to fiber optic. Hence physical addresses are inadequate for source to destination delivery of data in an internetwork environment.
- Logical Address is also called as IP Address (Internet Protocol address).
- At the network layer, device i.e. computers and routers are identified universally by their IP Address.
- IP addresses are universally unique.
- Currently there are two versions of IP addresses being used:
  - IPv4: 32 bit address.
  - IPv6: 128 bit address.

3. Port Address

- A logical address facilitates the transmission of data from source to destination device. But the source and the destination both may be having multiple processes communicating with each other.

  Ex. Users A & B are chatting with each other using Google Talk, Users B & C are exchanging emails using Hotmail. The IP address will enable transmitting data from A to B, but still the data needs to be delivered to the correct process. The data from A cannot be given to B on yahoo messenger since A & B are communicating using Google Talk.
- Since the responsibility of the IP address is over here there is a need of addressing that helps identify the source and destination processes. In other words, data needs to be delivered not only on the correct device but also on the correct process on the correct device.
- A Port Address is the name or label given to a process. It is a 16 bit address.
- Ex. TELNET uses port address 23, HTTP uses port address 80

4. Specific Address

- Port addresses address facilitates the transmission of data from process to process but still there may be a problem with data delivery.
  For Ex: Consider users A, B & C chatting with each other using Google Talk. Every user has two windows open, user A has two chat windows for B & C, and user B has two chat windows for A & C and so on for user C.
  Now a port address will enable delivery of data from user A to the correct process (in this case Google Talk) on user B but now there are two windows of Google Talk for user A & C available on B where the data can be delivered.
- Again the responsibility of the port address is over here and there is a need of addressing that helps identify the different instances of the same process.
- Such address are user friendly addresses and are called specific addresses.
- Other Examples: Multiple Tabs or windows of a web browser work under the same process
- that is HTTP but are identified using Uniform Resource Locators (URL), Email addresses.

IPv4

Packets in the IPv4 format are called datagram. An IP datagram consists of a header part and a text part (payload). The header has a 20-byte fixed part and a variable length optional part.
It is transmitted in big-endian order: from left to right, with the high order bit of the Version field going first.
IPv4 can be explained with the help of following points:

1. IP addresses
2. Address Space
3. Notations used to express IP address
4. Classfull Addressing
5. Subnetting
6. CIDR
7. NAT
8. IPv4 Header Format

1. IP addresses

Every host and router on the Internet has an IP address, which encodes its network number and host number. The combination is unique: in principle, no two machines on the Internet have the same IP address. An IPv4 address is 32 bits long they are used in the Source address and Destination address fields of IP packets. An IP address does not refer to a host but it refers to a network interface.

2. Address Space

An address space is the total number of addresses used by the protocol. If a protocol uses N bits to define an address, the address space is 2^N because each bit can have two different values (0 or 1) and N bits can have 2^N values. IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than 4 billion).

3. Notations

There are two notations to show an IPv4 address:

1. Binary notation

The IPv4 address is displayed as 32 bits.

ex. 11000001 10000011 00011011 11111111

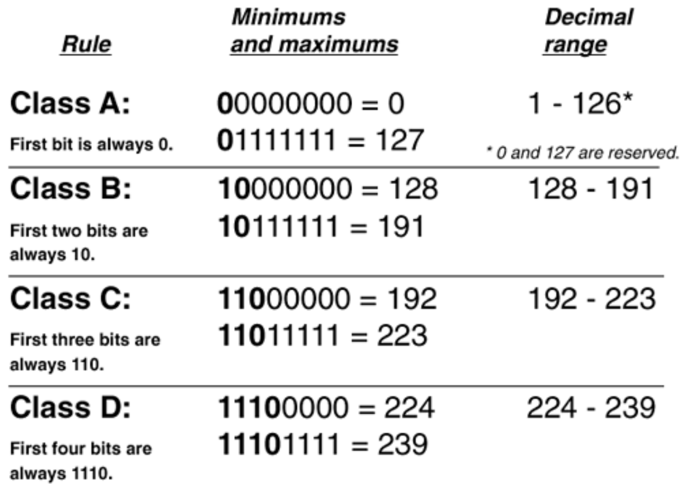
2. Dotted decimal notation

To make the IPv4 address easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. Each byte (octet) is 8 bits hence each number in dotted-decimal notation is a value ranging from 0 to 255.

