Data Communication

A/L ICT –Lesson 06

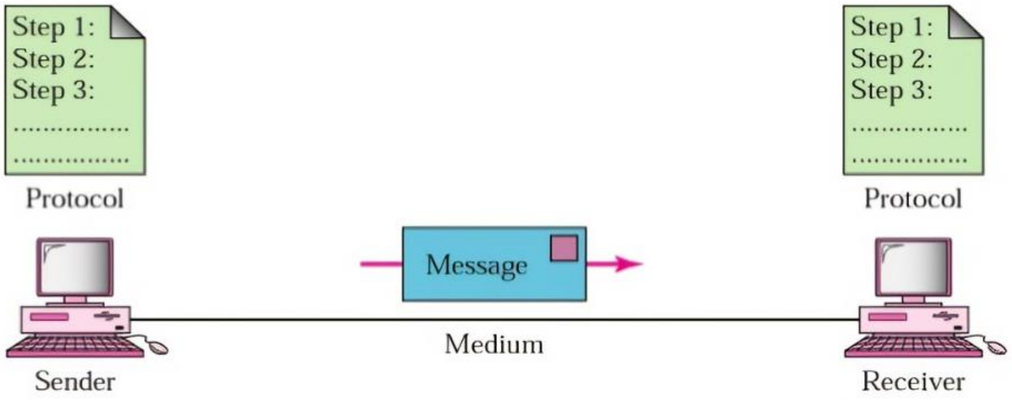
Computer networking refers to interconnected computing devices that can exchange data and share resources with each other. These networked devices use a system of rules, called communications protocols, to transmit information over physical or wireless technologies.

Data Communication

Introduction to data communication

Data communication is the process of transmitting data between two or more communicating devices over some transmission media. Establishing such connections between computing devices is called computer networking.

Components of a Data Communication



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

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

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

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

5. **Protocol** - a communication network protocol defines the order and the format of data when the data is exchanged between two networking devices. The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods.

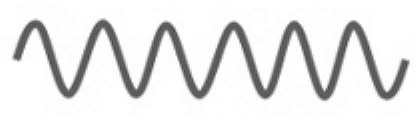
Computer Network: A computer network consists of two or more computers that are linked together using a communication medium in order to share resources.

Signals

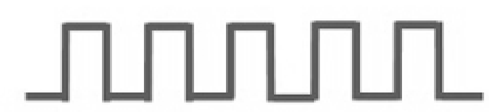
A signal is an electronic voltage or current, which varies with time. It is used to transfer data from one end to another.

Analog signal: Analog signals are in continuous wave form in nature and represented by continuous electromagnetic waves. Examples of such signals are sound, light and temperature etc.

Digital signal: Digital stands for discrete values and hence it means that they use specific values to represent any information. In digital signal, only two values are used to represent something i-e: 1 and 0 (binary values).



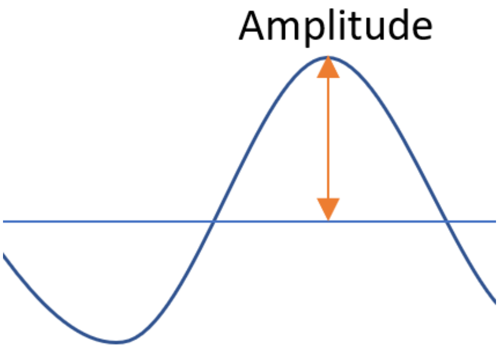
Analog Signal



Digital Signal

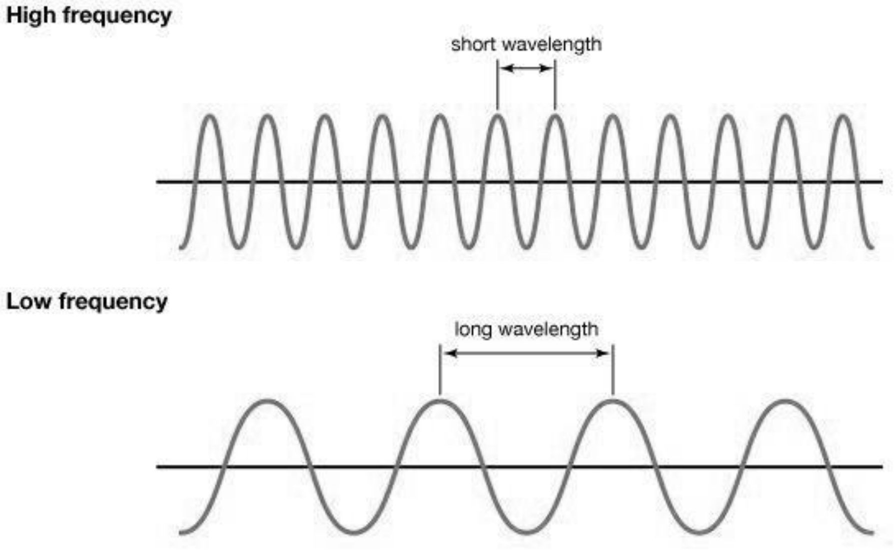
Properties of signals

Amplitude : The height of the wave measured in meters.

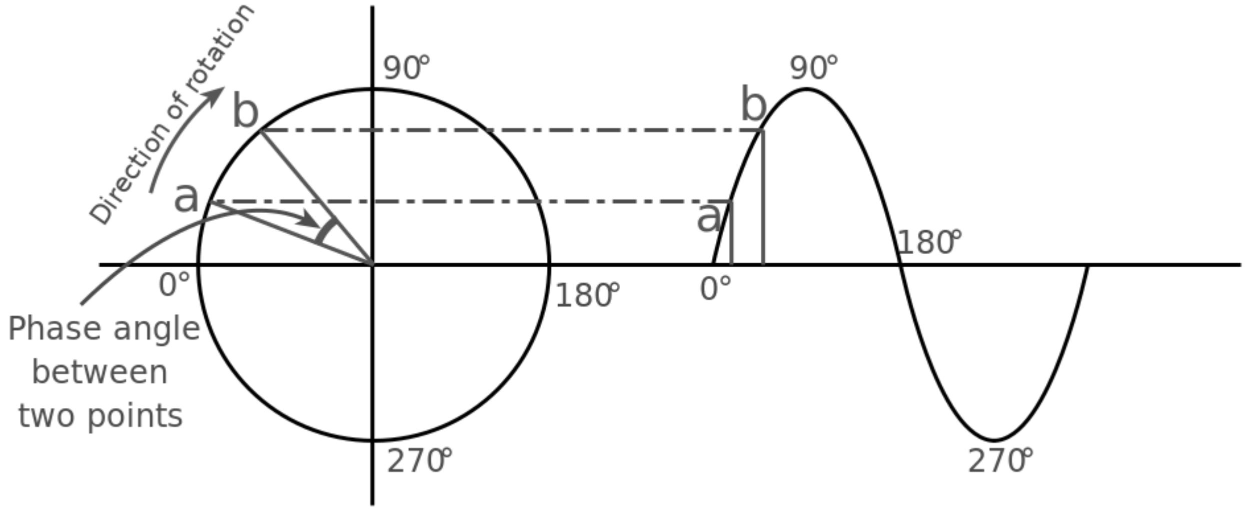


Frequency : The number of complete waves that pass a point in one Second, Measured in Hertz (Hz)

Wavelength : The distance between adjacent crests, measured in meters.



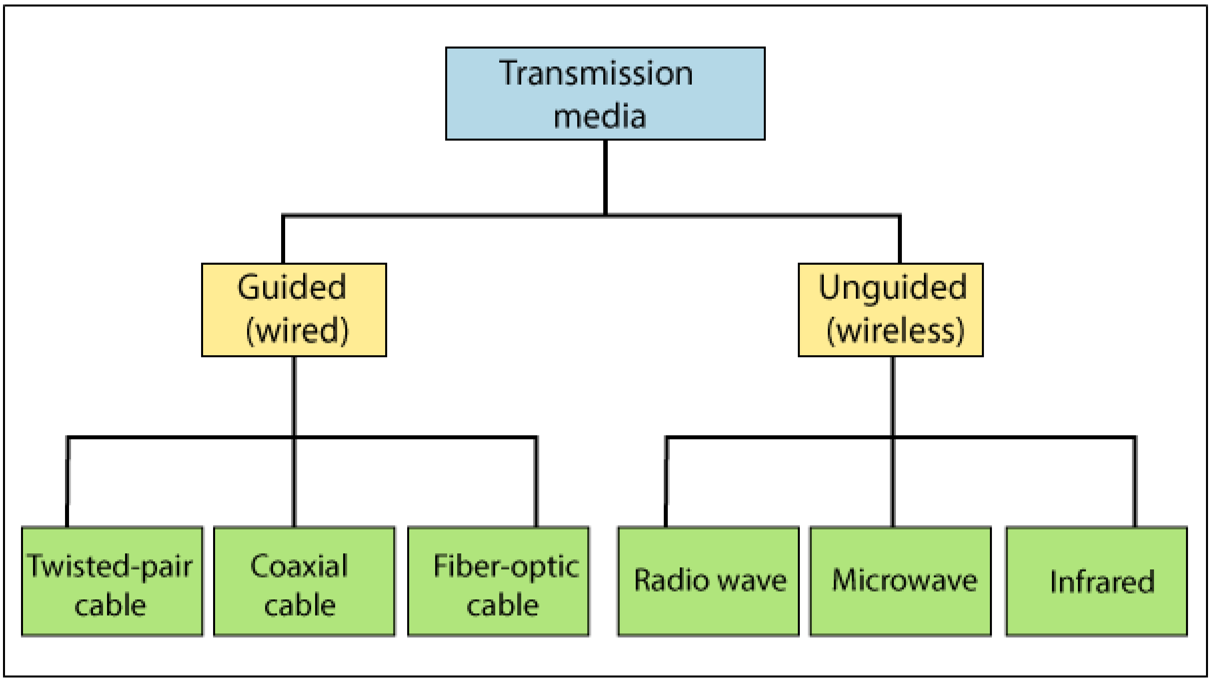
Phase : phase is a position of a point in time (instant) on a waveform cycle.



Propagation speed in a media : The speed at which a wave propagates through a given medium .The propagation speed also varies from medium to medium depending on the properties of the medium.

Transmission media

Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.



Guided / Wired : If the medium used for data transmission is a physical medium, it is called guided or wired. Wires are often called guided media because they guide the data transfer data from one point to another without altering the frequencies, data impairment are therefore reduced.

1. **Twisted Pair Cable -** Pairs of twisted copper wire are used for data transmission. There are two types.

