Syllabus of Computer Network

Content details	
Unit-I **Data communications concepts**: Digital and analog transmissions-Modem, parallel and serial transmission, synchronous and asynchronous communication. **Modes of communication:** Simplex, half duplex, full duplex. Types of Networks: LAN, MAN, WAN **Network Topologies:** Bus, Star, Ring, Mesh, Tree, Hybrid **Communication Channels**: Wired transmissions: Telephone lines, leased lines, switch line, coaxial cables-base band, broadband, optical fiber transmission. **Communication Switching Techniques**: Circuit Switching, Message Switching, Packet Switching.	
Unit-II **Network Reference Models**: OSI Reference Model, TCP/IP Reference Model, Comparison of OSI and TCP/IP Reference Models. **Transmission impairments –** Attenuation, Distortion, Noise. Multiplexing – Frequency division, Time division, Wavelength division. **Data Link Layer Design Issues:** Services provided to the Network Layer, Framing, Error Control (error detection and correction code), Flow Control, Data Link Layer in the Internet (SLIP, PPP)	
Unit-III **MAC sub layer**: CSMA/CD/CA, IEEE standards (IEEE802.3 Ethernet, Gigabit Ethernet, IEEE 802.4 Token Bus, IEEE 802.5 Token Ring) **Network Layer**: Design Issues, Routing Algorithms: Optimality Principle, Shortest Path Routing, Congestion Control Policies, Leaky bucket and token bucket algorithm, Concept of Internetworking	
Unit-IV **Transport Layer**: Design issues, Elements of transport protocols – Addressing, Connection establishment and release, Flow control and buffering, Introduction to TCP/UDP protocols.	

Session, Presentation and Application Layers: Session Layer – Design issues, remote procedure call. Presentation Layer – Design issues, Data compression techniques, Cryptography. Application Layer – Distributed application (client/server, peer to peer, cloud etc.), World Wide Web (WWW), Domain Name System (DNS), E-mail, File Transfer Protocol (FTP), HTTP as an application layer protocol.	

INDEX

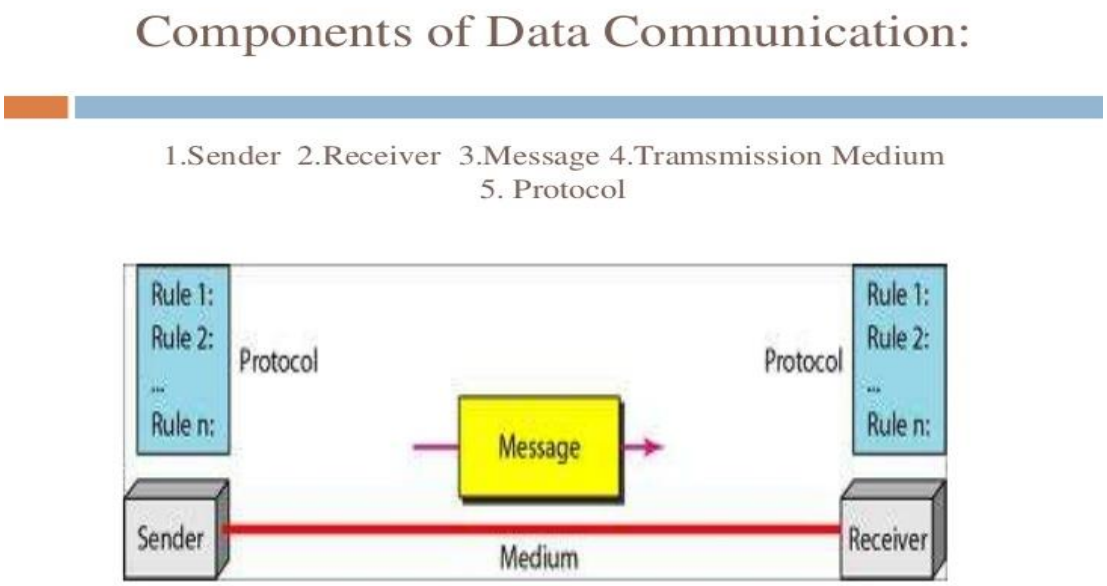
UNIT I

❖ Data Communications

In Data Communications, Exchange of data between two devices via some forms of transmission medium (such as wire cable) is Data Communications. For data communications to occur, the communicating devices must be part of a communication system made of a combination of hardware and software.

For example, a common example of data communications is a computer connected to the Internet via a Wi-Fi connection, which uses a wireless medium to send and receive data from one or more remote servers

The effectiveness of a data communication system depends on four fundamental characteristics:- delivery, accuracy, timeliness and jitter. A data communications system has five components:



1. Message: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. Sender: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

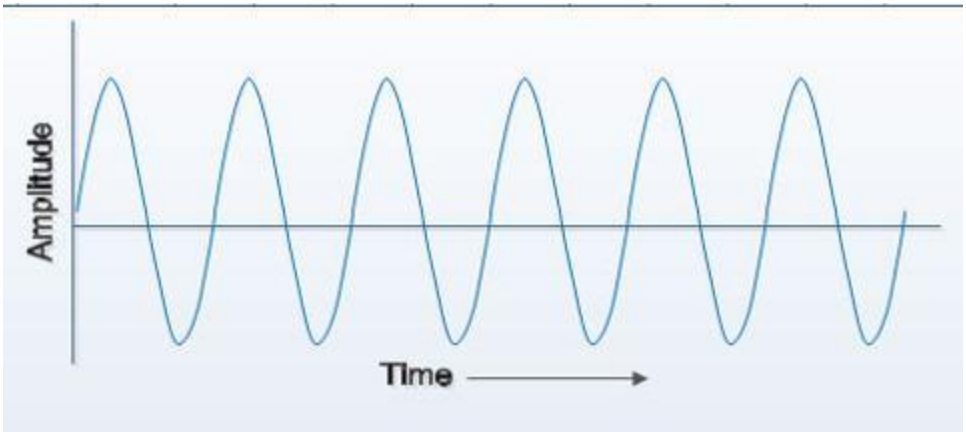
4. Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5. Protocol: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

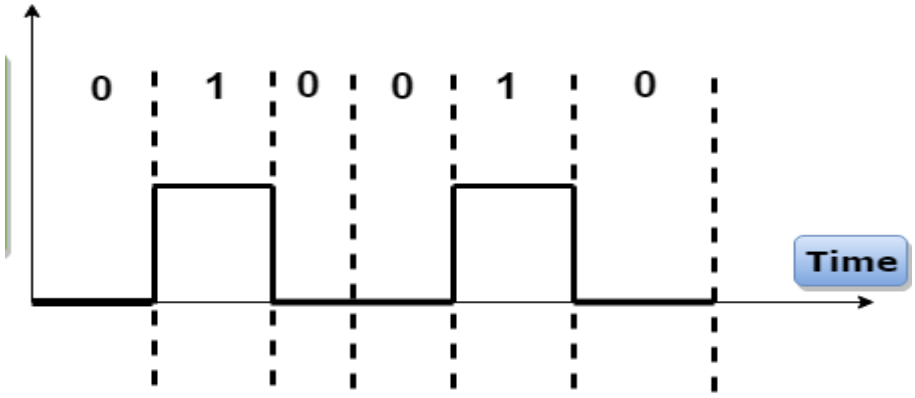
❖ Digital and analog transmissions

Analog transmission is a transmission method of conveying information using a continuous signal which varies in amplitude, phase, or some other property in proportion to that information.

Example: - phone call or a video signal.



Digital Transmission is the transmission of signals that vary discretely with time between two values of some physical quantity, one value representing the binary number 0 and the other representing 1.



Example:- Computer or a Keyboard

Advantages of Digital Signals

- **Digital Data** - Digital transmission certainly has the advantage where binary computer data is being transmitted. The equipment required to convert digital data to analog format and transmitting the digital bit streams over an analog network can be expensive, susceptible to failure, and can create errors in the information.
- **Compression** - Digital data can be compressed relatively easily, thereby increasing the efficiency of transmission. As a result, substantial volumes of voice, data, video and image information can be transmitted using relatively little raw bandwidth.
- **Security** - Digital systems offer better security. While analog systems offer some measure of security through the scrambling of several frequencies. Scrambling is fairly simple to defeat. Digital information, on the other hand, can be encrypted to create the appearance of a single, pseudorandom bit stream. Thereby, the true meaning of individual bits, sets of bits, or the total bit stream cannot be determined without having the key to unlock the encryption algorithm employed.
- **Quality** - Digital transmission offers improved error performance (quality) as compared to analog. This is due to the devices that boost the signal at periodic intervals in the transmission system in order to overcome the effects of attenuation. Additionally, digital networks deal more effectively with noise, which always is present in transmission networks.
- **Cost** - The cost of the computer components required in digital conversion and transmission has dropped considerably, while the ruggedness and reliability of those components has increased over the years.
- **Upgradeability** - Since digital networks are comprised of computer (digital) components, they are relatively easy to upgrade. Such upgrading can increase bandwidth, reduces the incidence of error and enhance functional value. Some upgrading can be effected remotely over a network, eliminating the need to dispatch expensive technicians for that purpose.
- **Management** - Generally speaking, digital networks can be managed much more easily and effectively due to the fact that such networks consist of

computerized components. Such components can sense their own level of performance, isolate and diagnose failures, initiate alarms, respond to queries, and respond to commands to correct any failure. Further, the cost of these components continues to drop.

Comparison between Analog and Digital Transmission

Sr. No.	Key	Digital System	Analog System
1	Signal Type	Digital System uses discrete signals as on/off representing binary format. Off is 0, On is 1.	Analog System uses continuous signals with varying magnitude.
2	Wave Type	Digital System uses square waves.	Analog system uses sine waves.
3	Technology	Digital system first transform the analog waves to limited set of numbers and then record them as digital square waves.	Analog systems record the physical waveforms as they are originally generated.
4	Transmission	Digital transmission is easy and can be made noise proof with no loss at all.	Analog systems are affected badly by noise during transmission.
5	Flexibility	Digital system hardware can be easily modulated as per the requirements.	Analog system's hardware are not flexible.

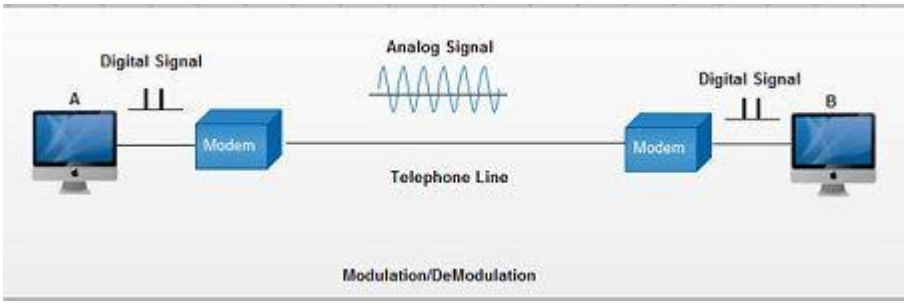
6	Bandwidth	Digital transmission needs more bandwidth to carry same information.	Analog transmission requires less bandwidth.
7	Memory	Digital data is stored in form of bits.	Analog data is stored in form of waveform signals.
8	Power requirement	Digital system needs low power as compare to its analog counterpart.	Analog systems consume more power than digital systems.
9	Best suited for	Digital system are good for computing and digital electronics.	Analog systems are good for audio/video recordings.
10	Cost	Digital system are costly.	Analog systems are cheap.
11	Example	Digital system are: Computer, CD, DVD.	Analog systems are: Analog electronics, voice radio using AM frequency.

❖ Modem

Modem is abbreviation for Modulator – Demodulator. Modems are used for data transfer from one computer network to another computer network through telephone lines. The computer network works in digital mode, while analog technology is used for carrying massages across phone lines.

Modulator converts information from **digital mode to analog mode** at the transmitting end and demodulator converts the same from **analog to digital at receiving end**. The process of converting analog signals of one computer network into digital signals of another computer network so they can be processed by a receiving computer is **referred to as digitizing.**

When an analog facility is used for data communication between two digital devices called Data Terminal Equipment (DTE), modems are used at each end. DTE can be a terminal or a computer.



The modem at the transmitting end converts the digital signal generated by DTE into an analog signal by modulating a carrier. This modem at the receiving end demodulates the carrier and hand over the demodulated digital signal to the DTE.

Types of Modem

Modems can be of several types and they can be categorized in a number of ways.

Categorization is usually based on the following basic modem features:

1. Directional capacity: half duplex modem and full duplex modem.

2. Connection to the line: 2-wire modem and 4-wire modem.

3. Transmission mode: asynchronous modem and synchronous modem.

Directional capacity

Half duplex

1. A **half duplex modem** permits transmission in one direction at a time.

2. If a carrier is detected on the line by the modem, I gives an indication of the incoming carrier to the DTE through a control signal of its digital interface.

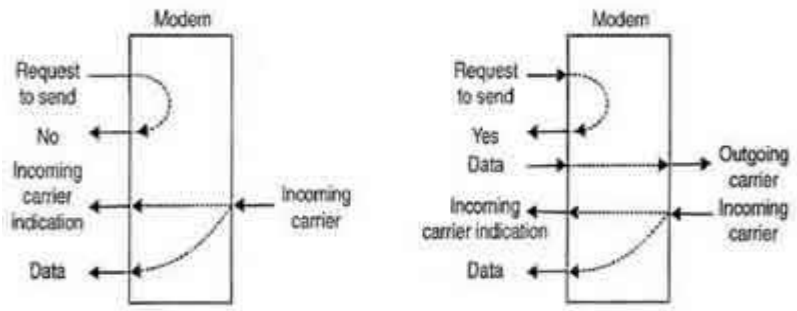
3. As long as they camel' IS being received; the modem does not give permission to the DTE to transmit data.

Example of a half-duplex device is a walkie-talkie, a two-way radio that has a push-to-talk button

Full duplex

Some modems can send and receive information at the same time, just as you can talk to a friend over the phone at the same time the friend is talking to you.

This mode of communication is called full duplex. Other modems can send as well as receive information, but not at the same instant in time



(a) Half Duplex Modem (b) Full Duplex Modem

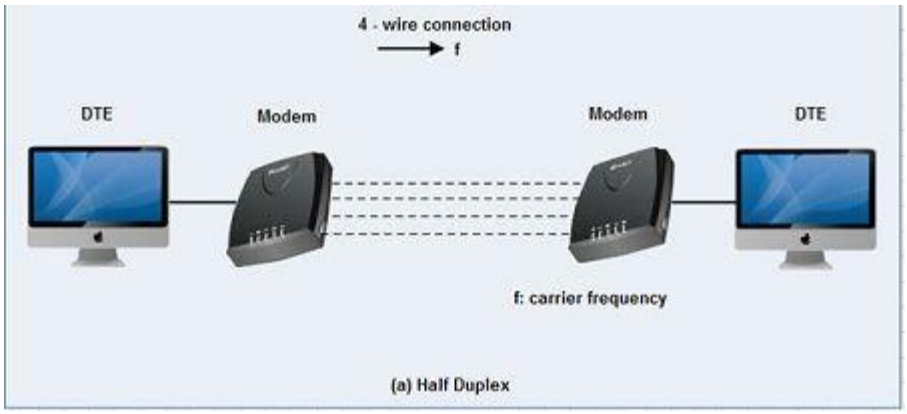
Example of full duplex mode is: Telephone

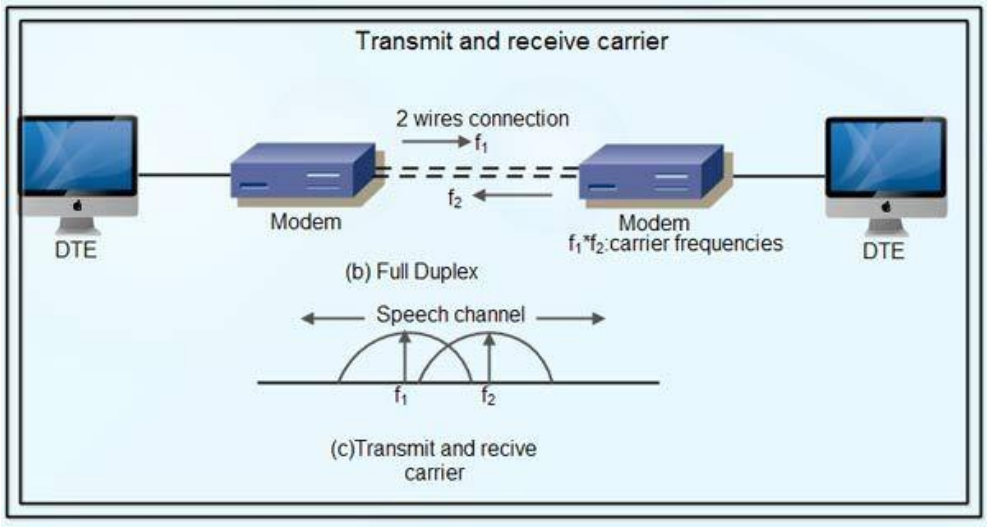
Connection to the line

2-wire Modem

- 2-wire modems use the same pair of wires for outgoing and incoming carriers.
- A leased 2-wireconrlection is usually cheaper than a 4-wire connection as only one pair of wires is extended to the subscriber's premises.

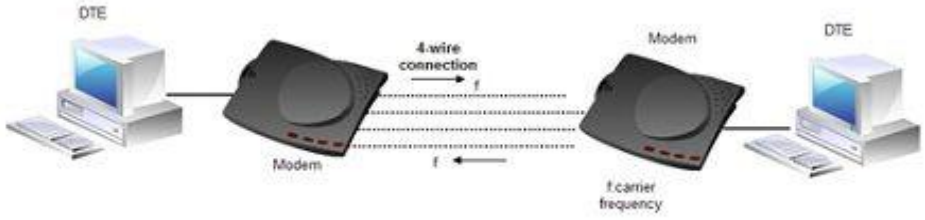
- The data connection established through telephone exchange is also a 2-wire connection.
- In 2-wire modems, half duplex mode of transmission that uses the same frequency for the incoming and outgoing carriers can be easily implemented.
- For full duplex mode of operation, it is necessary to have two transmission channels, one for transmit direction and the other for receive direction.
- This is achieved by frequency division multiplexing of two different carrier frequencies. These carriers are placed within the bandwidth of the speech channel.





4-Wire Modem

- In a 4-wire connection, one pair of wires is used for the outgoing carrier and the other pair is used for incoming carrier.
- Full duplex and half duplex modes of data transmission are possible on a 4-wire connection.
- As the physical transmission path for each direction is separate, the same carrier frequency can be used for both the directions.



4wire-Modem

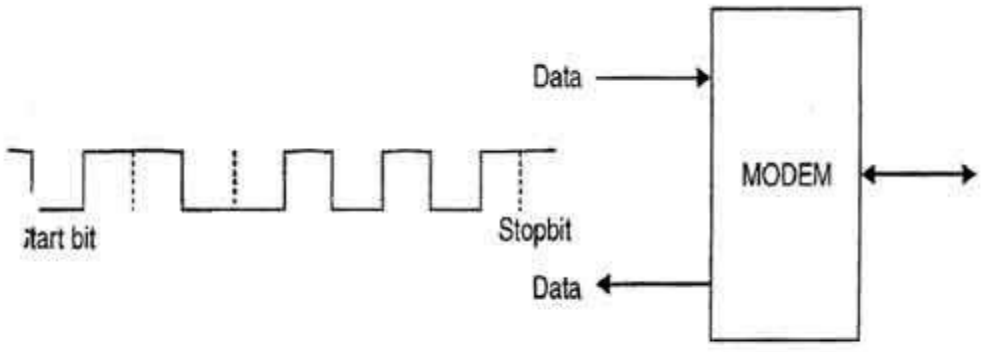
Asynchronous & Synchronous Modems

Asynchronous Modem

• Asynchronous modems can handle data bytes with start and stop bits.

• There is no separate timing signal or clock between the modem and the DTE.

• The internal timing pulses are synchronized repeatedly to the leading edge of the start pulse.



Asynchronous modem

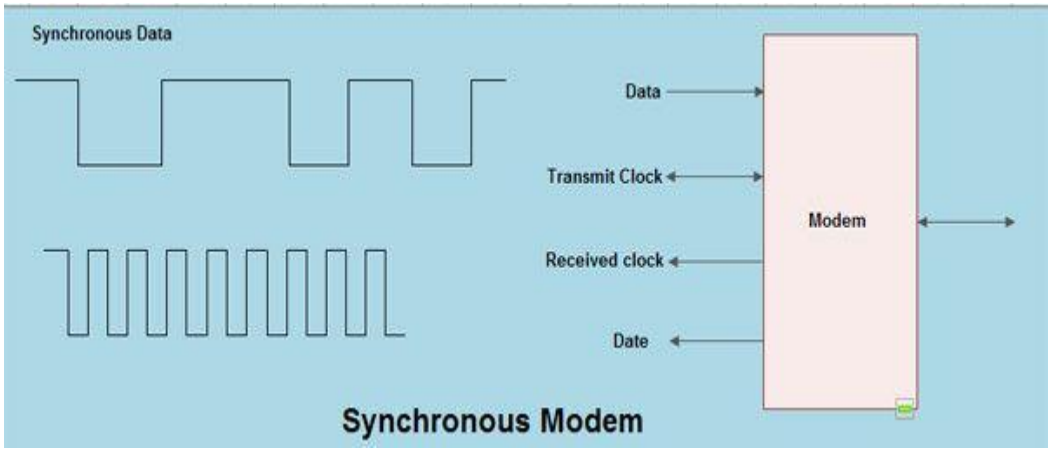
Synchronous Modem

• Synchronous modems can handle a continuous stream of data bits but requires a clock signal.

• The data bits are always synchronized to the clock signal.

• There are separate clocks for the data bits being transmitted and received.

• For synchronous transmission of data bits, the DTE can use its internal clock and supply the same to the modem.



❖ Data Transmission

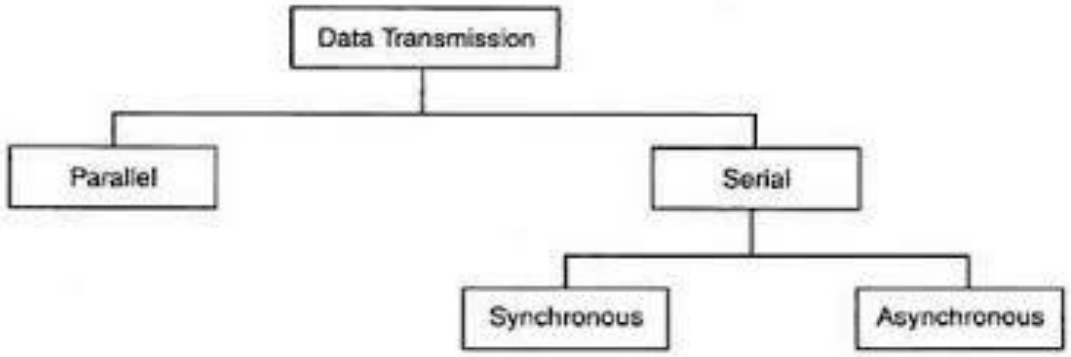
Data transmission is a means of transmitting digital or analog data over a communication medium to one or more devices. It allows the transmission and communication of devices in different environments: point-to-point, point-to-multipoint, or multipoint-to-multipoint.

Data transmission can either be analog or digital, but is mostly earmarked for sending and receiving digital data. As such, data transmission is also referred to as digital transmission or digital communications.

Types of Data Transmission

1. Parallel Transmission

2. Serial Transmission



Parallel transmission

1. In parallel transmission, all the bits of data are transmitted simultaneously on separate communication lines.

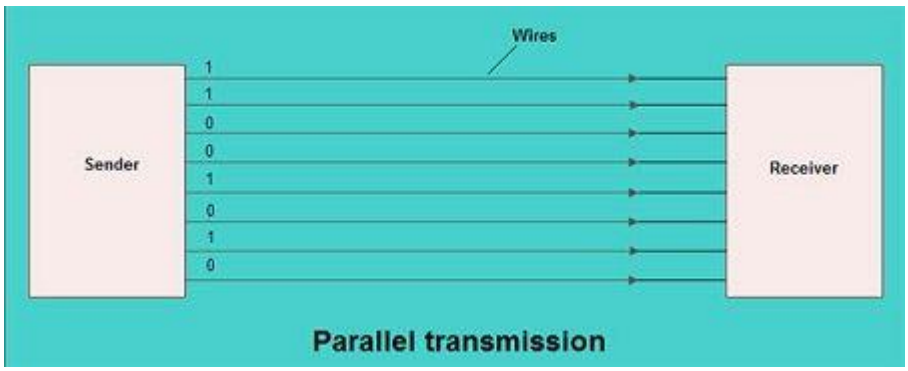
2. In order to transmit n bits, n wires or lines are used. Thus each bit has its own line.

3. All n bits of one group are transmitted with each clock pulse from one device to another i.e multiple bits are sent with each clock pulse.

4. Parallel transmission is used for short distance communication.

Example: - Computer to printer

As shown in fig. eight separate wires are used to transmit 8 bits data from sender to receiver.



Advantage of parallel transmission

- It is speedy way of transmitting data as multiple bits are transmitted simultaneously with a single clock pulse.

Disadvantage of parallel transmission

- It is costly method of data transmission as it requires *n* lines to transmit *n* bits at the same time.

Serial Transmission

Definition: When transferring data between two physically separate devices, especially if the separation is more than a few kilometers, for reasons of cost, it is more economical to use a single pair of lines. Data is transmitted as a single bit at a time using a fixed time interval for each bit. This mode of transmission is known as *bit-serial* transmission.

• In serial transmission, the various bits of data are transmitted serially one after the other.

• It requires only one communication line rather than *n* lines to transmit data from sender to receiver.

• Thus all the bits of data are transmitted on single line in serial fashion.

In serial transmission, only single bit is sent with each clock pulse.

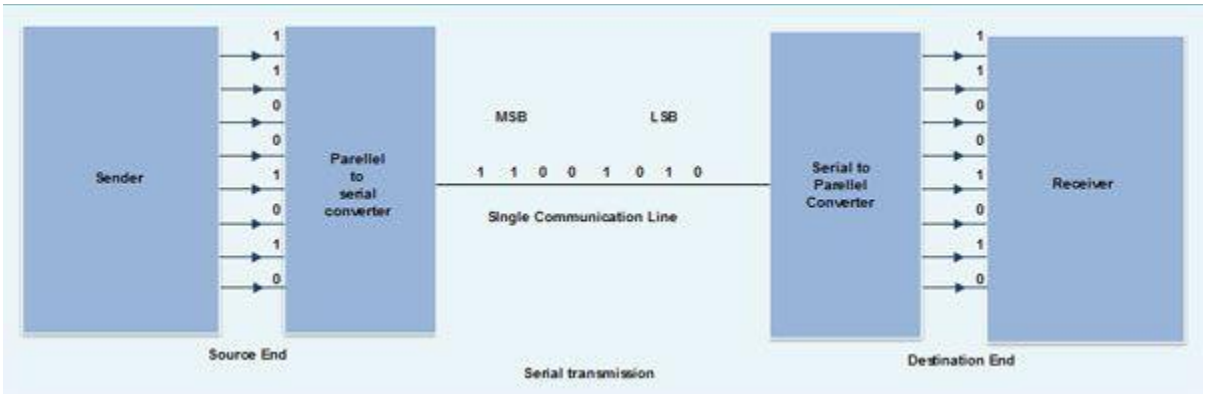
• As shown in fig., suppose an 8-bit data 11001010 is to be sent from source to destination. Then least significant bit (LSB) *i,e.* 0 will be transmitted first followed by other bits. The most significant bit (MSB) *i.e.* 1 will be transmitted in the end via single communication line.

• The internal circuitry of computer transmits data in parallel fashion. So in order to change this parallel data into serial data, conversion devices are used.

• These conversion devices convert the parallel data into serial data at the sender side so that it can be transmitted over single line.

• On receiver side, serial data received is again converted to parallel form so that the interval circuitry of computer can accept it

Example: - Computer to computer



Advantage of Serial transmission

- Use of single communication line reduces the transmission line cost by the factor of *n* as compared to parallel transmission.

Disadvantages of Serial transmission

- Use of conversion devices at source and destination end may lead to increase in overall transmission cost.
- This method is slower as compared to parallel transmission as bits are transmitted serially one after the other.

Types of Serial Transmission

- There are two types of serial transmission-**synchronous and asynchronous** both these transmissions use '**Bit synchronization**'
- Bit Synchronization is a function that is required to determine when the beginning and end of the data transmission occurs.
- Bit synchronization helps the receiving computer to know when data begin and end during a transmission. Therefore bit synchronization provides timing control.

Asynchronous Transmission

- Asynchronous transmission sends only one character at a time where a character is either a letter of the alphabet or number or control character *i.e.* it sends one byte of data at a time.
- Bit synchronization between two devices is made possible using start bit and stop bit.
- Start bit indicates the beginning of data *i.e.* alerts the receiver to the arrival of new group of bits. A start bit usually 0 is added to the beginning of each byte.
- Stop bit indicates the end of data *i.e.* to let the receiver know that byte is finished, one or more additional bits are appended to the end of the byte. These bits, usually 1s are called stop bits.

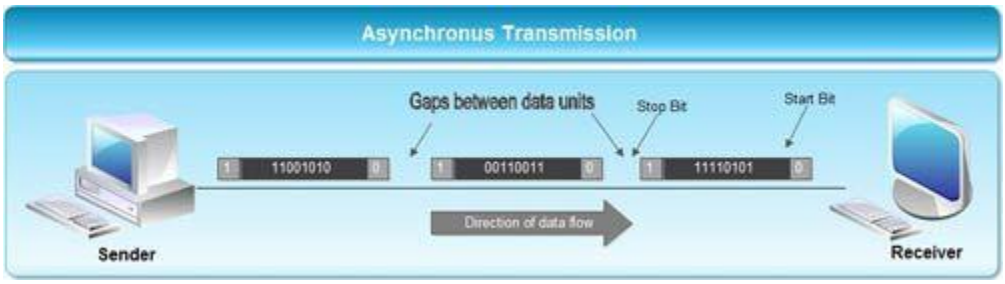
- Addition of start and stop increase the number of data bits. Hence more bandwidth is consumed in asynchronous transmission.
- There is idle time between the transmissions of different data bytes. This idle time is also known as Gap
- The gap or idle time can be of varying intervals. This mechanism is called Asynchronous, because at byte level sender and receiver need not to be synchronized. But within each byte, receiver must be synchronized with the incoming bit stream.

Example: - Email, Forums, Letters

Application of Asynchronous Transmission

1. Asynchronous transmission is well suited for keyboard type-terminals and paper tape devices. The advantage of this method is that it does not require any local

storage at the terminal or the computer as transmission takes place character by character.



2. Asynchronous transmission is best suited to Internet traffic in which information is transmitted in short bursts. This type of transmission is used by modems.

Advantages of Asynchronous transmission

1. This method of data transmission is cheaper in cost as compared to synchronous *e.g.* If lines are short, asynchronous transmission is better, because line cost would be low and idle time will not be expensive.
2. In this approach each individual character is complete in itself, therefore if character is corrupted during transmission, its successor and predecessor character will not be affected.
3. It is possible to transmit signals from sources having different bit rates.
4. The transmission can start as soon as data byte to be transmitted becomes available.
5. Moreover, this mode of data transmission in easy to implement.

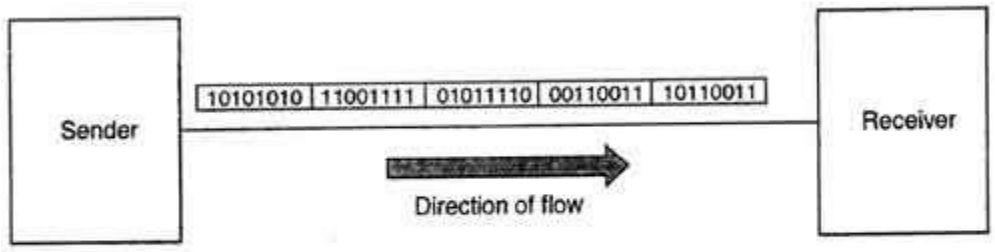
Disadvantages of asynchronous transmission

1. This method is less efficient and slower than synchronous transmission due to the overhead of extra bits and insertion of gaps into bit stream.
2. Successful transmission inevitably depends on the recognition of the start bits. These bits can be missed or corrupted.

Synchronous Transmission

- Synchronous transmission does not use start and stop bits.
- In this method bit stream is combined into longer frames that may contain multiple bytes.

- There is no gap between the various bytes in the data stream.



Synchronous Transmission

- In the absence of start & stop bits, bit synchronization is established between sender & receiver by 'timing' the transmission of each bit.
- Since the various bytes are placed on the link without any gap, it is the responsibility of receiver to separate the bit stream into bytes so as to reconstruct the original information.
- In order to receive the data error free, the receiver and sender operates at the same clock frequency.

An example of synchronous transmission would be the transfer of a large text file. Before the file is transmitted, it is first dissected into blocks of sentences. The blocks are then transferred over the communication link to the target location.

See the following illustration.

Figure 1. Synchronous transmission

- After the syn characters are received by the remote device, they are decoded and used to synchronize the connection. After the connection is correctly synchronized, data transmission may begin.

