DIWAKAR EDUCATION HUB

Data Communication and Computer Networks Unit – 9

As per updated syllabus

DIWAKAR EDUCATION HUB

2020

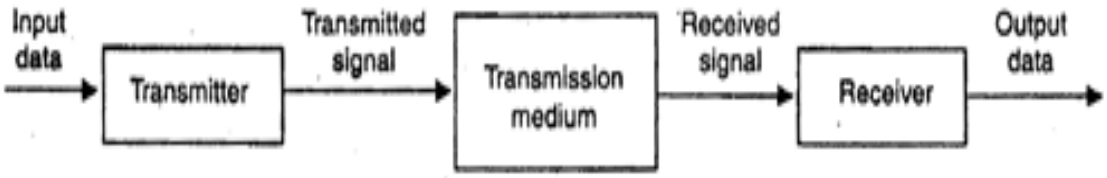
THE LEARN WITH EXPERTIES

Data communication

Data communication refers to the exchange of data between a source and a receiver via form of transmission media such as a wire cable. Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area.

The meanings of source and receiver are very simple. The device that transmits the data is known as source and the device that receives the transmitted data is known as receiver. Data communication aims at the transfer of data and maintenance of the data during the process but not the actual generation of the information at the source and receiver.

Datum mean the facts information statistics or the like derived by calculation or experimentation. The facts and information so gathered are processed in accordance with defined systems of procedure. Data can exist in a variety of forms such as numbers, text, bits and bytes. The Figure is an illustration of a simple data communication system.

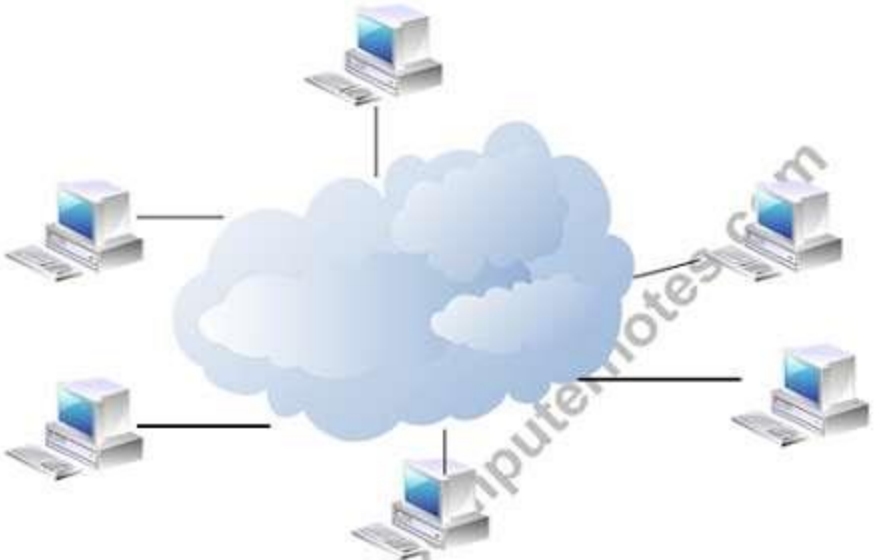


Simple Data Communication System

The term data used to describe information, under whatever form of words you will be using.

A data communication system may collect data from remote locations through data transmission circuits, and then outputs processed results to remote locations. Figure provides a broader view of data communication networks. The different data communication techniques which are presently in widespread use evolved gradually either to improve the data communication techniques already existing or to replace the same with better options and features. Then, there are

data communication jargons to contend with such as baud rate, modems, routers, LAN, WAN, TCP/IP, ISDN, during the selection of communication systems. Hence, it becomes necessary to review and understand these terms and gradual development of data communication methods.



A Data Communication System using Remote Locations

Components of data communication system

A Communication system has following components:

1. **Message**: It is the information or data to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.

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

2. **Sender**: It is the device/computer that generates and sends that message.

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

3. **Receiver**: It is the device or computer that receives the message. The location of receiver computer is generally different from the sender computer. The distance between sender and receiver depends upon the types of network used in between.