   I. **Unshielded Twisted Pair (UTP)** : The twisted copper wire pairs used for telephone connections. These are very flexible and low-priced. However, it is difficult to transmit data for a long distance through UTP wires. It is suitable for maximum of 100 meters.

   II. **Shielded Twisted Pair (STP) :** STP is a better quality and secure data transmission medium. However it is expensive.

2. **Coaxial Cable -** This consists of an electronic cable pair. The outer cable which is like a braided copper net produces electromagnetic field around the central cable. These two cables are separated by a plastic shield. These cables are expensive and used for TV antenna and CCTV.

3. **Fiber Optics cable** - Fiber Optics cable consists of a pair of an cables. There is a plastic jacket to separate the two cables. Core is a glass tube and there is glass cladding around it. The data transmission is carried out by while reflecting light. These are used in modern telephone networks. The cable is reletively more expensive.

Unguided/Wireless Media : Data is transmitted as signal through the air without using physical medium is called unguided/wireless media.

1. **Radio waves** - Data transmission is performed using radio waves. Wifi and Bluetooth are examples for radio waves based communication.
2. **Microwaves** - Microwaves travel in a linear mode. Transmission center is positioned facing each other. The distance between centers are decided based on geographical factor of the area. Microwaves are used in Satellite communication to transmit data as transponders. Satellite centers, which are positioned in the sky above 36000 km, capture data transmitted as microwaves through satellite towers positioned in the Earth and then transmit the data back to the required tower. Using this method, data can be transmitted to any distance. This is also used in internet communication.
3. **Infrared** - Infrared data transmission is used in TV remote controllers, wireless keyboards and mouse etc.

Properties of signal transmission media

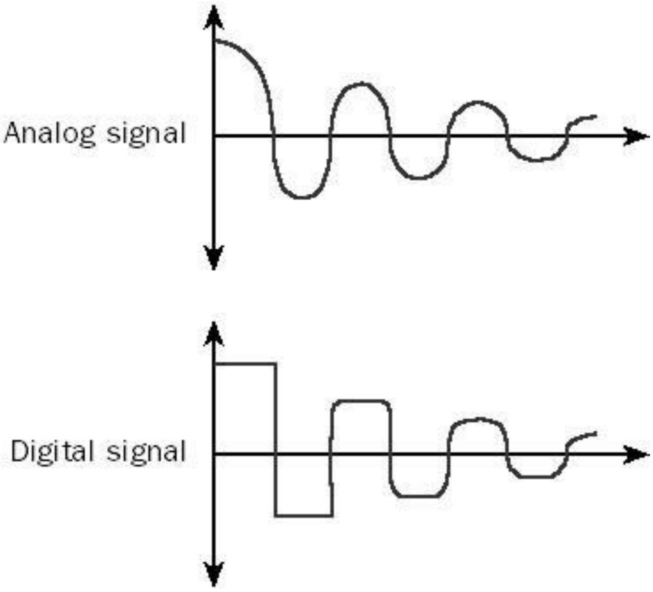
Latency : Network Latency is an expression of how much time it takes for a unit of data to travel from one point to another. Latency is usually measured in milliseconds.

Bandwidth : Bandwidth is a range of frequencies and measured in Hertz.

Transmission Impairment in Data Communication

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

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



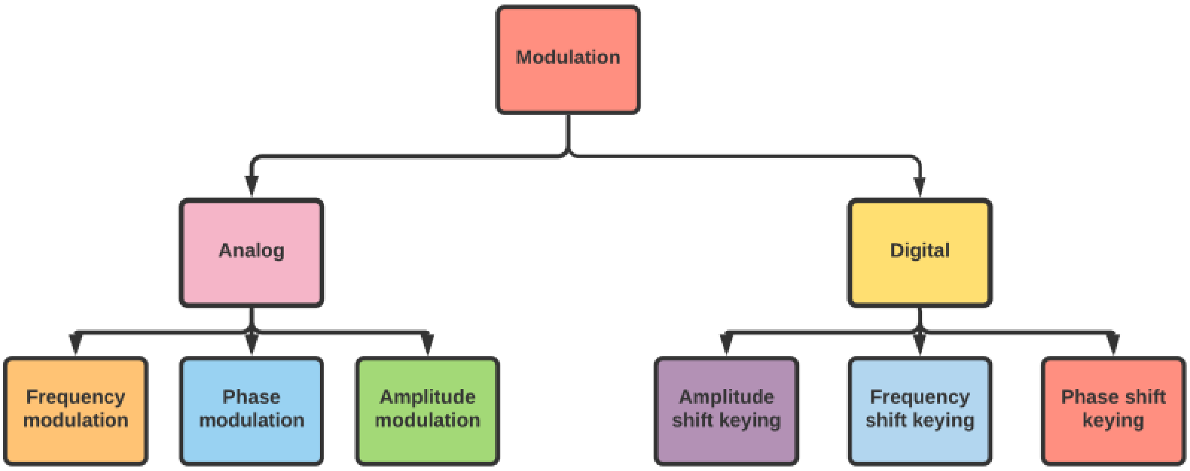
Distortion – Distortion is alteration (distort) of properties of a transferred signal caused by the capacitance and inductance of the communication medium.

Noise – The random or unwanted signal that mixes up with the original signal is called noise. There are several types of noise such as induced noise, crosstalk noise, thermal noise and impulse noise which may corrupt the signal.

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

Modulation

Modulation is the technique used to send information by modifying the basic characteristics such as frequency, amplitude and phase, of an electromagnetic signal (modulating signal) by attaching it to a higher frequency signal (carrier signal), producing a modulated signal. The most commonly used method is the Pulse Code Modulation (PCM).



Analog Modulaton

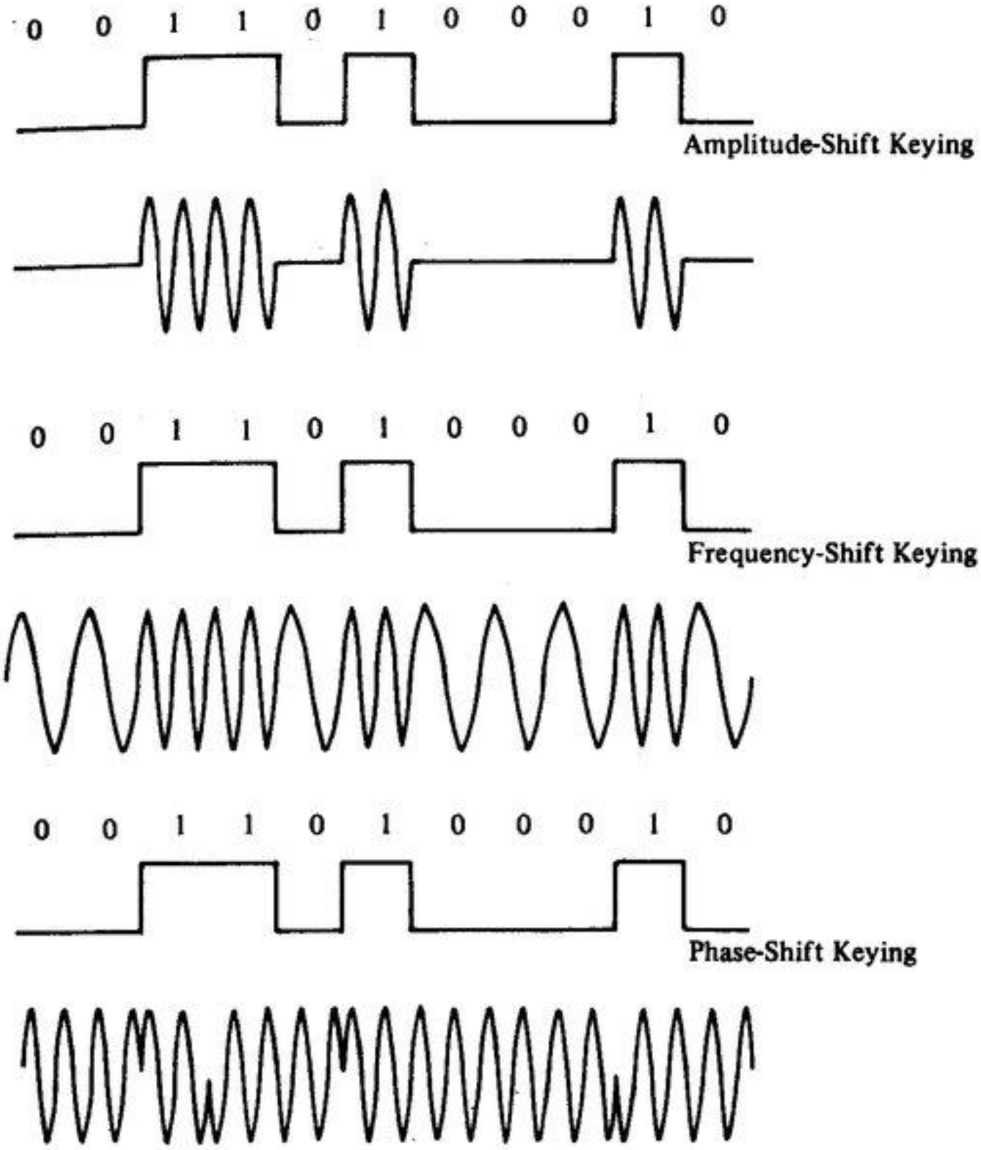
1. **Amplitude Modulation (AM)** : Amplitude of carrier signal varies according to the amplitude of modulating signal. The frequency or phase of the carrier signal remains unchanged.
2. **Frequency Modulation (FM)** : The carrier signal frequency changes according to the frequency of the Modulating signal.
3. **Phase Modulation (PM)** : The phase of a carrier signal is modulated in order to reflect the changes in voltage (amplitude) of an analog data signal.

Digital-to-Analog Conversion

If the modulating signal is a digital signal, then three modulation schemes can be used.

1. **Amplitude Shift Keying (ASK) :** In this conversion technique, the amplitude of an analog carrier signal is modified to reflect binary data. When binary data represents digit 1, the amplitude is held at 1, otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal .
2. **Frequency Shift Keying (FSK)** : In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.

3. **Phase Shift Keying (PSK)** : In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.

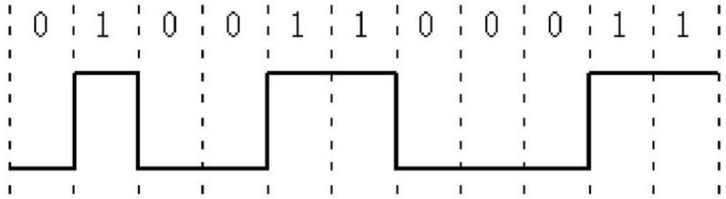


Synchronization : synchronization is used to ensure that the data streams are received and transmitted correctly between two devices. Usually a clock signal is transmitted in sequence with a data stream to maintain proper signal timing.