- An analogy of synchronous transmission would be the transmission of a large text document. Before the document is transferred across the synchronous line, it is first broken into blocks of sentences or paragraphs. The blocks are then sent over the communication link to the remote site.

- The timing needed for synchronous connections is obtained from the devices located on the communication link. All devices on the synchronous link must be set to the same clocking.

Application of Synchronous transmission

- Synchronous transmission is used for high speed communication between computers.

Advantage of Synchronous transmission

- This method is faster as compared to asynchronous as there are no extra bits (start bit & stop bit) and also there is no gap between the individual data bytes.

Disadvantages of Synchronous transmission

- It is costly as compared to asynchronous method. It requires local buffer storage at the two ends of line to assemble blocks and it also requires accurately synchronized clocks at both ends. This lead to increase in the cost.
- The sender and receiver have to operate at the same clock frequency. This requires proper synchronization which makes the system complicated.

Comparison between Serial and Parallel transmission

.NO	SERIAL TRANSMISSION	PARALLEL TRANSMISSION
1.	In serial transmission,	In Parallel Transmission, data

	data(bit) flows in bi-direction.	flows in multiple lines.
2.	Serial Transmission is cost efficient.	Parallel Transmission is not cost efficient.
3.	In serial transmission, one bit transferred at one clock pulse.	In Parallel Transmission, eight bits transferred at one clock pulse.
4.	Serial Transmission is slow in comparison of Parallel Transmission.	Parallel Transmission is fast in comparison of Serial Transmission.
5.	Generally, Serial Transmission is used for long distance.	Generally, Parallel Transmission is used for short distance.
6.	The circuit used in Serial Transmission is simple.	The circuit used in Parallel Transmission is relatively complex.

Comparison between Asynchronous and Synchronous.

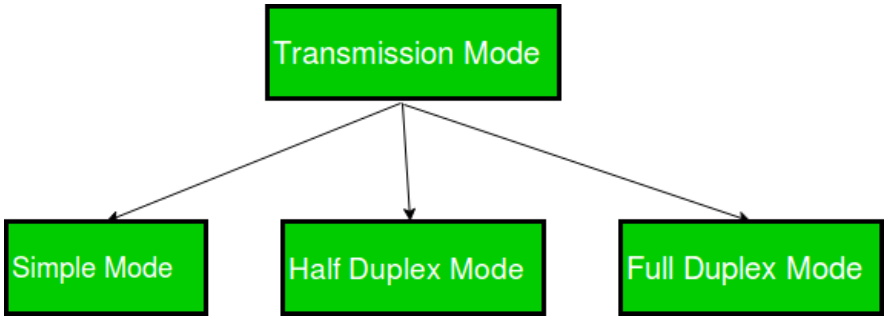
S.NO	SYNCHRONOUS TRANSMISSION	ASYNCHRONOUS TRANSMISSION
1.	In Synchronous transmission, Data is sent in form of blocks or frames.	In asynchronous transmission, Data is sent in form of byte or character.
2.	Synchronous transmission is fast.	Asynchronous transmission is slow.
3.	Synchronous transmission is costly.	Asynchronous transmission economical.
4.	In Synchronous transmission, time interval of transmission is constant.	In asynchronous transmission, time interval of transmission is not constant, it is random.
5.	In Synchronous transmission, There is no gap present between data.	In asynchronous transmission, There is present gap between data.

6.	Efficient use of transmission line is done in synchronous transmission.	While in asynchronous transmission, transmission line remains empty during gap in character transmission.
7.	Synchronous transmission needs precisely synchronized clocks for the information of new bytes.	Asynchronous transmission have no need of synchronized clocks as parity bit is used in this transmission for information of new bytes.

❖ Modes of Communication

Transmission mode means transferring of data between two devices. It is also known as communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected. There are three types of transmission mode:-

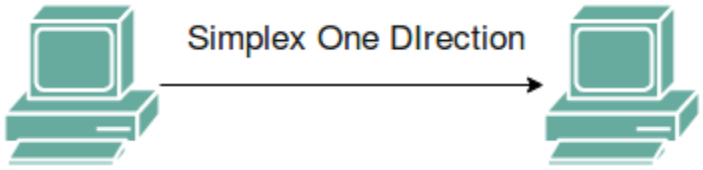
- Simplex Mode
- Half-Duplex Mode
- Full-Duplex Mode



Simplex Mode

In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.

Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.



Advantage of Simplex mode:

In simplex mode, the station can utilize the entire bandwidth of the communication channel, so that more data can be transmitted at a time.

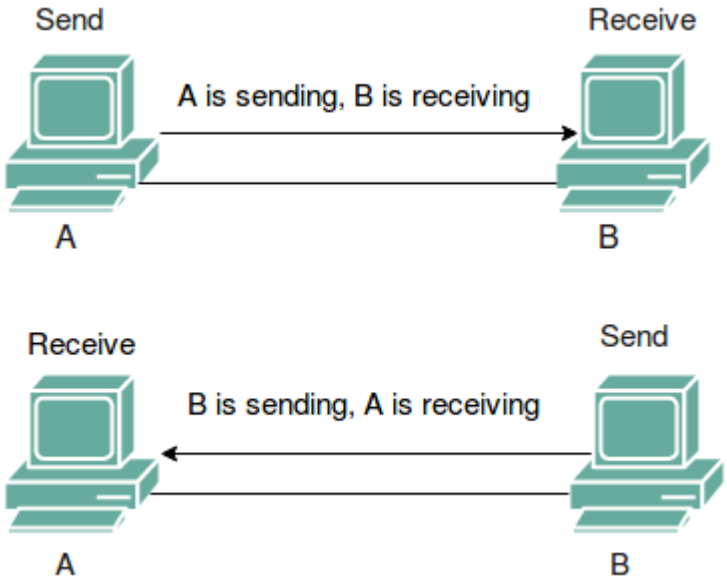
Disadvantage of Simplex mode:

Communication is unidirectional, so it has no inter-communication between devices.

Half-Duplex Mode

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both direction at the same time. The entire capacity of the channel can be utilized for each direction.

Example: Walkie- talkie in which message is sent one at a time and messages are sent in both the directions.



Advantage of Half-duplex mode:

In half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.

Disadvantage of Half-Duplex mode:

In half-duplex mode, when one device is sending the data, then another has to wait, this causes the delay in sending the data at the right time.

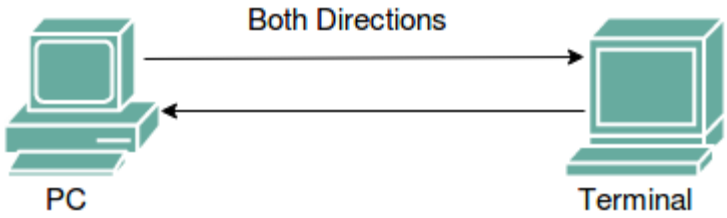
Full-Duplex Mode

In full-duplex mode, both stations can transmit and receive simultaneously. In full duplex mode, signals going in one direction share the capacity of the link with signals going in other direction, this sharing can occur in two ways:

- Either the link must contain two physically separate transmission paths, one for sending and other for receiving.
- Or the capacity is divided between signals travelling in both directions.

Full-duplex mode is used when communication in both direction is required all the time. The capacity of the channel, however must be divided between the two directions.

Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.



Advantage of Full-duplex mode:

Both the stations can send and receive the data at the same time.

Disadvantage of Full-duplex mode:

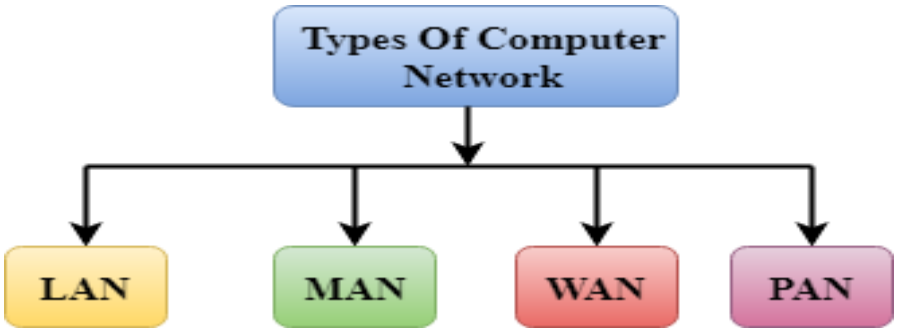
If there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.

❖ Types of Network

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

An example of a network is the Internet, which connects millions of people all over the world

A computer network can be categorized by their size. A computer network is mainly of four types:



- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

LAN(Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and Ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

An example of a LAN is what a small business uses to connect their computers together

Applications of LAN

- One of the computer in a network can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
- Connecting Locally all the workstations in a building to let them communicate with each other locally without any internet access.
- Sharing common resources like printers etc are some common applications of LAN.

Advantages of LAN

- **Resource Sharing:** Computer resources like printers, modems, DVD-ROM drives and hard disks can be shared with the help of local area networks. This reduces cost and hardware purchases.
- **Software Applications Sharing**: It is cheaper to use same software over network instead of purchasing separate licensed software for each client a network.
- **Easy and Cheap Communication**: Data and messages can easily be transferred over networked computers.
- **Centralized Data**: The data of all network users can be saved on hard disk of the server computer. This will help users to use any workstation in a network to access their data. Because data is not stored on workstations locally.
- **Data Security**: Since, data is stored on server computer centrally, it will be easy to manage data at only one place and the data will be more secure too.
- **Internet Sharing**: Local Area Network provides the facility to share a single internet connection among all the LAN users. In Net Cafes, single internet connection sharing system keeps the internet expenses cheaper.

Disadvantages of LAN

- **High Setup Cost:** Although the LAN will save cost over time due to shared computer resources, but the initial setup costs of installing Local Area Networks is high.
- **Privacy Violations**: The LAN administrator has the rights to check personal data files of each and every LAN user. Moreover he can check the internet history and computer use history of the LAN user.

- **Data Security Threat**: Unauthorized users can access important data of an organization if centralized data repository is not secured properly by the LAN administrator.
- **LAN Maintenance Job**: Local Area Network requires a LAN Administrator because, there are problems of software installations or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is needed at this full time job.
- **Covers Limited Area**: Local Area Network covers a small area like one office, one building or a group of nearby buildings.

PAN (Personal Area Network)

Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.

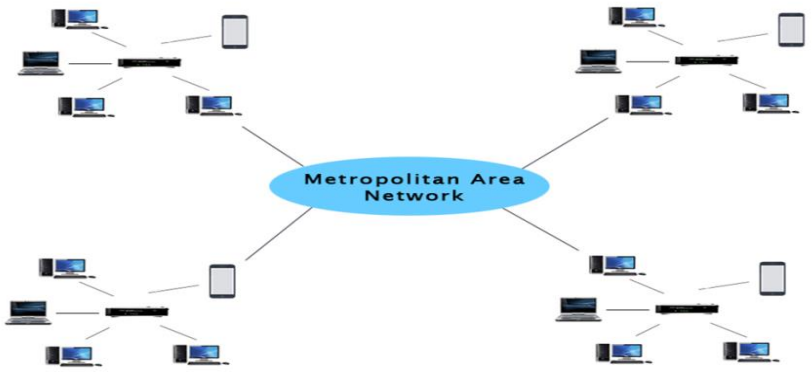
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- Thomas Zimmerman was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of 30 feet.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

Examples of wireless PAN devices include cell phone headsets, wireless keyboards, wireless mice, printers, bar code scanners and game consoles

MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).

An example of a MAN is a series of wireless routers distributed across a city



Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

Characteristics of MAN

- It generally covers towns and cities (50 km)
- Communication medium used for MAN are optical fibers, cables etc.
- Data rates adequate for distributed computing applications.

Advantages of MAN

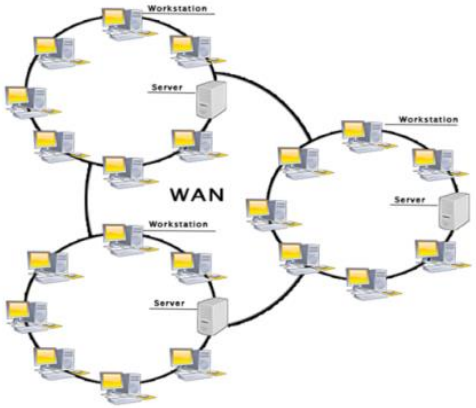
- Extremely efficient and provide fast communication via high-speed carriers, such as fibre optic cables.
- It provides a good back bone for large network and provides greater access to WANs.
- The dual bus used in MAN helps the transmission of data in both directions simultaneously.
- A MAN usually encompasses several blocks of a city or an entire city.

Disadvantages of MAN

- More cable required for a MAN connection from one place to another.
- It is difficult to make the system secure from hackers and industrial **espionage**(spying) graphical regions.

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, and Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

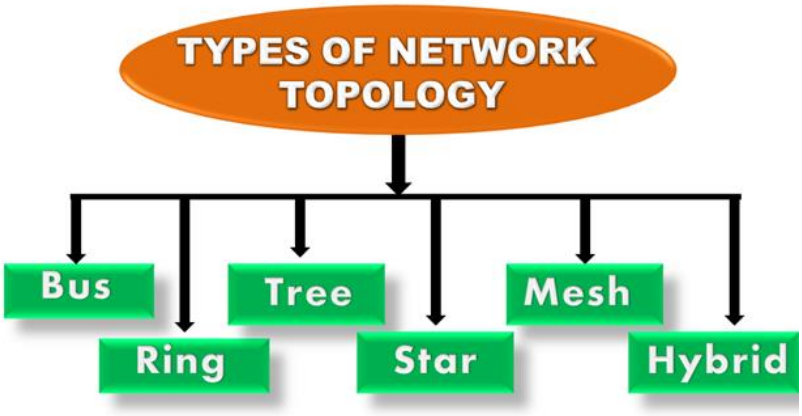
The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

❖ Network Topologies

Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

Physical topology is the geometric representation of all the nodes in a network.



Bus Topology

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (Ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- **An example** of bus topology is connecting two floors through a single line
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

Advantages of Bus topology:

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.

- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.

Token passing: It is a network access method in which token is passed from one node to another node.

Token: It is a frame that circulates around the network.

Working of Token passing

A token moves around the network, and it is passed from computer to computer until it reaches the destination.

The sender modifies the token by putting the address along with the data.

The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.

In a ring topology, a token is used as a carrier.

Advantages of Ring topology:

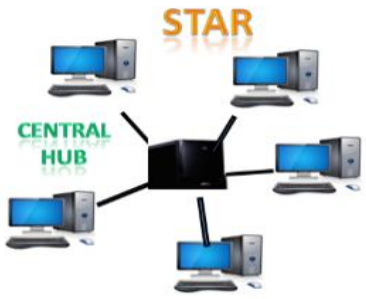
- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.

- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

Star Topology



- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.

- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.
- **Example** :- Video Router

Advantages of Star topology

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star topology

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.

- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

Tree topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.
- **Example** :- Different floors can be connected to each other through combining star topology network and central bus backbone

Advantages of Tree topology

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.

- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

Mesh topology

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an **example** of the mesh topology
- Tennis nets and football goals also **example** of mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.

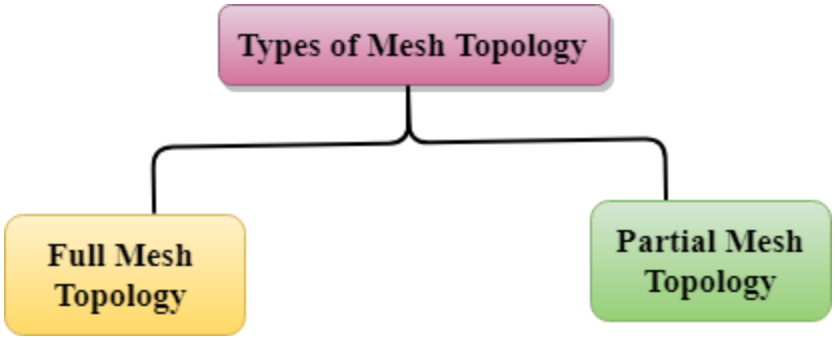
Mesh topology can be formed by using the formula:
Number of cables = (n*(n-1))/2;

Where n is the number of nodes that represents the network.

Mesh topology is divided into two categories:

Fully connected mesh topology

Partially connected mesh topology



Full Mesh Topology: In a full mesh topology, each computer is connected to all the computers available in the network.

Partial Mesh Topology: In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

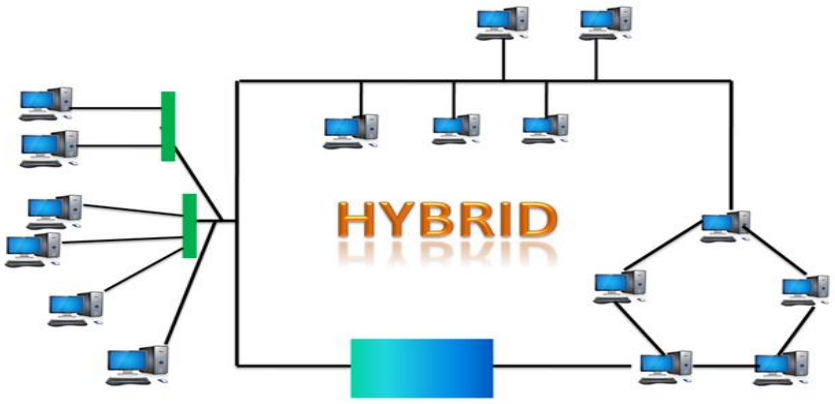
Advantages of Mesh topology:

- **Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.
- **Fast Communication:** Communication is very fast between the nodes.
- **Easier Reconfiguration:** Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

Hybrid Topology



- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will

not result in Hybrid topology. **For example**, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

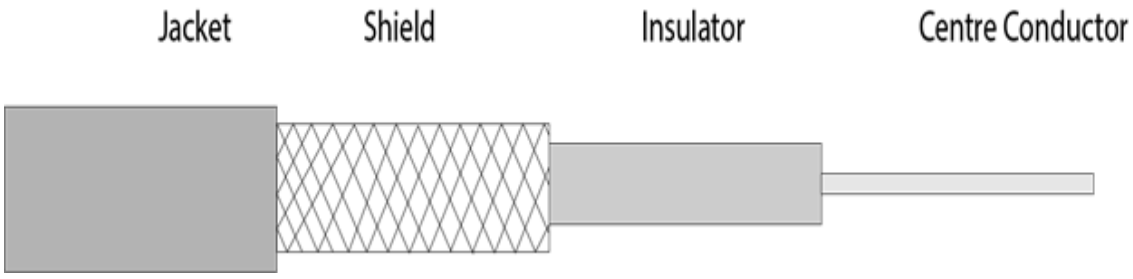
❖ Communications Channels

- 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.
- Wired channels include twisted pair wires used for telephone land lines, coaxial cables used for cable television networks, Category 6 cables used for LANs, and fiber-optic cables used for high capacity trunk lines.

- When you set up a wired connection, you don't have to worry about hackers intercepting your data from outside your house.
- There are ways to tap into a wired network, but they require physical access to the cable or fairly sophisticated snooping equipment
- For **example**, phone calls, text messages, emails, video, radio, and social media are all types of **communication channels**.

❖ Coaxial Cable

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



Coaxial cable is of two types:

- **Baseband transmission**: It is defined as the process of transmitting a single signal at high speed.
- **Broadband transmission**: It is defined as the process of transmitting multiple signals simultaneously.

Advantages of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

Disadvantages of Coaxial cable:

- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

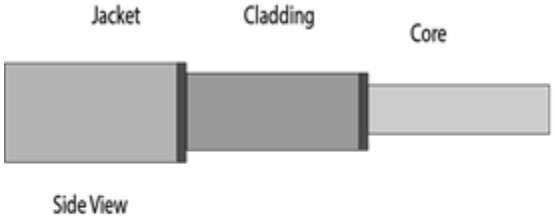
Key differences between baseband and broadband transmissions

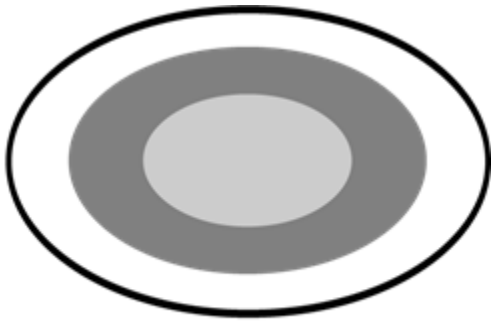
Baseband transmission	Broadband transmission
Transmit digital signals	Transmit analog signals
To boost signal strength, use repeaters	To boost signal strength, use amplifiers
Can transmit only a single data stream at a time	Can transmit multiple signal waves at a time
Support bidirectional communication simultaneously	Support unidirectional communication only
Support TDM based multiplexing	Support FDM based multiplexing
Use coaxial, twisted-pair, and fiber-optic cables	Use radio waves, coaxial cables, and fiber optic cables
Mainly used in Ethernet LAN networks	Mainly used in cable and telephone networks

❖ Optical Fibre Cable

- Fibre optic cable is a cable that uses electrical signals for communication.

- Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provide faster data transmission than copper wires.
- Diagrammatic representation of fibre optic cable:





Basic elements of Fibre optic cable:

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

Following are the advantages of fibre optic cable over copper:

- **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- **Faster speed**: Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.

- **Longer distances**: The fiber optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability**: The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier**: Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

❖ Telephone Lines

Telephone networks were developed late 1800s for transmitting voice in form of analog signals. It is also known as PSTN(Public switched Telephone Network)

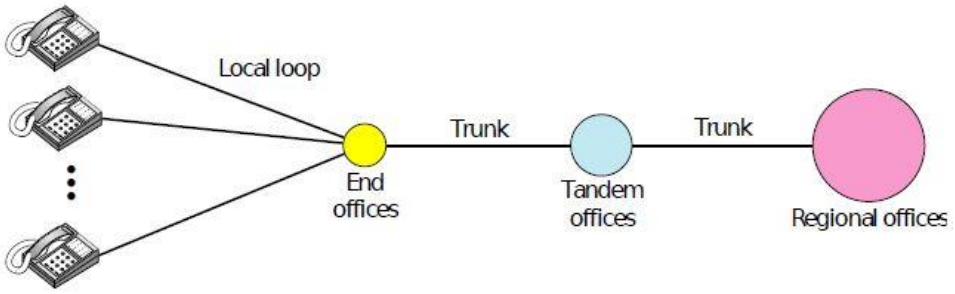
Telephone networks use circuit switching.

Initially, these system used analog switching service. In this ,two wire or four wire twisted pair cable was used to connect the subscriber's handset to the telephone network via exchange.

Now a days, telephone networks also carry digital data thereby providing digital services.

Telephone networks has three major components

- Local Loop
- Trunks
- Switching offices



Local Loop:- is a twisted pair cable that is used to connect the subscriber telephone to the nearest end office or local central office.

Trunks are transmission media that handle the communication between offices. A trunk large can handle large number of connections using multiplexing.

Switching Office are used to handle the calls between different subscribers. Switches are used to connect local loops and trunks and these switches move the calls from one trunk to another. Thus, these switching offices prevent the use of having a permanent physical connection between any two subscribers.

❖ Switch line

A switched line allows a physical transmission path to be established and dedicated to a single connection between two points of a network for the duration that the connection lasts. However, the switched network does not have dedicated links between the points or users, and therefore requires extra switching hardware.

The switching equipment provides a temporary communication path between the two user terminals, giving the two users exclusive use of the link. The communication path provided by the switched line may vary each time a connection is established between two users.

Switched lines are commonly used for ordinary voice telephone systems where the telephone company reserves the established physical path between a caller and the called number. The reservation lasts throughout the call and no one else can use the associated physical lines during this time.

A switching device such as a private branch network (PBX) is often used within an organization to provide users with the ability to share a number of external phone lines directly from their extensions. The PBX allows users to access and share a few external lines, and hence eliminates the need to assign each user an individual line.

Advantages of a switched line are:

- Low cost, especially if there is low usage or traffic between terminals
- Provides means to access and connect multiple distant machines
- Flexibility since many machines offering different services can be accessed
- Once a breakdown occurs on a connection to a facility, the user or machine can redial and obtain an alternative route to the facility.

❖ Leased Line

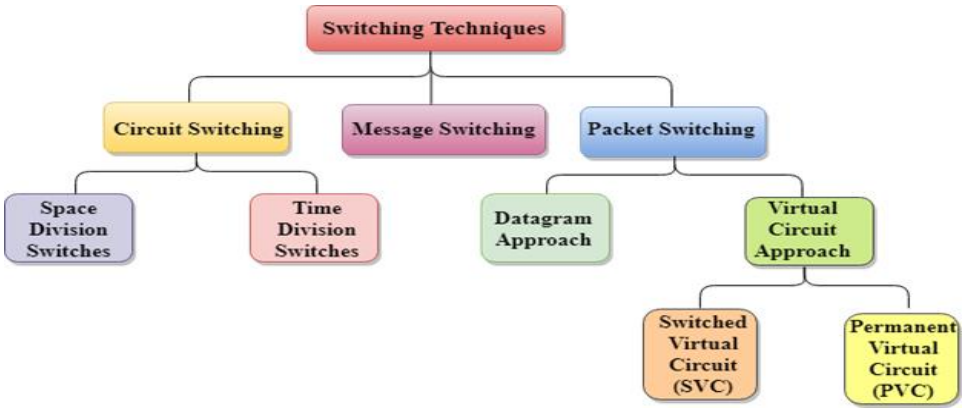
- A leased line is a dedicated line that provides permanent connection between customers.
- Such a line is usually taken on a lease by the customer.
- Leased line does not require the subscriber to dial telephone number of other subscriber i.e no dialing is needed
- Although the connection still passes through the switches in the telephone network, subscribers experience it as a single line.
- Leased lines can provide both analog as well as digital services to customers.

❖ Switching techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Classification of Switching Techniques

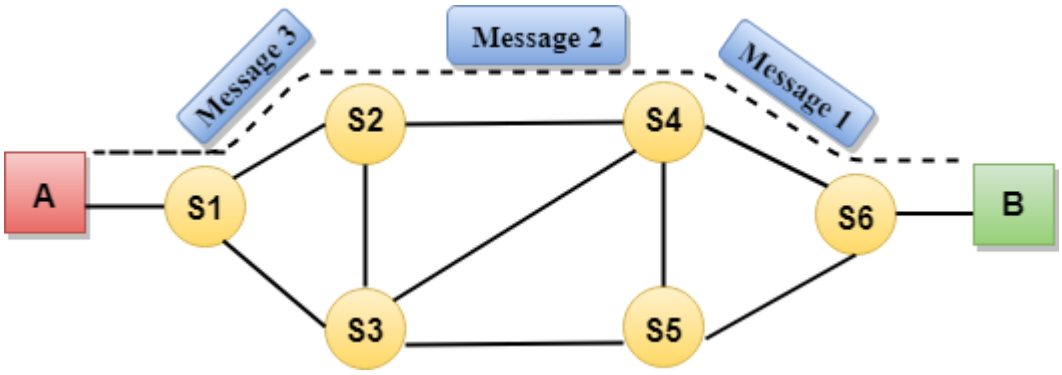


Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.
- Analog telephone network is a well-known **example** of circuit switching.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect



Circuit Switching can use either of the two technologies:

Space Division Switches:

Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of cross points.

Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic cross point or semiconductor gate that can be enabled or disabled by a control unit.

The Crossbar switch is made by using the semiconductor. **For example**, Xilinx crossbar switch using FPGAs.

Space Division Switching has high speed, high capacity, and non blocking switches.

Space Division Switches can be categorized in two ways:

Crossbar Switch

Multistage Switch

Crossbar Switch

The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n^2 intersection points known as **crosspoints.**

Disadvantage of Crossbar switch:

The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

Multistage Switch

Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.

- It reduces the number of crosspoints.
- If one path fails, then there will be an availability of another path.

Advantages of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.

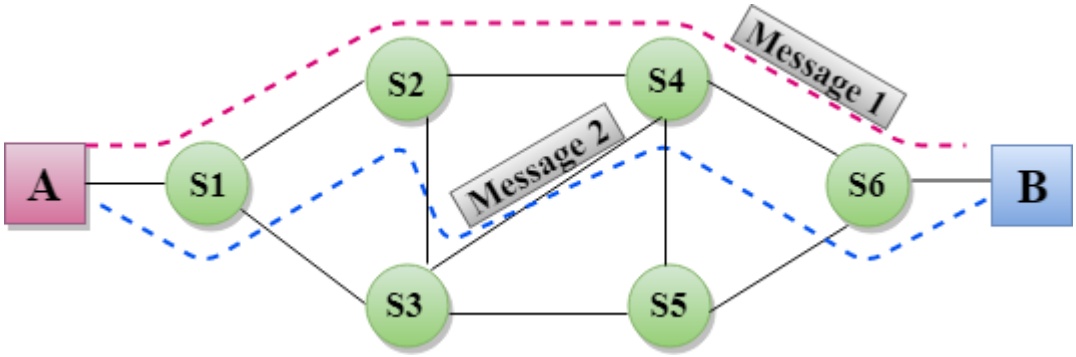
In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.

The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.

Message switches are programmed in such a way so that they can provide the most efficient routes.

Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**

Message switching treats each message as an independent entity.



Advantages Of Message Switching

- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages Of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.

- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.

The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.

Every packet contains some information in its headers such as source address, destination address and sequence number.

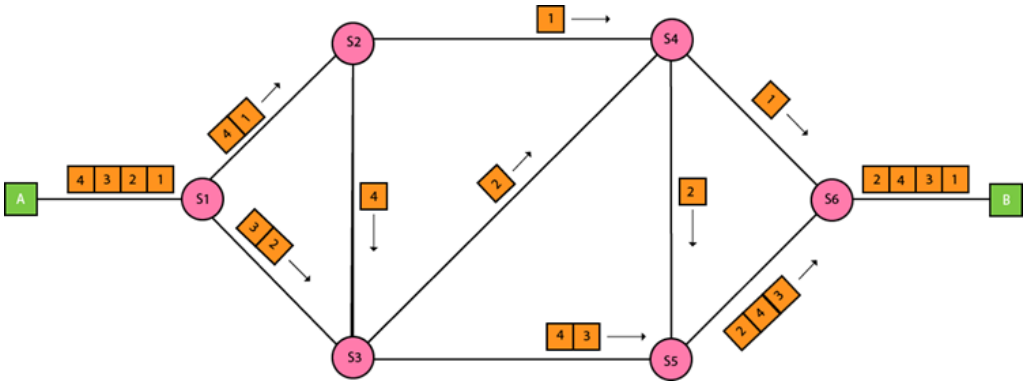
Packets will travel across the network, taking the shortest path as possible.

All the packets are reassembled at the receiving end in correct order.

If any packet is missing or corrupted, then the message will be sent to resend the message.

If the correct order of the packets is reached, then the acknowledgment message will be sent.

Examples of connectionless systems are Ethernet, Internet Protocol (IP), and the User Datagram Protocol (UDP).



Approaches of Packet Switching:

There are two approaches to Packet Switching:

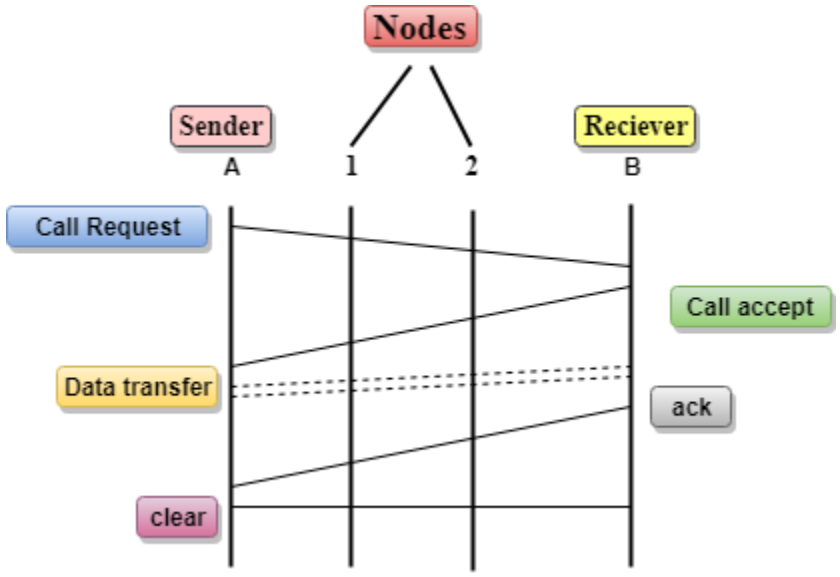
Datagram Packet switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:



In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.

Call request and call accept packets are used to establish a connection between the sender and receiver.

When a route is established, data will be transferred.

After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.

If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages Of Packet Switching:

Cost-effective: In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.

Reliable: If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.