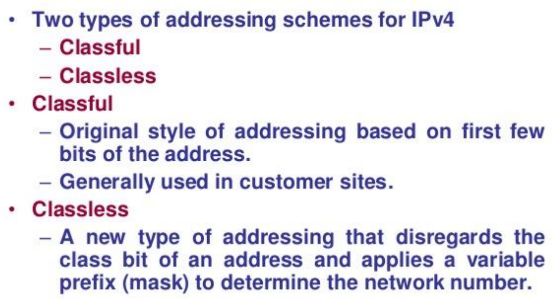
Ex. 129.11.11.239

4. Classful Addressing

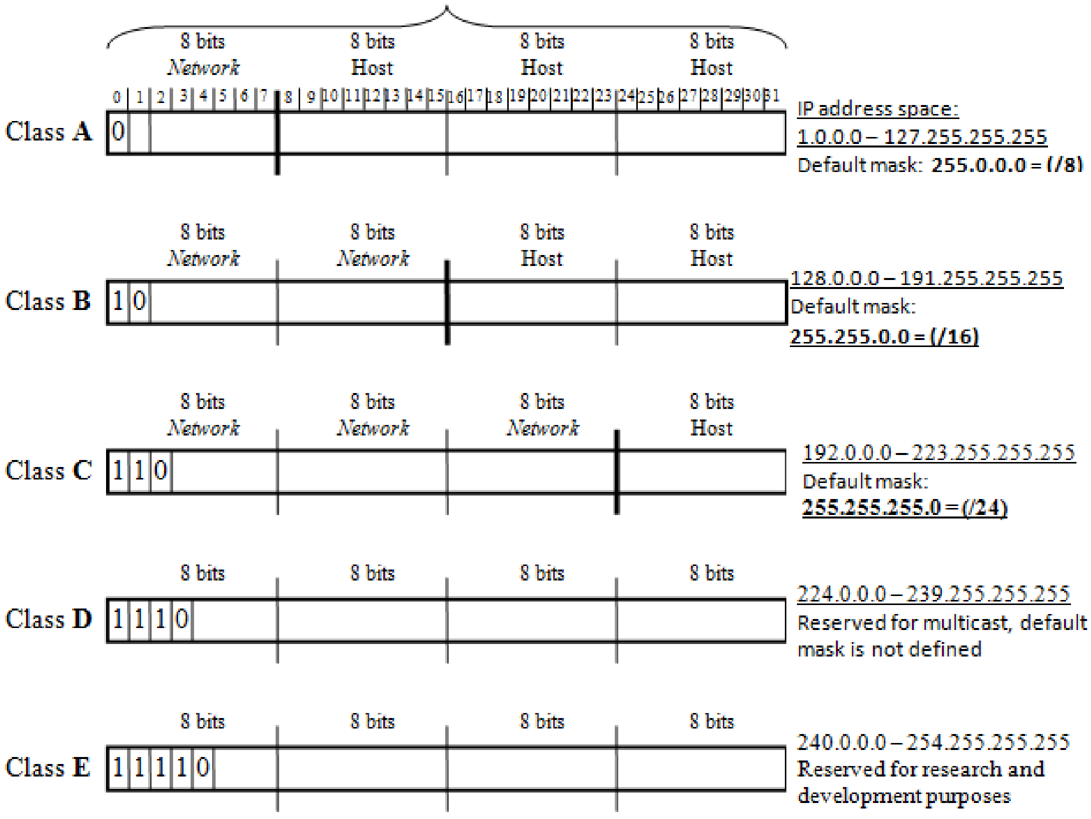
In classful addressing, the address space is divided into five classes: A, B, C, D, and E.