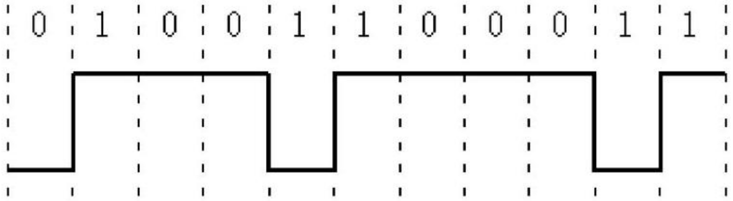
Signal Encoding Schemes

- Encoding is the conversion of data into digital signals. There are several ways to map digital data to digital signals. Some of them are −

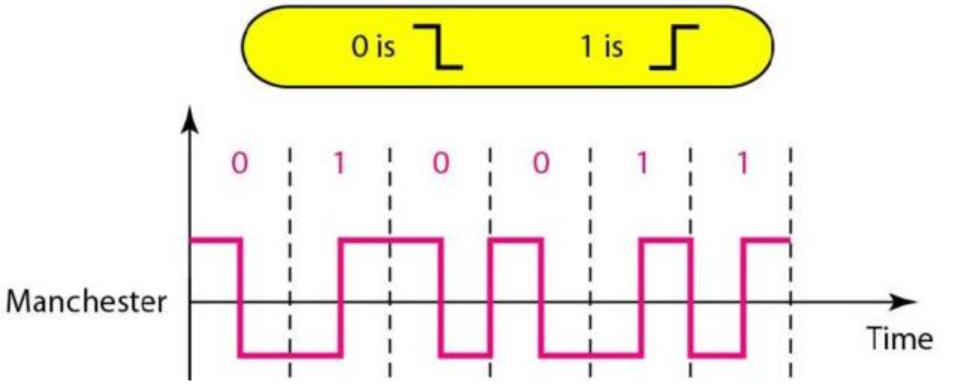
Non-return to Zero Level (NRZ-L): is an encoding scheme in which two different voltages for 0 and 1 bits are used to represent data and remain constant during a bit interval.



Non-return to Zero Inverted (NRZ-I): in this encoding scheme, in which a “1" is represented by a transition of the physical level, while a "0" has no transition.



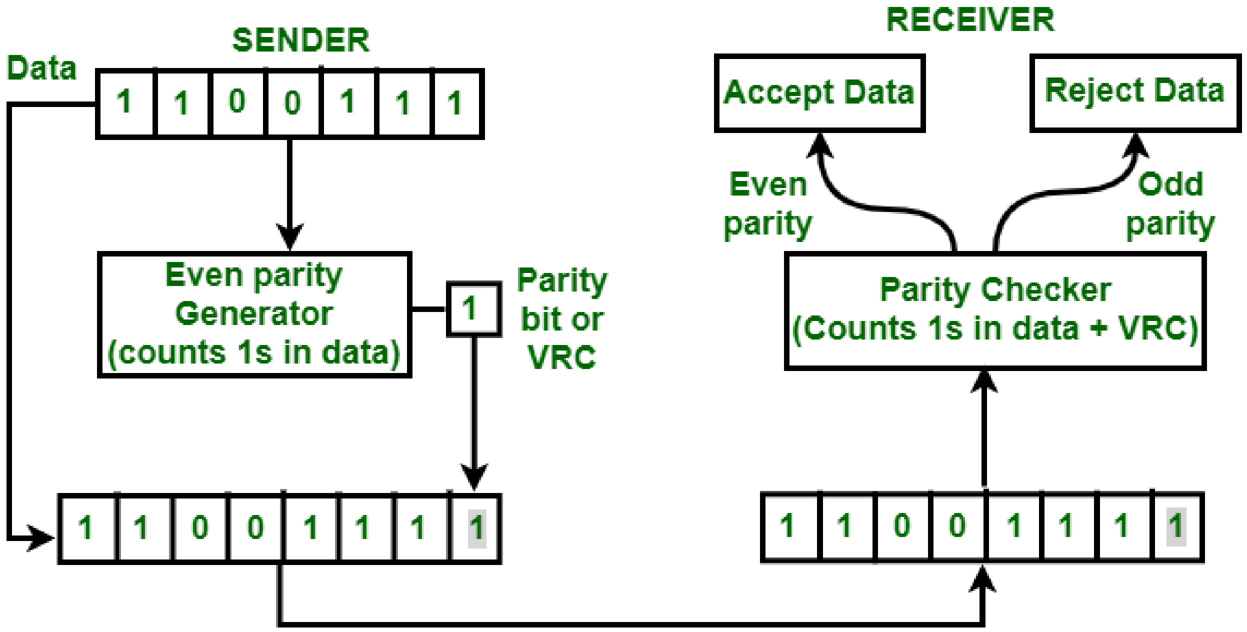
Manchester encoding: in Manchester encoding voltage changes from low to high or high to low in the middle of the signal.



Error Control: During data transmission, sometimes data bits may get flipped due to various reasons. In such situations the data bit received is in error. Error detection is the process of identifying that the data bit has been altered during transmission. Error correction and recovery mechanisms are used to correct the data bits received in error and to recover the actual data bits.

Parity Check: is one simple error detection mechanism where an extra bit of data is added and sent along with the original data bits to make number of 1s in the data as either even in the case of even parity, or odd in the case of odd parity.

Example –
If the source wants to transmit data unit 1100111 using even parity to the destination. The source will have to pass through Even Parity Generator.



Parity generator will count number of 1s in data unit and will add parity bit. In the above example, number of 1s in data unit is 5, parity generator appends a parity bit 1 to this data unit making the total number of 1s even i.e 6 which is clear from above figure. Data along with parity bit is then transmitted across the network. In this case, 11001111 will be transmitted. At the destination, This data is passed to parity checker at the destination. The number of 1s in data is counted by parity checker.If the number of 1s count out to be odd, e.g. 5 or 7 then destination will come to know that there is some error in the data. The receiver then rejects such an erroneous data unit.

Public Switched Telephone network (PSTN)

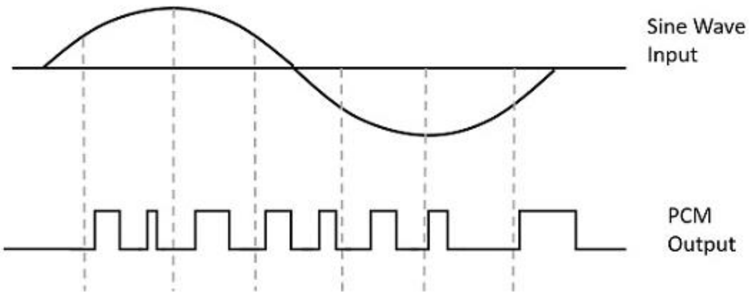
PSTN provides infrastructure and services for public telecommunication. The PSTN is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephony operators. These consist of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all interconnected by switching centers which allow most telephones to communicate with each other.

Modem

The modem is used to connect the computers of a computer network or a personal computer at home to the internet. The modem acts as a data translator. Digital signals sent from the computer is translated to analog signals and the analog signals send to the computer from the internet is translated to digital signals. This is called MOdulation and DEModulation. Hence, 'MODEM' is a combination of these two words. There are different types of MODEMs. Those are internal, external and wireless modems. Todays routers have a modem inbuilt in the device.

Different modulation schemes are used to modulate data and Pulse Code Modulation (PCM) is one method in which the samples of an analog signal are taken (called a pulse amplitude modulated signal) and then are shown that the original signal can be constructed at the receive end using these samples.

PCM (pulse code modulation) is a digital scheme for transmitting analog data. It converts an analog signal into digital form.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).



Network Topology

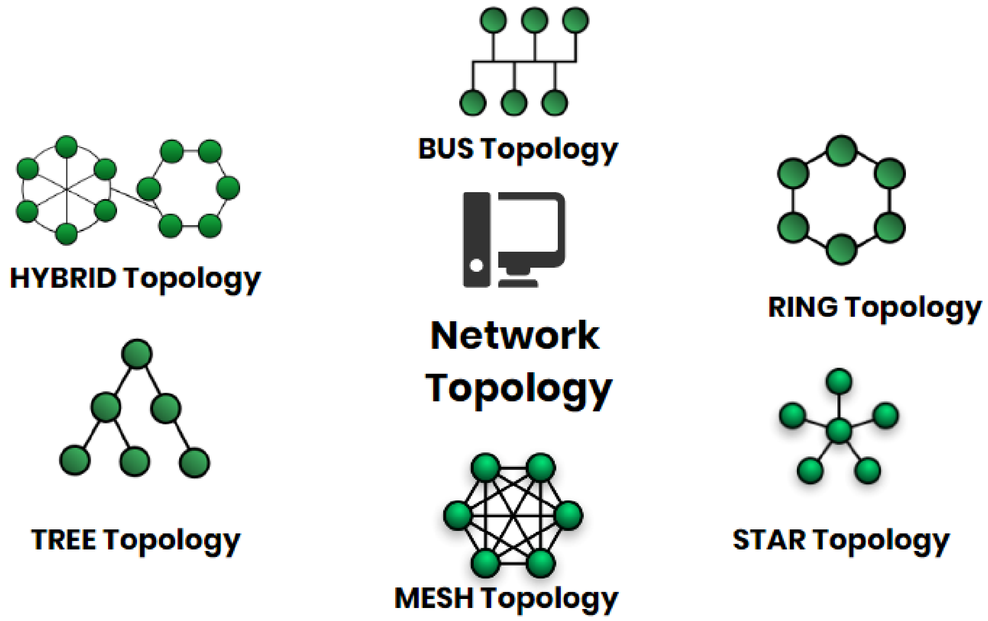
Network topology is the pattern of connection in designing computer network. There are different types of network topologies. Those are,

Bus Topology: A bus topology consists of a main run of cable with terminators at each end. All nodes (file server, workstations, and peripherals) are connected to the linear cable. This cable is called the backbone because any issue with the network affects all the computers in the network. This design is easy in networking and fewer cables are required. However, a limited number of computers can be connected.

Star Topology: A star topology is designed with each node is (file server, workstations, and peripherals) connected directly to a central network hub or switch. If hub goes down everything goes down, none of the devices can work without hub.