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

4. **Medium**: It is the channel or physical path through which the message is carried from sender to the receiver. The medium can be wired like twisted pair wire, coaxial cable, fiber-optic cable or wireless like laser, radio waves, and microwaves.

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

5. **Protocol**: It is a set of rules that govern the communication between the devices. Both sender and receiver follow same protocols to communicate with each other.

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

A protocol performs the following functions:

DIWAKAR EDUCATION HUB

1. **Data sequencing**. It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.

2. **Data routing**. Data routing defines the most efficient path between the source and destination.

3. **Data formatting**. Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.

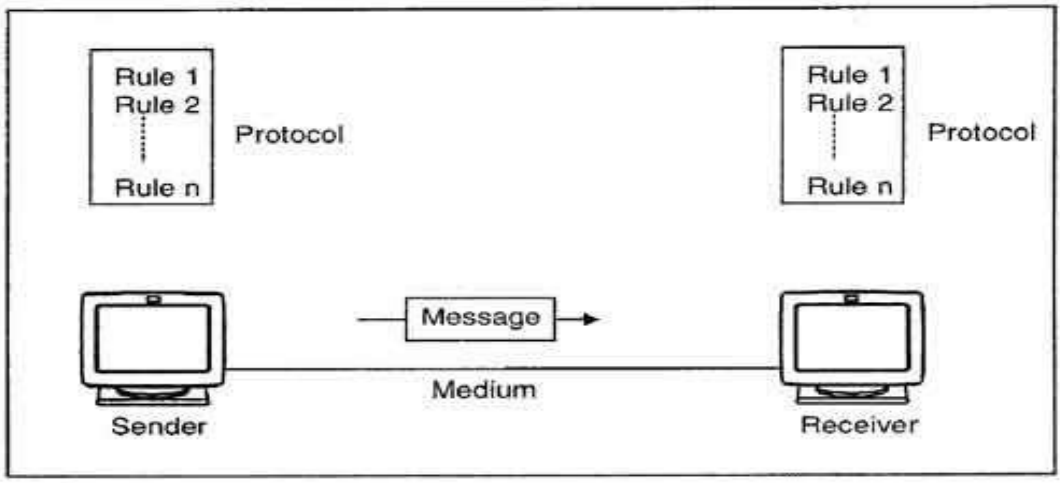
4. **Flow control**. A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.

5. **Error control**. These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.

6. **Precedence and order of transmission**. These rules ensure that all the nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.

7. **Connection establishment and termination**. These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.

DIWAKAR EDUCATION HUB



8. **Data security**. Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.

9. Log information. Several communication software are designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information may be used for charging the users of the network based on their usage of the network resources.

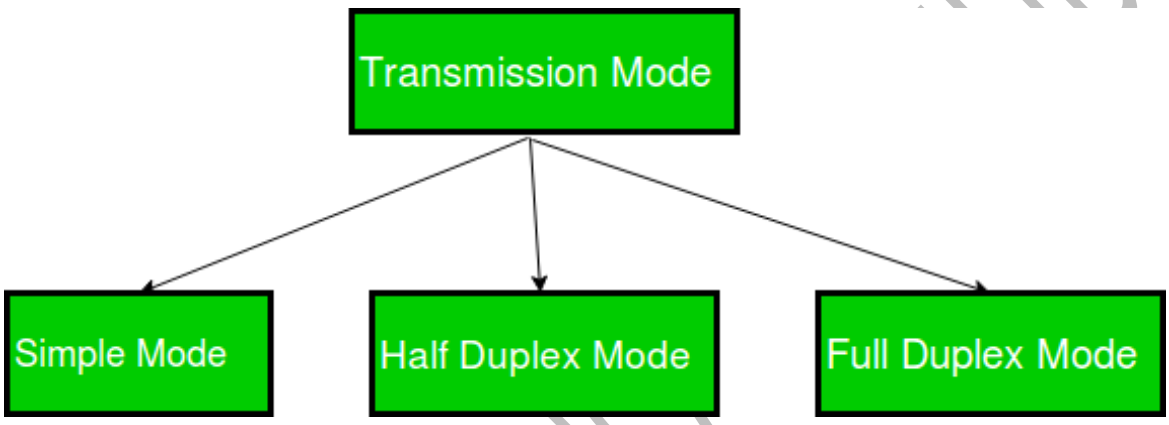
The effectiveness depends on four fundamental characteristics of data communications

1. Delivery: The data must be deliver in correct order with correct destination.
2. Accuracy: The data must be deliver accurately.
3. Timeliness: The data must be deliver in a timely manner.late delivered Data useless.
4. Jitter: It is the uneven delay in the packet arrival time that cause uneven quality.