Efficient: Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.
- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

UNIT II

❖ Network Reference Models

OSI Model

OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

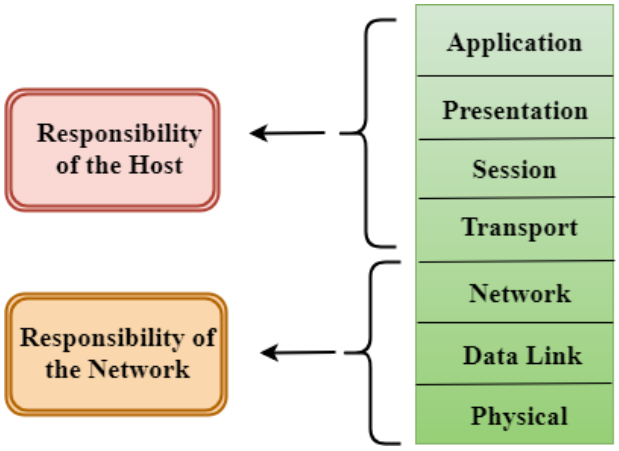
OSI consists of seven layers, and each layer performs a particular network function.

OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.

OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.

Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:



The OSI model is divided into two layers: upper layers and lower layers.

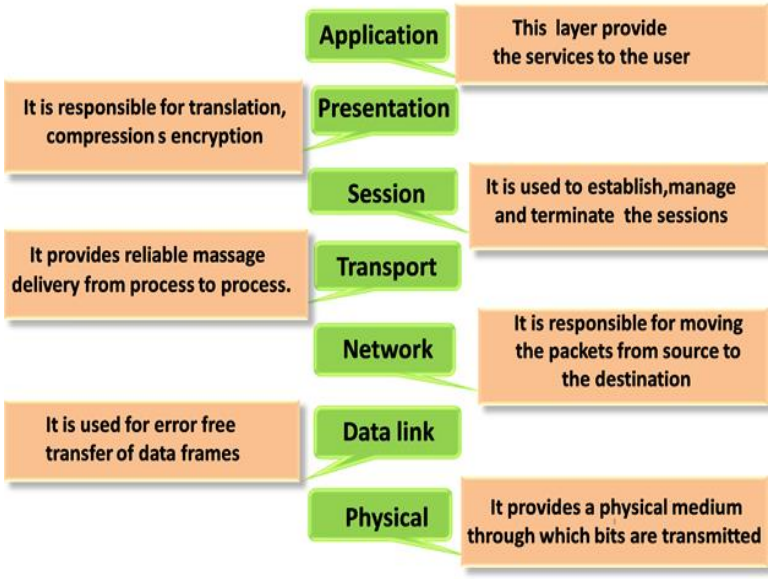
The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.

The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

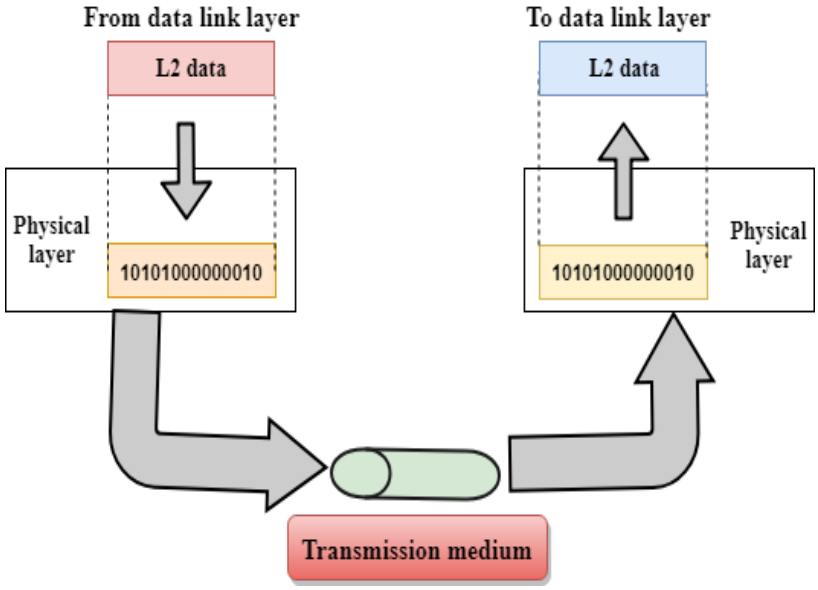
Functions of the OSI Layers

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

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



Physical layer



The main functionality of the physical layer is to transmit the individual bits from one node to another node.

It is the lowest layer of the OSI model.

It establishes, maintains and deactivates the physical connection.

It specifies the mechanical, electrical and procedural network interface specifications.

Example, the antenna and the amplifier, plug and socket for the network cable, the repeater, the stroke, the transceiver, the T-bar and the terminator.

Functions of a Physical layer:

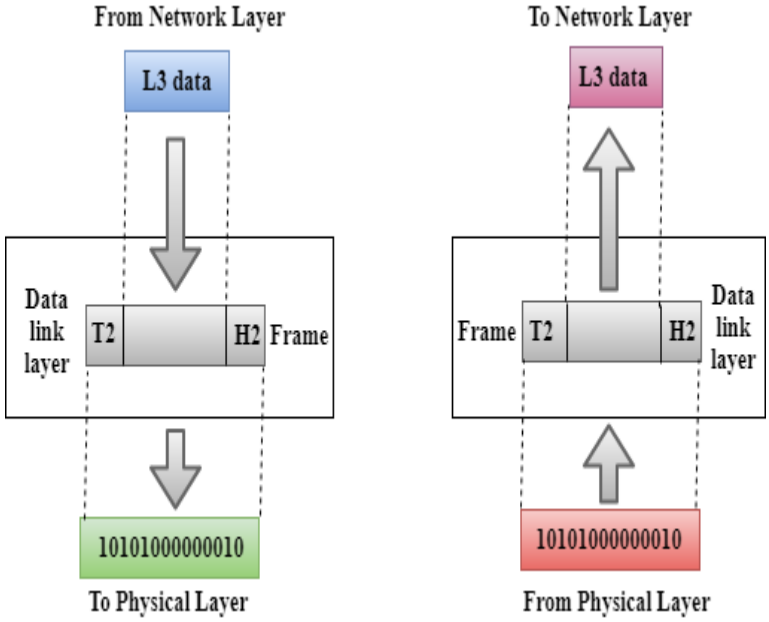
Line Configuration: It defines the way how two or more devices can be connected physically.

Data Transmission: It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.

Topology: It defines the way how network devices are arranged.

Signals: It determines the type of the signal used for transmitting the information.

Data-Link Layer



- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- **Examples of** data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP)

It contains two sub-layers:

Logical Link Control Layer

- It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
- It identifies the address of the network layer protocol from the header.
- It also provides flow control.

Media Access Control Layer

- A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
- It is used for transferring the packets over the network.

Functions of the Data-link layer

Framing: The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

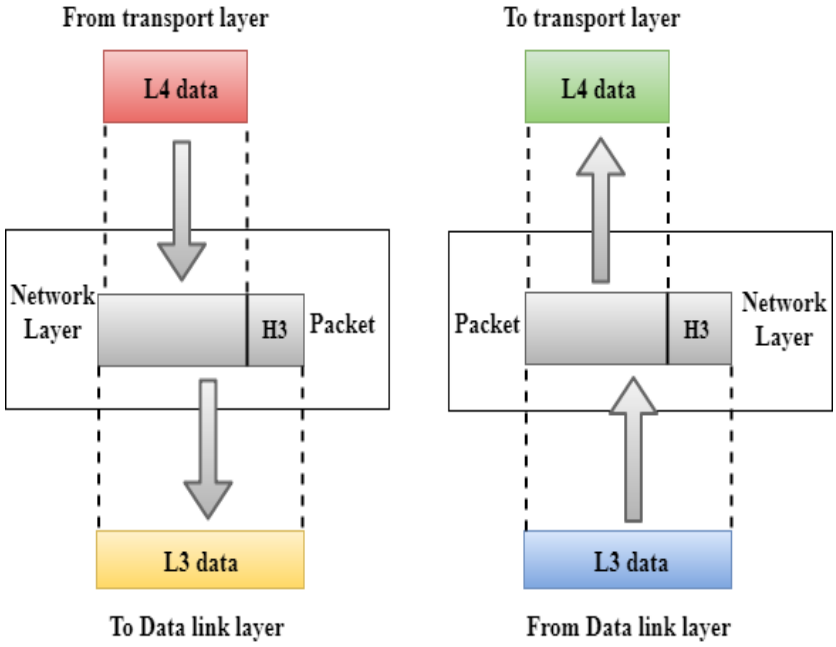
Physical Addressing: The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.

Flow Control: Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.

Error Control: Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.

Access Control: When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Network Layer



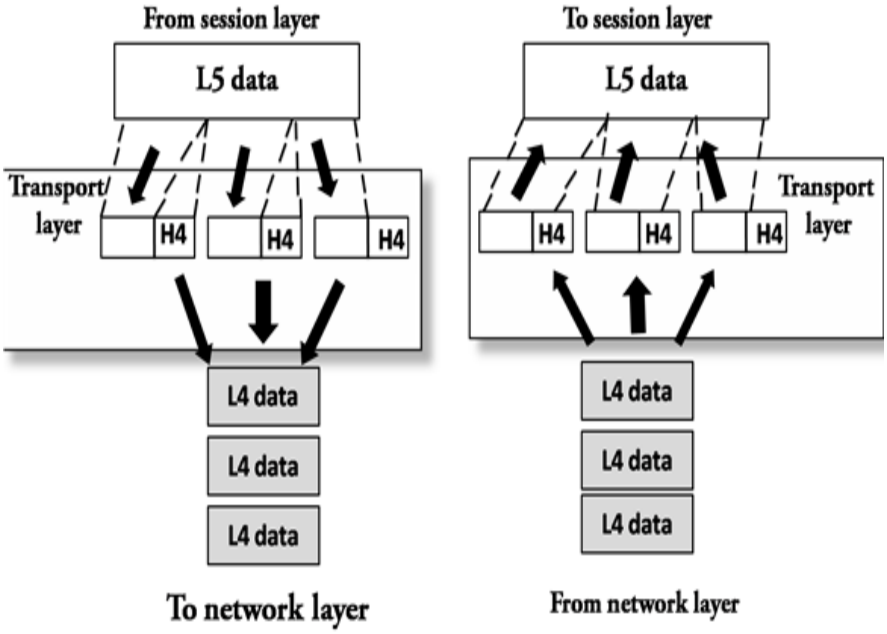
- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and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

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Transport Layer



The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.

TCP is the best-known **example** of the transport layer

The main responsibility of the transport layer is to transfer the data completely.

It receives the data from the upper layer and converts them into smaller units known as **segments**.

This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

Transmission Control Protocol

It is a standard protocol that allows the systems to communicate over the internet.

It establishes and maintains a connection between hosts.

When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

User Datagram Protocol

User Datagram Protocol is a transport layer protocol.

It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

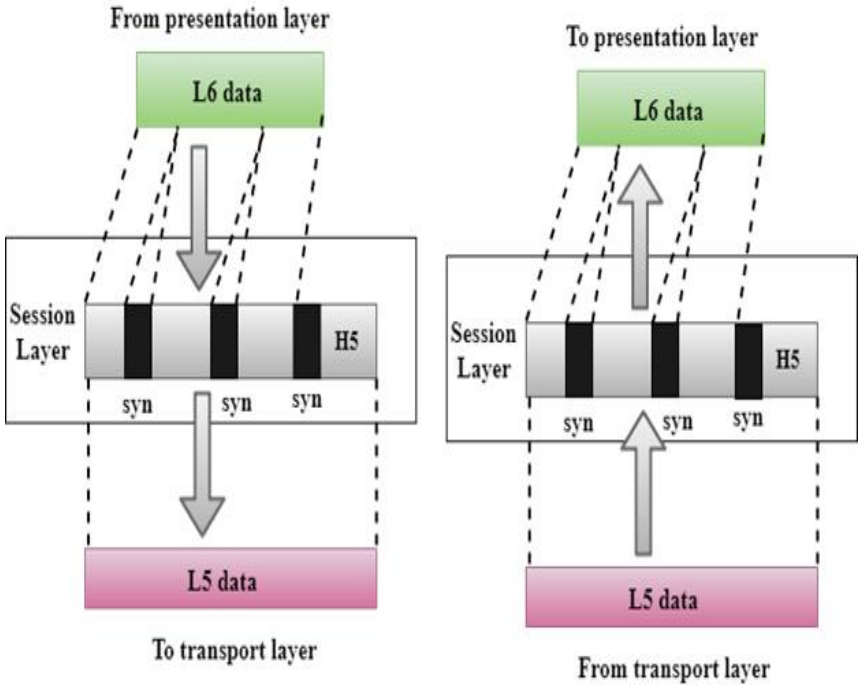
Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the

packets. In connection-oriented service, all the packets travel in the single route.

- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer



It is a layer 5 in the OSI model.

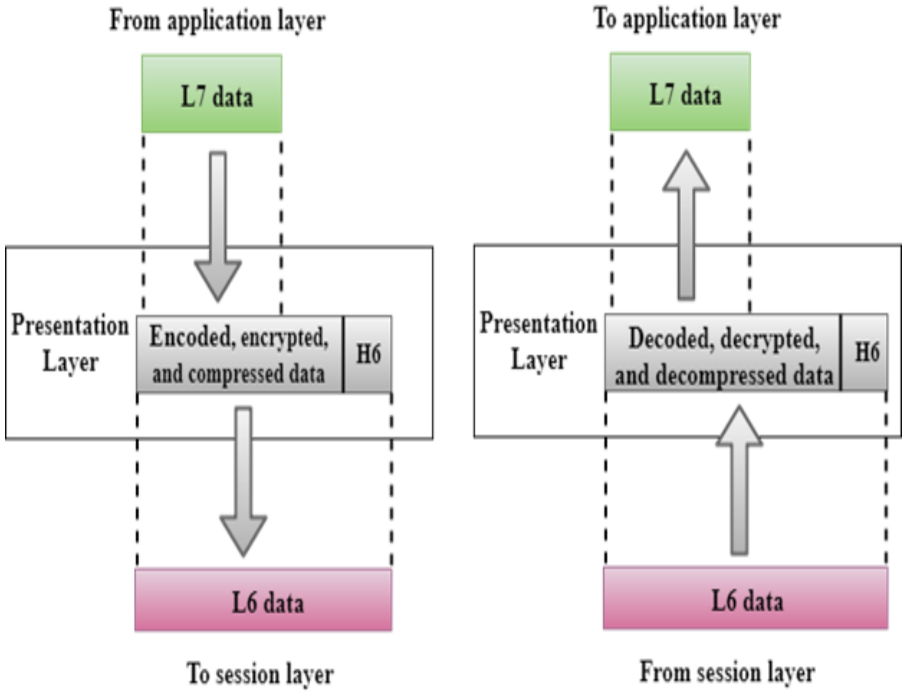
The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

Presentation Layer



A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.

It acts as a data translator for a network.

This layer is a part of the operating system that converts the data from one presentation format to another format.

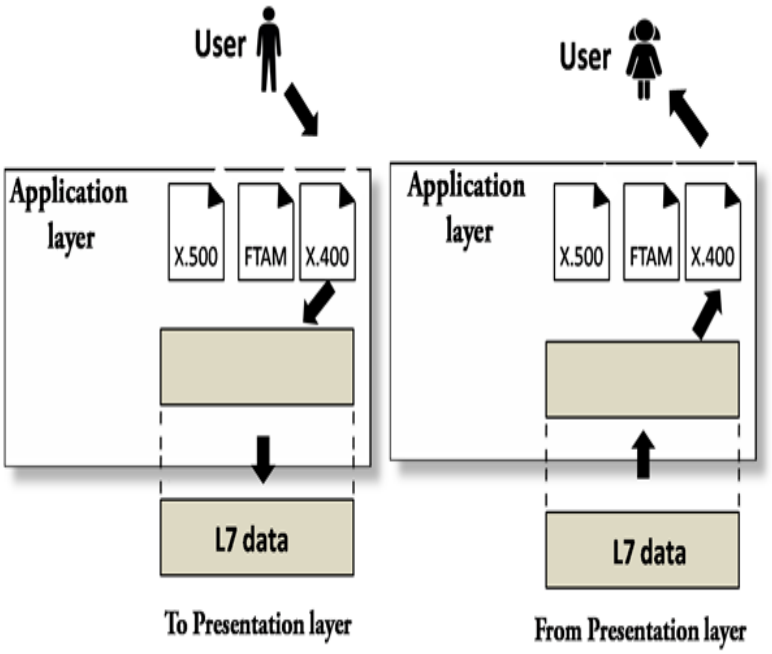
The Presentation layer is also known as the syntax layer.

Examples of presentation layer protocols are SSL, HTTP/ HTML (agent), FTP (server), AppleTalk Filing Protocol, Telnet,

Functions of Presentation layer:

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

Application Layer



An application layer serves as a window for users and application processes to access network service.

It handles issues such as network transparency, resource allocation, etc.

An application layer is not an application, but it performs the application layer functions.

This layer provides the network services to the end-users.

Functions of Application layer:

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

Advantages of the OSI Model

- Here are the major benefits/pros of using the OSI model:
- It helps you to standardize router, switch, motherboard, and other hardware
- Reduces complexity and standardizes interfaces
- Facilitates modular engineering
- Helps you to ensure interoperable technology
- Helps you to accelerate the evolution
- Protocols can be replaced by new protocols when technology changes.
- Provide support for connection-oriented services as well as connectionless service.
- It is a standard model in computer networking.
- Supports connectionless and connection-oriented services.
- It offers flexibility to adapt to various types of protocols.

Disadvantages of OSI Model

Here are some cons/ drawbacks of using OSI Model:

- Fitting of protocols is a tedious task.
- You can only use it as a reference model.
- It doesn't define any specific protocol.

- In the OSI network layer model, some services are duplicated in many layers such as the transport and data link layers
- Layers can't work in parallel as each layer need to wait to obtain data from the previous layer.

Comparison between osi and tcp/ip reference model

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built.	7. TCP/IP model is, in a way implementation of the OSI model.

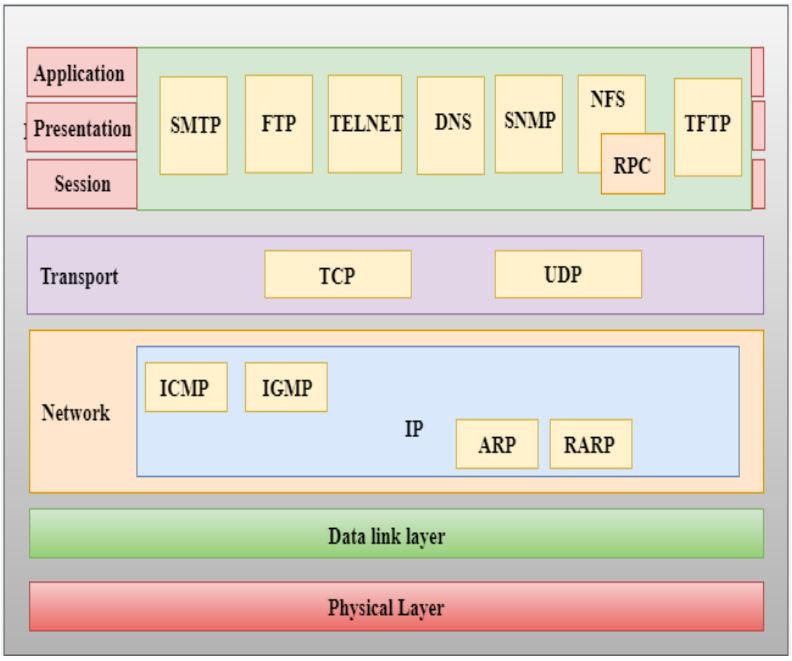
Generally it is used as a guidance tool.	
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

❖ **TCP/IP model**

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.

- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.
- Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:



Network Access Layer

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

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

Following are the protocols used in this layer are:

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

Following are the responsibilities of this protocol:

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

ARP Protocol

- ARP stands for **Address Resolution Protocol**.

- ARP is a network layer protocol which is used to find the physical address from the IP address.

The two terms are mainly associated with the ARP Protocol:

- **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
- **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.

An ICMP protocol mainly uses two terms:

- **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
- **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Transport Layer

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

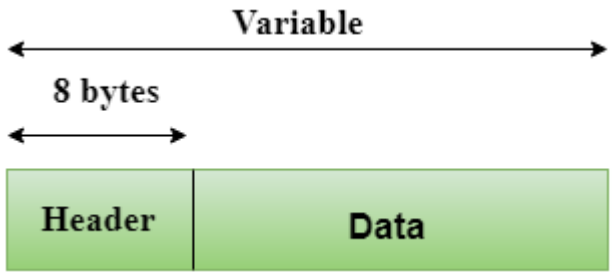
User Datagram Protocol (UDP)

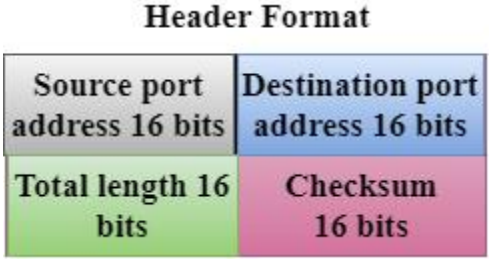
- It provides connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.

UDP consists of the following fields:

Source port address: The source port address is the address of the application program that has created the message.
Destination port address: The destination port address is the address of the application program that receives the message.
Total length: It defines the total number of bytes of the user datagram in bytes.
Checksum: The checksum is a 16-bit field used in error detection.

UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.





Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

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

Following are the main protocols used in the application layer:

HTTP: HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the

efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

SNMP: SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.

SMTP: SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

DNS: DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

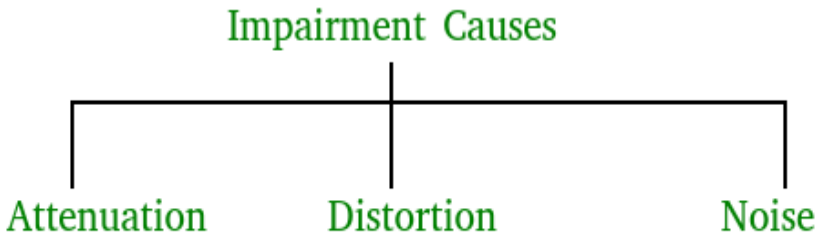
TELNET: It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.

FTP: FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

❖ Transmission impairments

In communication system, analog signals travel through transmission media, which tends to deteriorate the quality of analog signal. This imperfection causes signal impairment. This means that received signal is not same as the signal that was send.

Causes of impairment –



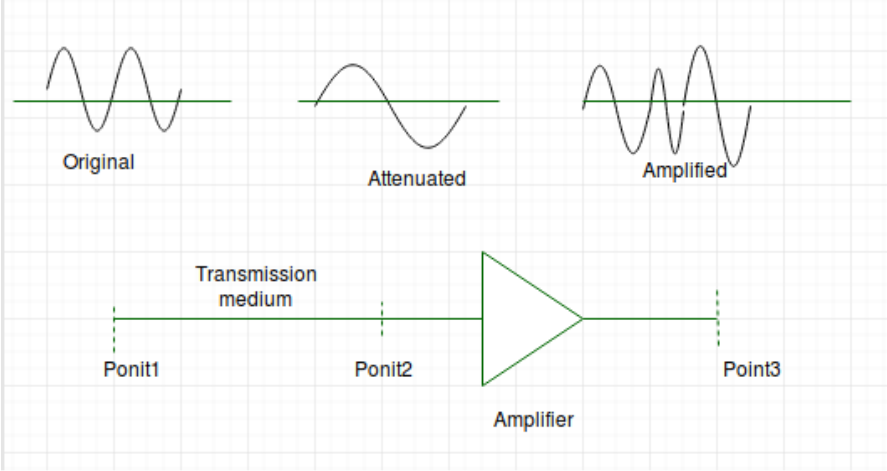
Attenuation – Here attenuation Means loss of energy that is the weaker signal. Whenever a signal transmitted through a medium it loses its energy, so that it can overcome by the resistance of the medium.

That is why a wire carrying electrical signals gets warm, if not hot, after a while. Some of the electrical energy is converted to heat in the signal.

Amplifiers are used to amplify the signals to compensate for this loss.

An example of this is Wi-Fi signal and strength getting noticeably weaker the further that your device is from the router

This figure shows the **effect of attenuation and amplification**:



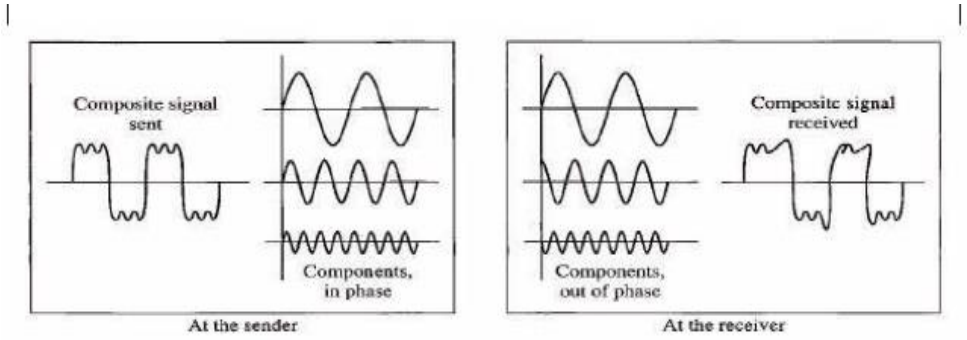
Attenuation is measured in **decibels(dB)**. It measures the relative strengths of two signals or one signal at two different point.

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.

Each component of frequency has its propagation speed traveling through a medium and therefore, different components have different delay in arriving at the final destination.

It means that signals have different phases at the receiver than they did at the source.

This figure shows the effect of distortion on a composite signal:



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.

Different types of noises are:

- Thermal noise
- Intermodulation noise
- Crosstalk
- Impulse noise

a) Thermal noise

The thermal noise is random motion of electrons in a conductor that creates an extra signal not originally sent by the transmitter.

It is also known as white noise because it is distributed across the entire spectrum (as the frequency encompass over a broad range of frequencies).

b) Intermodulation noise

More than one signal share a single transmission channel, intermodulation noise is generated.

For instance, two signals S1 and S2 will generate signals of frequencies (S1 + S2) and (s1 - S2), which may interfere with the signals of the same frequencies sent by the sender. due to If nonlinearity present in any part of the communication system, intermodulation noise is introduced.

c) Cross talk

Cross talk is an effect a wire on 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.

d) Impulse noise

Impulse noise is irregular pulses or spikes(a signal with high energy in a very short period) generated by phenomena like that comes from power lines, lightning, spark due to loose contact in electric circuits and so on.

❖ Multiplexing

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

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line. **For example**, in telecommunications, several telephone calls may be carried using one wire

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

Why Multiplexing?

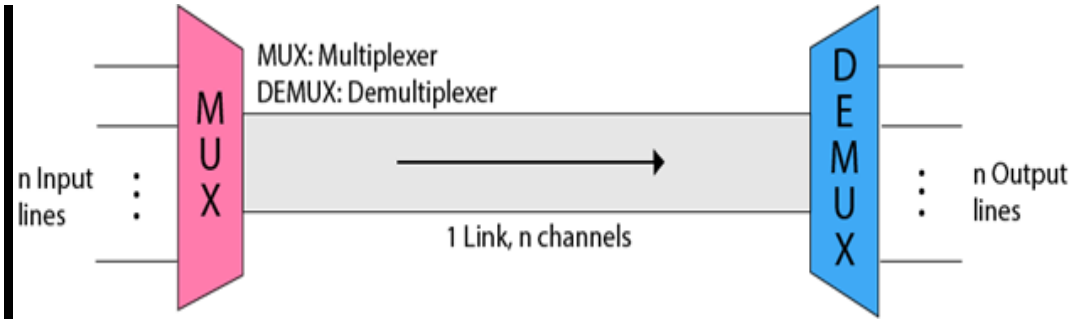
The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.

If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.

When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.

Transmission services are very expensive.

Concept of Multiplexing

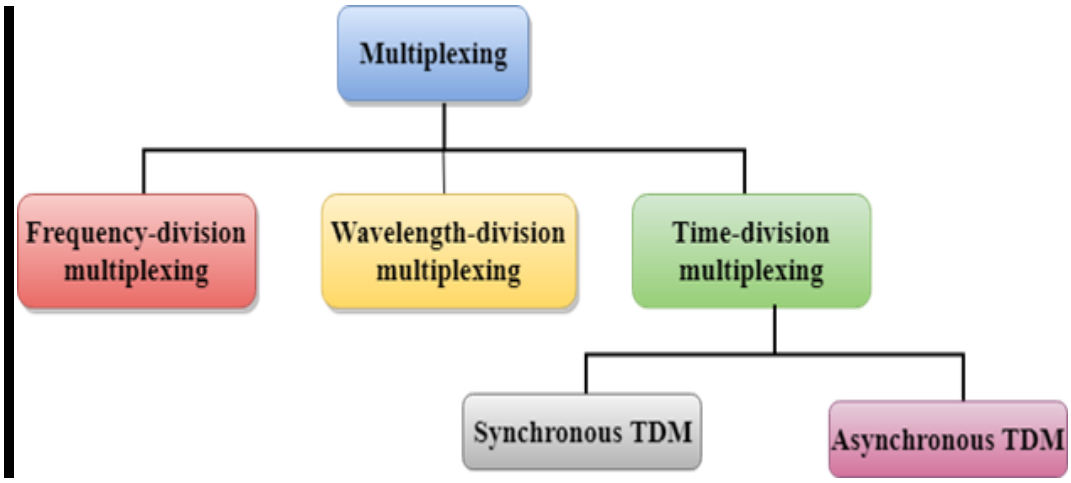


The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.

The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.
- Multiplexing Techniques
- Multiplexing techniques can be classified as:

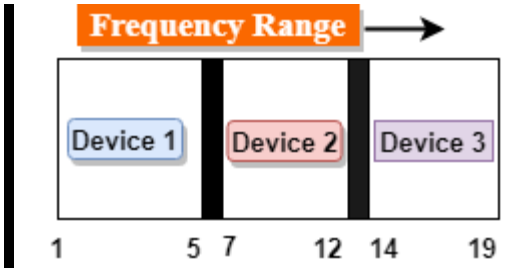


Frequency-division Multiplexing (FDM)

It is an analog technique.

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

Example of frequency-division multiplexing is radio and television broadcasting, in which multiple radio signals at different frequencies pass through the air at the same time



In the **above diagram**, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.

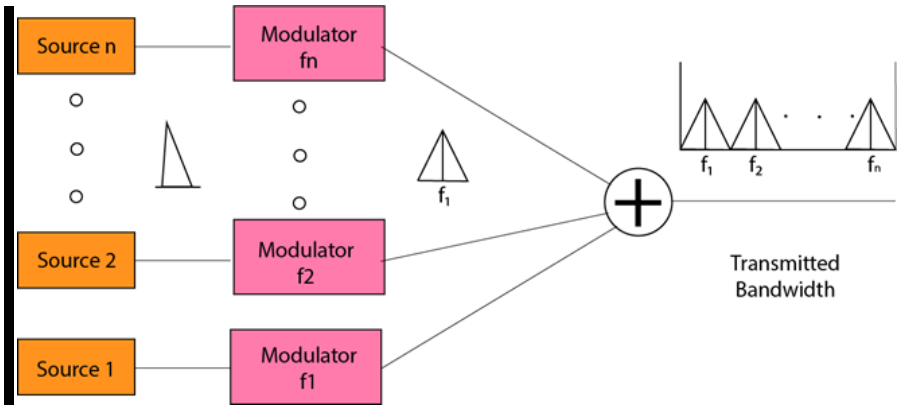
The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.

The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.

Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.

The carriers which are used for modulating the signals are known as **sub-carriers**. They are represented as f1,f2..fn.

FDM is mainly used in radio broadcasts and TV networks.



Advantages Of FDM:

- FDM is used for analog signals.
- FDM process is very simple and easy modulation.
- A Large number of signals can be sent through an FDM simultaneously.
- It does not require any synchronization between sender and receiver.

Disadvantages Of FDM:

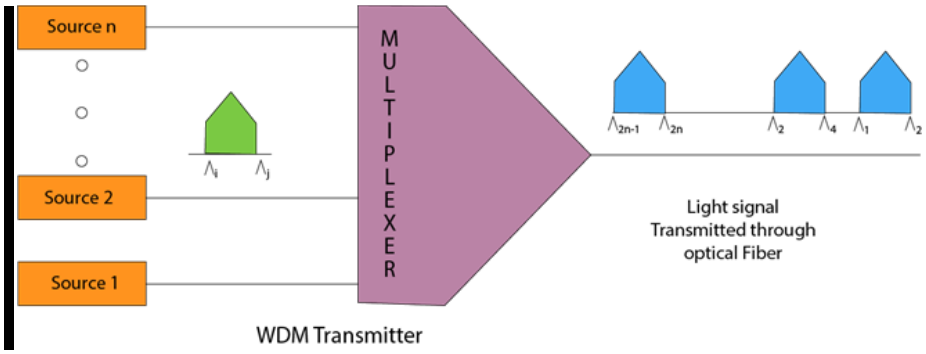
- FDM technique is used only when low-speed channels are required.
- It suffers the problem of crosstalk.
- A Large number of modulators are required.
- It requires a high bandwidth channel.

Applications Of FDM:

- FDM is commonly used in TV networks.

- It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Wavelength Division Multiplexing (WDM)



Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.

WDM is used on fibre optics to increase the capacity of a single fibre.

It is used to utilize the high data rate capability of fibre optic cable.

It is an analog multiplexing technique.