Ring Topology: in a ring topology each station is directly connected only to two of its neighbors. Messages sent between two stations pass through all of the stations in between (clockwise or counterclockwise). The breakdown of one computer or cable can lead to the breakdown of the entire network.

Mesh Topology: In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection with few hosts only. Since this is a complex connection pattern, it is costly and difficult to control. However, a breakdown of one computer does not affect the connections in the network. Mesh networking can be found on internet.



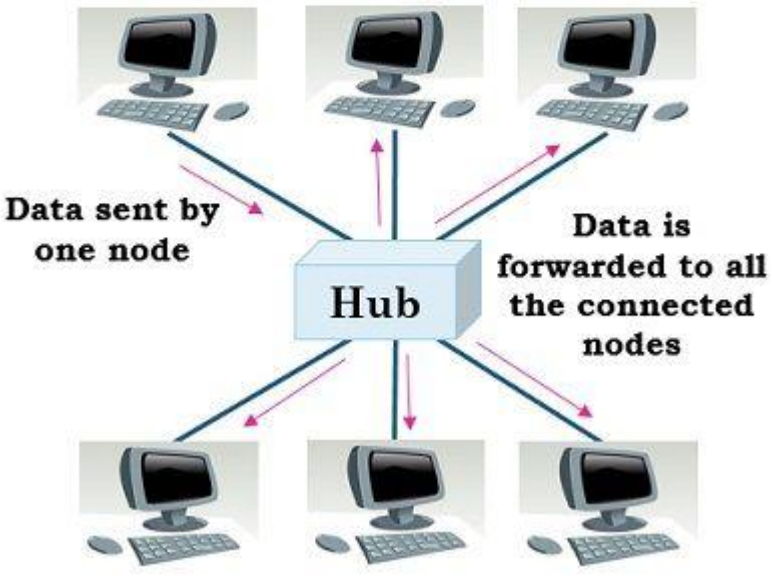
Topology	Advantages	Disadvantages
Bus	The easiest network topology for connecting peripherals or computers in a linear fashion. It is easy to connect or remove devices in this network without affecting any other device.	Bus topology is not great for large networks. If a main cable is damaged, whole network fails or splits into two. This network topology is very slow as compared to other topologies.
Ring	In this data flows in one direction which reduces the chance of packet collisions. Equal access to the resources. Speed to transfer the data is very high. Minimum collision. It is cheap to install and expand.	Due to the Uni-directional Ring, a data packet (token) must have to pass through all the nodes. If one workstation shuts down, it affects whole network or if a node goes down entire network goes down.
Star	It is very reliable – if one cable or device fails then all the others will still work.It is	Requires more cable than a linear bus. If hub goes down everything goes

	high-performing as no data collisions can occur. Easy fault detection because the link are often easily identified.	down, none of the devices can work without hub. Extra hardware is required (hubs or switches) which adds to cost.
Mesh	Failure during a single device won't break the network. Adding new devices won't disrupt data transmissions. This topology provides multiple paths to succeed in the destination and tons of redundancy.	It's costly as compared to the opposite network topologies i.e. star, bus, point to point topology. Installation is extremely difficult in the mesh. Maintenance needs are challenging with a mesh.

Switches and hubs:

Hubs and switches are common network devices that function as a common connection point for network devices that make up a network. **A switch** receives data in one of its incoming connections and forwards the data only on the outgoing connection which connects to the destination device. **A hub** receives data in one of its incoming connections and then shall forward the data to all of its outgoing connection.

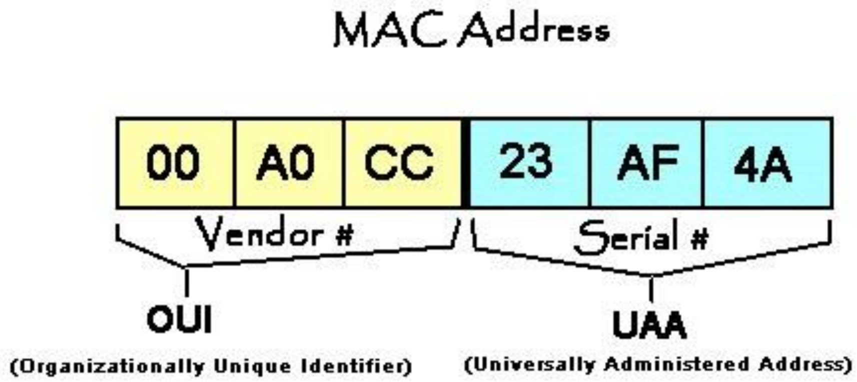
Differences between the switch and hub - The main difference is the data transmission speed. Hub sends the transmitted data to all computers but switch sends data to the relevant computer only. Here hub may create an unnecessary network data congestion. In this way a switch is a more intelligent device than a hub. In data transmission, hub uses half duplex mode and the switch uses full duplex mode.



Local Area Network (LAN): A local area network is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, or a university campus.

Media Access Control Address (MAC address)

MAC addresses are unique addresses assigned each network interface of a communicating device. MAC addresses are 48 bits long and are divided in to 6 blocks separated by colons. Each block is 8 bits long and is further divided in to two 4 bit blocks. Each four bit address is converted to hexadecimal number and a typical Mac address would look like 4A:8F:3C:4F:9E:3D. When devices send and receive data over a network, MAC addresses enable the unique identification of the device interface and the correct delivery of the data to the receivers interface.


MAC Address
00
A0
CC
23
AF
4A
Vendor #
Serial #
OUI
(Organizationally Unique Identifier)
UAA
(Universally Administered Address)

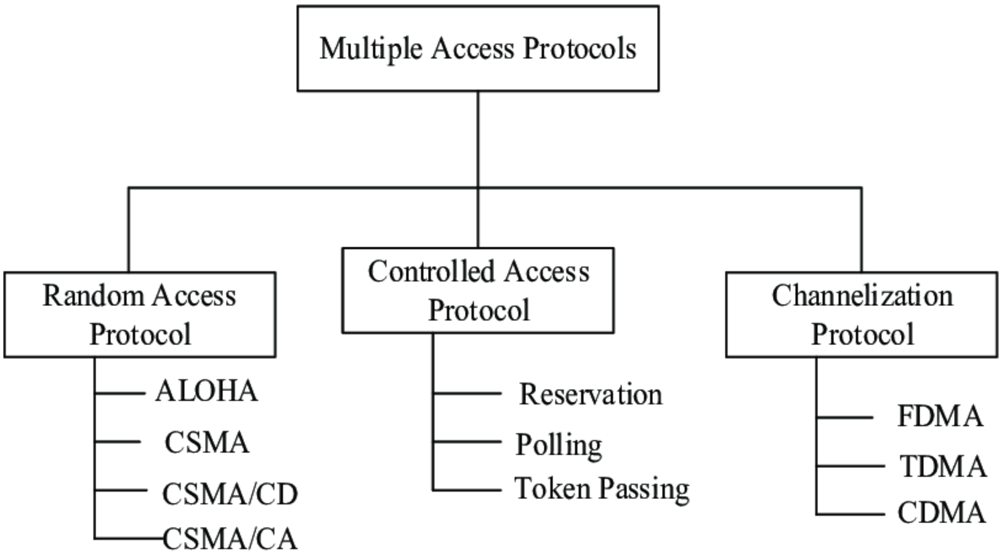
Frames : When data is generated at the source to be sent to the receiver over the communication link, at the Data link layer, data are encapsulated in to the Frame, where the data is inserted in to the frame and the MAC addresses of the sending device and the MAC address of the adjacent node are included in the header of the frame. Each frame is made depending on the quality of the link connecting ea pair of devices.

Protocol : A communication network protocol defines the order and the format of data when the data is exchanged between two networking devices. Many protocols exist in the networking world and medium access control protocols enable the orderly access to a common shared medium of communication. In bus topology, a common medium is shared by many devices and a medium access control protocol can ensure that the medium is accessed in an orderly manner therefore data collisions are avoided.

Multiple Access Control Protocols

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk.

For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created(data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.



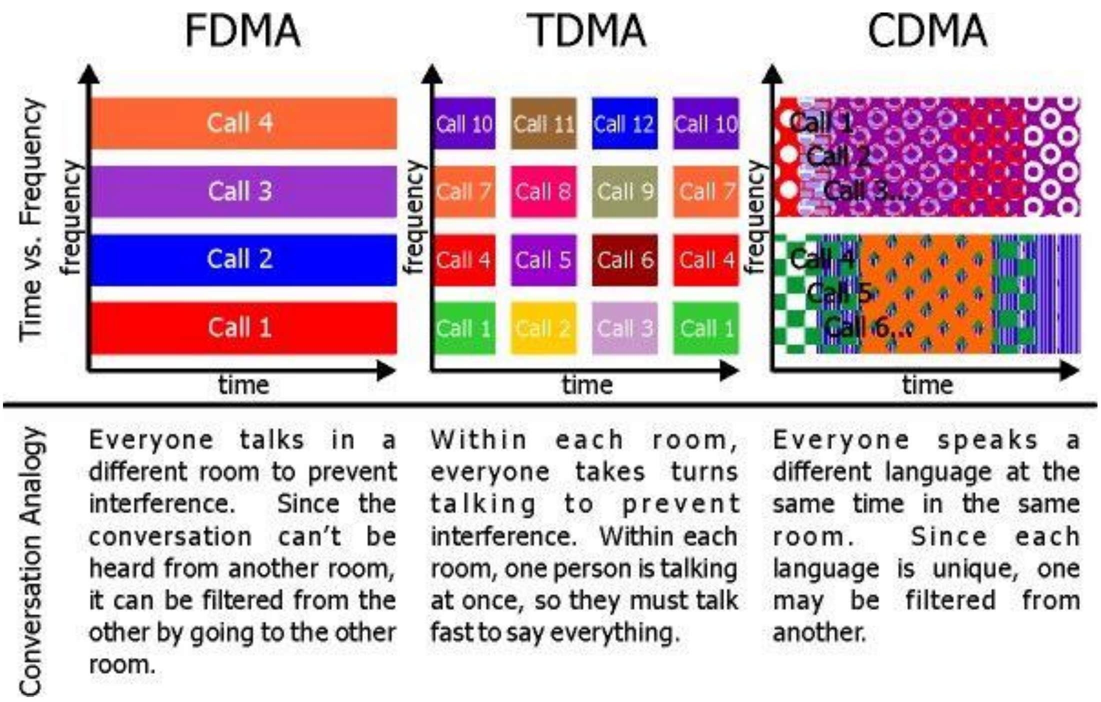
Channelization Protocols

Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations. The three channelization protocols are FDMA, TDMA, and CDMA.

In frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data. In other words, each band is reserved for a specific station, and it belongs to the station all the time. Each station also uses a bandpass filter to confine the transmitter frequencies. To prevent station interferences, the allocated bands are separated from one another by small guard bands.

In time-division multiple access (TDMA), the stations share the bandwidth of the channel in time. Each station is allocated a time slot during which it can send data. Each station transmits its data in is assigned time slot. The following figure shows the idea behind TDMA.

Code-Division Multiple Access(CDMA) simply means communication with different codes. CDMA differs from FDMA because only one channel occupies the entire bandwidth of the link. It differs from TDMA because all stations can send data simultaneously; there is no timesharing.



Everyone talks in a different room to prevent interference. Since the conversation can't be heard from another room, it can be filtered from the other by going to the other room.

Within each room, everyone takes turns talking to prevent interference. Within each room, one person is talking at once, so they must talk fast to say everything.

Everyone speaks a different language at the same time in the same room. Since each language is unique, one may be filtered from another.

ALOHA – It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

- **Pure Aloha:**

When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.

- **Slotted Aloha:**

It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

CSMA – Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium.If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

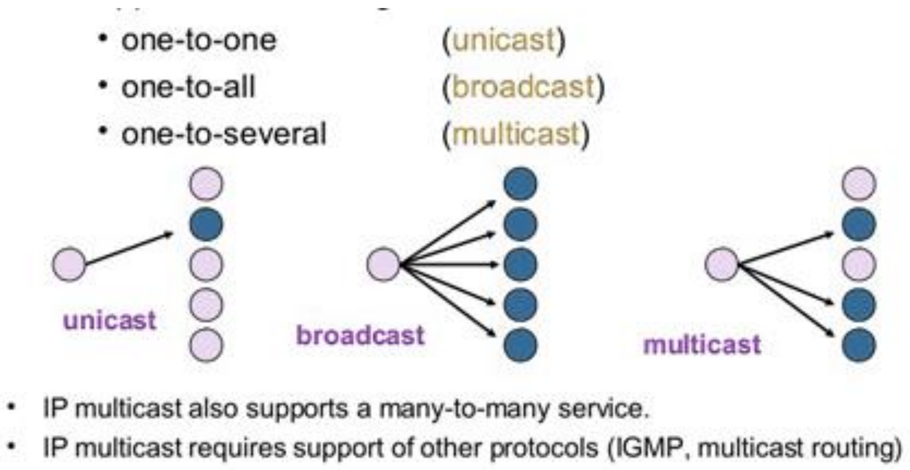
- **CSMA/CD** – Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected.
- **CSMA/CA** - Carrier-sense multiple access with collision avoidance in computer networking, is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be "idle".

Unicast, Broadcast and Multicast

Broadcast of messages involves sending a message to larger set of recipients.

In **Unicast** data is sent from one computer to another computer by including the unique address of the recipient in the message itself.

A **MultiCast** communication is from one device on the network to many, but not all, devices on the network.



- one-to-one (unicast)
- one-to-all (broadcast)
- one-to-several (multicast)

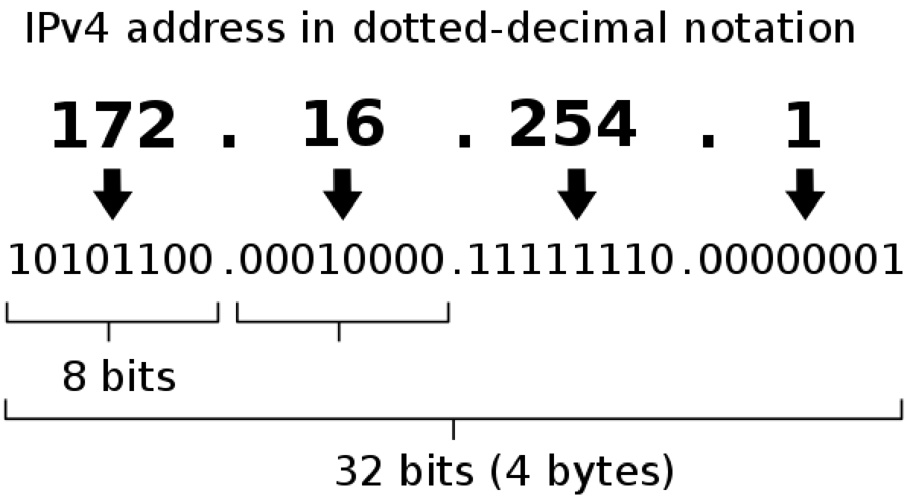
- IP multicast also supports a many-to-many service.
- IP multicast requires support of other protocols (IGMP, multicast routing)

Interconnection of Networks

A gateway is basically a device or a hardware which acts like a “gate” among the networks.Thus it can also be defined as a node which acts as an entrance for the other nodes in the network.It is also responsible for enabling the traffic flow within the network.Gateway uses more than one protocol for communication thus its activities are much more complex than a switch or a router. So a gateway is basically a device that is used for the communication among the networks which have a different set of protocols and is responsible for the conversion of one protocol into the other.For any kind of workplace, the gateway is a computer system which is responsible for routing the traffic from the main workstation to outside network. For homes, it is responsible for giving the access to the internet thus acting as an internet service provider.

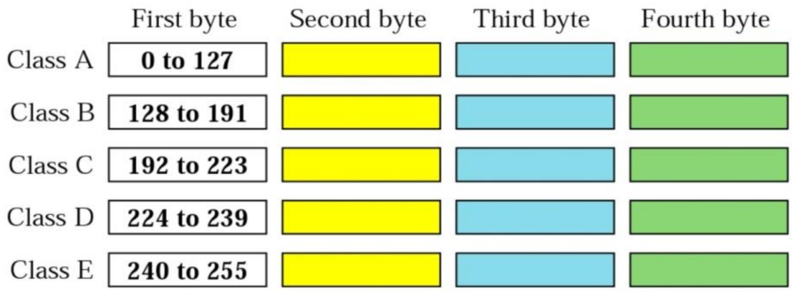
IP addresses are unique addresses assigned to each device On the network. IP Version 4 (IPv4) is 32 bits long and can address up to 4 billion devices. IPv4 has only 2^{32} addresses. IP Version 6 (IPv6) is 128 bits long and is plenty enough to address a huge number of networkable devices. Ipv6 has 2^{128} addresses.

Dotted decimal notation - For human convenience the IP address is written in dotted decimal notation. The 32-bit address is divided into 4 groups of 8 bits (an octet or a byte). Each octet is written as a decimal number ranging from 0 to 255. The decimal numbers are separated by periods, or dots.



CLASSES OF IP ADDRESSES

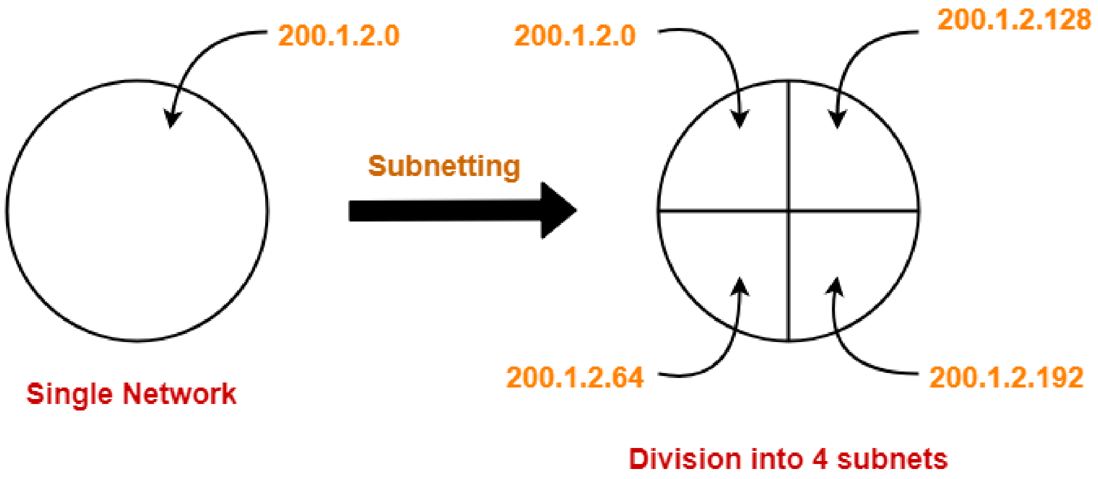
- Class of an IP address is identified using the first octet.



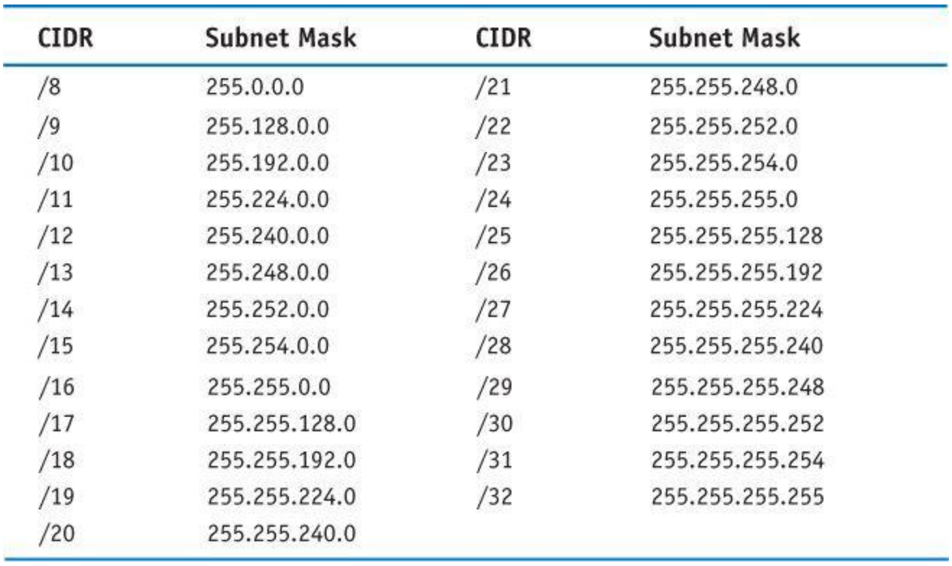
	First byte	Second byte	Third byte	Fourth byte
Class A	0 to 127	🟨	🟦	🟩
Class B	128 to 191	🟨	🟦	🟩
Class C	192 to 223	🟨	🟦	🟩
Class D	224 to 239	🟨	🟦	🟩
Class E	240 to 255	🟨	🟦	🟩

Assignment of IP addresses: All hosts in the same network are assigned the same address prefix. Address prefixes are assigned by central authority and are obtained from ISPs. Within a network each host is assigned a unique suffix locally by the network administrator.