Rule	***Minimums and maximums***	***Decimal range***
Class A: First bit is always 0.	00000000 = 0 01111111 = 127	1 - 126* * 0 and 127 are reserved.
Class B: First two bits are always 10.	10000000 = 128 10111111 = 191	128 - 191
Class C: First three bits are always 110.	11000000 = 192 11011111 = 223	192 - 223
Class D: First four bits are always 1110.	11100000 = 224 11101111 = 239	224 - 239



- **Two types of addressing schemes for IPv4**
  - **Classful**
  - **Classless**
- **Classful**
  - **Original style of addressing based on first few bits of the address.**
  - **Generally used in customer sites.**
- **Classless**
  - **A new type of addressing that disregards the class bit of an address and applies a variable prefix (mask) to determine the network number.**



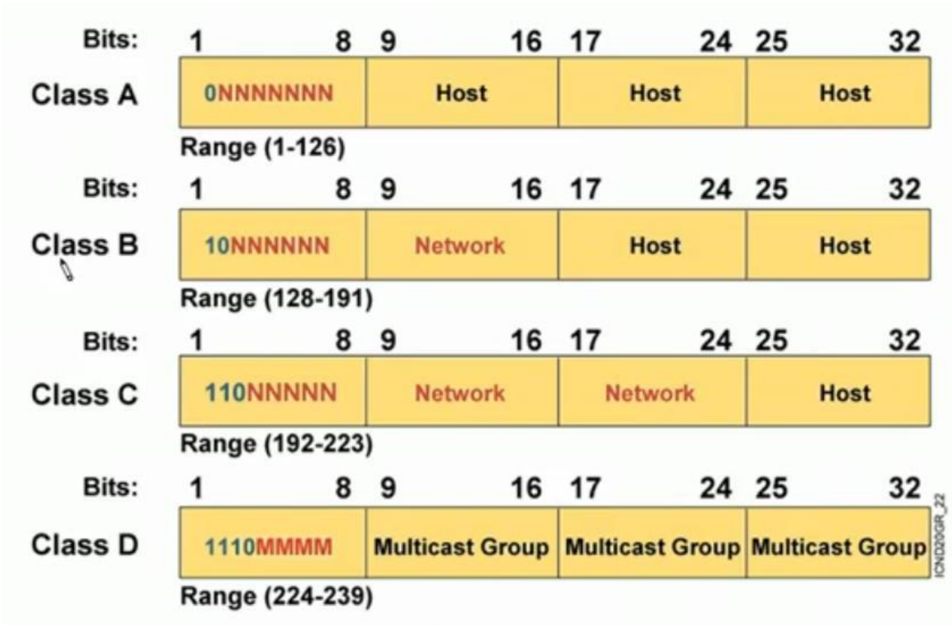
IP address space:
1.0.0.0 – 127.255.255.255
Default mask: **255.0.0.0 = (/8)**

128.0.0.0 – 191.255.255.255
Default mask:
255.255.0.0 = (/16)

192.0.0.0 – 223.255.255.255
Default mask:
255.255.255.0 = (/24)

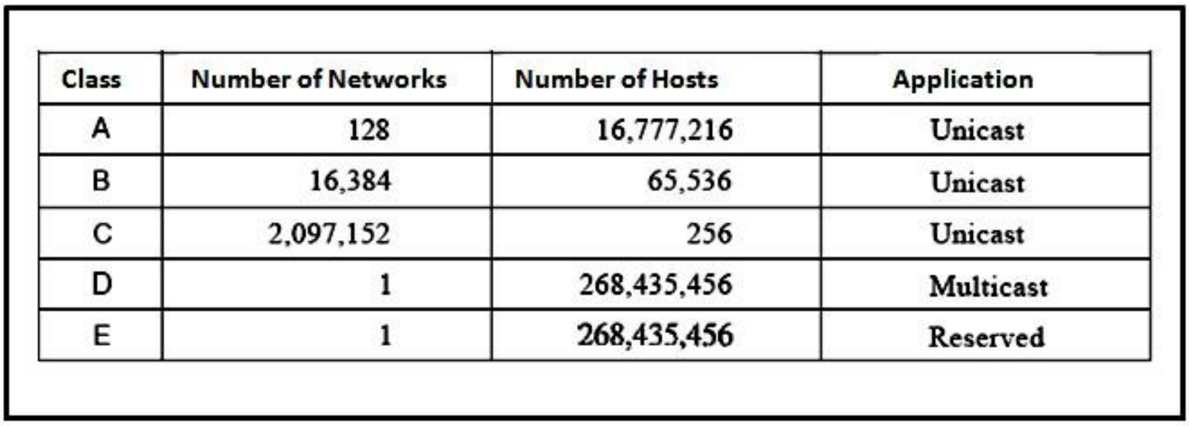
224.0.0.0 – 239.255.255.255
Reserved for multicast, default mask is not defined