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:-

DWAKAR EDUCATION

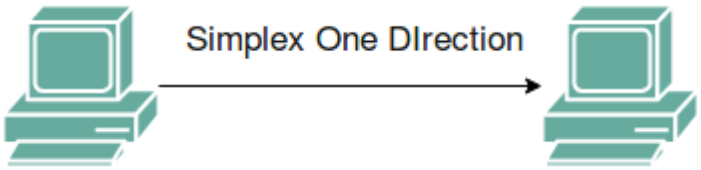
1. **Simplex Mode**
2. **Half-Duplex Mode**
3. **Full-Duplex Mode**



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.

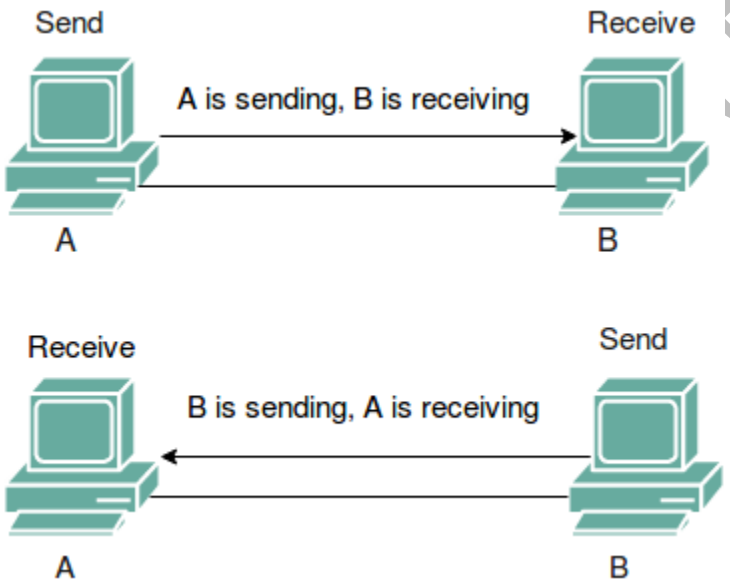


DIWAKAR EDUCATION HUB

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.



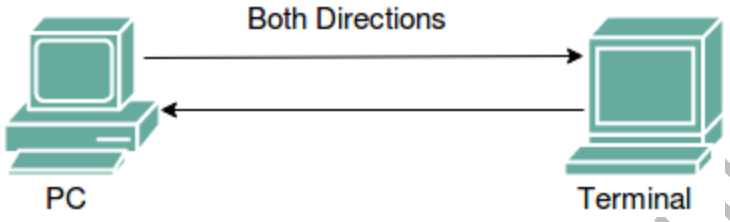
Full-Duplex Mode

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:

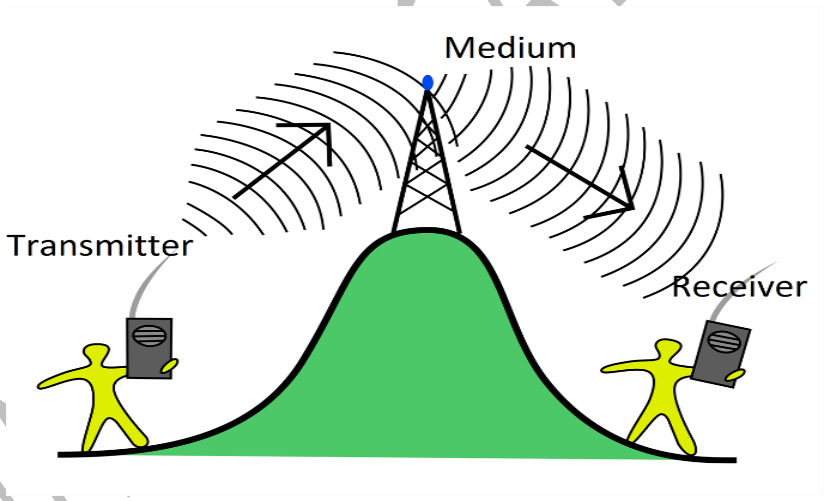
- Either the link must contain two physically separate transmission paths, one for sending and other for receiving.
- Or the capacity is divided between signals travelling in both directions.