Sub-netting is a technique used to overcome the problem of depletion of network address of a 32 bit addressing scheme. In sub-netting each physical network is assigned 32-bit address mask, which is used to identify networks among other networks. All machines in the subnet should have the same subnet mask.



Classless Inter Domain Routing (CIDR): instead of full class A, B or C networks, organizations can be allocated any number of addresses using this scheme. This scheme can help reducing the growth of the router tables.



CIDR	Subnet Mask	CIDR	Subnet Mask
/8	255.0.0.0	/21	255.255.248.0
/9	255.128.0.0	/22	255.255.252.0
/10	255.192.0.0	/23	255.255.254.0
/11	255.224.0.0	/24	255.255.255.0
/12	255.240.0.0	/25	255.255.255.128
/13	255.248.0.0	/26	255.255.255.192
/14	255.252.0.0	/27	255.255.255.224
/15	255.254.0.0	/28	255.255.255.240
/16	255.255.0.0	/29	255.255.255.248
/17	255.255.128.0	/30	255.255.255.252
/18	255.255.192.0	/31	255.255.255.254
/19	255.255.224.0	/32	255.255.255.255
/20	255.255.240.0		

With the ever-increasing demand for public IP addresses for Internet accesses, Internet would run out of available IP addresses. IPV6 is proposed to fix the problem of the limited address space of IPV4.

Private IPs: Three sets of address ranges are used for private use.

- 10.0.0.0 – 10.255.255.255 (10.0.0.0/8) – 16M addresses
- 172.16.0.0 – 172.31.255.255 (172.16.0.0/12) - 1M addresses
- 192.168.0.0 – 192.168.255.255 (192.168.0.0/16) – 64k addresses

Dynamic Host Configuration Protocol (DHCP) server: is a protocol used to assign IP addresses to arriving hosts. Rather than a network administrator manually assigning an IP address to each arriving host, the DHCP will assign IP addresses automatically.

Finding path to the Destination: When data leaves the source towards the destination, it needs to be routed through a series of networking devices to reach the destination. Routers take care of the job of routing the data from the source to destinations. Routing is the process of finding an efficient path from a source to a given destination through the network. Routers are special networking devices that are capable of communicating with similar devices over the network, collaborate among themselves and find paths for arriving data. Routers maintain a table of reachable destinations through them and these tables are called routing tables. Routers exchange these routing tables with other routers in the network from time to time to update the route details.

Packet Switching: When a message is generated at the source it is broken down into smaller chunks called packets. Each packet is assigned unique information to identify itself, switching information is added in the header of each packet and the transmitted independent of other packets.

Role of Transport Protocols

Since many network applications may be running on the same machine, computers need something to make sure the correct software application on the destination computer gets the data packets from the source machine and some way to make sure replies get routed to the correct application on the source computer. Each process of a running application communicates to the underlying network through a specially assigned interface called a port. Each port is assigned a unique number called port number and it is used in combination with the IP address of the device to identify each process uniquely that is running on a given host. When processes running on different computers send data to the same destination, the port numbers of different processes and the IP addresses are used to identify the processes correctly. The process of combining the port numbers and the IP addresses and the identifying the correct process is called multiplexing.

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

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

User Datagram Protocol: UDP is the no frills transport protocol for several wellknown application layer protocols such as DNS and SNMP. UDP is simple and suitable for query based communications and it is not connection oriented.

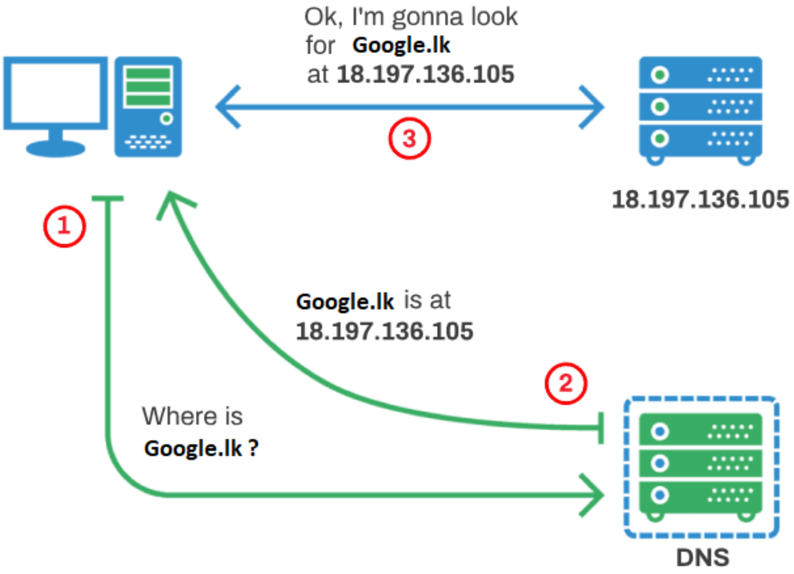
Transmission Control Protocol: TCP provides a reliable in order delivery of data. It is a connection oriented protocol and uses sequenced acknowledgment with retransmission of packets when necessary. TCP is used for applications such as web, and email.

TCP vs UDP	
TCP is a connection-oriented protocol	UDP is a connectionless protocol
TCP is comparatively slower than UDP	UDP is much faster
Can guarantee delivery of data	Cannot guarantee delivery of data
Does not support Broadcasting	Does support Broadcasting
Packets arrive in order at the receiver.	There is no sequencing of data in UDP.
Used by HTTPS, HTTP, SMTP, POP, FTP, etc	Video conferencing, streaming, DNS, VoIP, etc

Applications on the Internet

Domain Name System (DNS): DNS provides directory lookup service for given urls and the web addresses. The HTTP protocol uses the services of DNS to identify the matching web addresses of given URLs.

Humans, being different from computers, have difficulty in retaining lots of similar numbers in mind. Working with names is much easier for them and cause less errors. That is why we rarely see the numbers as URLs on the Internet. When a URL is entered to the browser to view a website, the request must first be translated from the readable written address into an IP address that can be routed. This translation is done by the Domain Name System (DNS). If a request is made to connect to certain website, for example www.yahoo. coin, the request is first sent to the DNS server to translate into the correct IP address of 209.191.122.70. The actual connection to the website is done with this IP address. This process happens behind the screen quickly that the user does not notice.



HTTP - The Hypertext Transfer Protocol is an application layer protocol for distributed, collaborative, and hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Client Server model: The client–server model is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients.

Servers

A server is a device with a particular set of programs or protocols that provide various services, which other machines or clients request, to perform certain tasks. Together, a server and its clients form a client/server network, which provides routing systems and centralized access to information, resources, stored data, etc.

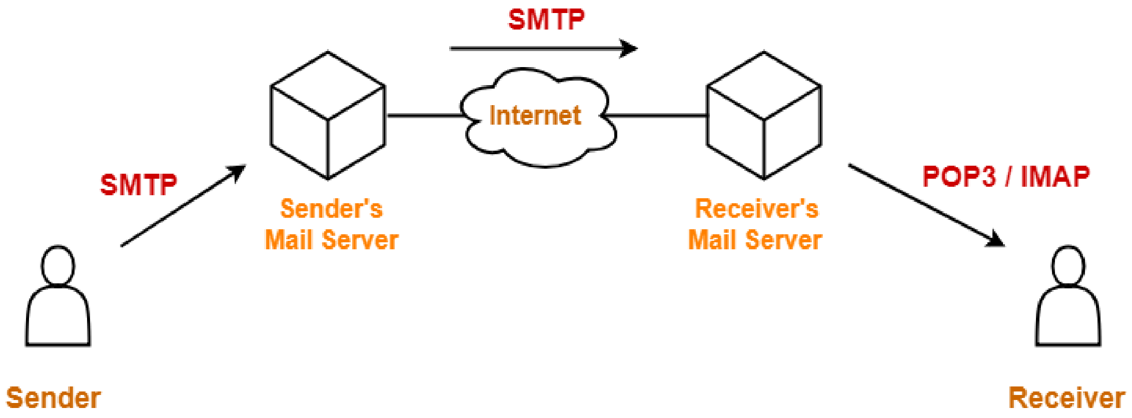
FILE SERVER - File Transfer Protocol (FTP) is one of the oldest server types. It is responsible for transferring files from server to a computer and vice versa.

PROXY SERVERS can easily be used to increase speeds and save bandwidth on a network by compressing traffic, caching files and web pages accessed by multiple users.By using a proxy, the website you access will not be able to log your real IP address, as it will log the proxy server's IP address instead.

DHCP SERVER Is a protocol used to assign IP addresses to arriving hosts. Rather than a network administrator manually assigning an IP address to each arriving host, the DHCP will assign IP addresses automatically.

WEB SERVER The web server is responsible for hosting website files and serve it up through a web browser. It loads an individual file of a web page and loads it to display in the browser as one complete page.

MAIL SERVER The mail server just is as important as a web server is. A mail server is to send/receive and store emails on the corporate networks through LANs and WANs and across the internet. Mail servers send and receive email using standard email protocols. For example, the SMTP protocol sends messages and handles outgoing mail requests. The IMAP and POP3 protocols receive messages and are used to process incoming mail.



PROTOCOLS

Simply, a protocol is a set of rules. A network protocol is a set of rules followed by the network. Network protocols are formal standards and policies made up of rules, procedures and formats that defines communication between two or more devices over a network.

Internet protocol suite is the set of communication protocols that implement the protocol stack on which the internet runs. The Internet protocol suite is sometimes called the TCP/IP protocol suite, after TCP\IP, which refers to the important protocols in it, the Transmission Control Protocol(TCP) and the Internet Protocol(IP). The Internet protocol suite can be described by the analogy with the OSI model, but there are some differences. Also not all of the layers correspond well.

The Transmission Control Protocol is the core protocol of the internet protocol suite. It originated in the network implementation in which it complemented the Internet Protocol. Therefore the entire suite is commonly referred to as TCP/IP. TCP provides reliable delivery of a stream of octets over an IP network. Ordering and error-checking are main characteristics of the TCP. All major Internet applications such as World Wide Web, email and file transfer rely on TCP. TCP provides a reliable in order delivery of data. It is a connection oriented protocol and uses sequenced acknowledgment with retransmission of packets when necessary. TCP is used for applications such as web, and email.