240.0.0.0 – 254.255.255.255
Reserved for research and development purposes



Netid and Hostid - In classful addressing, an IP address in class A, B, or C is divided into netid and hostid. These parts are of varying lengths, depending on the class of the address as shown above.

Information on the Number of networks and host in each class is given below:

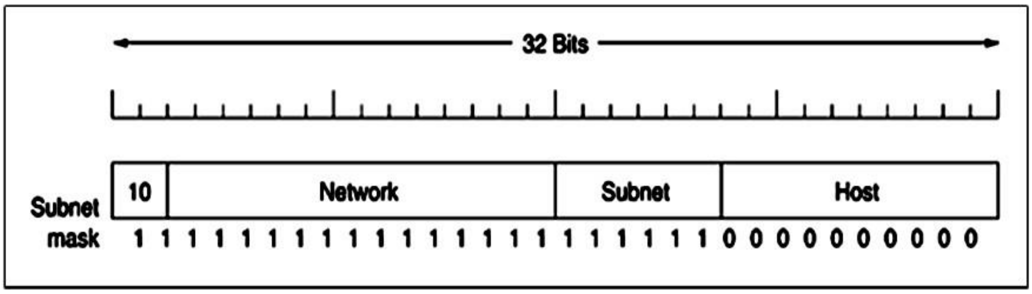


Class	Number of Networks	Number of Hosts	Application
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

- The IP address 0.0.0.0 is used by hosts when they are being booted.
- All addresses of the form 127.xx.yy.zz are reserved for loopback testing, they are processed locally and treated as incoming packets.

Subnetting

- It allows a network to be split into several parts for internal use but still act like a single network to the outside world.
- To implement subletting, the router needs a subnet mask that indicates the split between network + subnet number and host. Ex. 255.255.252.0/22. A||/22|| to indicate that the subnet mask is 22 bits long.
- Consider a class B address with 14 bits for the network number and 16 bits for the host number where some bits are taken away from the host number to create a subnet number.



1 : Class B network subnetted into 64 subnets.

- If 6 bits from the host Id are taken for subnet then available bits are :
  14 bits for network + 6 bits for subnet + 10 bits for host
- With 6 bits for subnet the number of possible subnets is 2^6 which is 64.
- With 10 bits for host the number of possible host are 2^{10} which is 1022 (0 & 1 are not available)

CIDR

A class B address is far too large for most organizations and a class C network, with 256 addresses is too small. This leads to granting Class B address to organizations who do not require all the address in the address space wasting most of it.

This is resulting in depletion of Address space. A solution is CIDR (Classless InterDomain Routing) The basic idea behind CIDR, is to allocate the remaining IP addresses in variable-sized blocks, without regard to the classes.

NAT (Network Address Translation)

The scarcity of network addresses in IPv4 led to the development of IPv6. IPv6 uses a 128 bit address, hence it has 2128 addresses in its address space which is larger than 232 addresses provided by IPv4. Transition from IPv4 to IPv6 is slowly occurring, but will take years to complete, because of legacy hardware and its incompatibility to process IPv6 address. NAT (Network Address Translation) was used to speed up the transition process

The only rule is that no packets containing these addresses may appear on the Internet itself. The three reserved ranges are:

10.0.0.0 – 10.255.255.255/8 (16,777,216 hosts)
172.16.0.0 – 172.31.255.255/12 (1,048,576 hosts)
192.168.0.0 – 192.168.255.255/16 (65,536 hosts)

Within the Organization, every computer has a unique address of the form 10.x.y.z. However, when a packet leaves the organization, it passes through a NAT box that converts the internal IP source address, 10.x.y.z, to the organizations true IP address, 198.60.42.12 for example.