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.



The communication system is a system which describes the information exchange between two points. The process of transmission and reception of information is called communication. The major elements of communication are the **Transmitter** of information, **Channel or medium** of communication and the **Receiver** of information.



Types Of Communication Systems

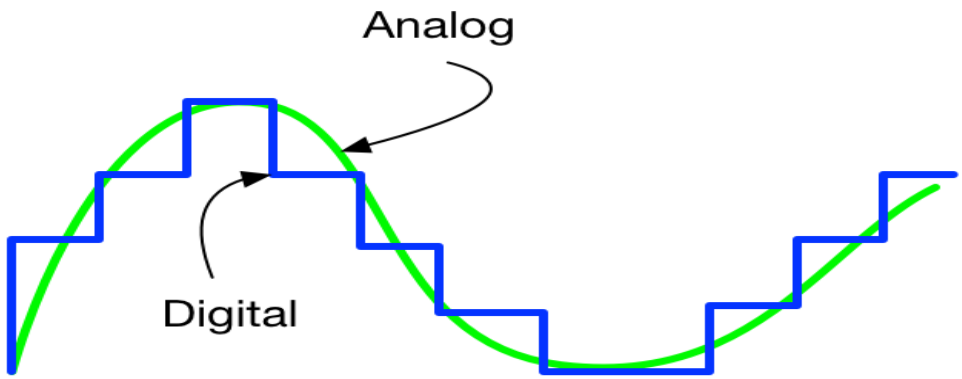
Depending on Signal specification or technology, the communication system is classified as follows:

(1) Analog

Analog technology communicates data as electronic signals of varying frequency or amplitude. Broadcast and telephone transmission are common examples of Analog technology.

(2) Digital

In digital technology, the data are generated and processed in two states: High (represented as 1) and Low (represented as 0). Digital technology stores and transmits data in the form of 1s and 0s.



Depending on the communication channel, the communication system is categorized as follows:

1. Wired (Line communication)

- Parallel wire communication
- Twisted wire communication
- Coaxial cable communication
- Optical fibre communication

2. Wireless (Space communication)

- Ground wave communication
- Skywave communication

- Space wave communication
- Satellite communication

Examples Of Communication Systems

The following are a few examples of communication systems:

1. Internet

2. Public Switched Telephone network

3. Intranet and Extranet

4. Television

Elements Of Communication Systems

The definitions of the terms used in the communication system are discussed below.

Information

Message or information is the entity that is to be transmitted. It can be in the form of audio, video, temperature, picture, pressure, etc.

Signal

The single-valued function of time that carries the information. The information is converted into an electrical form for transmission.

Transducer

A device or an arrangement that converts one form of energy to the other. An electrical transducer converts physical variables such as pressure, force, temperature into corresponding electrical signal variations. Example: Microphone – converts audio signals into electrical signals. Photodetector – converts light signals into electrical signals.

Amplifier

DIWAKAR EDUCATION HUB

The electronic circuit or device that increases the amplitude or the strength of the transmitted signal is called an amplifier. When the signal strength becomes less than the required value, amplification can be done anywhere in between transmitter and receiver. A DC power source will provide for the amplification.

Modulator

As the original message signal cannot be transmitted over a large distance because of their low frequency and amplitude, they are superimposed with high frequency and amplitude wave called carrier wave. This phenomenon of superimposing of message signal with a carrier wave is called modulation. And the resultant wave is a modulated wave which is to be transmitted.