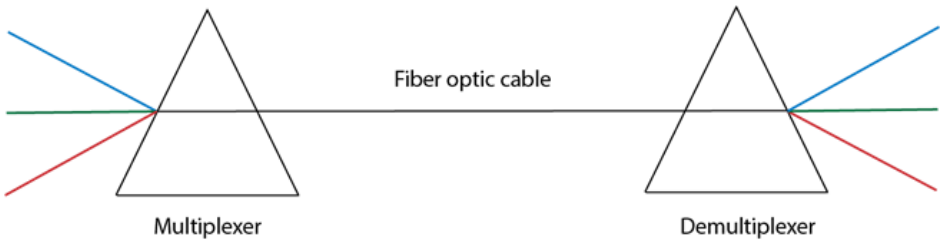
Optical signals from different source are combined to form a wider band of light with the help of multiplexer.

At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.

Multiplexing and Demultiplexing can be achieved by using a prism.

Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.

Prism also performs a reverse operation, i.e., demultiplexing the signal.



Benefits or advantages of WDM

Following are the benefits or **advantages of WDM**:

- Full duplex transmission is possible.
- Easier to reconfigure.
- Optical components are similar and more reliable.
- It provides higher bandwidth.
- This could be the best approach as it is simple to implement.
- High security

Drawbacks or disadvantages of WDM

Following are the **disadvantages of WDM**:

- Signals can not be very close.
- Light wave carrying WDM are limited to 2-point circuit.
- Scalability is a concern as OLT (Optical Line Termination) has to have transmitter array with one transmitter for each ONU (Optical Network Unit). Adding a new ONU could be problem unless transmitters were provisioned in advance. Each ONU must have a wavelength specific laser.
- Cost of system increases with addition of optical components.
- (WDM in PON:) Inefficiency in BW utilization, difficulty in wavelength tuning, difficulty in cascaded topology

Time Division Multiplexing

It is a digital technique.

In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.

In **Time Division Multiplexing technique**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.

A user takes control of the channel for a fixed amount of time.

In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.

In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.

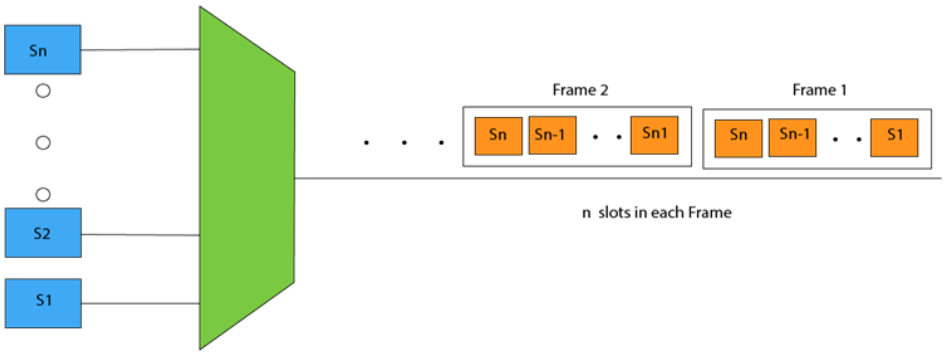
It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

There are two types of TDM:

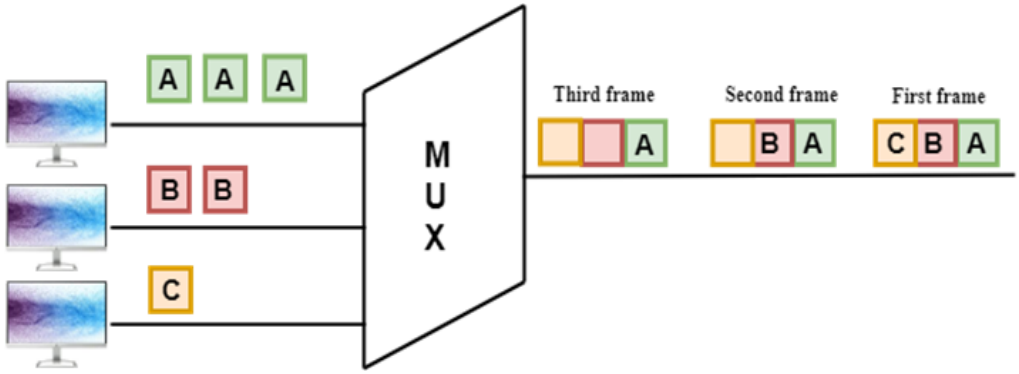
- Synchronous TDM
- Asynchronous TDM

Synchronous TDM

- A Synchronous TDM is a technique in which time slot is preassigned to every device.
- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.
- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.
- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.
- If there are n devices, then there are n slots.



Concept Of Synchronous TDM



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

Advantages

- An order is maintained
- No addressing information is required channel capacity should be large

Disadvantages Of Synchronous TDM:

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

Asynchronous TDM

An asynchronous TDM is also known as Statistical TDM.

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

An asynchronous TDM technique dynamically allocates the time slots to the devices.

In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.

Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.

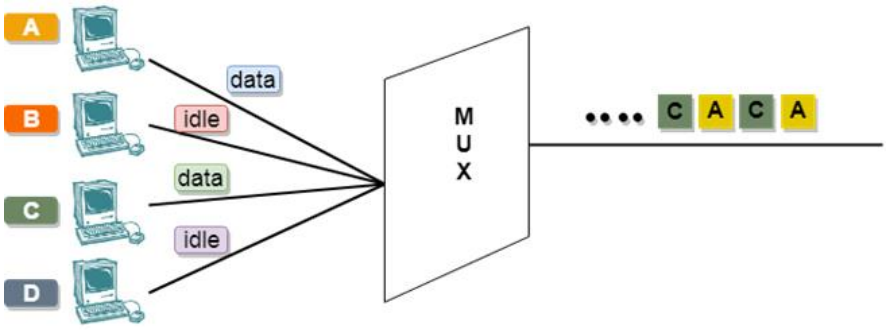
In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

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

In Synchronous TDM, if there are n sending devices, then there are n time slots. In Asynchronous TDM, if there are n sending devices, then there are m time slots where m is less than n (**m<n**).

The number of slots in a frame depends on the statistical analysis of the number of input lines.

Concept Of Asynchronous TDM



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

Advantages of Asynchronous TDM

- Code utilization of communication channel.
- TDM circuitry is not very complex.
- communication link of low capacity is used
- The problem of crosstalk is not severe
- Full available channel bandwidth can be utilize for each channel

Disadvantages of Asynchronous TDM

- Frames have different size
- Requires buffers
- Address information is needed

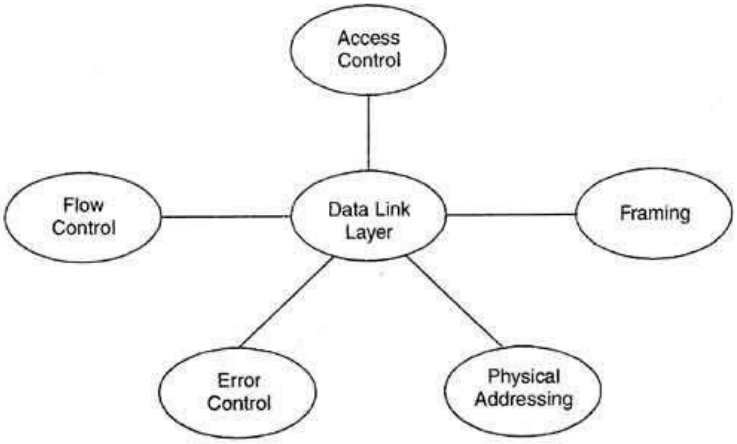
❖ Data Link Layer Design Issues

The data link layer in the OSI (Open System Interconnections) Model, is in between the physical layer and the network layer. This layer converts the raw transmission facility provided by the physical layer to a reliable and error-free link.

The main functions and the design issues of this layer are

- Providing services to the network layer
- Framing

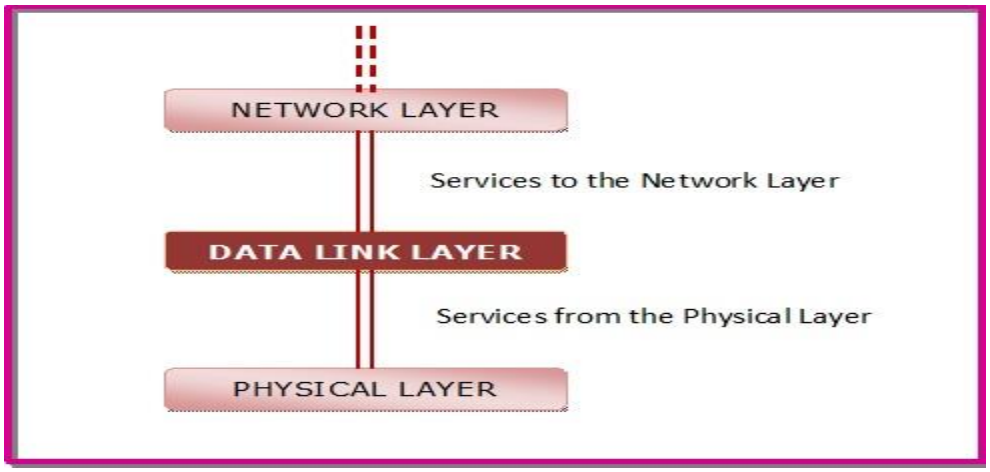
- Error Control
- Flow Control



Functions of data link layer

❖ Services to the Network Layer

In the OSI Model, each layer uses the services of the layer below it and provides services to the layer above it. The data link layer uses the services offered by the physical layer. The primary function of this layer is to provide a well defined service interface to network layer above it.



The types of services provided can be of three types −

- Unacknowledged connectionless service

- Acknowledged connectionless service
- Acknowledged connection - oriented service
- Unacknowledged connectionless service

Types of Services

The data link layer offers three types of services.

Unacknowledged connectionless service − Here, the data link layer of the sending machine sends independent frames to the data link layer of the receiving machine. The receiving machine does not acknowledge receiving the frame. No logical connection is set up between the host machines. Error and data loss is not handled in this service. This is applicable in Ethernet services and voice communications. An **example** can be Ethernet.

Acknowledged connectionless service − Here, no logical connection is set up between the host machines, but each frame sent by the source machine is acknowledged by the destination machine on receiving. If the source does not receive the acknowledgment within a stipulated time, then it resends the frame. This is used in Wifi (IEEE 802.11) services.

Acknowledged connection-oriented service − This is the best service that the data link layer can offer to the network layer. A logical connection is set up between the two machines and the data is transmitted along this logical path. The frames are numbered, that keeps track of loss of frames and also ensures that frames are received in correct order.

❖ Framing in Data Link Layer

Frames are the small data units created by the data link layer and the process of creating frames by the data link is known as framing.

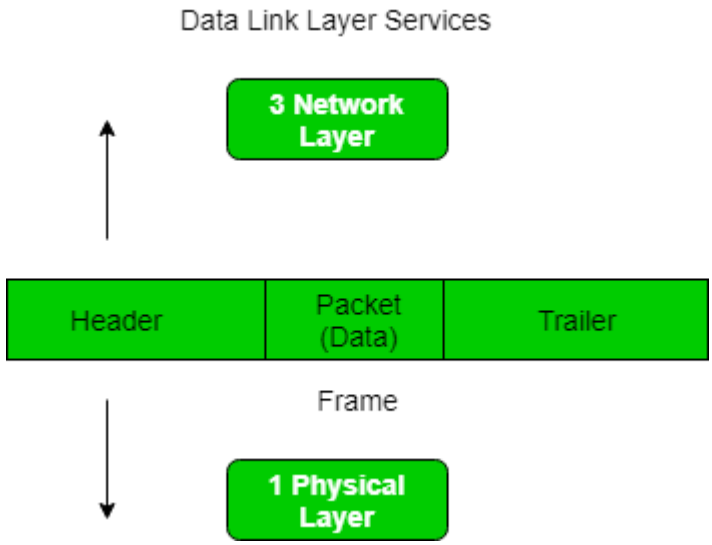
On the source side, data link layer receives the bit stream from network layer and divide it into discrete frames.

It then computers the checksum for each frame and add it to frame. checksum provide the error detection mechanism.

On the destination side, data link layer receives these frames form physical layer & recomputes the checksum of each frame.

If this newly computed checksum is different from the one contained in the frame, then data link layer knows that an error has occurred. **Example** of Framing is ATM cells.

Data link layer then discard this erronous frame & ask for retransmission



At data link layer, it extracts message from sender and provide it to receiver by providing sender's and receiver's address. The advantage of using frames is that data is broken up into recoverable chunks that can easily be checked for corruption.

Problems in Framing –

Detecting start of the frame: When a frame is transmitted, every station must be able to detect it. Station detect frames by looking out for special sequence of bits that marks the beginning of the frame i.e. SFD (Starting Frame Delimeter).

How do station detect a frame: Every station listen to link for SFD pattern through a sequential circuit. If SFD is detected, sequential circuit alerts station. Station checks destination address to accept or reject frame.

Detecting end of frame: When to stop reading the frame.

Types of framing – There are two types of framing:

1. Fixed size – The frame is of fixed size and there is no need to provide boundaries to the frame, length of the frame itself acts as delimiter.

Drawback: It suffers from internal fragmentation if data size is less than frame size

Solution: Padding

2. Variable size – In this there is need to define end of frame as well as beginning of next frame to distinguish. This can be done in two ways:

Length field – We can introduce a length field in the frame to indicate the length of the frame. Used in Ethernet(802.3**)**. The problem with this is that sometimes the length field might get corrupted.

End Delimeter (ED) – We can introduce an ED(pattern) to indicate the end of the frame. Used in Token Ring. The problem with this is that ED can occur in the data. This can be solved by:

Different framing method implemented by data link layer are:

1. Character count

- This method specifies the number of characters that are present in a particular frame.
- This information (character count) is specified by using a special field in the header of frame.
- When the data link layer at the destination sees the character count, it comes to known how many characters are present in the frame. With this information it is able to detect the end of the frame.

As shown in the fig. there are four frames of sizes 3,4,7 and 2 characters respectively.

Character count

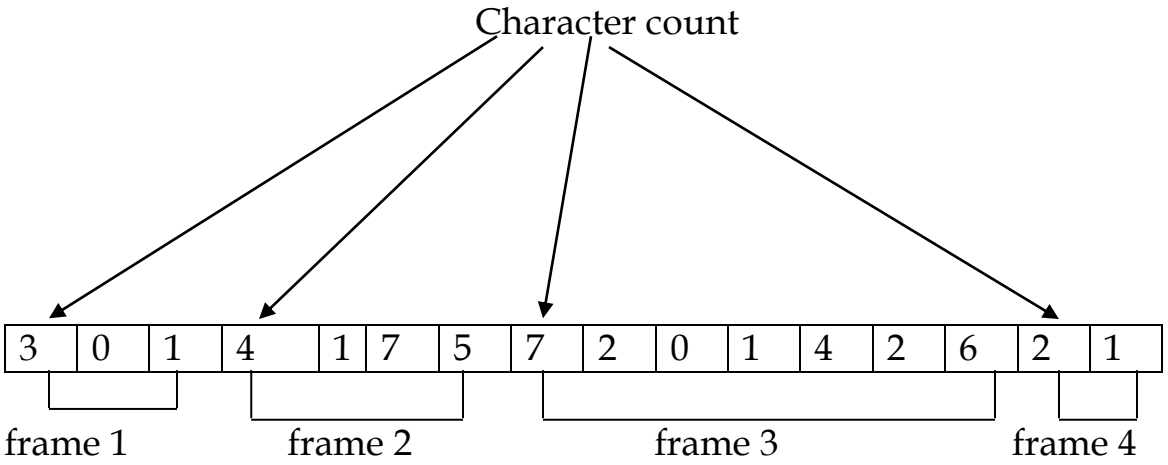
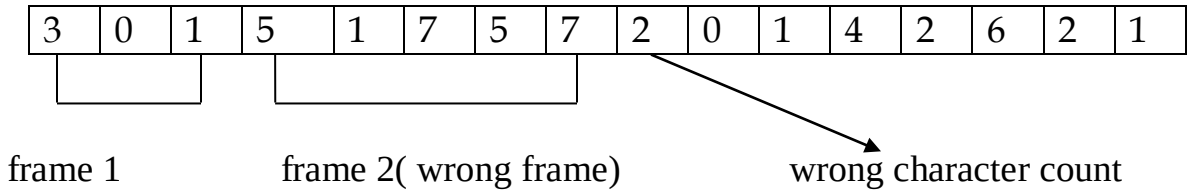


Fig : Character count method

The major problem with this method is that the character count can be changed due to an error during transmission. In such a situation destination will get out of synchronization and will not be able to identify the start of next frame.

As shown in fig 6.4, the character count of second frame is changed from 4 to 5 . As a result , all other succeeding frames are disturbed.



2. Starting & Ending characters with character Stuffing

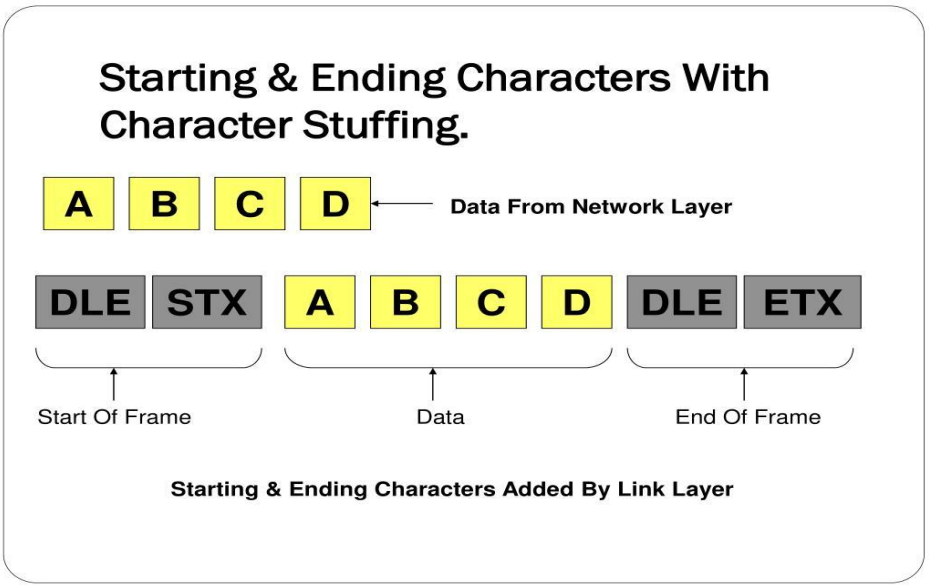
In this method, each frame starts & ends with a special character that mark the beginning & end of a frame.

Each frame begins with the ASCII character sequence DLE STX (Data link Escape start of text) and ends with ASCII character sequence DLE ETX (Data link escape end of text)

With these ASCII characters the problem of resynchronization after an error which was prominent is character count is solved .

Even if the destination loses the track of frame boundaries, the problem can be solved by just looking for DLE STX or DTE ETX to start with new frame.

This framing method is shown in fig.



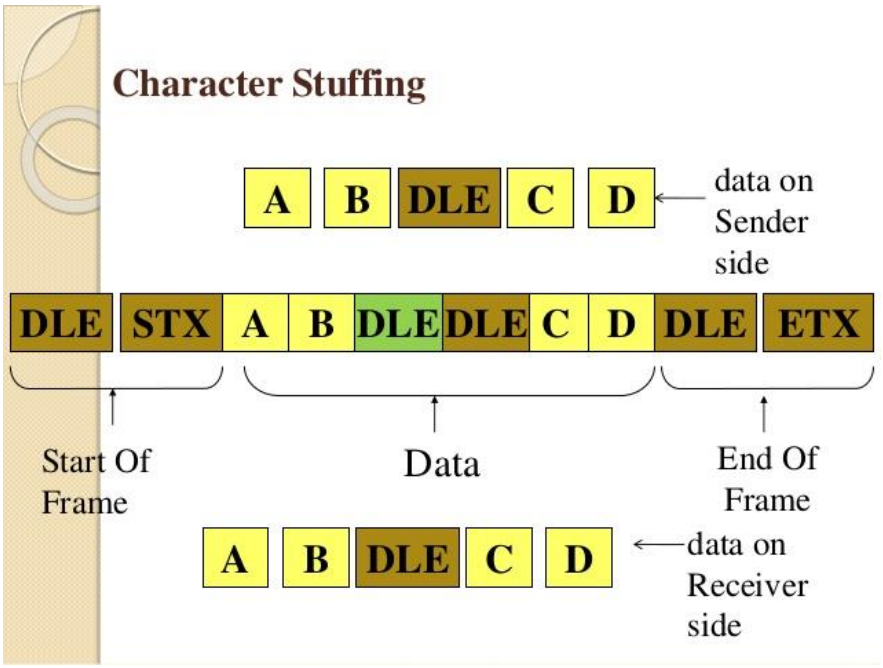
The major problem can arise in this method when DLE STX or DLE ETX occur as data. In this case these characters that are present as data may be misinterpreted as start or end of frame.

To handle this problem a technique called character stuffing is used. In character stuffing, the data link layer on sender side adds an ASCII DLE characters just before each DLE character in data. Now there are two DLE characters present in data.

ON receiver side, data link layer will remove this additional DLE character that was stuffed by sender's data link layer & will pass the data to network layer. This process of removing additional DLE is called destuffing.

Thus a framing DLE STX or DLE ETX is distinguished from one in the data by the presence or absence of a single Dle.

Therefore DLEs in data are always doubled as shown In fig.



3. Starting & ending flags with bit stuffing

In this method, each frame begins & ends with a special bit pattern 01111110

Therefore each frame starts with 01111110 & also ends with 01111110.

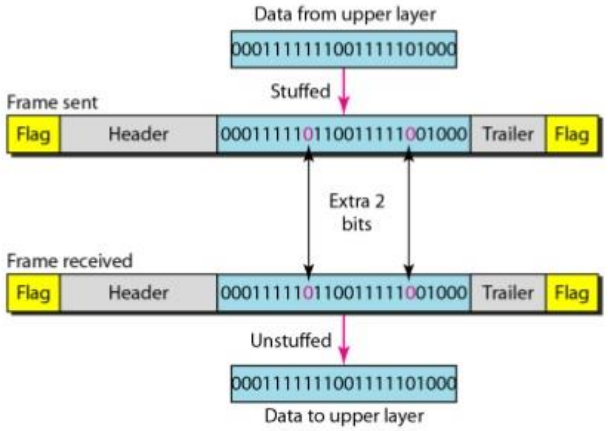
The main advantages of this method over the previous method is that it allows data frames with arbitrary number of bits and also allows character code with an arbitrary number of bits per character

The main problem arises in this method when the flag byte 01111110 appears as data.

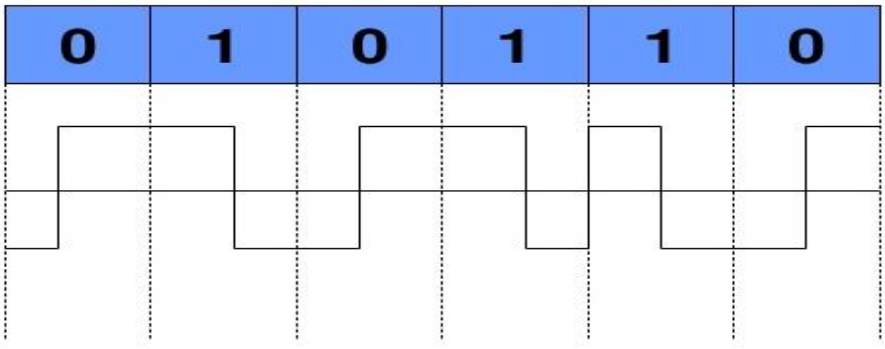
This problem is handled by a technique called bit stuffing that is similar to character stuffing.

Whenever the sender data link layer detects the presence of five consecutive ones in data, it automatically stuffs a 0 bit into outgoing bit stream. This is known as bit stuffing

When the receiver sees five consecutive ones in the bit stream, it automatically removes the 0 bit



4. Physical layer coding violation



Menchester Encoding

Some LANs encode each bit of data by using two physical bit i.e. Manchester coding is used

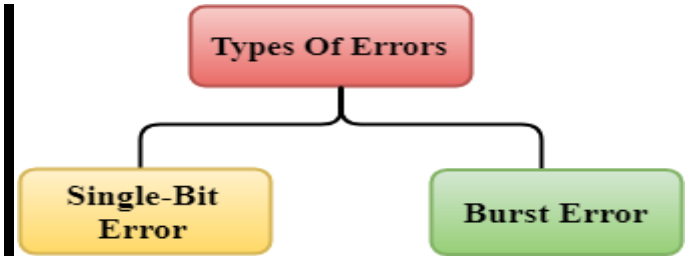
In this method bit 1 is encoded into high low (10) pair and bit 0 is encoded into low high (01) pair .

❖ Error Control

Error Detection

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

Types Of Errors

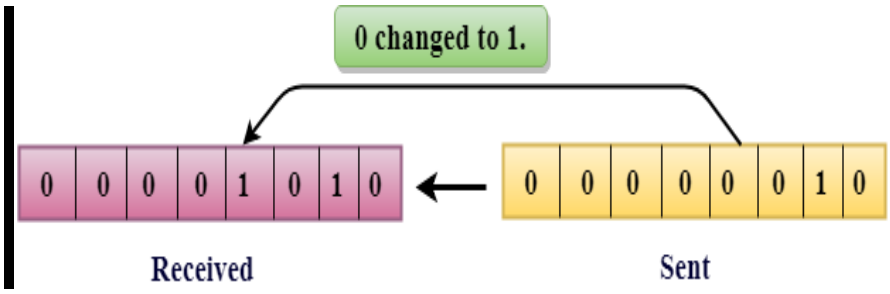


Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

Single-Bit Error:

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1.

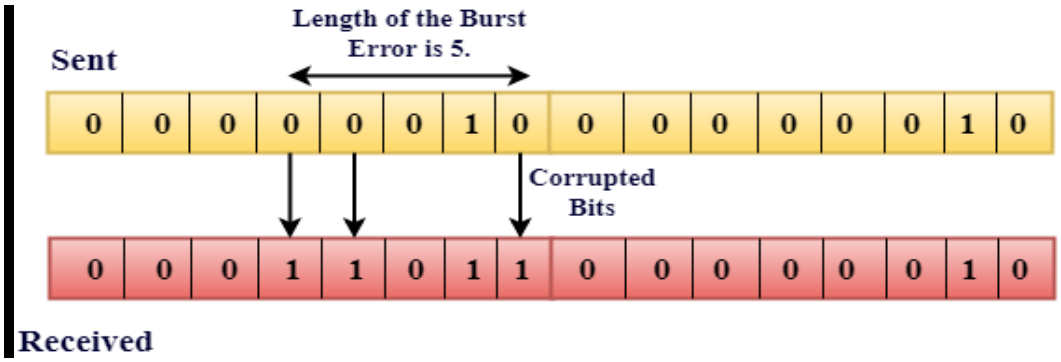
Single-Bit Error does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.

Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

Burst Error

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

The Burst Error is determined from the first corrupted bit to the last corrupted bit.



The duration of noise in Burst Error is more than the duration of noise in Single-Bit.

Burst Errors are most likely to occur in Serial Data Transmission.

The number of affected bits depends on the duration of the noise and data rate.

❖ Error Detecting Techniques:

The most popular Error Detecting Techniques are:

- Single parity check

- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

Single Parity Check

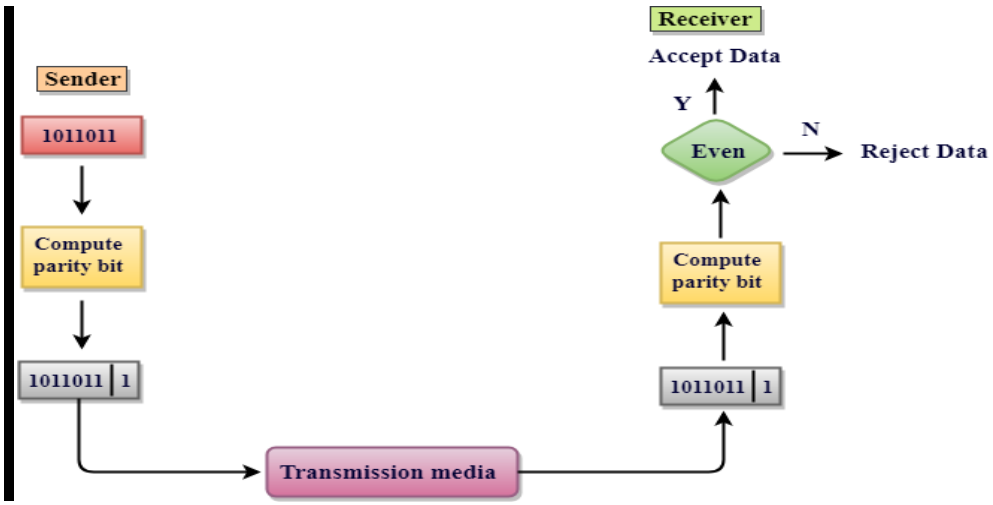
Single Parity checking is the simple mechanism and inexpensive to detect the errors.

In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.

If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.

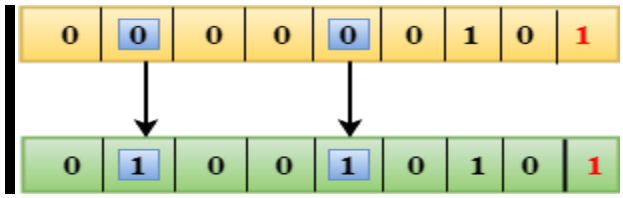
At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.

This technique generates the total number of 1s even, so it is known as even-parity checking.



Drawbacks Of Single Parity Checking

- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.



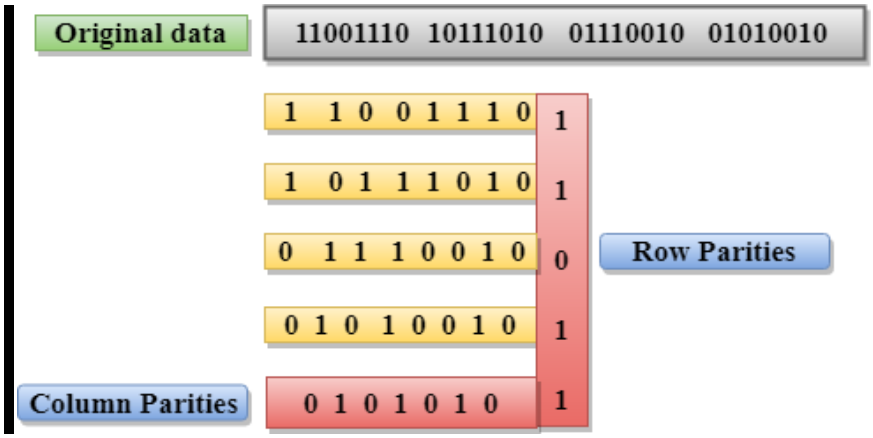
Two-Dimensional Parity Check

Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.

Parity check bits are computed for each row, which is equivalent to the single-parity check.

In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.

At the receiving end, the parity bits are compared with the parity bits computed from the received data.



Drawbacks Of 2D Parity Check

If two bits in one data unit are corrupted and two bits exactly the same position in another data unit is also corrupted, then 2D Parity checker will not be able to detect the error.

This technique cannot be used to detect the 4-bit errors or more in some cases.

Checksum

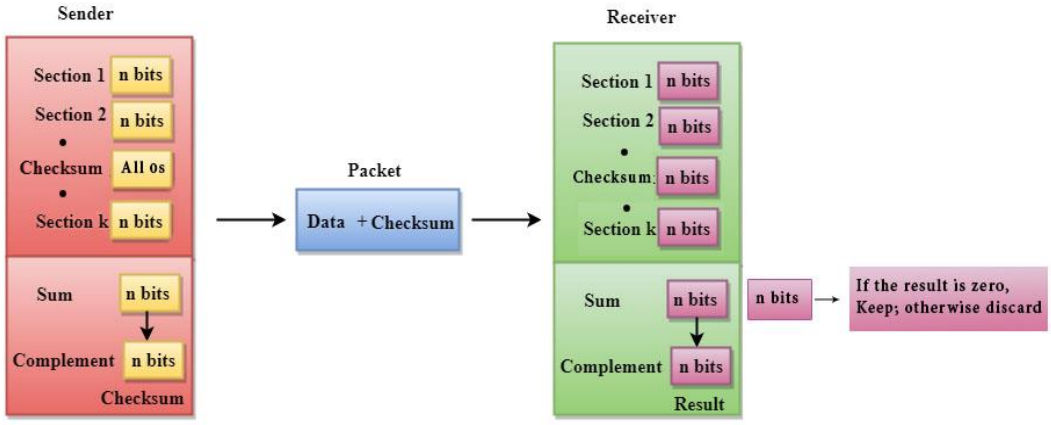
A Checksum is an error detection technique based on the concept of redundancy.

It is divided into two parts:

Checksum Generator

A Checksum is generated at the sending side. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network.

Suppose L is the total sum of the data segments, then the checksum would be ?L



The Sender follows the given steps:

- The block unit is divided into k sections, and each of n bits.
- All the k sections are added together by using one's complement to get the su m.
- The sum is complemented and it becomes the checksum field.
- The original data and checksum field are sent across the network.