Modulation

The Process of converting analog data to analog signal is called Modulation.

Types of Modulation:

Signal modulation can be divided into two broad categories:

- Analog modulation
- Digital modulation

Analog or digital refers to how the data is modulated onto a sine wave. Ex AM, FM, PM.

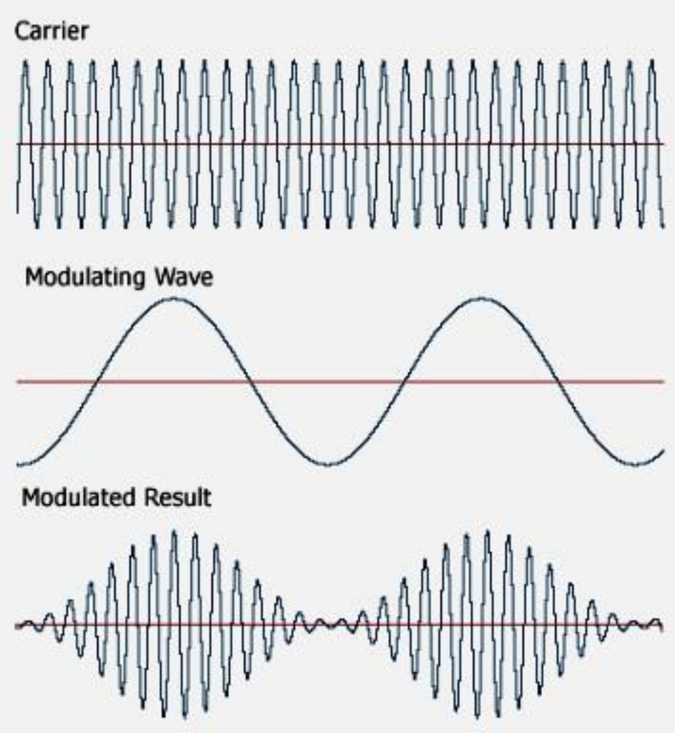
If analog audio data is modulated onto a carrier sine wave, then this is referred to as analog modulation.

Digital modulation is used to convert digital data to analog signal. Ex ASK, FSK, PSK.

Analog Modulation

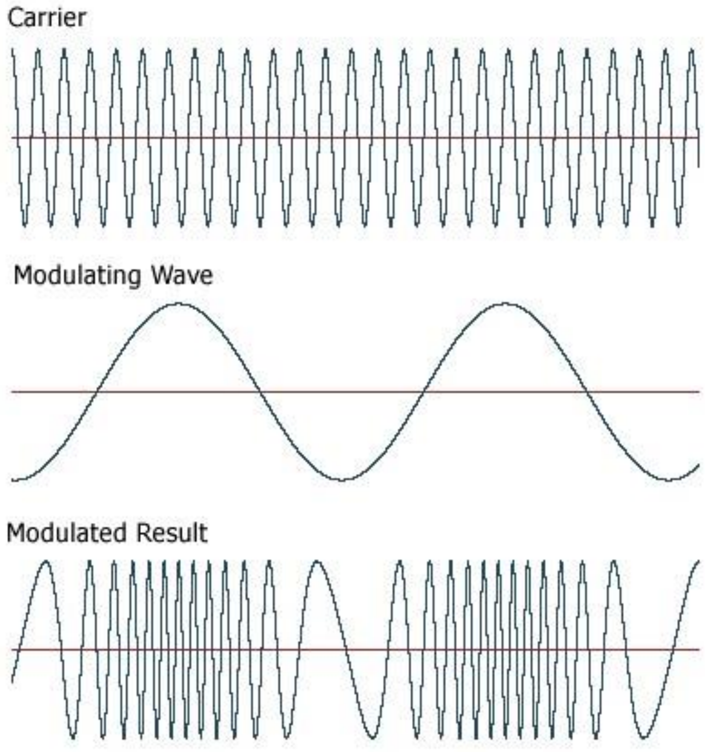
AM

Amplitude modulation is a type of modulation where the amplitude of the carrier signal is varied in accordance with modulating signal. The envelope, or boundary, of the amplitude modulated signal embeds modulating signal. Amplitude Modulation is abbreviated AM.