Again there are different types of Modulation.

i. Amplitude Modulation (AM)

The process of changing the amplitude of the signal wave by impressing or superimposing it on a high-frequency carrier wave, keeping its frequency constant is called amplitude modulation.

ii. Frequency Modulation (FM)

Frequency modulation is a technique in which the frequency of the message signal is varied by modulating with a carrier wave. It is better than deficient than amplitude modulation because it eliminates noise from various sources.

iii. Phase Modulation (PM)

The phase of the carrier wave changes the phase of the signal wave. The phase shift after modulation is dependent on the frequency of the carrier wave as well. Phase modulated waves are immune to noise to a greater extent.

Transmitter

It is the arrangement that processes the message signal into a suitable form for transmission and subsequently reception.

DIWAKAR EDUCATION HUB

Antenna

An Antenna is a structure or a device that is radiate and receive electromagnetic waves. So, they are used in both transmitters and receivers. An antenna is basically a metallic object, often a collection of wires. The electromagnetic waves are polarised according to the position of the antenna.

Channel

A channel refers to a physical medium such as wire, cables, space through which the signal is passed from transmitter to the receiver. There are many channel impairments that affect the channel performance to a pronounced level. Noise, Attenuation and distortion to mention the major impairments.

Noise

Noise is one of the channel imperfection or impairment in the received signal at the destination. There are external and internal sources that cause noise. External sources include interference, i.e. interference from nearby transmitted signals (cross talk), interference generated by natural source such as lightning, solar or cosmic radiation, from automobile generated radiation, etc. The external noise can be minimised and eliminated by appropriate design of the channel, shielding of cables. Also by digital transmission external noise can be much minimised.

Internal sources include noise due to random motion and collision of electrons in the conductors, thermal noise due to diffusion and recombination of charge carriers in other electronic devices. Internal noise can be minimised by cooling and using digital technology for transmission.

- A different cable design.
- Proper design of the channel.
- Use digital transmission
- Using BPF or LPF at the receiver side.

Attenuation

DIWAKAR EDUCATION HUB

Attenuation is a problem caused by the medium. When the signal is propagating for a longer distance through a medium, depending on the length of the medium the initial power decreases. The loss in initial power is directly proportional to the length of the medium. Using amplifiers, the signal power is strengthened or amplified so as to reduce attenuation. Also, digital signals are comparatively less prone to attenuation than analogue signals.

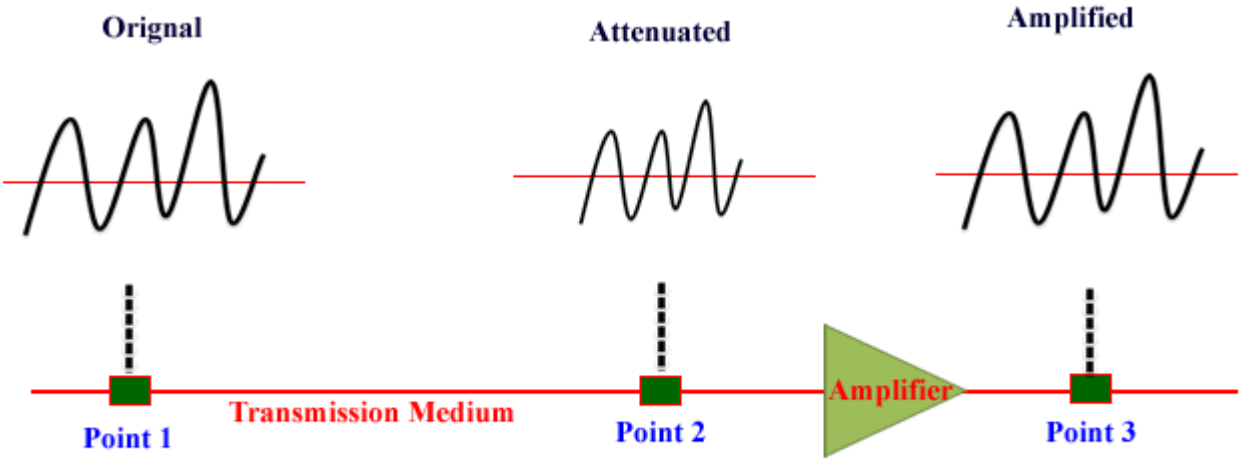


Fig: Effect of Attenuation

Distortion

It is also another type of channel problem. When the signal is distorted, the distorted signal may have frequency and bandwidth different from the transmitted signal. The variation in the signal frequency can be linear or non-linear.