Checksum Checker

A Checksum is verified at the receiving side. The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented. If the complement of the sum is zero, then the data is accepted otherwise data is rejected.

The Receiver follows the given steps:

- The block unit is divided into k sections and each of n bits.
- All the k sections are added together by using one's complement algorithm t o get the sum.
- The sum is complemented.
- If the result of the sum is zero, then the data is accepted otherwise the data is discarded.

Cyclic Redundancy Check (CRC)

CRC is a redundancy error technique used to determine the error.

Following are the steps used in CRC for error detection:

In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.

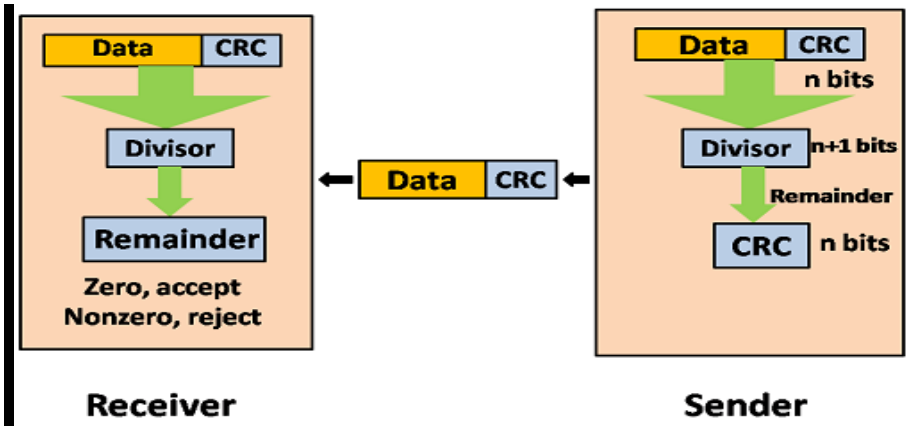
Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.

Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.

The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

If the resultant of this division is zero which means that it has no error, and the data is accepted.

If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.



Let's understand this concept through an example:

Suppose the original data is 11100 and divisor is 1001.

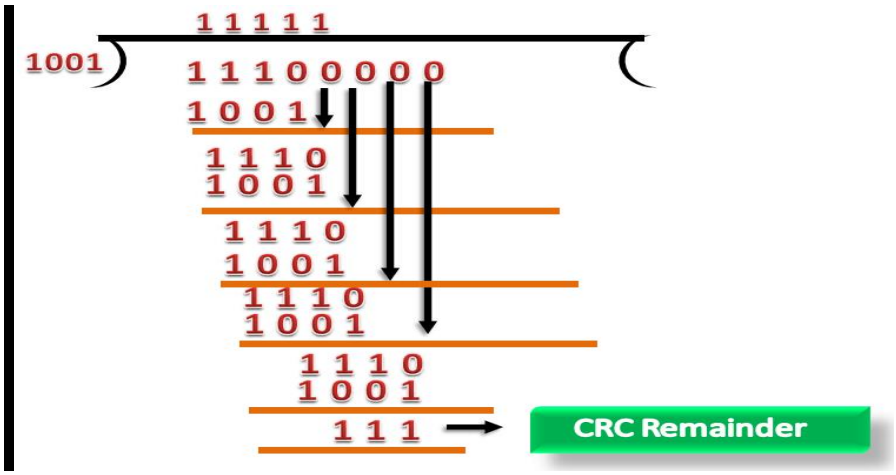
CRC Generator

A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.

Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.

The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.

CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.



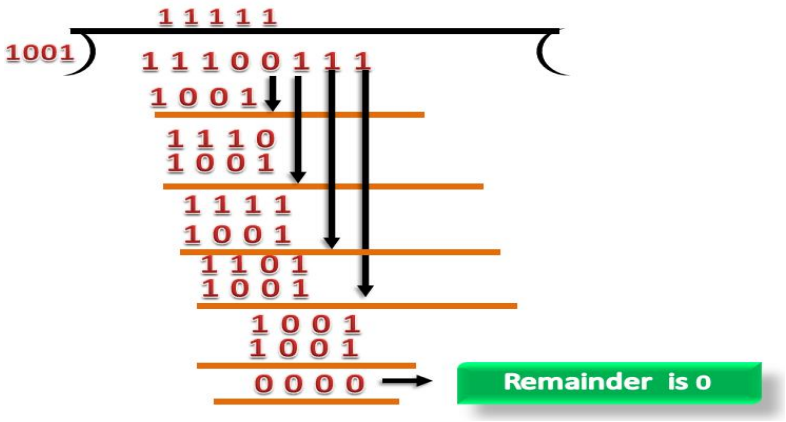
CRC Checker

The functionality of the CRC checker is similar to the CRC generator.

When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.

A string is divided by the same divisor, i.e., 1001.

In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted.



❖ Error Correction

Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.

Error Correction can be handled in two ways:

Backward error correction: Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.

Forward error correction: In this case, the receiver uses the error-correcting code which automatically corrects the errors.

A single additional bit can detect the error, but cannot correct it.

For correcting the errors, one has to know the exact position of the error. **For example,** If we want to calculate a single-bit error, the error correction code will determine which one of seven bits is in error. To achieve this, we have to add some additional redundant bits.

Suppose r is the number of redundant bits and d is the total number of the data bits. The number of redundant bits r can be calculated by using the formula:

$2^r >= d+r+1$

The value of r is calculated by using the above formula. For example, if the value of d is 4, then the possible smallest value that satisfies the above relation would be 3.

To determine the position of the bit which is in error, a technique developed by R.W Hamming is Hamming code which can be applied to any length of the data unit and uses the relationship between data units and redundant units.

Hamming Code

Parity bits: The bit which is appended to the original data of binary bits so that the total number of 1s is even or odd.

Even parity: To check for even parity, if the total number of 1s is even, then the value of the parity bit is 0. If the total number of 1s occurrences is odd, then the value of the parity bit is 1.

Odd Parity: To check for odd parity, if the total number of 1s is even, then the value of parity bit is 1. If the total number of 1s is odd, then the value of parity bit is 0.

Algorithm of Hamming code:

An information of 'd' bits are added to the redundant bits 'r' to form d+r.

The location of each of the (d+r) digits is assigned a decimal value.

The 'r' bits are placed in the positions 1,2,.....2^{k-1}.

At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determines the position of an error.

Relationship b/w Error position & binary number.

Error Position	Binary Number
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Let's understand the concept of Hamming code through an example:

Suppose the original data is 1010 which is to be sent.

Total number of data bits 'd' = 4

Number of redundant bits r : $2^r >= d+r+1$

$2^r >= 4+r+1$

Therefore, the value of r is 3 that satisfies the above relation.

Total number of bits = d+r = 4+3 = 7;

Determining the position of the redundant bits

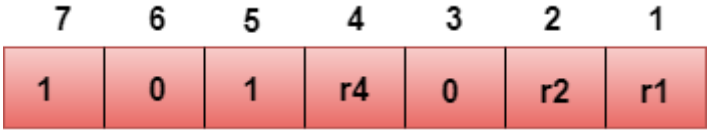
The number of redundant bits is 3. The three bits are represented by r1, r2, r4. The position of the redundant bits is calculated with corresponds to the raised power of 2. Therefore, their corresponding positions are **1, 2^1, 2^2**.

The position of r1 = 1

The position of r2 = 2

The position of r4 = 4

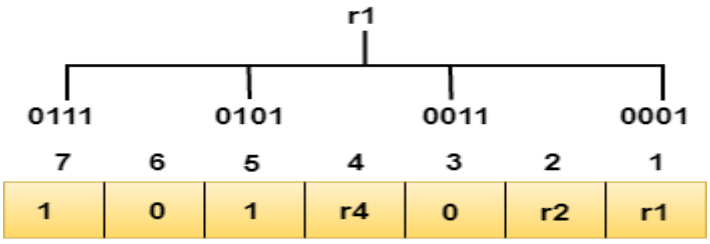
Representation of Data on the addition of parity bits:



Determining the Parity bits

Determining the r1 bit

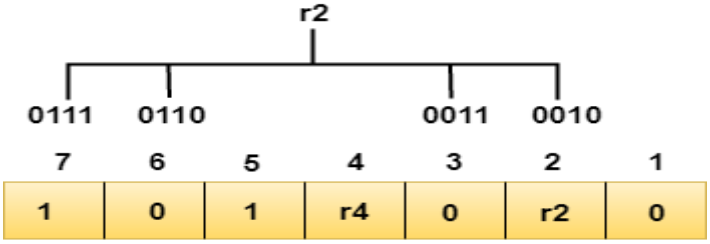
The r1 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the first position.



We observe from the above figure that the bit positions that includes 1 in the first position are 1, 3, 5, 7. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r1 is **even, therefore, the value of the r1 bit is 0**.

Determining r2 bit

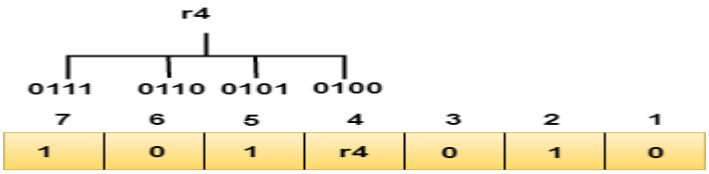
The r2 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the second position.



We observe from the above figure that the bit positions that includes 1 in the second position are **2, 3, 6, 7**. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r2 is **odd, therefore, the value of the r2 bit is 1**.

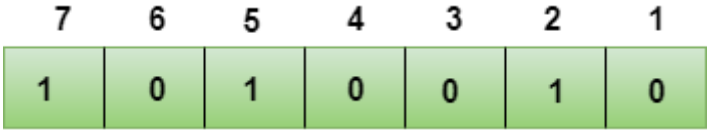
Determining r4 bit

The r4 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the third position.



We observe from the above figure that the bit positions that includes 1 in the third position are **4, 5, 6, 7**. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r4 is **even, therefore, the value of the r4 bit is 0**.

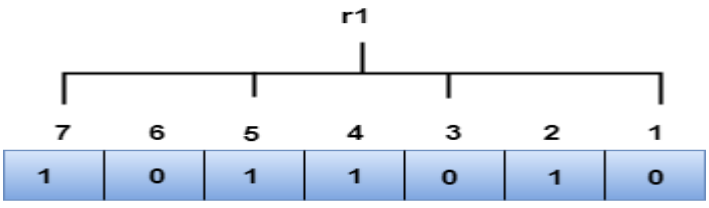
Data transferred is given below:



Suppose the 4th bit is changed from 0 to 1 at the receiving end, then parity bits are recalculated.

R1 bit

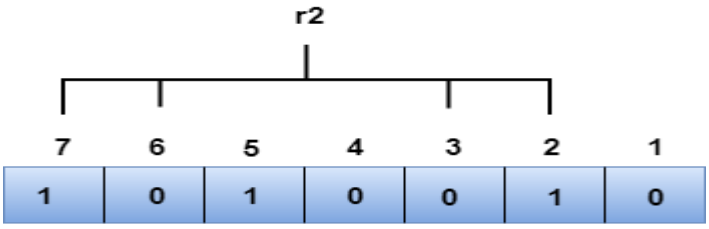
The bit positions of the r1 bit are 1,3,5,7



We observe from the above figure that the binary representation of r1 is 1100. Now, we perform the even-parity check, the total number of 1s appearing in the r1 bit is an even number. Therefore, the value of r1 is 0.

R2 bit

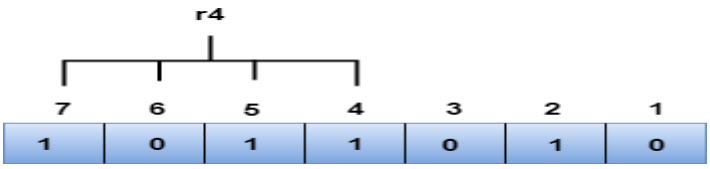
The bit positions of r2 bit are 2,3,6,7.



We observe from the above figure that the binary representation of r2 is 1001. Now, we perform the even-parity check, the total number of 1s appearing in the r2 bit is an even number. Therefore, the value of r2 is 0.

R4 bit

The bit positions of r4 bit are 4,5,6,7.



We observe from the above figure that the binary representation of r4 is 1011. Now, we perform the even-parity check, the total number of 1s appearing in the r4 bit is an odd number. Therefore, the value of r4 is 1

❖ Flow Control

It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.

The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.

It requires a buffer, a block of memory for storing the information until they are processed.

Two methods have been developed to control the flow of data:

- Stop-and-wait
- Sliding window

Stop-and-wait

- In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.
- When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop-and-wait

The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

Disadvantage of Stop-and-wait

Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link.

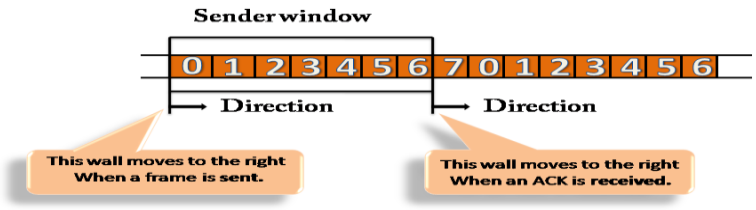
Sliding Window

- The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
- In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.
- A single ACK acknowledge multiple frames.
- Sliding Window refers to imaginary boxes at both the sender and receiver end.

- The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
- Frames can be acknowledged even when the window is not completely filled.
- The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1.....
- The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement.
- When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. **For example**, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

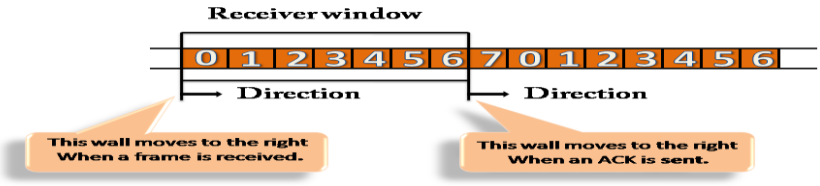
Sender Window

- At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.
- Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.
- **For example**, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2).



Receiver Window

- At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.
- When the new frame arrives, the size of the window shrinks.
- The receiver window does not represent the number of frames received, but it represents the number of frames that can be received before an ACK is sent**. For example**, the size of the window is w, if three frames are received then the number of spaces available in the window is (w-3).
- Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.
- Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1. In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two spaces before an acknowledgement is sent.



Data link layer in the internet (SLIP, PPP)

We know that internet consists of individual machines that are connected to each other. Basically it is wide area network that is built up from point to point leased lines.

In these point to point lines two major data link protocols are used –SLIP and PPP

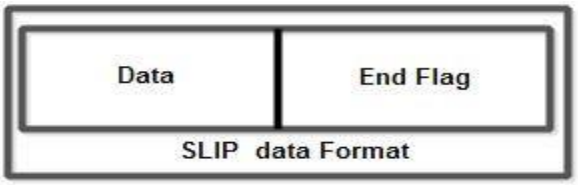
Today, millions of users access internet by connecting their home PCs to server of an internet service provider (ISP) that make use of PPP. Such users make use of modems and are connected to internet via telephone lines.

Sometimes the home PC just function as a character oriented terminals that log on to the ISPs time sharing system. Such a mode does not provide graphical Internet service such as www. users can only commands and run programs. This type of system is called shell account.

❖ SLIP(Serial line IP)

- This protocol was developed by Rick Adams in 1984.
- The initial purpose of this protocol was to connect sun workstation to the internet over a dial –up line using modem.
- Using this protocol, workstations ends raw IP packets over the line with a flag byte at the end for framing purpose.
- If the flag byte occurs inside the IP packet, then character stuffing technique is used to solve this problem.
- **Although SLIP is the simple protocol but it has some major problems. These are**
- It does not perform any error detection and correction.

- SLIP support only IP .(internet protocol).So it cannot be used for other networks that do not make use of IP.
- It does not support the allocation of dynamic IP address. Both the communication sites should be assigned a specific IP address before hand and both sites should know each other's address.
- SLIP does not provide any authentication. So both the communicating sites do not know with whom they are communicating.
- SLIP is not an approved internet standard, so many different and incompatible versions exist that makes networking difficult.
- A special END character marks the end of data.
- If an END character occurs naturally in data, SLIP includes a special ESC character before the END character so that receiving computer does not prematurely stop receiving the packet.



❖ PPP(Point –to-point protocol)

Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds. Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.

Services Provided by PPP

The main services provided by Point - to - Point Protocol are −

- Defining the frame format of the data to be transmitted.
- Defining the procedure of establishing link between two points and exchange of data.

- Stating the method of encapsulation of network layer data in the frame.
- Stating authentication rules of the communicating devices.
- Providing address for network communication.
- Providing connections over multiple links.
- Supporting a variety of network layer protocols by providing a range os services.

PPP Frame

PPP is a byte - oriented protocol where each field of the frame is composed of one or more bytes. The fields of a PPP frame are −

Flag − 1 byte that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.

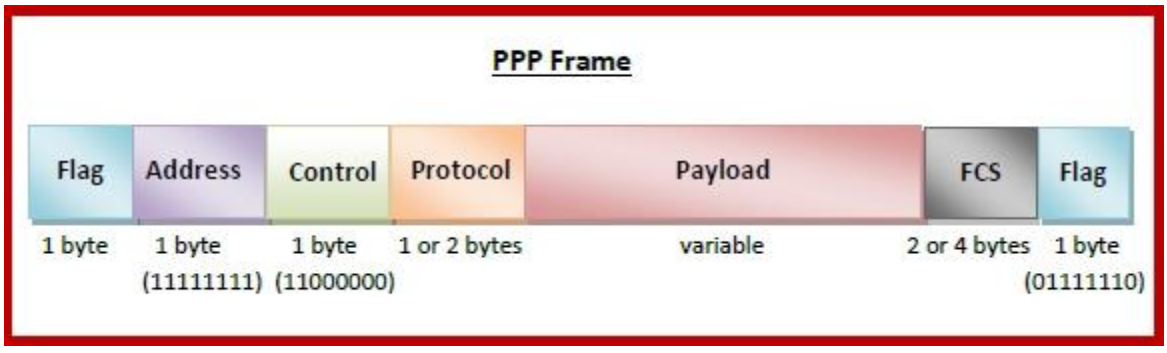
Address − 1 byte which is set to 11111111 in case of broadcast.

Control − 1 byte set to a constant value of 11000000.

Protocol − 1 or 2 bytes that define the type of data contained in the payload field.

Payload − This carries the data from the network layer. The maximum length of the payload field is 1500 bytes. However, this may be negotiated between the endpoints of communication.

FCS − It is a 2 byte or 4 bytes **frame check sequence** for error detection. The standard code used is CRC (cyclic redundancy code)



Byte Stuffing in PPP Frame − Byte stuffing is used is PPP payload field whenever the flag sequence appears in the message, so that the receiver does not consider it as the end of the frame. The escape byte, 01111101, is stuffed before

every byte that contains the same byte as the flag byte or the escape byte. The receiver on receiving the message removes the escape byte before passing it onto the network layer.

UNIT III

❖ MAC sub Layer

The medium access control (MAC) is a sub layer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

❖ CSMA/CD (Carrier sense multiple access with collision Detection)

- CSMA/CD is a protocol in which the station senses the carrier or channel before transmitting frame just as in persistent and non-persistent CSMA. If the channel is busy, the station waits.
- Additional feature in CSMA/CD is that the stations can detect the collisions. The stations abort their transmission as soon as they detect a collision. In CSMA this feature is not present. The stations continued their transmission even thought they find that the collision has occurred. This leads to the wastage of channel time.
- However this problem is handled in CSMA/CD. In CSMA/CD, the station that places its data onto the channel after sensing the channel, continues to sense the channel even after the data transmission and waits for predetermined amount of time & then sends its data again.
- As soon as a collision is detected, the transmitting station releases a jam signal.
- Jam signal will alert the other stations. The stations are not supposed to transmit immediately after the collision has occurred. Otherwise there is a possibility that the same frames would collide again.
- After some back off delay time the stations will retry the transmission. If the collision occurs again then the back off delay time is increased progressively.
- Therefore the CSMA/CD method consists of alternating transmission period and collisions with idle periods when none of the stations is transmitting.

- **For example**, in a hub network, two devices can send packets at the same time. This can cause a collision.

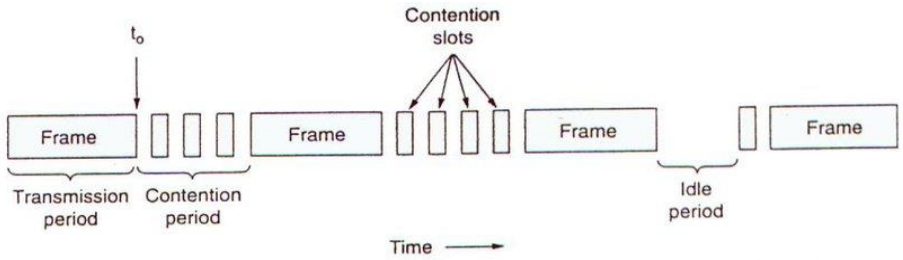
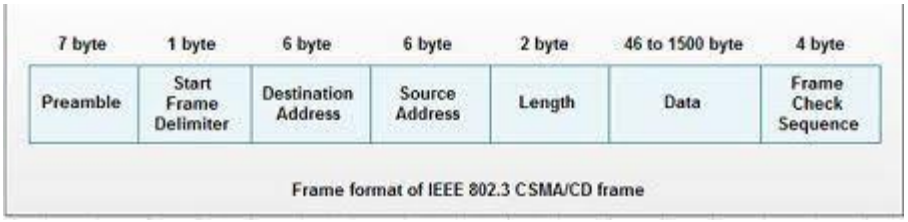


Fig. 4-5. CSMA/CD can be in one of three states: contention, transmission, or idle.

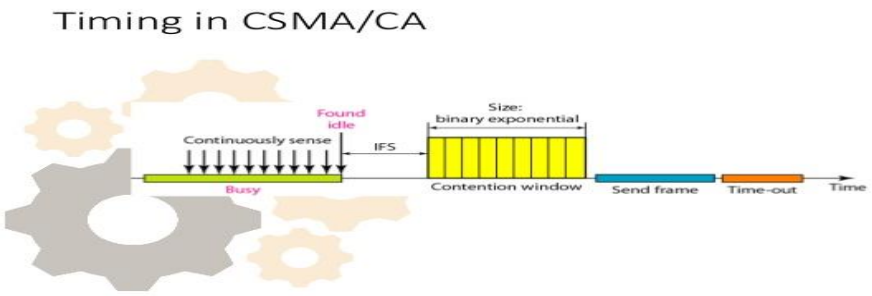
Frame Format of CSMA/CD



1. **Preamble:** - It is seven bytes (56bits) that provides bit synchronization. It consists of alternating 0s and 1s . The purpose is to provide alert and timing pulse.
2. **Start frame delimiter (SFD)** :- It is one byte field with unique pattern: 10101011. It marks the beginning of frame.
3. **Destination Address**: - It is six byte field that contains physical address of packet's destination.
4. **Source Address**:- It is also a six byte field and contains the physical address of source or last device to forward the packet .
5. **Length:**- This two byte field specifies the length or number of bytes in data field.
6. **Data:** - It can be of 46 t0 1500 bytes, depending upon the type of frame and the length of the information field.
7. **Frame check sequence**: - This for byte field contains CRC for error detection.

❖ CSMA/CA (Carrier sense multiple Access with Collision Avoidance)

- CSMA/CA protocol is used in wireless networks because they cannot detect the collision so the only solution is collision avoidance.
- CSMA/CA avoids the collisions using three basic techniques
    1. Interframe space
    2. Contention window
    3. Acknowledgments



1. Interframe Space (IFS)

- Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called interframe space(IFS)
- When channel is sensed to be idle, it may be possible that same distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.
- Therefore the purpose of IFS time is to allow this transmitted signal to reach other stations.
- If after this IFS time, the channel is still idle, the station can send, but it still needs to wait a time equal to contention time.
- IFS variable can also be used to define the priority of a station or a frame.

2. Contention Window

- Contention window is an amount of time divided into slots.
- A station that is ready to send choses a random number of slots as its wait time.
- The number of slots in the window changes according to the binary exponential back off strategy. It means that it is of one slot the first

time and then doubles each time the station cannot detect an idle channel after the IFS time.

- This is very similar to the p- persistent method except that a random outcome defines the number of slot taken by the waiting station.
- In contention window the station needs to sense the channel after each time slot.
- If the station finds the channel busy, it does not restart the process. It just stops the timer & restarts it when the channel is sensed as idle.

3. Acknowledgment

- Despite all the precautions , collisions may occur and destroy the data.
- The positive acknowledgment and the time out timer can help guarantee that receiver has received the frame.

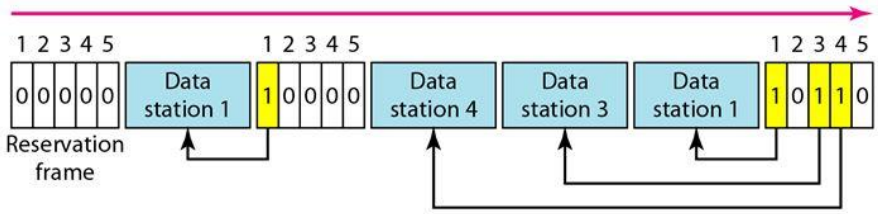
4. Controlled Access Protocol

- In this method, the station consult each other to find which station has a right to send.
- A station cannot send unless it has been authorized by other stations.
- The different controlled access methods are:
  a) Reservation
  b) Polling
  c) Token Passing

1. Reservation

- In reservation method, a station needs to make a reservation before sending data.
- The time is divided into intervals. In each interval, a reservation frame preceeds the data frames sent in that interval.
- If there are N stations in the system, there are exactly N reservation mini slots in the reservation frame.
- Each mini slot belongs to a station.
- When a station needs to send a data frame, it make a reservation in its own mini slot.
- The stations that have made reservations can send their data frame after the reservation frame.

- Fig shows a situation with five stations and a reservation frame with five mini slots.
- In the first interval, only stations 1,3 and 4 have made reservations. In second interval only sation 1 has made a reservation.



2. Polling

- Polling method work in those networks where primary and secondary stations exit.
- All data exchanges are made through primary device even when the final destination is a secondary device.
- Primary device controls the link and secondary device follows the instruction.
- Polling method has two different modes, Poll & select.

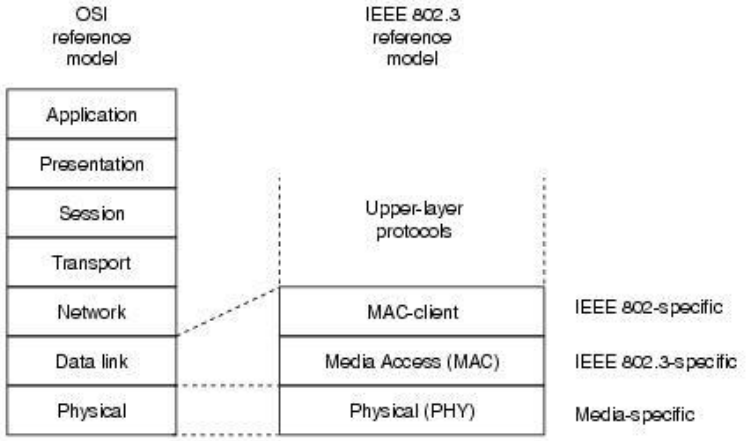
3. Token passing

- Token passing method is used in those networks where the stations are organized in a logical ring.
- In ring, network, each station has a predecessor and a successor
- In such networks , a special packet called token is circulated through the ring
- Station that possesses the token has the right to access the channel and transmit its data
- Wherever any station has some data to sent, it waits for the token. It transmits data only after it get the possession of the token.
- After transmitting the data, the station releases the token and passes it to the next station in the ring.

❖ IEEE Standards

- The Institution of Electrical Engineers (IEEE) has developed several standards for LAN's. These standards are collectively known as IEEE 802 or Project 802.

- The various standards differ at the physical layer and MAC sub layer but are compatible at the data link layer.
- The IEEE project 802 divides data link layer into two sublayers: logical link control (LLC) and medium access control (MAC) .



Logical Link Control (LLC)

- The data link layer performs framing, flow control and error control
- In IEEE project 802 , flow control, error control and part of framing duties are performed by logical link control. Framing is performed both LLC and MAC sublayers.
- LLC provides one single data link control protocol for all IEEE LANs
- This single LLC protocol can provided interconnectivity between different LANs as it makes the MAC sublayer transparent. On the other hand MAC provides different protocols for the different LANs
- LLC thus provide flow control and error control for the upper layer protocols.

Medium Access Control (MAC)

- MAC sublayer of IEEE project 802 defines the specific access methods for each LAN. **For Example**, it defines CSM/CD as the media access method for Ethernet LANs and token passing method for token ring and token Bus LANs.

The various IEEE 802 Standards are:

- 802.1 Network management and Internetworking
- 802.2 Logical Link Control
- 802.3 Ethernet or CSMA/CD
- 802.4 Token bus
- 802.5 Token Ring
- 802.6 Metropolitan Area networks or Distributed Queue Dual Bus
- 802.7 Band Pass technical Advisory Group
- 802.8 Fiber Optic Technical Advisory Group
- 802.9 Integrated data and voice network
- 802.10 Security working group
- 802.11 Wireless LAN

❖ IEEE 802.3: Ethernet

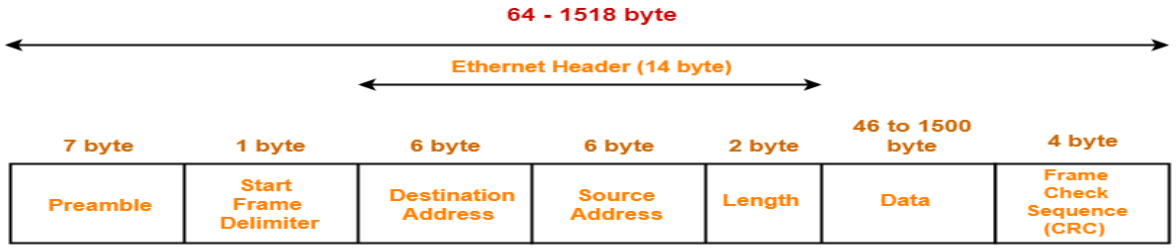
- Ethernet is a multi-access network in which set of nodes share a common link.
- IEEE 802.3 standard is for a 1- persistent CSMA/CD LAN. Whenever a station wants to transmit, it senses the carrier to determine the channel is idle or busy. The stations can detect the collision i.e whenever two or more stations transmit simultaneously and their frames collide, the stations abort their transmissions.
- The Ethernet was originally created in 1976 at Xerox's Palo Alto Research center (PARC). The Xerox Ethernet was so successful that Xerox, DEC, and Intel created a standard for a 10 mbps Ethernet. This standard formed the basis for 802.3.
- The standard Ethernet was improved to create new implementations with better performance and speed. Therefore several different Ethernet were created These are:
  a) Standard Ethernet (10 mbps)
  b) Fast Ethernet (100 mbps)
  c) Gigabit Ethernet (1 gbps)
  d) Ten- gigabit Ethernet (10 Gbps)

a) Standard Ethernet

In standard Ethernet , the MAC sublayer governs the operation of access method. If frames the data received from the upper layer and passes them to the physical layer.

MAC sublayer Functions

The various fields of traditional Ethernet are



IEEE 802.3 Ethernet Frame Format

- **Preamble**: It is seven bytes field of alternating 0s and 1s that provides bit synchronization.
- **Start Frame Delimiter (SFD)** : This one byte field contains bit pattern 10101011 that warns the station that this is the last chance for synchronization.
- **Destination Address (DA)** : It is 6 bytes field and contains the physical address of the destination station.
- **Source Address (SA)** : It is also a 6 bytes field & contains the physical address of the sender of packet.
- **Length :** This field tells how many bytes are present in the data field
- **Data:** It contains 46 to 1500 bytes of data.
- **CRC**: This 4 bytes field contains error detection information.

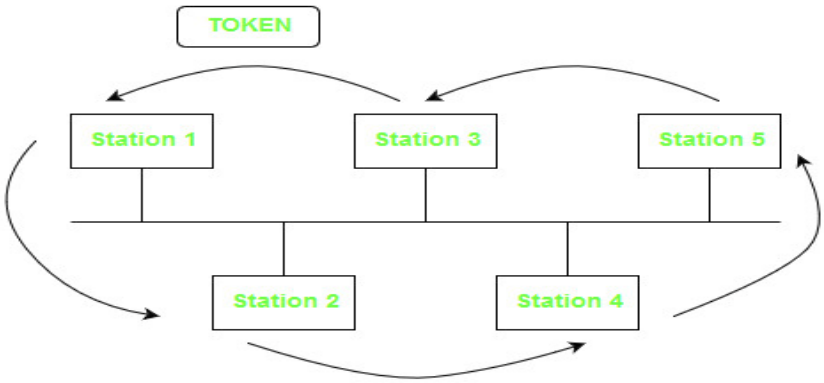
❖ Gigabit Ethernet

- Gigabit Ethernet provides the data rate of 1 GBPS or 1000 Mbps.
- IEEE created Gibabit Ethernet under the name 802.3z.
- It is compatible with standard or East Ethernet.
- It also uses similarly 48 bit hexadecimal addressing scheme.
- The frame format is also similar to standard Ethernet.