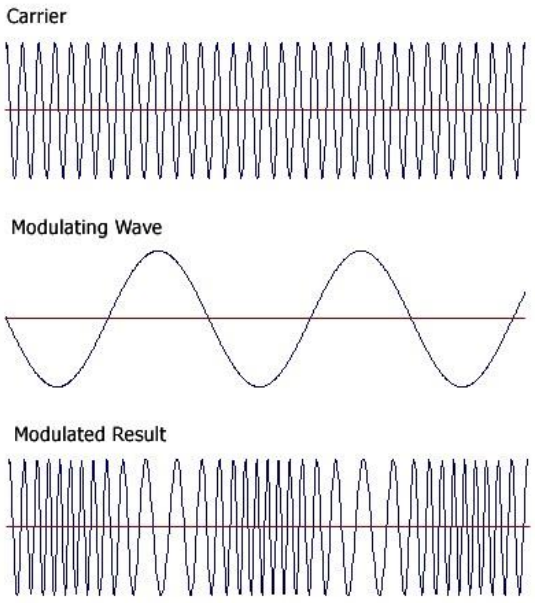
FM

Frequency modulation is a type of modulation where the frequency of the carrier is varied in accordance with the modulating signal. The amplitude of the carrier remains constant. The information-bearing signal (the modulating signal) changes the instantaneous frequency of the carrier. Since the amplitude is kept constant, FM modulation is a low-noise process and provides a high quality modulation technique which is used for music and speech in hifidelity broadcasts. Frequency Modulation is abbreviated FM.

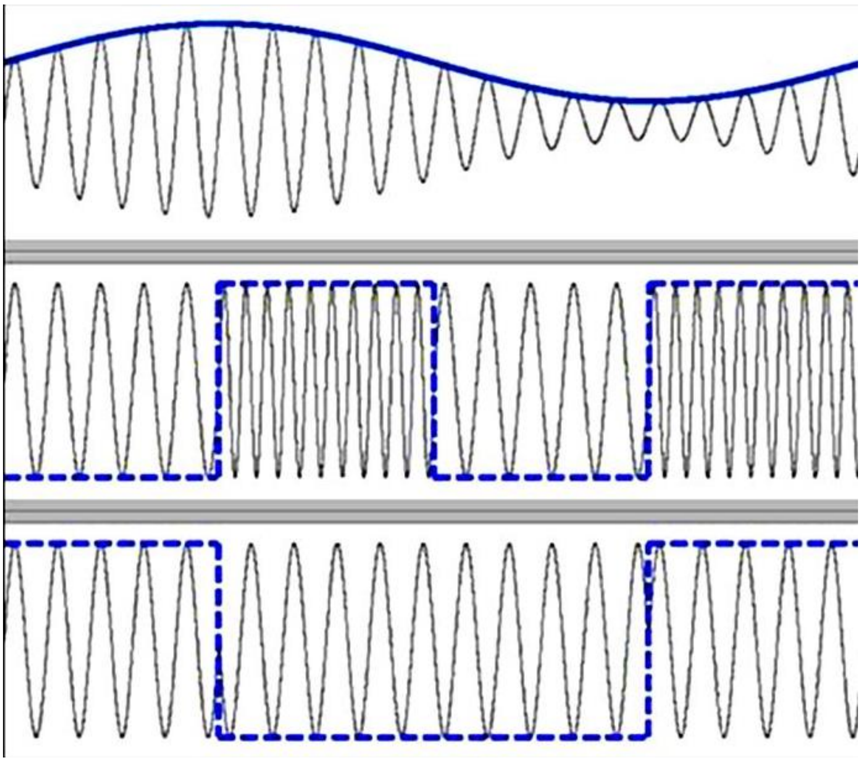


PM

In phase modulation, the instantaneous phase of a carrier wave is varied from its reference value by an amount proportional to the instantaneous amplitude of the modulating signal. Phase Modulation is abbreviated PM.