The Internet Protocol is the principal protocol in the Internet protocol suite for relaying data across networks. Its routing function essentially establishes the internet. Historically it was the connectionless datagram service in the original Transmission Control Program; the other being the connection oriented protocol(TCP). Therefore, the Internet protocol suite is referred as TCP/IP.

Hypertext Transfer Protocol (HTTP) is the foundation of data communication for the World Wide Web. The hypertext is structured text that uses hyperlinks between nodes containing texts. The HTTP is the application protocol for distributed and collaborative hypermedia information system. The default port of HTTP is 80 and 443 is the secured port.

File Transfer Protocol (FTP) is the most common protocol used in the file transferring in the Internet and within private networks. The default port of FTP is 20/21.

Secured Shell (SSH) is the primary method used to manage the network devices securely at the command level. It usually used as the alternative of the Telnet which does not support secure connections. The default port of SSH is 22.

Telnet is the primary method used to manage network devices at the command level. Unlike SSH, Telnet does not provide a secure connection, but it provides a basic unsecured connection. The default port of Telnet is 23.

Simple Mail Transfer Protocol (SMTP is used for two primary functions. It is used to transfer email from source to destination between mail servers and it is used to transfer email from end users to a mail system. The default port of SMTP is 25 and secured (SMTPS) is 465 (Not standard).

Domain Name System (DNS) is used to convert the domain name to IP address. There are root servers, TLDs and authoritative servers in the DNS hierarchy. The default port of DNS is 53.

The Post Office Protocol version 3(pop3) is one of the two main protocols used to retrieve mail from the internet. It is very simple as it allows the client to retrieve complete content from the server mail box and deletes contents from the server. The default port of POP3 is 110 and secured is 995.

Internet Message Access Protocol (IMAP) version 3 is another main protocol that used to retrieve mail from a server. IMAP does not delete the content from the mail box of the server. The default port of IMAP is 143 and secured is 993.

The Simple Network Management Protocol is used to manage networks. It has abilities to monitor, configure and control network devices. SNMP traps can also be configured on network devices to notify a central server when specific action are occurring. The default port of SNMP is 161/162.

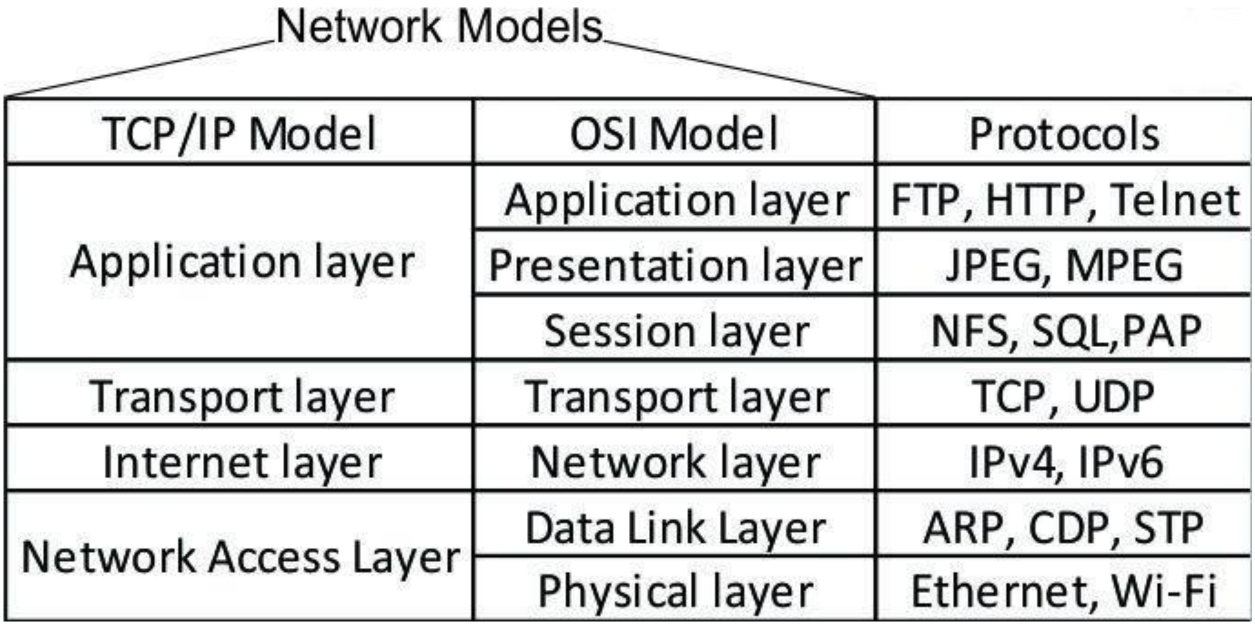
Hypertext Transfer Protocol over SSL/TLS (HTTPS) is used with HTTP to provide same services, but with a secured connection which is provided by SSL or TLS. The default port of HTTPS is 443.

User Datagram Protocol(UDP) is the no frills transport protocol for several wellknown application layer protocols such as DNS and SNMP. UDP does not guarantee ordered delivery of data.

TCP/IP Model

Application Layer- Consists of applications and processes that uses the network.
Host- Host Transport Layer- Provides end to end data delivery services
Internet layer –Defines the datagram and handles the routing of data

Network Access Layer – consists of routing for accessing physical network



Network Models

TCP/IP Model	OSI Model	Protocols
Application layer	Application layer	FTP, HTTP, Telnet
	Presentation layer	JPEG, MPEG
	Session layer	NFS, SQL,PAP
Transport layer	Transport layer	TCP, UDP
Internet layer	Network layer	IPv4, IPv6
Network Access Layer	Data Link Layer	ARP, CDP, STP
	Physical layer	Ethernet, Wi-Fi

Network Access Layer

- lowest layer in TCP/IP hierarchy
- provides the means to deliver data to the other devices on the network
- defines how to use the network to transmit IP datagram
- encapsulates IP datagram into frames
- maps IP addresses to physical addresses in Ethernet

Internet Layer

- manages connections across the network and isolates the upper layer protocols
- handles addressing and delivery of data
- Internet Protocol (IP) does all these functions

Transport layer

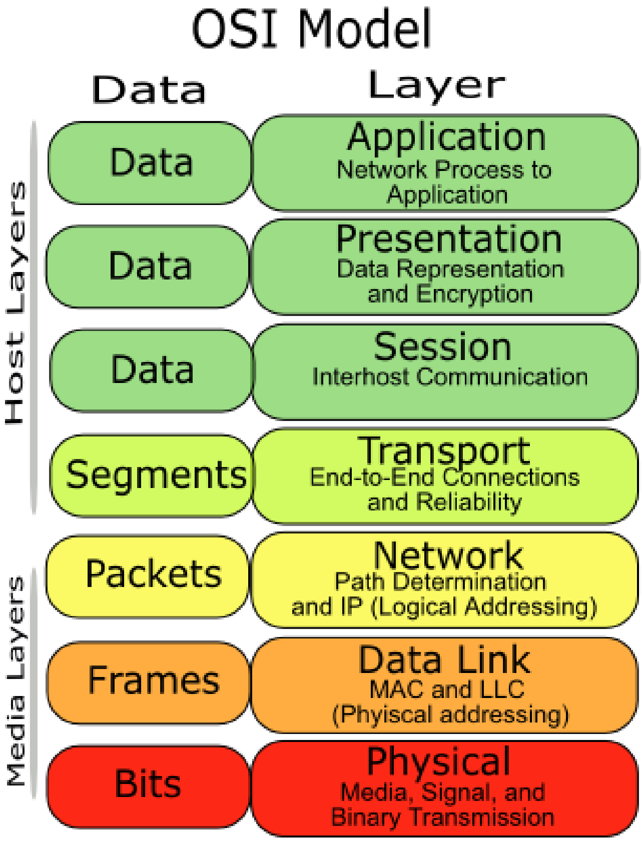
- This layer is concerned with the transmission of the data. The two main protocols that operate at this layer are, Transport Control Protocol (TCP), User Datagram Protocol (UDP)

Application layer

- The application layer is concerned with providing network services to applications. There are many application network processes and protocols that work at this layer, including HTTP, SMTP and FTP.

OSI model

The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software.


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Phyiscal addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Using the OSI model, the communications between computing systems are done through seven abstraction layers; it's easy to remember the sequence of OSI Model 7 Layers using this simple sentence: "*All people seem to need data processing.*"

All = Application Layer, People = Presentation Layer, Seem = Session Layer, To = Transport Layer, Need = Network Layer, Data = Data Link Layer, Processing = Physical Layer

- **Application Layer**

The application layer provides an interface between end-users and software applications. It receives data from end-users, and displays received data for them. This layer does not contain the end-user applications; instead, it facilitates communications with the lower layers. Some protocols found within this layer include HTTP, HTTPS, FTP, TFTP, Telnet, SNMP, DNS, Rlogin, SMTP, POP3, IMAP, and LDAP.

- **Presentation Layer**

This layer facilitates the presentation of Data to the upper layer. Mainly, it provides the encoding scheme and encryption/decryption for secure transmission. For instance, it translates applications format to network format and vice-versa. Protocols of this layer: JPEG, BMP, GIF, TIF, PNG, MP3, MIDI, ASCII & ANSI, etc.

- **Session Layer**

When two computing devices need to communicate, a session must be created, which happens at this layer. Some of this layer's functions are the establishment, management (coordination), and termination of sessions. A good example of how this layer function is a telephone call where you first establish the connection, exchange a message, and finally terminate the session. Some of the protocols of this layer are SIP, NFS, SQL, ASP, and RDBMS.

- **Transport Layer**

This layer, often considered the heart of the OSI model, is responsible for controlling data flow between two devices. For example, this layer determines the amount of data needed to send and the location where it should be sent. This layer is also responsible for data flow and error control. For instance, the flow control determines the optimal speed of sending data to avoid flooding the receiver with data if the connection speed is different between the two communicating parties. Simultaneously, error control ensures retransmitting the data again if some packets were lost on the receiver side. This layer's best-known example protocol is the TCP protocol, which resides as part of the TCP/IP protocol suite. Some other protocols on this layer are TCP, UDP, and SPX.

- **Network Layer**

The network layer is responsible for data packet forwarding and routing data between routers. It facilitates data transfer between two devices residing in two different networks. For example, if you want to send a message from your computer in New York to a server in San Francisco, there are thousands of routers and –maybe- millions of paths between these two points. However, the routers at this layer help you do this efficiently by automatically selecting the nearest way. The network layer is also responsible for translating the logical addresses into physical addresses and is responsible for data fragmentation. Hence, it breaks segments of data into smaller units called packets before sending them to other networks.