- It operates in both half duplex and full duplex mode.
- In half duplex mode, CSMA/CD access method is used whereas in full duplex mode CSMA/CD is not required.

❖ IEEE 802.4: Token Bus

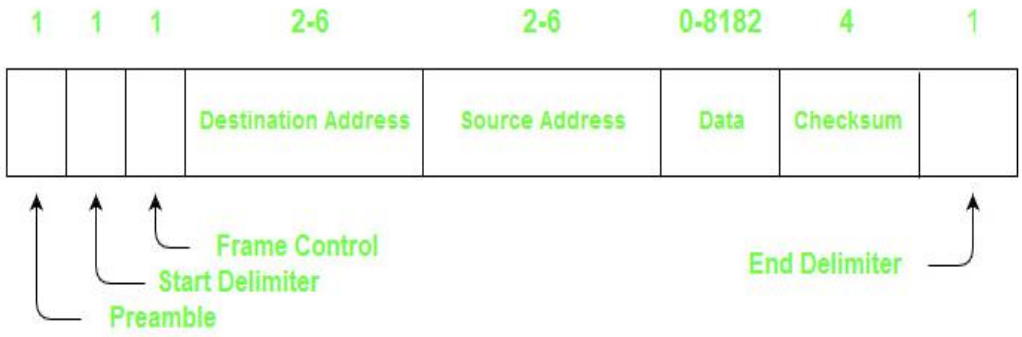
- IEEE 802.4 standard for media access control is known as token bus.
- Physically, the token bus is a linear or tree shape cable to which the stations are attached.



- Each station knows the address of the station to its left and right i.e address of the preceding station and the station.
- When the logical ring is initialized, the highest numbered station may send the first frame.
- After doing so, it passes the permission to its immediate neighbor by sending a special control frame to it. This control frame is called a token.
- In such a way, a token circulates round logical ring, and only the station holding a token is allowed to transmit data.
- In such a case, there is no collision as only one station possesses a token at any given time.
- In token bus, each station receives each frame, the station whose address is specified in the frame processes it and the other stations discard the frame.
- When a station passes the token, it sends a token to its logical neighbor irrespective of where that station is physically located on the cable.

Frame Format:

The various fields of the frame format are:

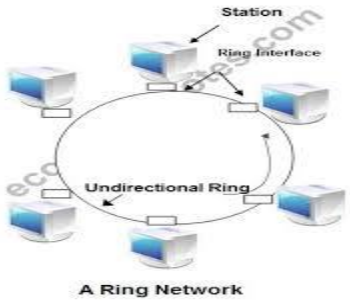


1. **Preamble –** It is used for bit synchronization. It is 1 byte field.
2. **Start Delimiter –** These bits marks the beginning of frame. It is 1 byte field.
3. **Frame Control –** This field specifies the type of frame – data frame and control frames. It is 1 byte field.
4. **Destination Address –** This field contains the destination address. It is 2 to 6 bytes field.
5. **Source Address –** This field contains the source address. It is 2 to 6 bytes field.
6. **Data –** If 2 byte addresses are used than the field may be upto 8182 bytes and 8174 bytes in case of 6 byte addresses.
7. **Checksum –** This field contains the checksum bits which are used to detect errors in the transmitted data. It is 4 bytes field.
8. **End Delimiter –** This field marks the end of frame. It is 1 byte field.

❖ IEEE 802.5: Token Ring

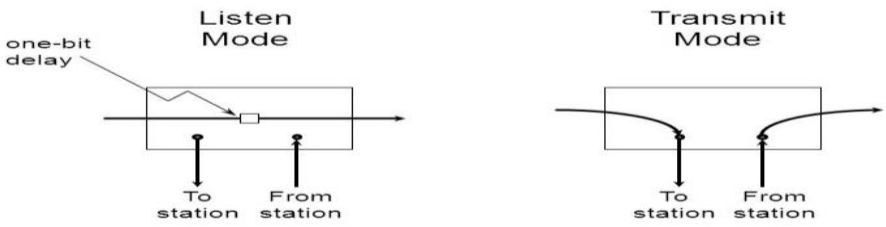
- IEEE 802.5 standard is known as token ring.
- A ring consist of a collection of ring interface connected by point to point lines i.e. ring interface of one station is connected to the ring interface of its left station as well as right station.
- These point to point link can be created with twisted pair, coaxial cable or fiber optics.
- Each bit arriving at an interface is copied into a 1 bit buffer.
- In this buffer the bit is checked and may be modified and is then copied out to the ring again.
- This copying of bit in the buffer introduces a 1 bit delay at each interface.

- In ring networking a token is circulated around the ring. A token is a special bit pattern
- There is only one token in the network
- In order to transmit data, a station has to seize the token and remove it form the ring.
- The token is seized by changing only one bit in the token. Whenever the station transmit data it adds into token to the first three bytes of beginning of the data frame.
- Since only one station can possess the token and transmit data at any given time, there is no collision.



A Ring Network

- There are two operating modes of ring interfaces. There are listen and transmit.
- In **listen mode**, the input bits are simply copied to output with a delay of 1-bit time.
- In **transmit mode** the connection between input and outputs is broken by the interface so that is can insert its own data. The station comes in transmit mode when it captures the token
- The frames are acknowledged by the destination in a very simple manner. The sender sends frames to receiver with ACK bit 0. The receiver on receiving frames, copies data into its buffer, verifies the checksum and set the ACK bit to 1.
- The verified frames come back to sender, where they are removed from the ring.



- After this transmission , sender creates a new token and places it on the ring.
- When there is no traffic on the network, the token keeps on circulating in the ring unless some station captures it by turning the value of bit to 1 from 0.
- A station can hold a token for a specific duration of time. During this time, it has to complete its transmission and regenerates the token in ring.
- Under light load, token circulates in ring while under heavy load, queues of data to send are built up on nodes.
- Whenever a station finishes its transmission, the other station grabs the token and starts its own transmission.

Comparison of IEEE 802.3, 802.4 and 802.5 standard

S.NO.	IEEE 802.3	IEEE 802.4	IEEE 802.5
1.	Topology used in IEEE 802.3 is Bus Topology.	Topology used in IEEE 802.4 is Bus or Tree Topology.	Topology used in IEEE 802.5 is Ring Topology.
2.	Size of the frame format in IEEE 802.3 standard is 1572 bytes.	Size of the frame format in IEEE 802.4 standard is 8202 bytes.	Frame format in IEEE 802.5 standard is of the variable size.

S.NO.	IEEE 802.3	IEEE 802.4	IEEE 802.5
3.	There is no priority given in this standard.	It supports priorities to stations.	In IEEE 802.5 priorities are possible
4.	Size of the data field is 0 to 1500 bytes.	Size of the data field is 0 to 8182 bytes.	No limit is of the size of the data field.
5.	Minimum frame required is 64 bytes.	It can handle short minimum frames.	It supports both short and large frames.
6.	Efficiency decreases when speed increases and throughput is affected by the collision.	Throughput & efficiency at very high loads are outstanding.	Throughput & efficiency at very high loads are outstanding.
7.	Modems are not required.	Modems are required in this standard.	Like IEEE 802.4, modems are also required in it.

S.NO.	IEEE 802.3	IEEE 802.4	IEEE 802.5
8.	Protocol is very simple.	Protocol is extremely complex.	Protocol is moderately complex.
9.	It is not applicable on Real time applications, interactive Applications and Client-Server applications.	It is applicable to Real time traffic.	It can be applied for Real time applications and interactive applications because there is no limitation on the size of data.

❖ Network Layer Design Issues

Services provided to transport layer

- The network layer services to transport layer at network layer/ transport layer interface.
- The network layer services are designed to provide following goals:

a) The services should be independent of the subnet technology.

b) The transport layer should be shielded from the number, type and topology of the subnets present

c) The network addresses available to transport layer should use a uniform numbering plan even across LANs and WANs.

The network layer can provide two different types of services.

a) Reliable connection oriented
b) Unreliable Connectionless.

- **In reliable connection oriented** services user is given reliable end to end connection. For e.g. ATM networks has connection oriented network layer.
  1) Before sending data, a network layer on the sender side setup a connection to its peer on the receiving side. Each connection is given a specific identifier.
  2) After setting up a connection , the two processes can either into negotiation about the parameters, quality and cost of service to be provided.
  3) The various packet are delivered in specific order i.e. according to the sequence number.
  4) Communication is full duplex
  5) Flow control is automatically provided
- **In unreliable Connectionless** services , no connection is established before the data transfer. The user simply bundles up his information together, puts an address on it and then sends it off. It does not offer any guarantee of data delivery. **For example**: the internet has a connectionless network layer.

Internal Organization of the network layer

- The subnets are organized by using two different approaches connection oriented and connectionless.
- In connection oriented services , a connection is established before any data transfer take place. This connection is known as virtual circuit.
- In connectionless services, the individual packets are called datagram.

Virtual Circuit Approach

- In virtual circuit approach, a route form source to destination is chosen.
- The route is chosen during the connection establishment phase.
- This route is used for all the traffic flowing over the connection i.e. every packet form source to destination will follow this route only

- When the data transfer is over, the connection is released and the virtual circuit is also terminated
- In virtual circuit subnet, each packet contains short virtual circuit number, sequence number, checksum in its header.
- If packets flowing over a given virtual circuit always take the same route through subnet, each router must remember where to forward packets for each of the currently open virtual circuits passing through it.

The various Advantages of virtual circuit approach are :

- Each packet contains only VC number and not full destination address. This reduces significant amount of overhead and a lot of bandwidth is saved.
- Virtual circuit approaches provides congestion control within the subnet as enough buffers can be reserved in advance for each virtual circuit, when the connection is established.
- In VC approach address parsing is easy and does not consume much time as each router just uses the circuit number t index into a table to find out where the packet should go.

Disadvantages of Virtual circuit are:

- The set up phase of virtual circuit approach takes a lot of time and also consumers various recourses.
- Virtual circuit requires a lot of table space within routers, so large amount of router memory is used up by VC table.
- If any router crashes, all the virtual circuits that passed through the failed router are terminated.

Datagram Approach

- In datagram approach, no routers are established form source to destination before data transfer.
- Each packet is routed independently.
- The different packets of same message may follow different router form source to destination.

- In datagram subnet no circuit is established before data transfer or released afterward.
- Datagram subnets are more robust and adapt to failures and congestion more easily than virtual circuit subnets.
- Each datagram must contain the full source and destination address. For large networks, these addresses can be quite long.
- In datagram approach, the routers do not have a table with one entry for each open virtual circuit. rather ,the tables on these routers provide information about the outgoing line to be used for each possible information about the outgoing line to be used for each possible destination router.

Advantages of Datagram Approaches

- Tables on routers consume less memory space as they need not to include virtual circuit information
- Establishment and release of networks or transport layer connection do not require any special work on the part of routers.
- If any datagram router crashes or fails, only those users will suffer whose packets are queued up in the router at that time. Therefore crash of one router does not effect entire system

Disadvantages of datagram Approach

- Every packet has to include full address of source and destination that leads to a significant amount of overhead. As a result of this a lot of bandwidth is wasted.
- The address parsing is difficult as more complicated procedure is required to determine the path of the packet.
- With a datagram approach , congestion avoidance is more difficult

❖ Routing Algorithm

- One of the important functions of network layer is routing the packets form source machine to the destination machine.
- To perform this routing, network layer defines several different algorithms.

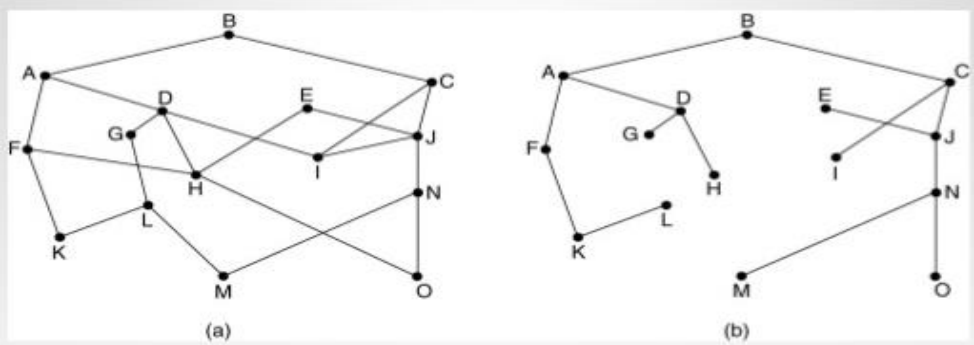
- These routing algorithms play a vital role in network and are used to define routes for packets.
- A routing algorithm is a part of network layer software that decides to which output line an incoming packet should be transmitted.
- If subnet uses a datagram approach , then the choice of route has to be made for each incoming packet.
- If the subnet uses virtual circuit approach, then the decision has to be taken for every virtual circuit.
- A routing algorithm should possess some desirable properties like correctness, simplicity, robustness, stability, fairness and optimality.

1. **Correctness:** - The routing should be done properly and correctly so that the packets may reach their proper destination.
2. **Simplicity:** - The routing should be done in a simple manner so that the overhead is as low as possible. With increasing complexity of the routing algorithms the overhead also increases.
3. **Stability:** - The routing algorithm should be stable under all circumstances.
4. **Fairness:-** Every node connected to the network should get a fair chance of transmitting their packets. This is usually done on FCFS basis.
5. **Robustness:-** Once a network becomes operational ,it may be expected to run continuously for years without any failures. The algorithm designed for routing should be robust enough to handle hardware and software failure and should be able to cope with changes in the topology and traffic without requiring all jobs in all hosts to be aborted and the network rebooted every time some router goes down.
6. **Optimality:-** The routing algorithm should be optimal in terms of though put and minimizing mean packet delays.

❖ Optimality Principle

- The general statement about optimal routes without regard to network topology or traffic is known as optimality principle.
- It states that if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.

- This can be elaborated as, call the part of the route from I to J as r1 and the rest of the route as r2. If a route better than r2 existed form J to K, it could be concatenated with r1 to improve the route form I to K, contradicting our statement that r1 r2 is optimal.
- As a direct consequence of the optimality principle, we can see that the set of optimal routes from all source to a given destination from a tree rooted at the destination.



(A) A SUBNET. (B) A SINK TREE FOR ROUTER B.

- Sink tree is not necessarily unique. Other trees with the same path lengths may exist.
- All the routing algorithms are supposed to discover and use the sink trees for all routers.

❖ Shortest Path Routing

- In shortest path routing algorithm, a graph of the subnet is created.
- In this graph, each node represents the router and each are represents a link or communication line.
- In order to select the shortest path from a sender to receiver , the algorithm finds the shortest path between then on the graph.
- Several different metrics can be used to find out the shortest path between the router.
- One way of measuring path length is the number of hops i.e. this approach counts the number of intermediate routers that are lying in the path from sender to receiver.

- Other way is to find the total length of physical channel between a pair of routers.
- Various other metrics are also possible such as mean queuing and transmission delay. In this case, the path taking shortest time to deliver the packets from one router to the other may be chosen i.e. fastest path is the shortest path rather than the path with the fewest arcs or kilometers.
- The labels on the arcs can be computed as a function of the distance, bandwidth, average traffic, communication cost, mean queue length, measured delay etc.
- The algorithm weights various parameters and computer the shortest path based on any one or combination of criterions stated above.

Dijkstra's Algorithm

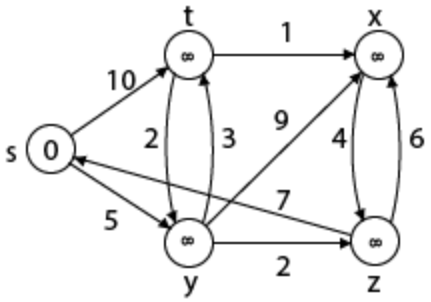
It is a greedy algorithm that solves the single-source shortest path problem for a directed graph G = (V, E) with nonnegative edge weights, i.e., w (u, v) ≥ 0 for each edge (u, v) ∈ E.

Dijkstra's Algorithm maintains a set S of vertices whose final shortest - path weights from the source s have already been determined. That's for all vertices v ∈ S; we have d [v] = δ (s, v). The algorithm repeatedly selects the vertex u ∈ V - S with the minimum shortest - path estimate, inserts u into S and relaxes all edges leaving u.

Because it always chooses the "lightest" or "closest" vertex in V - S to insert into set S, it is called as the **greedy strategy**.

Analysis: The running time of Dijkstra's algorithm on a graph with edges E and vertices V can be expressed as a function of |E| and |V| using the Big - O notation. The simplest implementation of the Dijkstra's algorithm stores vertices of set Q in an ordinary linked list or array, and operation Extract - Min (Q) is simply a linear search through all vertices in Q. In this case, the running time is O $(|V^2|+|E|=O(V^2)$.

Example:



Solution:

Step1: Q =[s, t, x, y, z]

We scanned vertices one by one and find out its adjacent. Calculate the distance of each adjacent to the source vertices.

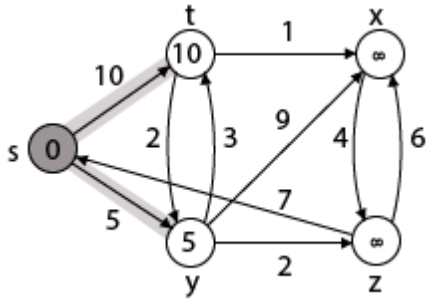
We make a stack, which contains those vertices which are selected after computation of shortest distance.

Firstly we take's' in stack M (which is a source)

1. M = [S] Q = [t, x, y, z]

Step 2: Now find the adjacent of s that are t and y.

1. Adj [s] → t, y [Here s is u and t and y are v]



Case - (i) s → t

d [v] > d [u] + w [u, v]

d [t] > d [s] + w [s, t]

∞ > 0 + 10 [false condition]

Then **d [t] ← 10**

π [t] ← 5

Adj [s] ← t, y

Case - (ii) s→ y

d [v] > d [u] + w [u, v]

d [y] > d [s] + w [s, y]

∞ > 0 + 5 [false condition]

∞ > 5

Then **d [y] ← 5**

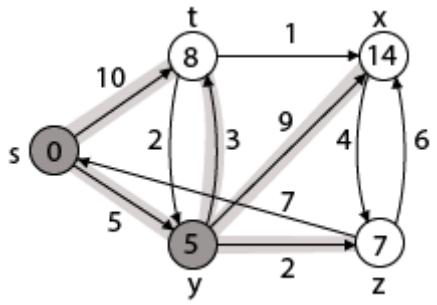
π [y] ← 5

By comparing case (i) and case (ii)

Adj [s] → t = 10, y = 5

y is shortest

y is assigned in 5 = [s, y]



Step 3: Now find the adjacent of y that is t, x, z.

1. Adj [y] → t, x, z [Here y is u and t, x, z are v]

Case - (i) y →t

d [v] > d [u] + w [u, v]

d [t] > d [y] + w [y, t]

10 > 5 + 3

10 > 8

Then d [t] ← 8

π [t] ← y

Case - (ii) y → x

d [v] > d [u] + w [u, v]

d [x] > d [y] + w [y, x]

∞ > 5 + 9

$\infty > 14$

Then $d[x] \leftarrow 14$

$\pi[x] \leftarrow 14$

Case - (iii) $y \rightarrow z$

$d[v] > d[u] + w[u, v]$

$d[z] > d[y] + w[y, z]$

$\infty > 5 + 2$

$\infty > 7$

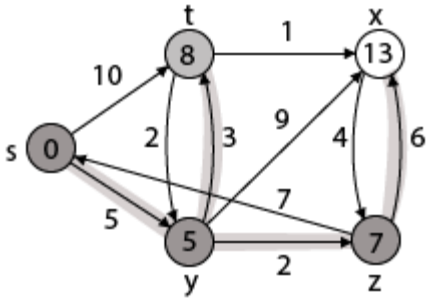
Then $d[z] \leftarrow 7$

$\pi[z] \leftarrow y$

By comparing case (i), case (ii) and case (iii)

Adj [y] → x = 14, t = 8, z =7

z is shortest **z is assigned in 7 = [s, z]**



Step - 4 Now we will find adj [z] that are s, x

1. Adj [z] → [x, s] [Here z is u and s and x are v]

Case - (i) $z \rightarrow x$

$d[v] > d[u] + w[u, v]$

$d[x] > d[z] + w[z, x]$

$14 > 7 + 6$

$14 > 13$

Then $d[x] \leftarrow 13$

$\pi[x] \leftarrow z$

Case - (ii) $z \rightarrow s$

$d[v] > d[u] + w[u, v]$

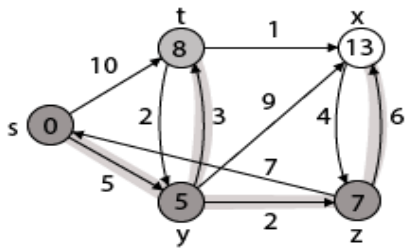
$d[s] > d[z] + w[z, s]$

$0 > 7 + 7$

0 > 14

∴ This condition does not satisfy so it will be discarded.

Now we have x = 13.



Step 5: Now we will find Adj [t]

Adj [t] → [x, y] [Here t is u and x and y are v]

Case - (i) t → x

d [v] > d [u] + w [u, v]

d [x] > d [t] + w [t, x]

13 > 8 + 1

13 > 9

Then **d [x] ← 9**

π [x] ← t

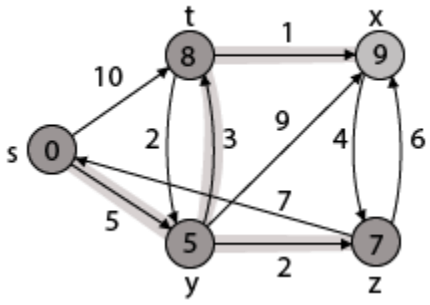
Case - (ii) t → y

d [v] > d [u] + w [u, v]

d [y] > d [t] + w [t, y]

5 > 10

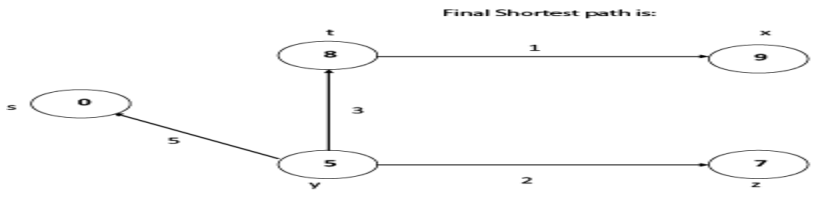
∴ This condition does not satisfy so it will be discarded.



Thus we get all shortest path vertex as

Weight from s to y is 5
Weight from s to z is 7
Weight from s to t is 8
Weight from s to x is 9

These are the shortest distance from the source's' in the given graph.



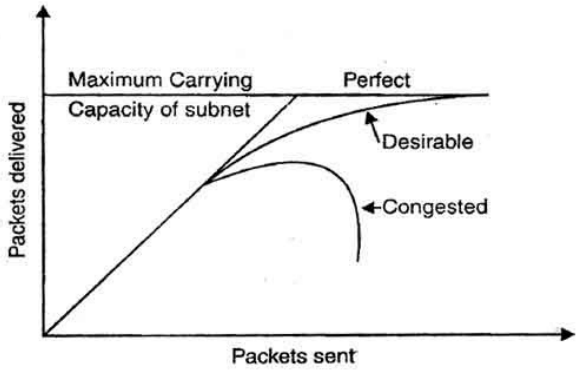
Disadvantage of Dijkstra's Algorithm:

1. It does a blind search, so wastes a lot of time while processing.
2. It can't handle negative edges.
3. It leads to the acyclic graph and most often cannot obtain the right shortest path.
4. We need to keep track of vertices that have been visited

❖ Congestion Control Policies

Congestion

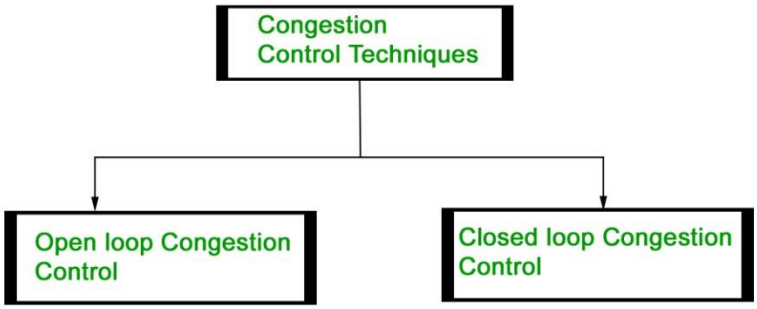
- Congestion is an important issue that can arise in packet switched network.
- Congestion is a situation in computer networks in which the performance of network is degraded due to the presence of too many packets in the subnet.



- Congestion in a network may occur when the load on the network is greater than the capacity of the network.
- When the number of packets dumped into the subnet by the hosts is within its carrying capacity, they are all delivered. At this stage number of packets delivered is proportional to the number of packets sent and no congestion take place.
- As the traffic increases too far, the routers are no longer able to cope up and they start losing packets. With the further increase in the traffic, performance degrades more and more packets and more packets are lost and congestion worsens.

❖ Congestion Control techniques

Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:



Open Loop Congestion Control

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

Policies adopted by open loop congestion control –

1. **Retransmission Policy:**
   It is the policy in which retransmission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network. To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.
2. **Window Policy :**
   The type of window at the sender side may also affect the congestion. Several packets in the Go-back-n window are resent, although some packets may be received successfully at the receiver side. This duplication may increase the

congestion in the network and making it worse.
Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.

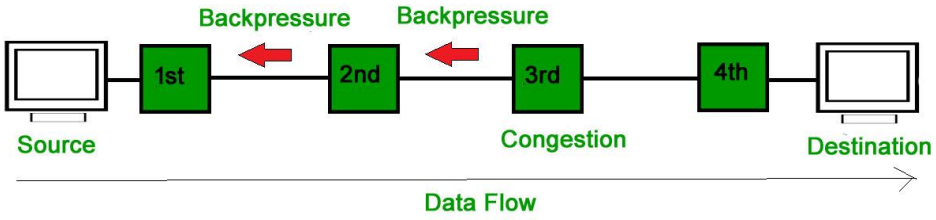
3. **Discarding Policy :**
   A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discards the corrupted or less sensitive package and also able to maintain the quality of a message.
   In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.
4. **Acknowledgment Policy :**
   Since acknowledgement are also the part of the load in network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.
   The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send a acknowledgment only if it has to sent a packet or a timer expires.
5. **Admission Policy :**
   In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

All the above policies are adopted to prevent congestion before it happens in the network.

Closed Loop Congestion Control

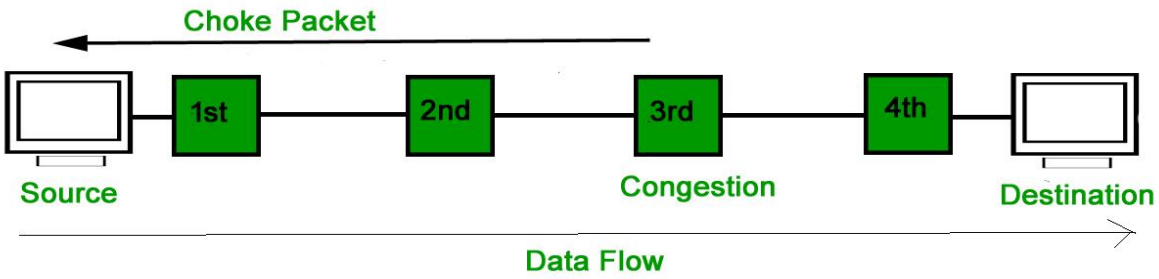
Closed loop congestion control technique is used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

1. **Backpressure:**
   Backpressure is a technique in which a congested node stop receiving packet from upstream node. This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow. The backpressure technique can be applied only to virtual circuit where each node has information of its above upstream node.



In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and informs the source to slow down.

2. **Choke Packet Technique :**
   Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitor its resources and the utilization at each of its output lines. whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets has traveled are not warned about congestion.



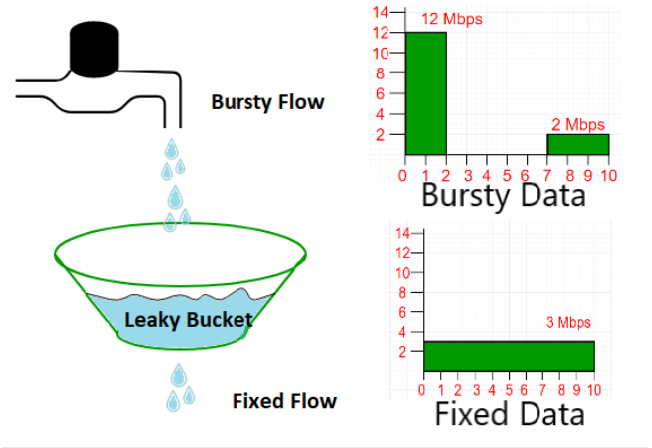
3. **Implicit Signaling:**
   In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is congestion.
4. **Explicit Signaling:**
   In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating different packet as in case of choke

packet technique.
Explicit signaling can occur in either forward or backward direction.

- **Forward Signaling:** In forward signaling signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopt policies to prevent further congestion.
- **Backward Signaling :** In backward signaling signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

❖ Leaky bucket Algorithm

- It is a traffic shaping mechanism that controls the amount and the rate of the traffic sent to the network.
- A leaky bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate.
- Imagine a bucket with a small hole at the bottom
- The rate at which the water is poured into the bucket is not fixed and can vary but it leaks from the bucket at a constant rate.
- Also, when the bucket is full, any additional water that enters into the bucket spills over the sides and is lost.
- The same concept can be applied to packets in the network.

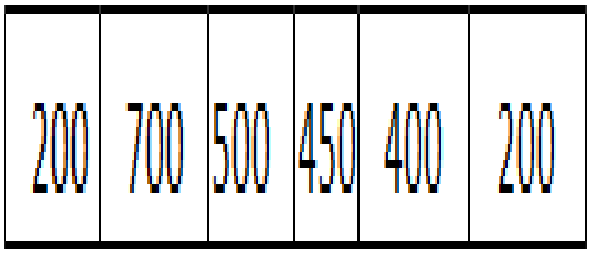


Consider that data is coming from the source at variable speeds. Suppose that a source sends data at 12mbps for 4 seconds. Then there is no data for 3 seconds. The source again transmits data at a rate of 10 mbps for 2 seconds. Thus, in a time span of 9 seconds, 68 Mb data has been transmitted.

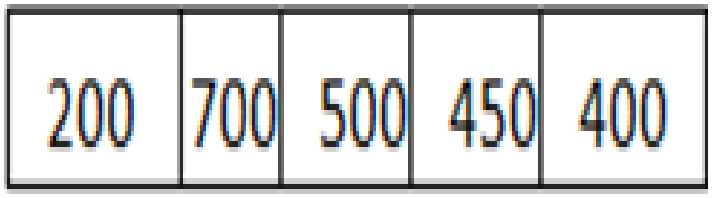
The following is an algorithm for variable-length packets:

1. Initialize a counter to n at the tick of the clock.
2. If n is greater than the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.
3. Reset the counter and go to step 1.

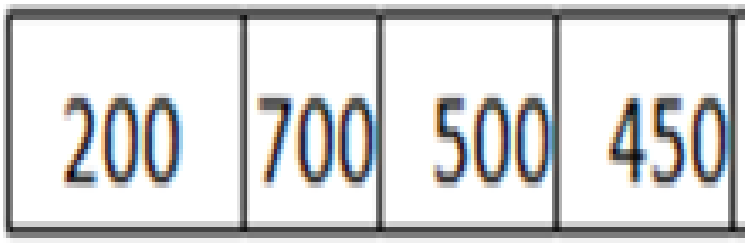
Example – Let n=1000



Packet=
Since n> front of Queue i.e. n>200
Therefore, n=1000-200=800
Packet size of 200 is sent to the network.



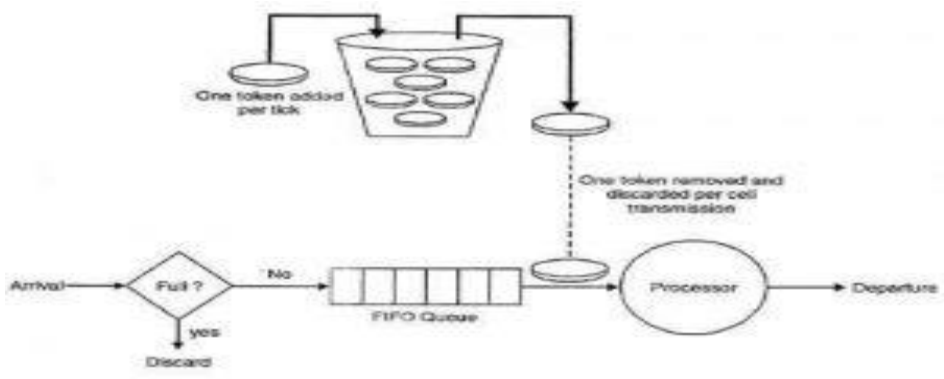
Now Again n>front of the queue i.e. n > 400
Therefore, n=800-400=400
Packet size of 400 is sent to the network.