Receiver

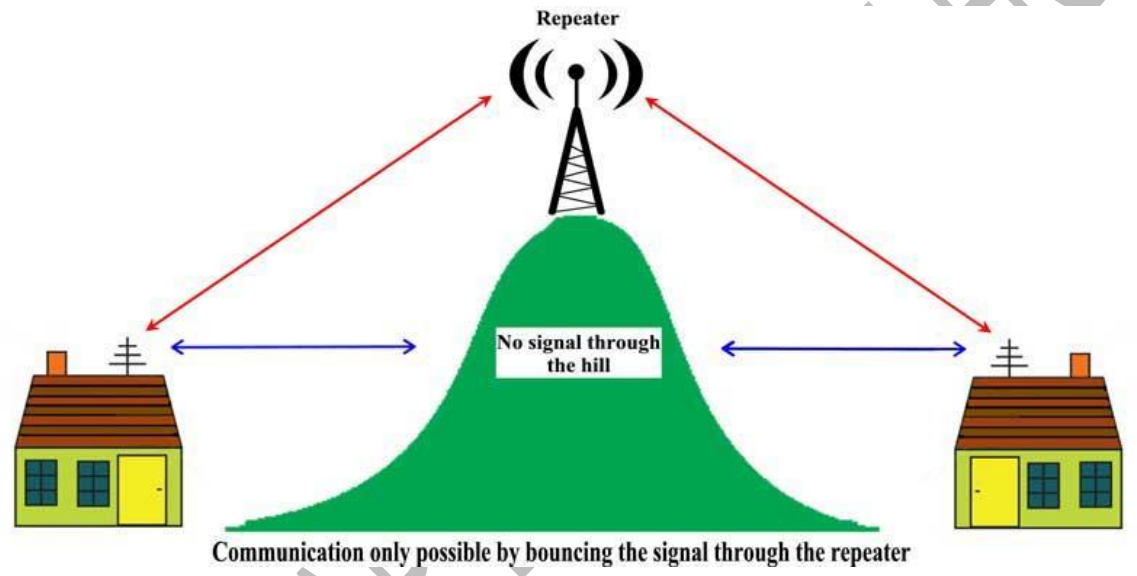
An arrangement that extracts the message or information from the transmitted signal at the output end of the channel and reproduces it in a suitable form as the original message signal is a receiver.

Demodulator

It is the inverse phenomenon of modulation. The process of separation of message signal from the carrier wave takes place in the demodulator. The information is retrieved from the modulated wave.