- **Data Link Layer**

This layer provides a connection between two devices residing on the same physical network, for example, between two devices in the same LAN. This layer receives packets from the network layer and breaks them into small units called frames. The data link layer also performs data flow and error control within intranets. It contains two other sub-layers: the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. Most ordinarily, networking switches operate at this layer. Some protocols within this layer are PPP, HDLC, ATM, Frame Relay, SLIP, and Ethernet.

- **Physical Layer**

This layer exists at the bottom of the OSI layer. It represents the OSI model's physical component, including cable type, radio frequencies (when using a Wireless connection), the layout of pins, and voltages. This layer is responsible for delivering the raw data from the sending device's physical layer to the receiving device's physical layer. Popular devices found at this layer include network hubs, cabling, repeaters, and modems.

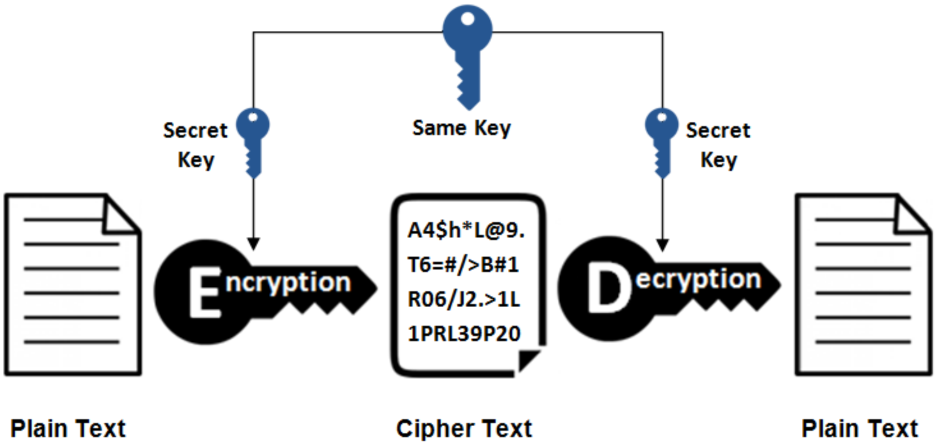
The advantages of the OSI model are,

- ✓ It is a generic model and acts as a guidance tool to develop any network model.
- ✓ It is a layered model. Changes are one layer do not affect other layers, provided that the interfaces between the layers do not change drastically.
- ✓ It distinctly separates services, interfaces, and protocols. Hence, it is flexible in nature. Protocols in each layer can be replaced very conveniently depending upon the nature of the network.
- ✓ It supports both connection-oriented services and connectionless services.

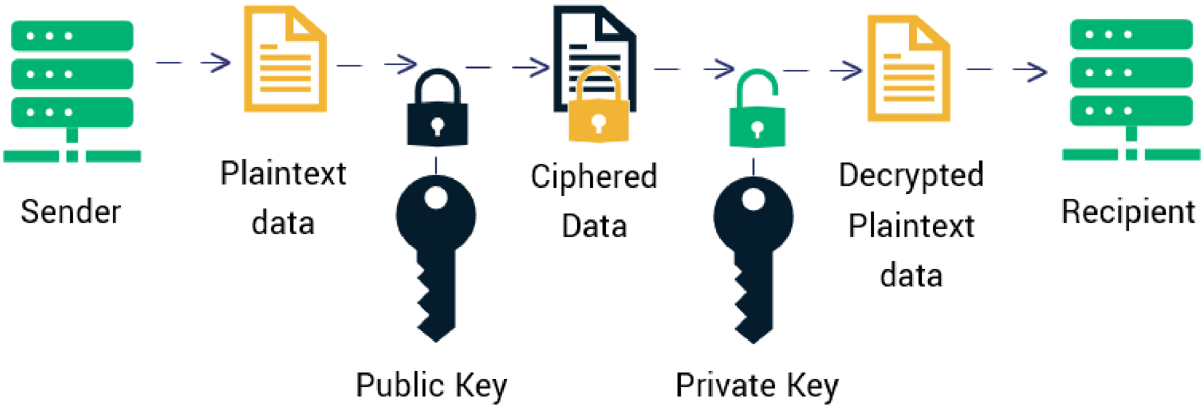
Network Security

Encryption is a technique used in cryptography which provides confidentiality of transmitting data.There are two types of encryption:

Symmetric Key Encryption - The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. When using symmetric key encryption users must share a common key prior to exchange of information.



Asymmetric Key Encryption - The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Every user in this system needs to have a pair of dissimilar keys, private key and public key. These keys are mathematically related – when one key is used for encryption, the other can decrypt the cipher text back to the original plaintext.



Digital signature - Usually a validity document contains a signature under it and which makes the receiver to trust the content in it. Similar to usual documents, digital documents should also have a signature. Thus digital signatures help to authenticate the sources of messages. Digital signatures allow us to verify the author, date and time of signatures, authenticate the message contents.

Threats

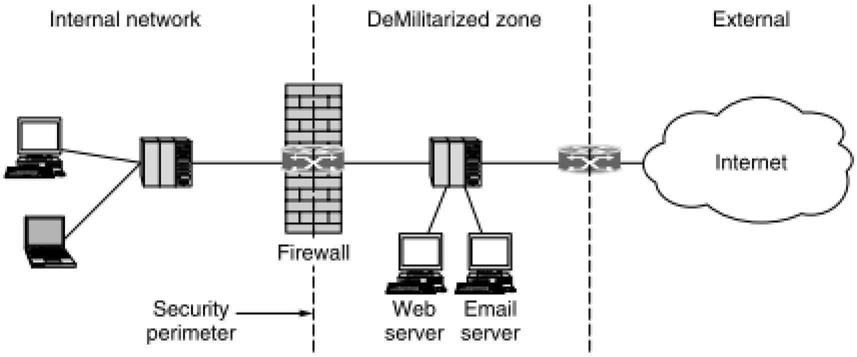
- Viruses - A program which enters into the system, runs and performs malicious activities unknowingly.
- Trojans - Any malicious computer program used to invade into a computer by misleading users
- Malware- The software that is written for malicious purposes

- Phishing – An attempt to obtain sensitive information such as usernames, passwords, and credit card details by pretending as a trustworthy person.

Protection against unauthorized malicious accesses

- **Firewalls:** a network security device that monitors and filters incoming and outgoing network traffic. A firewall is essentially the barrier that sits between a private internal network and the public Internet.
- **Antivirus software:** are software that detect and quarantine the malicious software that tries to harm a computer.
- **Computer users** must be properly educated to protect the network devices against malicious attacks and unauthorized accesses. Passwords must be chosen with utmost care and antivirus software must be periodically updated to protect the system from attacks.

A DMZ (demilitarized zone) Network is a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic. A common DMZ is a subnetwork that sits between the public internet and private networks.



The role of ISPs and technologies used for connecting Home Networks

ISPs: An Internet service provider (ISP) is an organization that provides services to accessing and using the Internet services. Internet service providers may be organized in various forms.

Use of MODEMs

DSL: Refers collectively to all types of digital subscriber lines and **ADSL** is the asymmetric digital subscriber line, ADSL is a type of DSL broadband communications technology used for connecting to the Internet. ADSL allows more data to be sent over existing copper telephone lines, when compared to traditional modem lines.

Advantages of DSL

- **Independent services:** Loss of high speed data does not mean you lose your telephone service. Imagine your telephone, television, and Internet access going out when a cable company amplifier/repeater dies.

- **Security:** Unlike cable modems, each subscriber can be configured so that it will not be on the same network. In some cable modem networks, other computers on the cable modem network are left visibly vulnerable and are easily susceptible to break ins as well as data destruction.
- **Integration:** DSL will easily interface with ATM, Nx64, and WAN technology. Telecommuting may get even easier.

Advantages ADSL

- **Cheaper rates**: Internet service providers (ISPs) provide a simple ADSL connection to the Internet, using the highest possible speed with usually a static IP address.
- **Fully configurable:** WAN engineers have total control over the VPN tunnel created between sites. They are able to perform on-the-fly configuration changes to compensate for any network problems or help rectify any problem that might arise.
- **High-speed access which enables easy net surfing and fast streaming contents access:** ADSL is a broadband service. It offers data transmission at much greater speeds and capacity than narrowband services like ISDN and dialup analog modems. ADSL enables you to download high-volume data files effortlessly.

A home LAN that uses private Ips

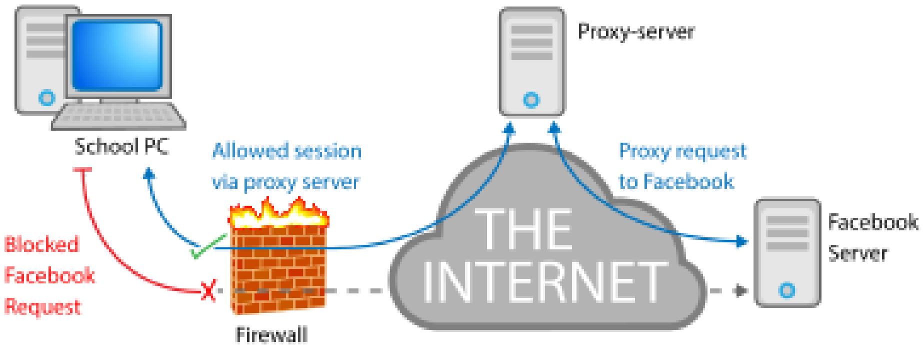
A public IP address is an IP address that can be accessed over the Internet. Like postal address used to deliver a postal mail to your home, a public IP address is the globally unique IP address assigned to a computing device. Your public IP address can be found at What is my IP Address page. Private IP address, on the other hand, is used to assign computers within your private space without letting them directly expose to the Internet.

For example, if you have multiple computers within your home you may want to use private IP addresses to address each computer within your home. In this scenario, your router gets the public IP address, and each of the computers, tablets and smartphones connected to your router (via wired or wifi) gets a private IP address from your router via DHCP protocol.

Network Address Translation /Proxies

Network address translation (NAT) is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. The technique was originally used for ease of rerouting traffic in IP networks without readdressing every host.

A **proxy server** is a computer that acts as an intermediary between the user's computer and the Internet. It allows client computers to make indirect network connections to other network services. A Proxy server solves the IP address issues when connecting a large corporation to the internet.



Useful links

https://www.youtube.com/playlist?list=PLSNNzog5eydvsPPMwn-6waomQXOOxZew4

https://www.youtube.com/playlist?list=PL7zRJGi6nMRzg0LdsR7F3olyLGoBcIvvg