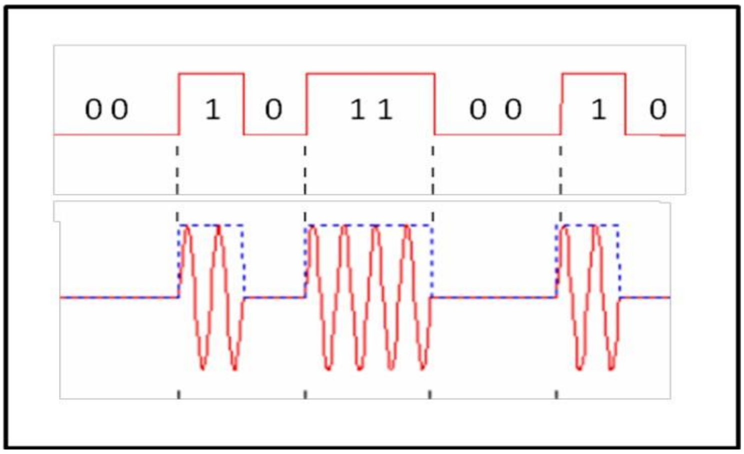
Comparison of AM, FM, PM



Digital Modulation

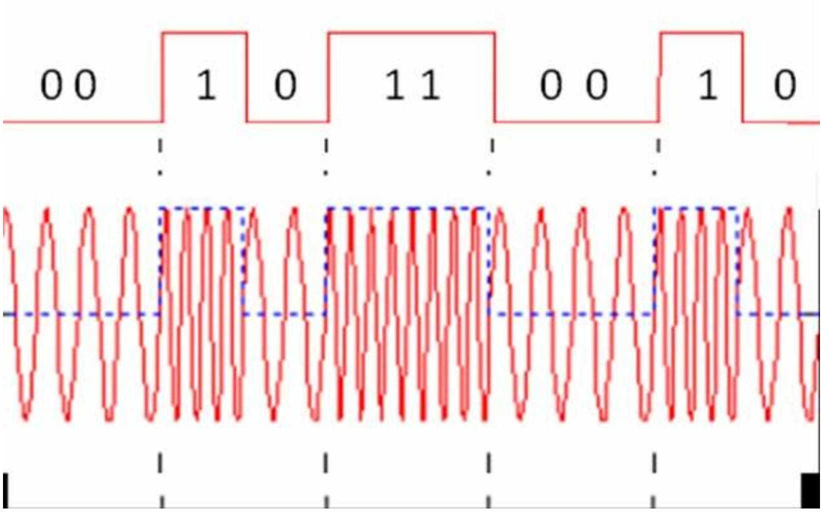
ASK

In amplitude shift keying, the amplitude of the carrier signal is varied to create signal elements. Both frequency and phase remain constant while the amplitude changes. ASK is normally implemented using only two levels and is hence called binary amplitude shift keying. Bit 1 is transmitted by a carrier of one particular amplitude. To transmit Bit 0 we change the amplitude keeping the frequency is kept constant