Since n< front of queue
Therefore, the procedure is stop.
Initialize n=1000 on another tick of clock.
This procedure is repeated until all the packets are sent to the network.

❖ Token Bucket Algorithm

- The leaky bucket algorithm allows only an average rate of data flow. Its major problem is that it cannot deal with bursty data.
- A leaky bucket algorithm does not consider the idle time of the host. **For example**, if the host was idle for 10 seconds and now it is willing to sent data at a very high speed for another 10 seconds, the total data transmission will be divided into 20 seconds and average data rate will be maintained.
- To overcome this problem, a token bucket algorithm is used. A token bucket algorithm allows bursty data transfers.
- A token bucket algorithm is a modification of leaky bucket in which leaky bucket contains tokens.
- In this algorithm, a tokens are generated at every clock tick.
- Thus, a token bucket algorithm allows idle hosts to accumulate credit for the future in form of tokens.



Token bucket algorithm

Advantage of token Bucket over leaky bucket –

- If bucket is full in token Bucket , tokens are discard not packets. While in leaky bucket, packets are discarded.
- Token Bucket can send large bursts at a faster rate while leaky bucket always sends packets at constant rate.

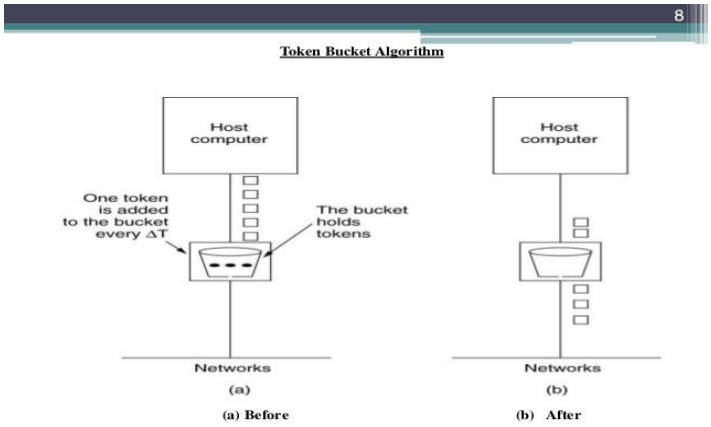
Implementation of token bucket algorithm

1. This algorithm make use of a variable or counter that counts the token. This counter is initialized to zero.
2. The counter is incremented by 1, each time a token is generated
3. Whenever a packet is sent, the counter is decremented by one.

4. When the counter becomes zero, no packets can be sent.

For example, a) token bucket contains 5 token and 7 packets are waiting to be transmitted.

In order to get transmitted, each packet captures and destroy one token.



Difference between Leaky and Token buckets

LEAKY BUCKET	TOKEN BUCKET
When the host has to send a packet, packet is thrown in bucket.	In this leaky bucket holds tokens generated at regular intervals of time.
Bucket leaks at constant rate	Bucket has maximum capacity.
Bursty traffic is converted into uniform traffic by leaky bucket.	If there is a ready packet, a token is removed from Bucket and packet is send.

LEAKY BUCKET	TOKEN BUCKET
In practice bucket is a finite queue outputs at finite rate	If there is a no token in bucket, packet cannot be send.

❖ Concept of Internetworking

Introduction of Internetworking

- When two or more different networks are connected together to form a bigger network, it is known as internet of internetwork.
- These different network may be based on different technologies and may use different protocols like TCP/IP, SNA, Decent, NCP/IPX , apple talk and other specialized protocols for satellites and cellular networks.
- Besides protocols, there are several other parameters that differentiate network **For example**, packet size, flow control etc.

There are chiefly 3 unit of Internetworking:

1. Extranet
2. Intranet
3. Internet

Intranets and extranets might or might not have connections to the net. If there is a connection to the net, the computer network or extranet area unit is usually shielded from being accessed from the net if it is not authorized. The net isn't thought-about to be a section of the computer network or extranet, though it should function a portal for access to parts of associate degree extranet.

1. **Extranet –** It's a network of the internetwork that's restricted in scope to one organization or entity however that additionally has restricted connections to the networks of one or a lot of different sometimes, however not essential. It's very lowest level of Internetworking, usually enforced in an exceedingly personal area. Associate degree extranet may additionally be classified as a Man, WAN, or different form of network however it cannot encompass one local area network i.e. it should have a minimum of one reference to associate degree external network.

2. **Intranet –** This associate degree computer network could be a set of interconnected networks, which exploits the Internet Protocol and uses IP-based tools akin to web browsers and FTP tools, that's underneath the management of one body entity. That body entity closes the computer network to the remainder of the planet and permits solely specific users. Most typically, this network is the internal network of a corporation or different enterprise. An outsized computer network can usually have its own internet server to supply users with browse able data.

3. **Internet –** A selected Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and personal networks based mostly upon the Advanced analysis comes Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense additionally home to the World Wide Web (WWW) and cited as the 'Internet' to differentiate from all different generic Internetworks. Participants within the web, or their service suppliers, use IP Addresses obtained from address registries that management assignments.

Connecting Devices: Networking and Internetworking devices

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub:-** These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.
- **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
- **Intelligent Hub :-** It work like active hubs and include remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

3. Bridge – A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

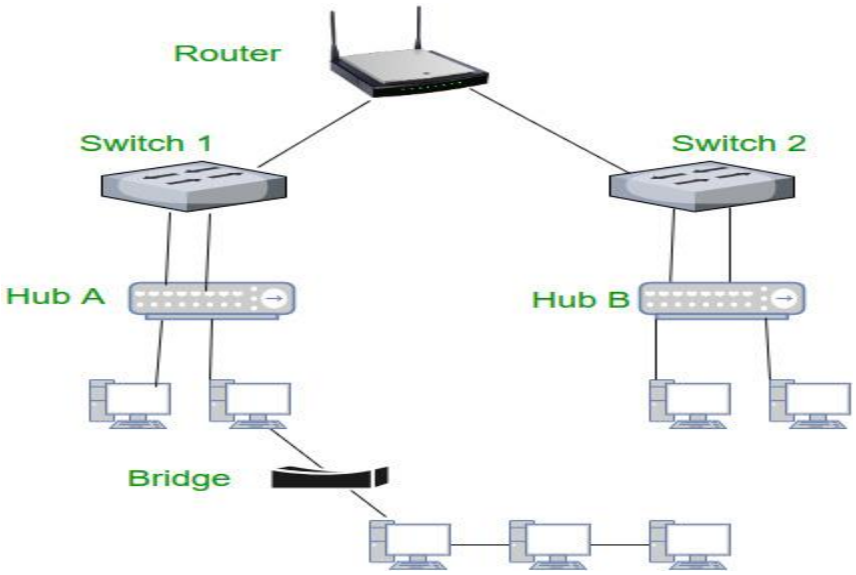
Types of Bridges

- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the
  bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of
  the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges:-** In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data that makes it very efficient as it does not forward packets that have errors and

forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



6. **Gateway** – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

7. **Brouter** – It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

UNIT IV

Transport Layer

- The transport layer is a 4th layer from the top.
- The main role of the transport layer is to provide the communication services directly to the application processes running on different hosts.
- The transport layer provides a logical communication between application processes running on different hosts. Although the application processes on different hosts are not physically connected, application processes use the logical communication provided by the transport layer to send the messages to each other.
- The transport layer protocols are implemented in the end systems but not in the network routers.
- A computer network provides more than one protocol to the network applications. **For example**, TCP and UDP are two transport layer protocols that provide a different set of services to the network layer.
- All transport layer protocols provide multiplexing/demultiplexing service. It also provides other services such as reliable data transfer, bandwidth guarantees, and delay guarantees.
- Each of the applications in the application layer has the ability to send a message by using TCP or UDP. The application communicates by using either of these two protocols. Both TCP and UDP will then communicate with the internet protocol in the internet layer. The applications can read and write to the transport layer. Therefore, we can say that communication is a two-way process.

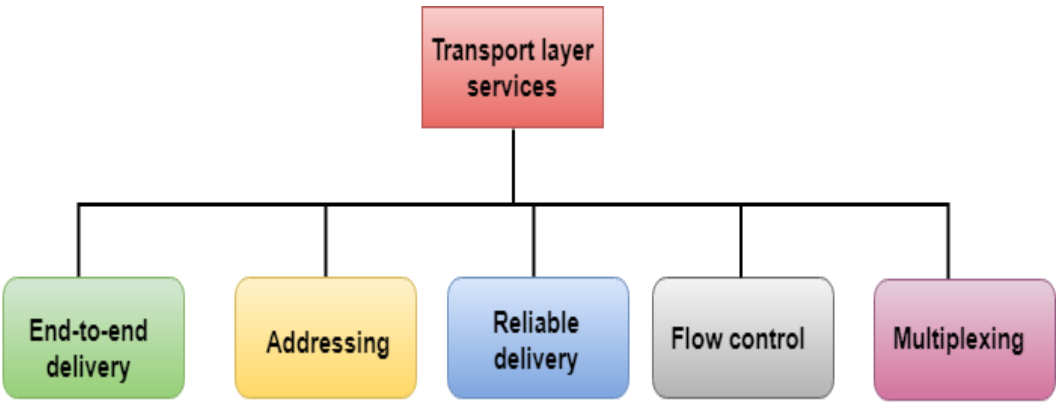
Services provided by the Transport Layer

The services provided by the transport layer are similar to those of the data link layer. The data link layer provides the services within a single network while the transport layer provides the services across an internetwork made up of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.

The services provided by the transport layer protocols can be divided into five categories:

- End-to-end delivery
- Addressing
- Reliable delivery

- Flow control
- Multiplexing



End-to-end delivery:

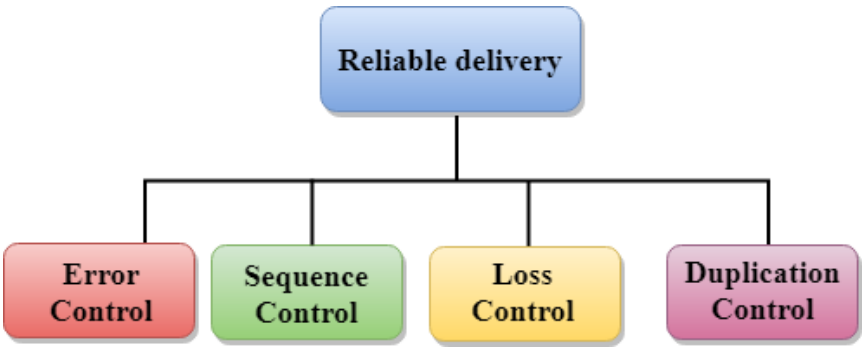
The transport layer transmits the entire message to the destination. Therefore, it ensures the end-to-end delivery of an entire message from a source to the destination.

Reliable delivery:

The transport layer provides reliability services by retransmitting the lost and damaged packets.

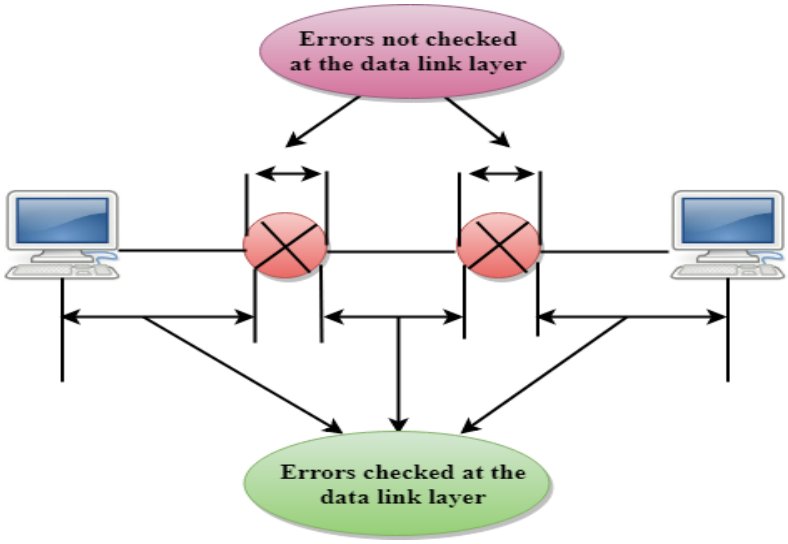
The reliable delivery has four aspects:

- Error control
- Sequence control
- Loss control
- Duplication control



Error Control

- The primary role of reliability is **Error Control**. In reality, no transmission will be 100 percent error-free delivery. Therefore, transport layer protocols are designed to provide error-free transmission.
- The data link layer also provides the error handling mechanism, but it ensures only node-to-node error-free delivery. However, node-to-node reliability does not ensure the end-to-end reliability.
- The data link layer checks for the error between each network. If an error is introduced inside one of the routers, then this error will not be caught by the data link layer. It only detects those errors that have been introduced between the beginning and end of the link. Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.



Sequence Control

- The second aspect of the reliability is sequence control which is implemented at the transport layer.
- On the sending end, the transport layer is responsible for ensuring that the packets received from the upper layers can be used by the lower layers. On the receiving end, it ensures that the various segments of a transmission can be correctly reassembled.

Loss Control

Loss Control is a third aspect of reliability. The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver?s transport layer to identify the missing segment.

Duplication Control

Duplication Control is the fourth aspect of reliability. The transport layer guarantees that no duplicate data arrive at the destination. Sequence numbers are used to identify the lost packets; similarly, it allows the receiver to identify and discard duplicate segments.

Flow Control

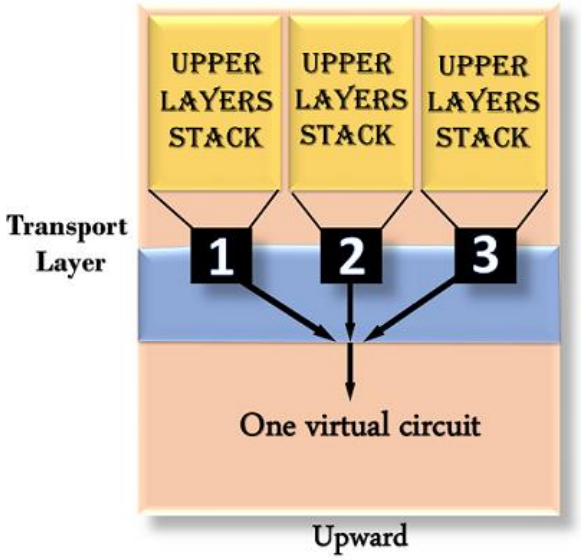
Flow control is used to prevent the sender from overwhelming the receiver. If the receiver is overloaded with too much data, then the receiver discards the packets and asking for the retransmission of packets. This increases network congestion and thus, reducing the system performance. The transport layer is responsible for flow control. It uses the sliding window protocol that makes the data transmission more efficient as well as it controls the flow of data so that the receiver does not become overwhelmed. Sliding window protocol is byte oriented rather than frame oriented.

Multiplexing

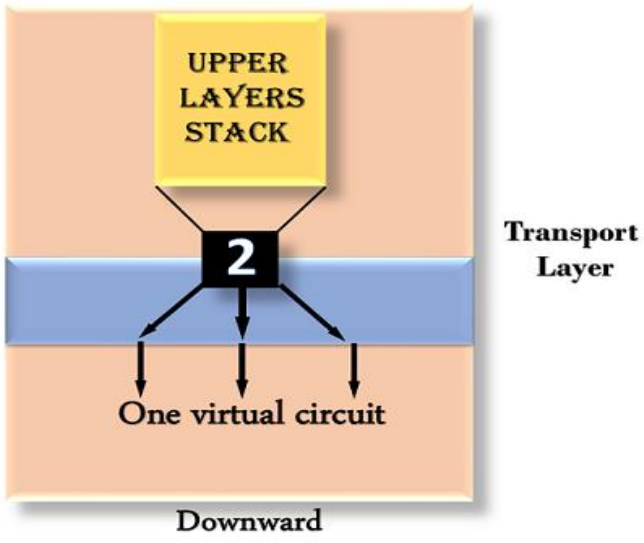
The transport layer uses the multiplexing to improve transmission efficiency.

Multiplexing can occur in two ways:

- **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.



- **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.



Design Issues with Transport Layer

- Accepting data from Session layer, split it into segments and send to the network layer.

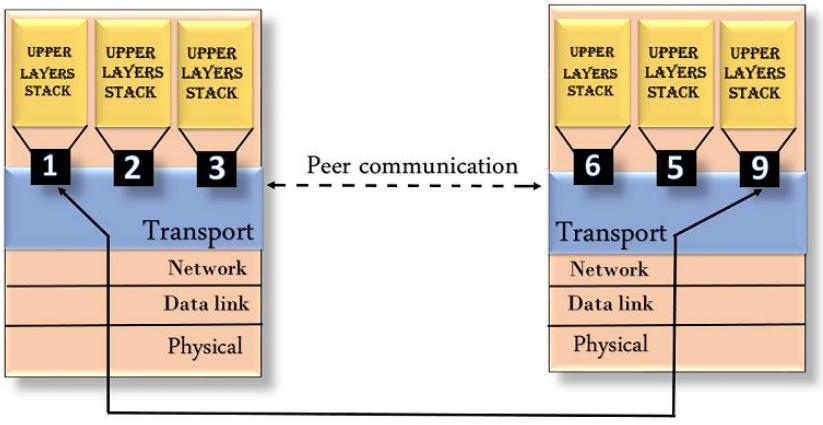
- Ensure correct delivery of data with efficiency.
- Isolate upper layers from the technological changes.
- Error control and flow control.

Elements of transport protocols

Following are the elements of transport protocols.

Addressing

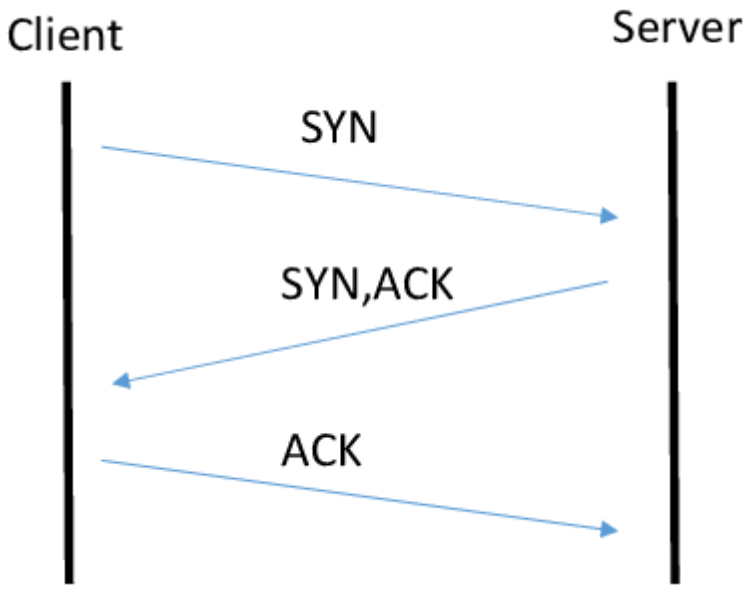
- According to the layered model, the transport layer interacts with the functions of the session layer. Many protocols combine session, presentation, and application layer protocols into a single layer known as the application layer. In these cases, delivery to the session layer means the delivery to the application layer. Data generated by an application on one machine must be transmitted to the correct application on another machine. In this case, addressing is provided by the transport layer.
- The transport layer provides the user address which is specified as a station or port. The port variable represents a particular TS user of a specified station known as a Transport Service access point (TSAP). Each station has only one transport entity.
- The transport layer protocols need to know which upper-layer protocols are communicating.



Connection Establishment and release

TCP Connection Establishment:

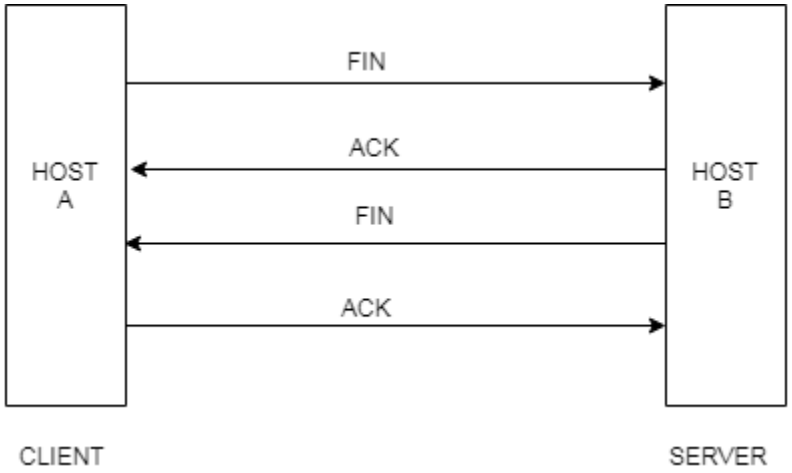
- To make the transport services reliable. TCP hosts must establish a connection-oriented session with one another. Connection establishment is performed by using a **three way handshake** mechanism.
- A three way handshake synchronizes both ends of a connection by allowing both sides to agree upon initial sequence numbers. This mechanism also guarantees that both sides are ready to transmit data and know that the other side is ready to transmit as well.
    - This is necessary so that packets are not transmitted or re-transmitted during session establishment or after session termination.
- Each host randomly chooses a sequence number used to track bytes within the stream it is sending and receiving. Then, the three way handshake proceeds in the manner.



- The requesting end (HOST A) sends a SYN segment specifying the port number of the server that the client wants to get connected to, and the clients initial sequence number (x)
- The server (HOST B) responds with its own SYN segment containing the server's initial sequence number (y) the server also acknowledges the client SYN by acknowledging the clients SYN plus one (x+1) A SYN consumes one sequence number.
- The client must acknowledge this SYN from the server by acknowledging the servers SYN plus one. (SEQ. = X + 1, ACK = Y + 1).
- This is how a TCP connection is established.

Connection termination protocol [connection release]

- While it takes three segments to establish a connection, It takes four to terminate a connection.
- Since a TCP connection is full duplex (that is, data flows in each direction independently of the other direction), the connection should be terminated in both the direction independently.
- When a TCP program on a host receives a FIN, it informs the application that the other end has terminated the data flow.
- The receipt of a FIN only means there will be no more data flowing in that direction. A TCP can still send data after receiving a FIN
- The end that first issues the close (e.g. sends the first FIN) (FIN is finish)performs the active close and the other end (that receives this FIN) performs the passive choice.

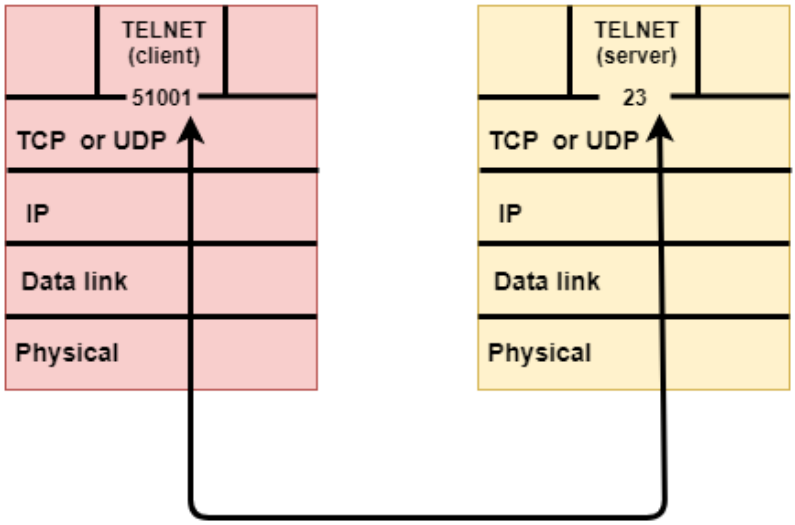


- When the server receives the FIN it sends back an ACK of the received sequence number plus one. A FIN consumes a sequence number, just like a SYN
- At this point the servers TCP also delivers an end of file to the application (the discard server)
- The server then closes its connection and its TCP sends a FIN to the client. The clients TCP informs the application and sends an ACK to server by incrementing the received sequence number by one.
- Connections are normally initiated by the client, with the first SYN going from the client to the server.

- A client or server can actively close the connection (i.e. send the first FIN). But in practice generally the client determines when the connection should be terminated, since client processes are often driven by an interactive user, who enters something like quit to terminate

Transport Layer protocols

- The transport layer is represented by two protocols: TCP and UDP.
- The IP protocol in the network layer delivers a datagram from a source host to the destination host.
- Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.
- An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.
- Each port is defined by a positive integer address, and it is of 16 bits.

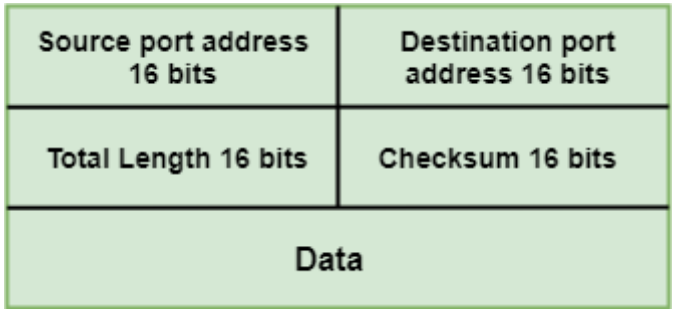


UDP

- UDP stands for **User Datagram Protocol**.
- UDP is a simple protocol and it provides nonsequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.
- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format

The user datagram has a 16-byte header which is shown below:



- **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
- **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
- **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
- **Checksum:** The checksum is a 16-bit field which is used in error detection.

Disadvantages of UDP protocol

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

TCP

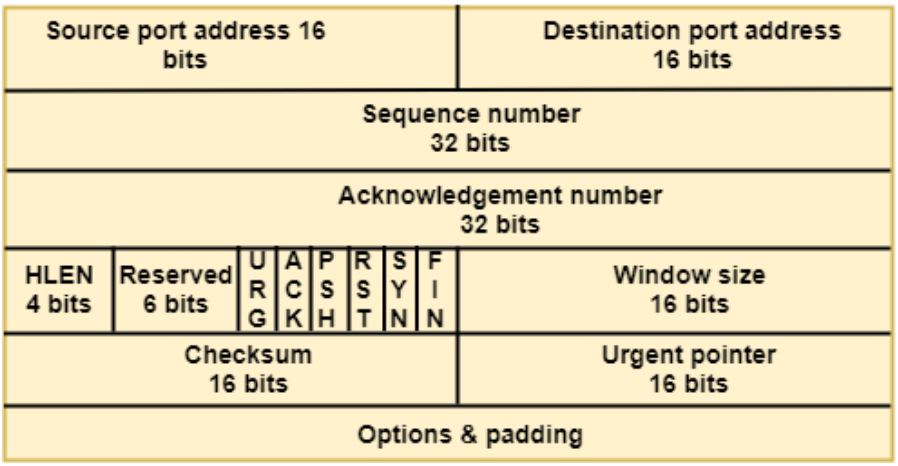
- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

Features Of TCP protocol

- **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
- **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.
  The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
- **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
- **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.

- **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
- **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
    - Establish a connection between two TCPs.
    - Data is exchanged in both the directions.
    - The Connection is terminated.

TCP Segment Format



- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.

- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
- **Reserved:** It is a six-bit field which is reserved for future use.
- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

Differences b/w TCP & UDP

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor it retransmits the damaged frame.

❖ Design issues in Session Layer

Session Layer is one of the Seven Layers of OSI Model. Physical layer, Data Link Layer and Network Layer lack some services such as establishment of a session between communicating systems. This is managed by Session Layer which particularly behaves as a dialog controller between communicating system thus facilitating interaction between them.

Before looking into design issues, here are some of functions of Session Layer:

Dialog Control –
Session layer allows two systems to enter into a dialog exchange mechanism which can either be full or half-duplex.

Managing Tokens –
The communicating systems in a network try to perform some critical operations and it is Session Layer
which prevents collisions which might occur while performing these operations which would otherwise result in a loss.

Synchronization –
Checkpoints are the midway marks that are added after a particular interval during stream of data
transfer. These points are also referred to as synchronization points. The Session layer permits process to add these checkpoints.

For example, suppose a file of 400 pages is being sent over a network, then it is highly beneficial to set up a checkpoint after every 50 pages so that next 50 pages are sent only when previous pages are received and acknowledged.

❖ Design Issues with Session Layer:

Establish sessions between machines –
The establishment of session between machines is an important service provided by session layer. This session is responsible for creating a dialog between connected machines. The Session Layer provides mechanism for opening, closing and managing a session between end-user application processes, i.e. a semi-

permanent dialogue. This session consists of requests and responses that occur between applications.

Enhanced Services –
Certain services such as checkpoints and manangement of tokens are the key features of session layer and thus it becomes necessary to keep enhancing these features during the layer's design.

To help in Token management and Synchronization –
The session layer plays an important role in preventing collision of several critical operation as well as ensuring better data transfer over network by establishing synchronization points at specific intervals. Thus it becomes highly important to ensure proper execution of these services.

❖ Remote Procedure Call

A remote procedure call is an interprocess communication technique that is used for client-server based applications. It is also known as a subroutine call or a function call.

A client has a request message that the RPC translates and sends to the server. This request may be a procedure or a function call to a remote server. When the server receives the request, it sends the required response back to the client. The client is blocked while the server is processing the call and only resumed execution after the server is finished.

The sequence of events in a remote procedure call are given as follows −

The client stub is called by the client.

The client stub makes a system call to send the message to the server and puts the parameters in the message.

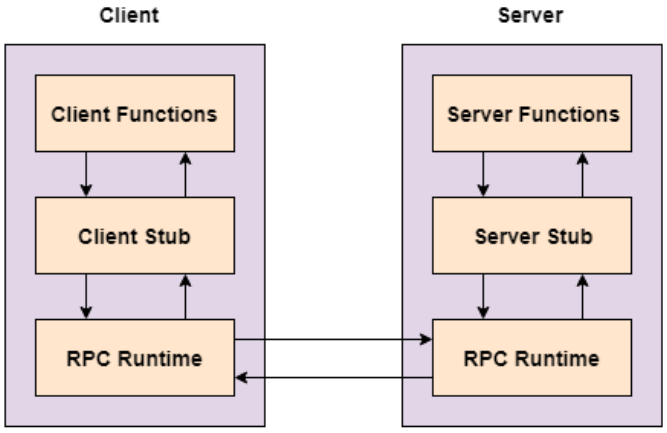
The message is sent from the client to the server by the client's operating system.

The message is passed to the server stub by the server operating system.

The parameters are removed from the message by the server stub.

Then, the server procedure is called by the server stub.

A diagram that demonstrates this is as follows −



Advantages of Remote Procedure Call

Some of the advantages of RPC are as follows −

- Remote procedure calls support process oriented and thread oriented models.
- The internal message passing mechanism of RPC is hidden from the user.
- The effort to re-write and re-develop the code is minimum in remote procedure calls.
- Remote procedure calls can be used in distributed environment as well as the local environment.
- Many of the protocol layers are omitted by RPC to improve performance.

Disadvantages of Remote Procedure Call

Some of the disadvantages of RPC are as follows −

- The remote procedure call is a concept that can be implemented in different ways. It is not a standard.
- There is no flexibility in RPC for hardware architecture. It is only interaction based.
- There is an increase in costs because of remote procedure call.

❖ Presentation Layer – Design issues

The syntax and the semantics of the information exchanged between two communication systems is managed by the presentation layer of the OSI Model.

Before going through the design issues in the presentation layer, some of its main functions are:

Translation –
It is necessary that the information which is in the form of numbers, characters and symbols needs to be changed to the bit streams. The presentation layer handles the different encoding methods used by different machines .It manages the translation of data between the format of network requires and computer.

Encryption –
The data encryption at the transmission end as well as the decryption at the receiver end is managed by the presentation layer.

Compression –
In order to reduce the number of bits to be transmitted, the presentation layer performs the data compression. It increases efficiency in case of multimedia files **such as audio, video etc.**

❖ Design issues with Presentation Layer:

Standard way of encoding data
The presentation layer follows a standard way to encode data when it needs to be transmitted. This encoded data is represented as character strings, integers, floating point numbers, and data structures composed of simple components. It is handled differently by different machines based on the encoding methods followed by them.

Maintaining the Syntax and Semantics of distributed information
The presentation layer manages and maintains the syntax as well as logic and meaning of the information that is distributed.

Standard Encoding on the wire

The data structures that are defined to be exchanged need to be abstract along with the standard encoding to be used "on the wire"

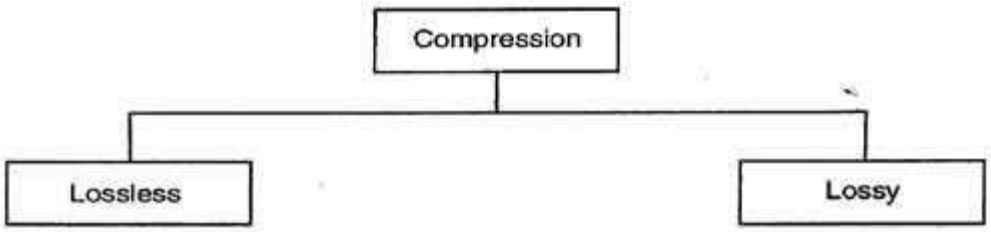
❖ Data compression techniques

Data compression is the function of presentation layer in OSI reference model. Compression is often used to maximize the use of bandwidth across a network or to optimize disk space when saving data.