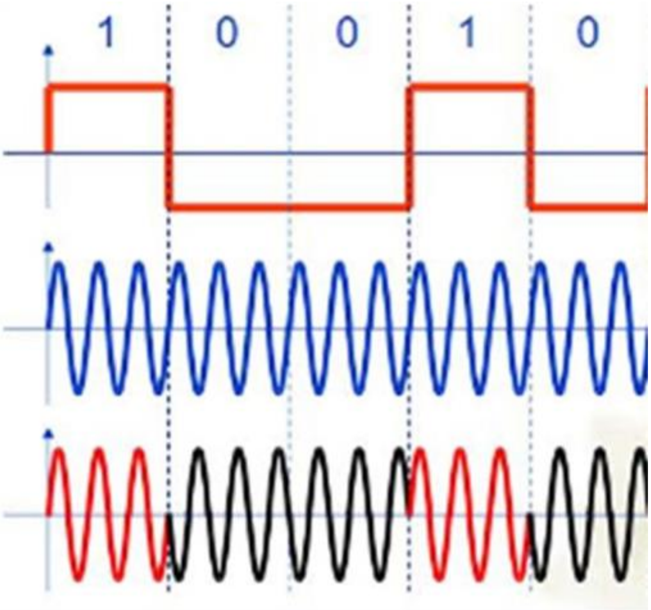
FSK

In Frequency shift keying, we change the frequency of the carrier wave. Bit 0 is represented by a specific frequency, and bit 1 is represented by a different frequency. In the figure below frequency used for bit 1 is higher than frequency used for bit 0



PSK

Phase shift keying (PSK) is a method of transmitting and receiving digital signals in which the phase of a transmitted signal is varied to convey information. Both amplitude and frequency remain constant as the phase changes. The simplest form of PSK has only two phases, 0 and 1. If the phase of the wave does not change, then the signal state stays the same (low or high). If the phase of the wave changes by 180 degrees, that is, if the phase reverses, then the signal state changes (from low to high or from high to low)

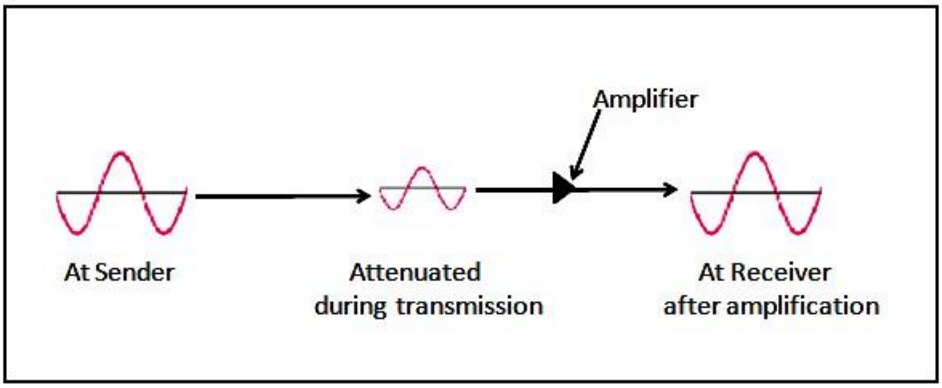


Transmission Impairments and Types

Data is transmitted through transmission medium which are not perfect. The imperfection causes signal impairment. Due to the imperfection error is introduced in the transmitted data i.e. the original signal at the beginning of the transmission is not the same as the signal at the Receiver. There are three causes of impairment: attenuation, distortion, and noise as shown below

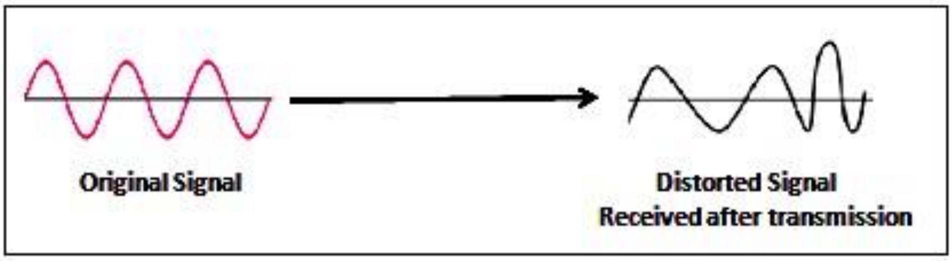
Attenuation

Attenuation results in loss of energy. When a signal travels through a medium, it loses some of its energy in overcoming the resistance of the medium. The electrical energy in the signal may converted to heat. To compensate for this loss, amplifiers are used to amplify the signal. Figure below shows the effect of attenuation and amplification.



Distortion

Distortion changes the shape of the signal as shown below



Noise

Noise is any unwanted signal that is mixed or combined with the original signal during transmission. Due to noise the original signal is altered and signal received is not same as the one sent.