There are two general types of compression algorithms:

1. Lossless compression

2. Lossy compression



Types of Compression

Lossless Compression

Lossless compression compresses the data in such a way that when data is decompressed it is exactly the same as it was before compression i.e. there is no loss of data.

A lossless compression is used to compress file data such as executable code, text files, and numeric data, because programs that process such file data cannot tolerate mistakes in the data.

Lossless compression will typically not compress file as much as lossy compression techniques and may take more processing power to accomplish the compression.

Lossless Compression Algorithms

The various algorithms used to implement lossless data compression are:

1. Run length encoding

2. Differential pulse code modulation

3. Dictionary based encoding

1. Run length encoding

• This method replaces the consecutive occurrences of a given symbol with only one copy of the symbol along with a count of how many times that symbol occurs. Hence the names 'run length'.

For example, the string AAABBCDDDD would be encoded as 3A2BIC4D.

• A real life example where run-length encoding is quite effective is the fax machine. Most faxes are white sheets with the occasional black text. So, a run-length encoding scheme can take each line and transmit a code for while then the number of pixels, then the code for black and the number of pixels and so on.

• This method of compression must be used carefully. If there is not a lot of repetition in the data then it is possible the run length encoding scheme would actually increase the size of a file.

2. **Differential pulse code modulation**

• In this method first a reference symbol is placed. Then for each symbol in the data, we place the difference between that symbol and the reference symbol used.

For example, using symbol A as reference symbol, the string AAABBC DDDD would be encoded as AOOOl123333, since A is the same as reference symbol, B has a difference of 1 from the reference symbol and so on.

3. **Dictionary based encoding**

• One of the best known dictionary based encoding algorithms is Lempel-Ziv (LZ) compression algorithm.

• This method is also known as substitution coder.

• In this method, a dictionary (table) of variable length strings (common phrases) is built.

• This dictionary contains almost every string that is expected to occur in data.

• When any of these strings occur in the data, then they are replaced with the corresponding index to the dictionary.

• In this method, instead of working with individual characters in text data, we treat each word as a string and output the index in the dictionary for that word.

For example, let us say that the word "compression" has the index 4978 in one particular dictionary; it is the 4978th word is usr/share/dict/words. To compress a body of text, each time the string "compression" appears, it would be replaced by 4978.

Lossy Compression

Lossy compression is the one that does not promise that the data received is exactly the same as data send i.e. the data may be lost.

This is because a lossy algorithm removes information that it cannot later restore.

Lossy algorithms are used to compress still images, video and audio.

Lossy algorithms typically achieve much better compression ratios than the lossless algorithms.

Audio Compression

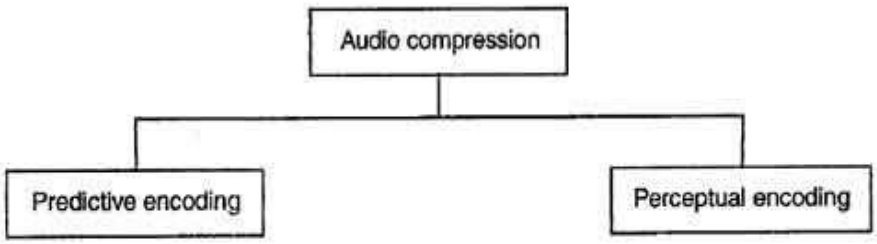
• Audio compression is used for speech or music.

• For speech, we need to compress a 64-KHz digitized signal; For music, we need to compress a 1.411.MHz signal

Two types of techniques are used for audio compression:

1. Predictive encoding

2. Perceptual encoding



Techniques of audio compression

Predictive encoding

• In predictive encoding, the differences between the samples are encoded instead of encoding all the sampled values.

• This type of compression is normally used for speech.

• Several standards have been defined such as GSM (13 kbps), G. 729 (8 kbps), and G.723.3 (6.4 or 5.3 kbps).

Perceptual encoding

• Perceptual encoding scheme is used to create a CD-quality audio that requires a transmission bandwidth of 1.411 Mbps.

• MP3 (MPEG audio layer 3), a part of MPEG standard uses this perceptual encoding.

• Perceptual encoding is based on the science of psychoacoustics, a study of how people perceive sound.

• The perceptual encoding exploits certain flaws in the human auditory system to encode a signal in such a way that it sounds the same to a human listener, even if it looks quite different on an oscilloscope.

• The key property of perceptual coding is that some sounds can mask other sound. **For example**, imagine that you are broadcasting a live flute concert and all of a sudden someone starts striking a hammer on a metal sheet. You will not be able to hear the flute any more. Its sound has been masked by the hammer.

• Such a technique explained above is called frequency masking-the ability of a loud sound in one frequency band to hide a softer sound in another frequency band that would have been audible in the absence of the loud sound.

• Masking can also be done on the basis of time. For example: Even if the hammer is not striking on a metal sheet, the flute will be inaudible for a short period of time because the ears turn down its gain when they start and take a finite time to turn up again.

• Thus, a loud sound can numb our ears for a short time even after the sound has stopped. This effect is called temporal masking.

MP3

• MP3 uses these two phenomena, i.e. frequency masking and temporal masking to compress audio signals.

• In such a system, the technique analyzes and divides the spectrum into several groups. Zero bits are allocated to the frequency ranges that are totally masked.

• A small number of bits are allocated to the frequency ranges that are partially masked.

• A larger number. of bits are allocated to the frequency ranges that are not masked.

• Based on the range of frequencies in the original analog audio, MP3 produces three data rates: 96kbps, 128 kbps and 160 kbps.

❖ Cryptography

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.

Secure Communication refers to the scenario where the message or data shared between two parties can’t be accessed by an adversary. In Cryptography, an

Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security.

Features of Cryptography are as follows:

Confidentiality:
Information can only be accessed by the person for whom it is intended and no other person except him can access it.

Integrity:
Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

Non-repudiation:
The creator/sender of information cannot deny his or her intention to send information at later stage.

Authentication:
The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:
In general there are three types Of cryptography:

Symmetric Key Cryptography:
It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System (DES).

Hash Functions:
There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

Asymmetric Key Cryptography:
Under this system a pair of keys is used to encrypt and decrypt information. A

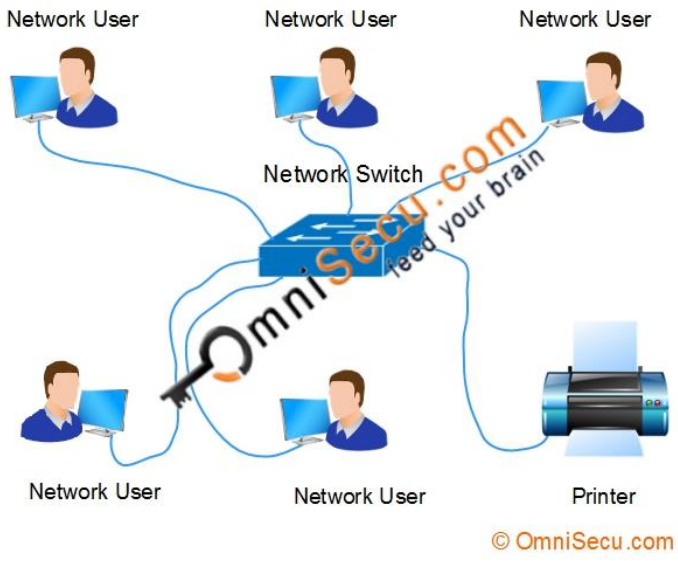
public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

❖ Application Layer – Distributed application

Peer to peer networks

A peer to peer network has no dedicated servers. In a peer to peer network, a number of workstations (or clients) are connected together for sharing devices, information or data. All the workstations (clients) are considered equal. Any one computer can act as client or server at any instance. This network is ideal for small networks where there is no need for dedicated servers, like home networks, small business networks, or retail shops. The Microsoft term for peer to peer network is "Workgroup".

There is no limitation for the number of computers in a peer to peer network. But peer to peer implementations are meant for small networks. Typically, a Workgroup contain less than 10 workstations.



Advantages of Peer to Peer networking

Some advantages of peer to peer computing are as follows −

Each computer in the peer to peer network manages itself. So, the network is quite easy to set up and maintain.

In the client server network, the server handles all the requests of the clients. This provision is not required in peer to peer computing and the cost of the server is saved.

It is easy to scale the peer to peer network and add more nodes. This only increases the data sharing capacity of the system.

None of the nodes in the peer to peer network are dependent on the others for their functioning.

Disadvantages of Peer to Peer networking

Some disadvantages of peer to peer computing are as follows −

It is difficult to backup the data as it is stored in different computer systems and there is no central server.

It is difficult to provide overall security in the peer to peer network as each system is independent and contains its own data.

Client-Server Model

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

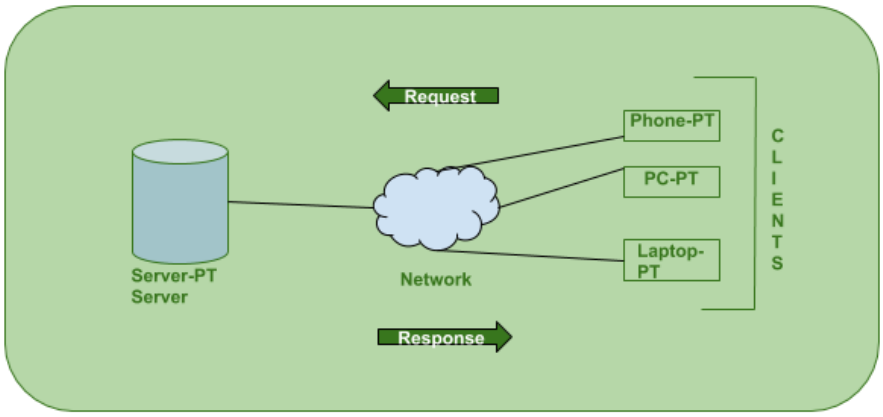
How the Client-Server Model works?

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

Client: When we talk the word Client, it mean to talk of a person or an organization using a particular service. Similarly in the digital world a Client is a computer (Host) i.e. capable of receiving information or using a particular service from the service providers (Servers).

Servers: Similarly, when we talk the word Servers, It mean a person or medium that serves something. Similarly in this digital world a Server is a remote computer which provides information (data) or access to particular services.

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



How the browser interacts with the servers?
There are few steps to follow to interact with the servers a client.

User enters the URL(Uniform Resource Locator) of the website or file. The Browser then requests the DNS(DOMAIN NAME SYSTEM) Server.

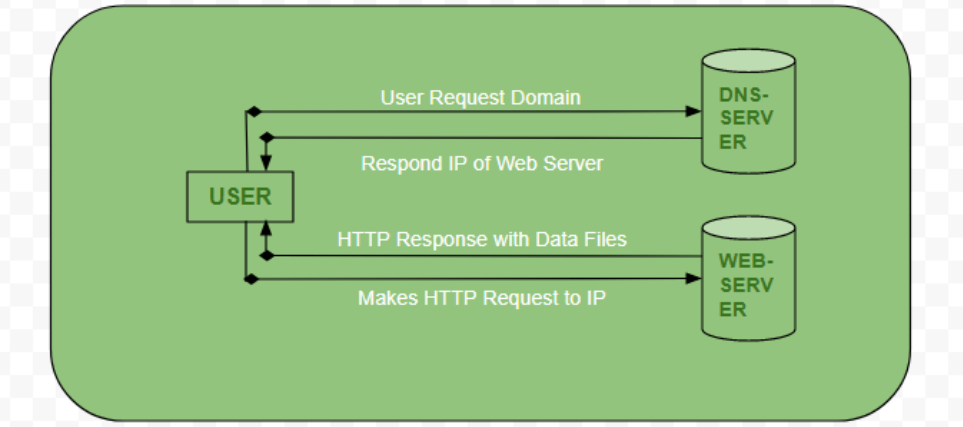
DNS Server lookup for the address of the WEB Server.

DNS Server responds with the IP address of the WEB Server.

Browser sends over an HTTP/HTTPS request to WEB Server's IP (provided by DNS server).

Server sends over the necessary files of the website.

Browser then renders the files and the website is displayed. This rendering is done with the help of DOM (Document Object Model) interpreter, CSS interpreter and JS Engine collectively known as the JIT or (Just in Time) Compilers.



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.

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.

Cloud

Cloud networking, or cloud-based networking, gives users access to networking resources through a centralized third-party provider operating inter-connected servers. This involves connecting to a Wide Area Network (WAN) or other internet-based technology, and helps to distribute content quickly and securely.

By using a cloud network an organization can deliver content more rapidly, reliably, and securely, without having to bear the costs and difficulties of building

and operating its own network. A variety of organizations may find value in using a cloud network, including web content providers, ecommerce businesses, cloud service providers, enterprises using public or private cloud services, or network operators looking to extend their network reach.

How does cloud networking work?

Cloud networking allows users to build networks using cloud-based services. A reliable cloud network provides centralized management, control and visibility, **for example**, managing devices in different physical locations using the internet. It can be used for connectivity, security, management and control.

Using cloud architecture in thousands of different locations globally, cloud networking allows organizations to deliver content faster and monitor their devices and operations in real-time. It also helps to keep them abreast of any network security issues, including monitoring high volumes of traffic.

The advantages of using cloud networking software

A cloud network is instrumental in the delivery of digital content for a multitude of industries. It offers the following benefits:

Versatility

With the increasing availability of online content, many enterprises have turned to cloud networking for better content distribution. It can be used for web content providers, ecommerce retailers, cloud service providers, organizations using public or private cloud services, or network operators looking to extend their network reach.

Speed

Using a cloud network guarantees the faster delivery of content thanks to the use of thousands of servers across the world. This means that content has less physical distance to travel between servers, giving the final end users faster access.

Reliability

Cloud security solutions available as part of cloud networking ensure that users are protected from the latest web security threats. There is also less risk of server downtime thanks to server load balancing.

Cost-saving

By using a cloud network, organizations can save money on building and operating their own networks, as well as avoiding the potential technical issues that come with these.

❖ WWW

World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc. The WWW, along with internet, enables the retrieval and display of text and media to your device.

The building blocks of the Web are web pages which are formatted in HTML and connected by links called "hypertext" or hyperlinks and accessed by HTTP. These links are electronic connections that link related pieces of information so that users can access the desired information quickly. Hypertext offers the advantage to select a word or phrase from text and thus to access other pages that provide additional information related to that word or phrase.

A web page is given an online address called a Uniform Resource Locator (URL). A particular collection of web pages that belong to a specific URL is called a website, e.g., www.facebook.com, www.google.com, etc. So, the World Wide Web is like a huge electronic book whose pages are stored on multiple servers across the world.

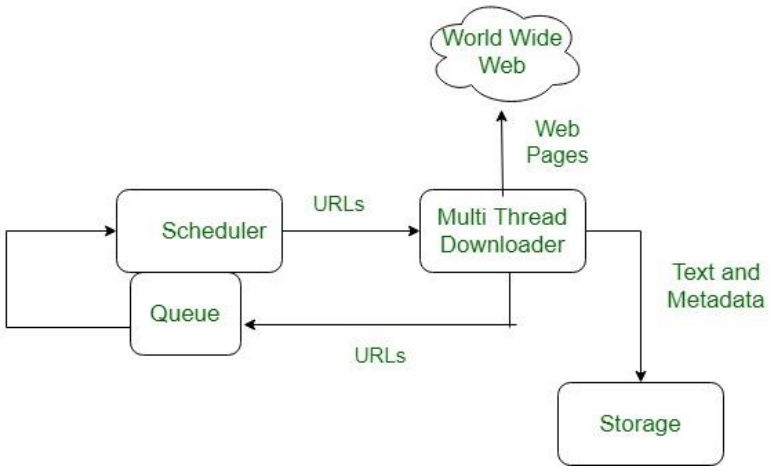
Small websites store all of their WebPages on a single server, but big websites or organizations place their WebPages on different servers in different countries so that when users of a country search their site they could get the information quickly from the nearest server.

So, the web provides a communication platform for users to retrieve and exchange information over the internet. Unlike a book, where we move from one page to another in a sequence, on World Wide Web we follow a web of hypertext links to visit a web page and from that web page to move to other web pages. You need a browser, which is installed on your computer, to access the Web

History:
It is a project created, by Timothy Berner's Lee in 1989, for researchers to work together effectively at CERN. is an organisation, named World Wide Web Consortium (W3C), was developed for further development in web. This organisation is directed by Tim Berner's Lee, aka father of web.

System Architecture:
From user's point of view, the web consists of a vast, worldwide connection of documents or web pages. Each page may contain links to other pages anywhere in the world. The pages can be retrieved and viewed by using browsers of which internet explorer, Netscape Navigator, Google, Chrome, etc are the popular ones. The browser fetches the page requested interprets the text and formatting commands on it, and displays the page, properly formatted, on the screen.

The basic model of how the web works is shown in figure below. Here the browser is displaying a web page on the client machine. When the user clicks on a line of text that is linked to a page on the abd.com server, the browser follows the hyperlink by sending a message to the abd.com server asking it for the page.



Here the browser displaying web page on the client machine when the user clicks on a line of text that is linked to a page on abd.com, the v browser follows the hyperlink by sending a message to abd.com server asking it for the page.

Working of WWW:
The World Wide Web is based on several different technologies : Web browsers, Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP).

An Web browser is used to access webpages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interface provided by Web browsers. Initially Web browsers were used only for surfing the Web but now they have become more universal. Web browsers can be used for several tasks including conducting searches, mailing, transferring files, and much more. Some of the commonly used browsers are **Internet Explorer, Opera Mini, Google Chrome.**

Features of WWW:

- HyperText Information System
- Cross-Platform
- Distributed

- Open Standards and Open Source
- Uses Web Browsers to provide a single interface for many services
- Dynamic, Interactive and Evolving.
- "Web 2.0"

Components of Web
There are 3 components of web:

Resource Locator (Uniform URL): serves as system for resources on web.

HyperText Transfer Protocol (HTTP): specifies communication of browser and server.

Hyper Text Markup Language (HTML): defines structure, organization and content of webpage.

❖ Domain Name System (DNS) in Application Layer

DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Requirement

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

Domain :
There are various kinds of DOMAIN :

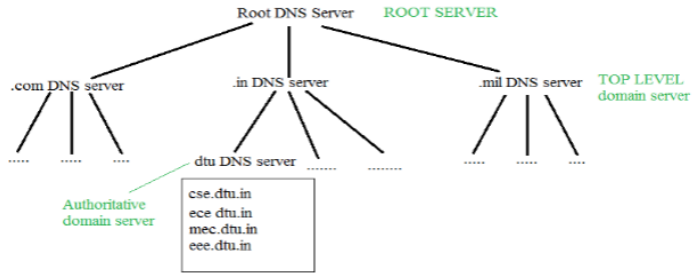
Generic domain : .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.

Country domain .in (india) .us .uk

Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping.So DNS can provide both the mapping **for example** to find

the ip addresses of geeksforgeeks.org then we have to type nslookup www.geeksforgeeks.org.

Organization of Domain

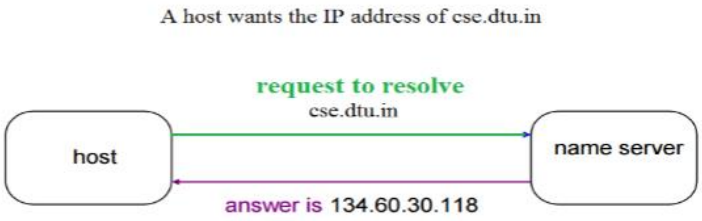


It is Very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately,
there should not be a lot of delay for that to happen organization of database is very important.
DNS record – Domain name, ip address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.

Namespace – Set of possible names, flat or hierarchical . Naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value –

Name server – It is an implementation of the resolution mechanism.. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.

Name to Address Resolution



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

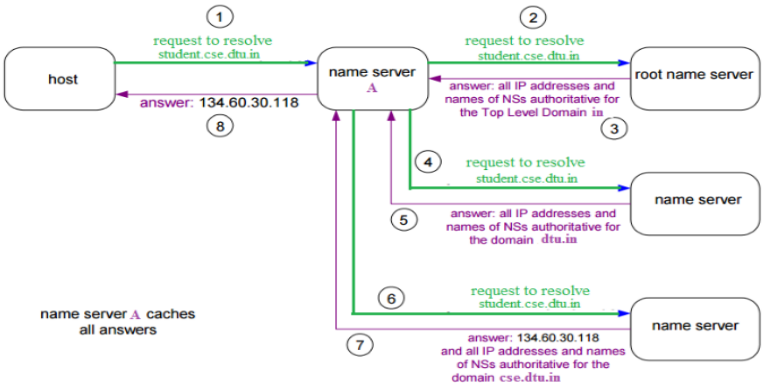
Hierarchy of Name Servers

Root name servers – It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.

Top level server – It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.

Authoritative name servers This is organization's DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative ip address.

Domain Name Server



The client machine sends a request to the local name server, which, if root does not find the address in its database, sends a request to the root name server, which in turn, will route the query to an intermediate or authoritative name server. The root name server can also contain some host Name to IP address mappings. The intermediate name server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.

❖ Email

Email is a service which allows us to send the message in electronic mode over the internet. It offers an efficient, inexpensive and real time mean of distributing information among people.

E-Mail Address

Each user of email is assigned a unique name for his email account. This name is known as E-mail address. Different users can send and receive messages according to the e-mail address.

E-mail is generally of the form username@domainname. For example, webmaster@tutorialspoint.com is an e-mail address where webmaster is username and tutorialspoint.com is domain name.

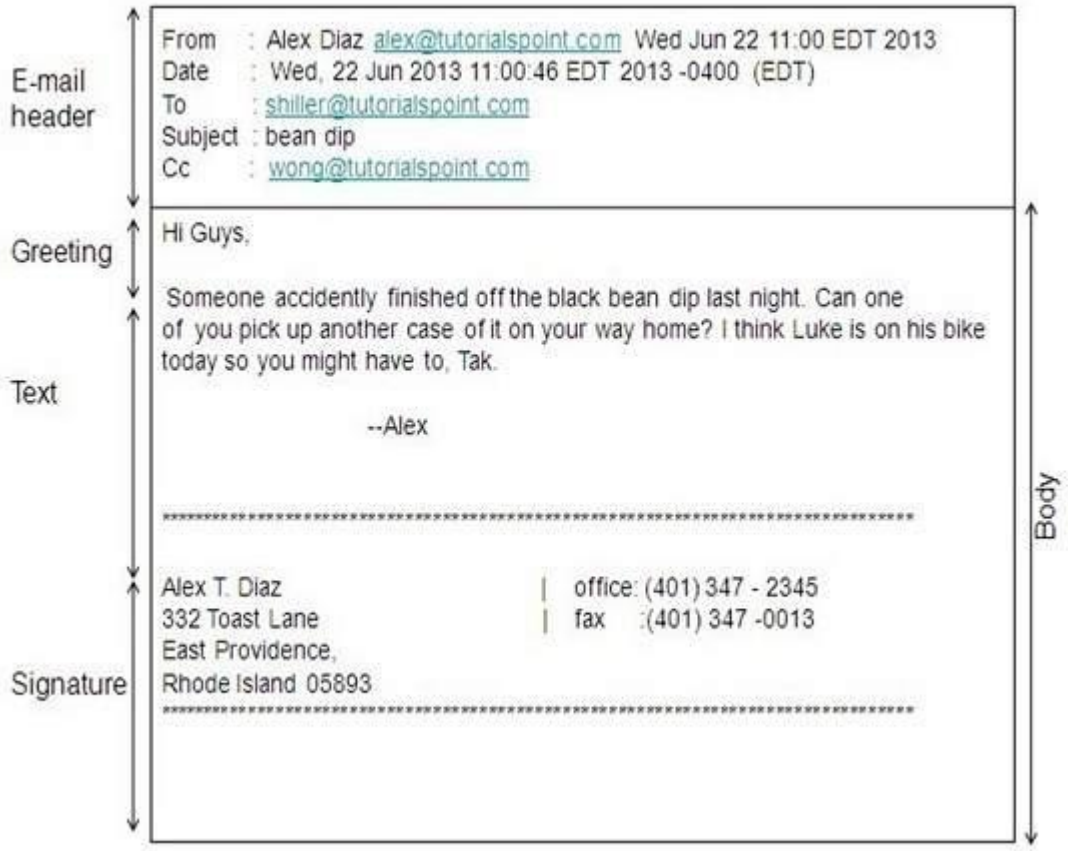
The username and the domain name are separated by @ (at) symbol.

E-mail addresses are not case sensitive.

Spaces are not allowed in e-mail address.

E-mail Message Components

E-mail message comprises of different components: E-mail Header, Greeting, Text, and Signature. These components are described in the following diagram:



E-mail Header

The first five lines of an E-mail message is called E-mail header. The header part comprises of **following fields:**

From

Date

To

Subject

CC

BCC

From

The From field indicates the sender's address i.e. who sent the e-mail.

Date

The Date field indicates the date when the e-mail was sent.

To

The To field indicates the recipient's address i.e. to whom the e-mail is sent.

Subject

The Subject field indicates the purpose of e-mail. It should be precise and to the point.

CC

CC stands for Carbon copy. It includes those recipient addresses whom we want to keep informed but not exactly the intended recipient.

BCC

BCC stands for Black Carbon Copy. It is used when we do not want one or more of the recipients to know that someone else was copied on the message.

G**reeting**

Greeting is the opening of the actual message. Eg. Hi Sir or Hi Guys etc.

Text

It represents the actual content of the message.

Signature

This is the final part of an e-mail message. It includes Name of Sender, Address, and Contact Number.

Advantages

E-mail has proved to be powerful and reliable medium of communication. Here are the benefits of E-mail:

Reliable

Convenience

Speed

Inexpensive

Printable

Global

Generality

Reliable

Many of the mail systems notify the sender if e-mail message was undeliverable.

Convenience

There is no requirement of stationary and stamps. One does not have to go to post office. But all these things are not required for sending or receiving an mail.

Speed

E-mail is very fast. However, the speed also depends upon the underlying network.

Inexpensive

The cost of sending e-mail is very low.

Printable

It is easy to obtain a hardcopy of an e-mail. Also an electronic copy of an e-mail can also be saved for records.

Global

E-mail can be sent and received by a person sitting across the globe.

Generality

It is also possible to send graphics, programs and sounds with an e-mail.

Disadvantages

Apart from several benefits of E-mail, there also exists some disadvantages as discussed below:

Forgery

Overload

Misdirection

Junk

No response

Forgery

E-mail doesn't prevent from forgery, that is, someone impersonating the sender, since sender is usually not authenticated in any way.

Overload

Convenience of E-mail may result in a flood of mail.

Misdirection

It is possible that you may send e-mail to an unintended recipient.

Junk

Junk emails are undesirable and inappropriate emails. Junk emails are sometimes referred to as spam.

No Response

It may be frustrating when the recipient does not read the e-mail and respond on a regular basis.

Services provided by E-mail system :

Composition –
The composition refer to process that creates messages and answers. For composition any kind of text editor can be used.

Transfer –
Transfer means sending procedure of mail i.e. from the sender to recipient.

Reporting –
Reporting refers to confirmation for delivery of mail. It help user to check whether their mail is delivered, lost or rejected.

Displaying –
It refers to present mail in form that is understand by the user.

Disposition –
This step concern with recipient that what will recipient do after receiving mail i.e save mail, delete before reading or delete after reading.

❖ FTP

FTP stands for File transfer protocol.

FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.

It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.

It is also used for downloading the files to computer from other servers.

Objectives of FTP

It provides the sharing of files.

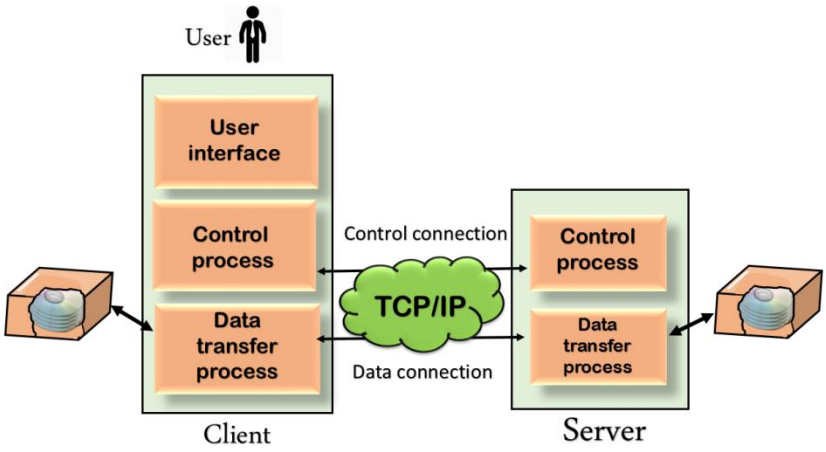
It is used to encourage the use of remote computers.

It transfers the data more reliably and efficiently.

Why FTP?

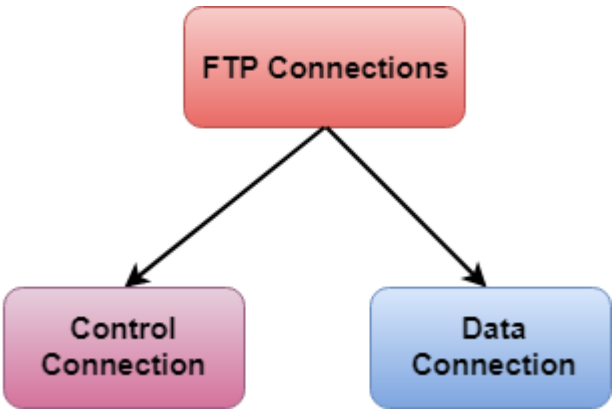
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. **For example**, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures.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

Mechanism of FTP



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

There are two types of connections in FTP:



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

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

FTP Clients

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

It allows a user to connect to a remote host and upload or download the files.

It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.

The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

Speed: One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.

Efficient: It is more efficient as we do not need to complete all the operations to get the entire file.

Security: To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.

Back & forth movement: FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.

FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.

Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.

It is not compatible with every system.

❖ HTTP

HTTP stands for **HyperText Transfer Protocol**.

It is a protocol used to access the data on the World Wide Web (www).

The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.

This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.

HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.

HTTP is used to carry the data in the form of MIME-like format.

HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

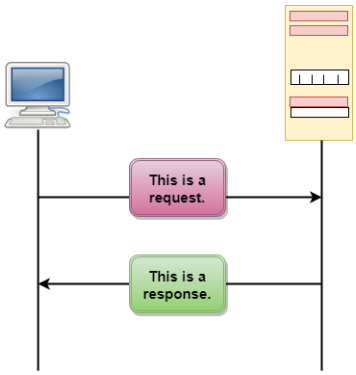
Features of HTTP:

Connectionless protocol: HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.

Media independent: HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.

Stateless: HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

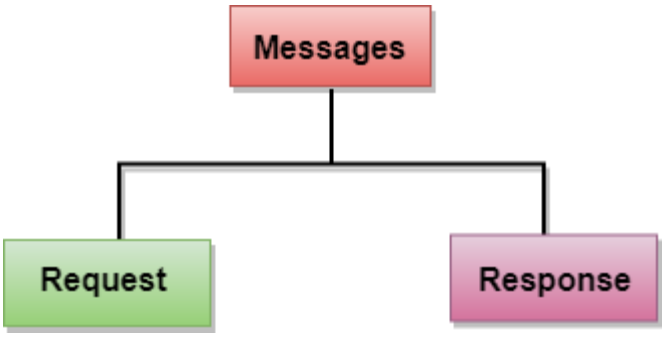
HTTP Transactions



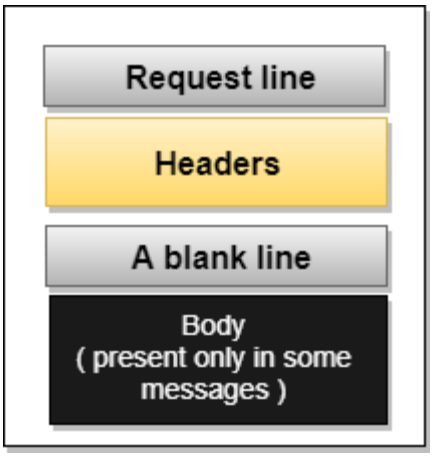
The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

Messages

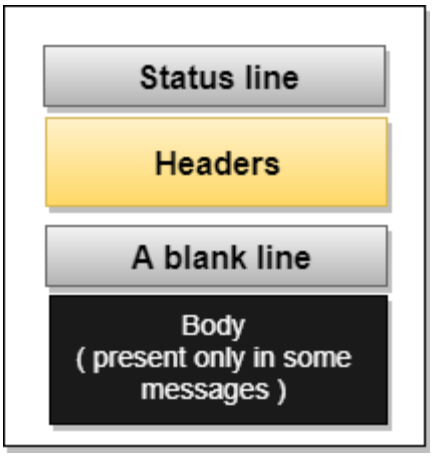
HTTP messages are of two types: request and response. Both the message types follow the same message format.



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



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



Uniform Resource Locator (URL)

A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).

The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.

The URL defines four parts: method, host computer, port, and path.

Method: The method is the protocol used to retrieve the document from a server. **For example**, HTTP.

Host: The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.

Port: The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.

Path: Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.