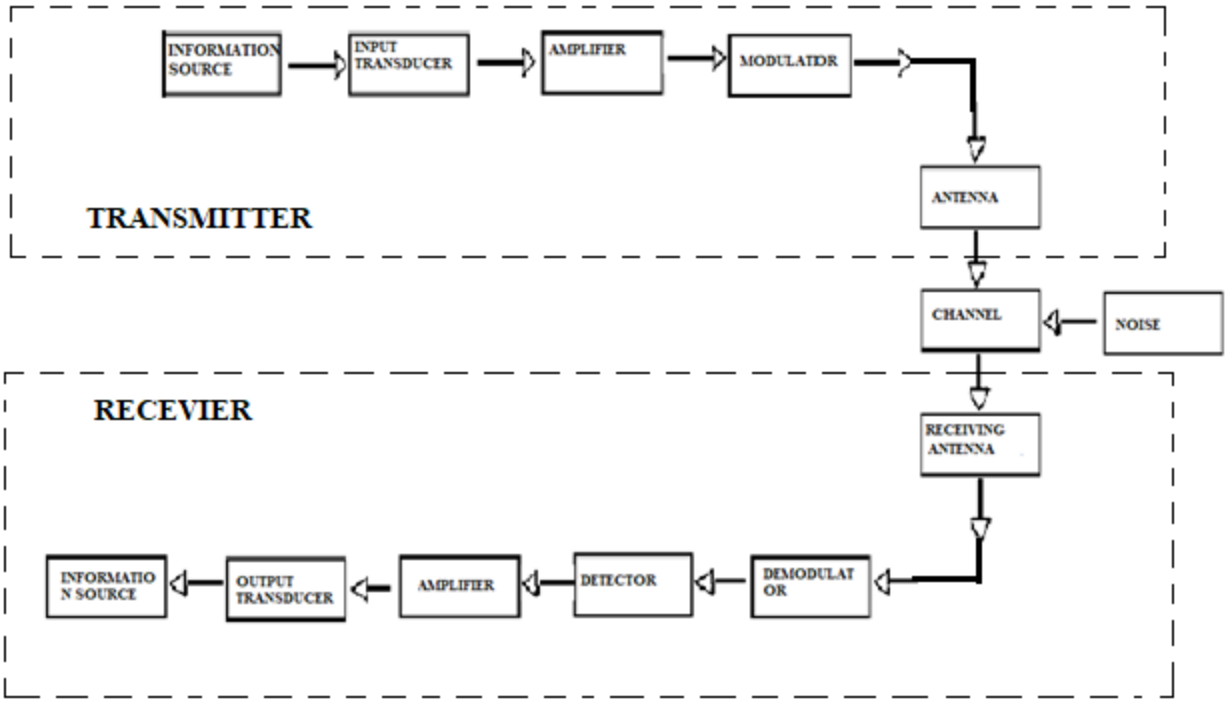
Repeaters

Repeaters are placed at different locations in between the transmitter and receiver. A repeater receives the transmitted signal, amplifies it and send it to the next repeater without distorting the original signal.



Block Diagram of Communication Systems

The block diagram given below represents the flow of the signal from the source to the destination. The role of every device and arrangement discussed above is better understood.



Difference between the Analog signals and Digital signals

Analog signals	Digital signals
Analog signals are difficult to get analysed at first.	Digital signals are easy to analyse.
Analog signals are more accurate than digital signals.	Digital signals are less accurate.
Analog signals take time to be stored. It has infinite memory.	Digital signals can be easily stored.
To record an analog signal, the technique used, preserves the original	In recording digital signal, the sample signals are taken and preserved.

signals.	
There is a continuous representation of signals in analog signals.	There is a discontinuous representation of signals in digital signals.
Analog signals produce too much noise.	Digital signals do not produce noise.
Examples of analog signals are Human voice, Thermometer, Analog phones etc.	Examples of digital signals are Computers, Digital Phones, Digital pens, etc.

Conversion of Analog signals to Digital signals

Most of the image sensors are in the analog signal, and digital processing cannot be applied on it, as it requires infinite memory to store because signals have an infinite value that is why we cannot store it.

To create a digital image we can convert data into digital form.

For the conversion there are two steps:

1. Sampling
2. Quantization

To convert an analog signal into a digital signal, both its axis(x,y) are converted into digital format.

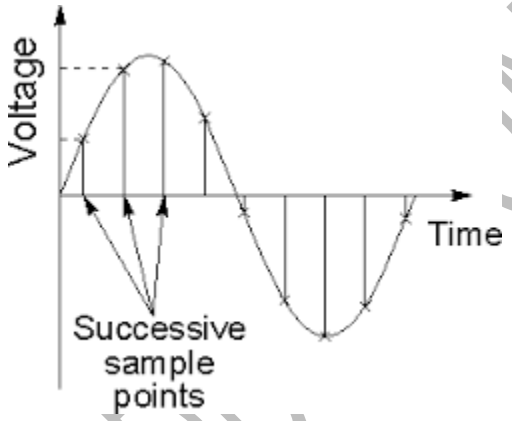


DIWAKAR EDUCA

As we can see that image is continuous in its coordinates(x-y). So sampling deals with digitizing of co-ordinates and quantization deals with digitizing the amplitude.

Sampling

In analog signals, there are continuous electrical signals that vary with time. With the help of subsystem, a sampler extracts continuous signals for the sampling of signals.



(Sampling of signals)

Sampling is done along the x-axis of signals that continuously differs with time. It is divided into two category one is sampling and other is downsampling.

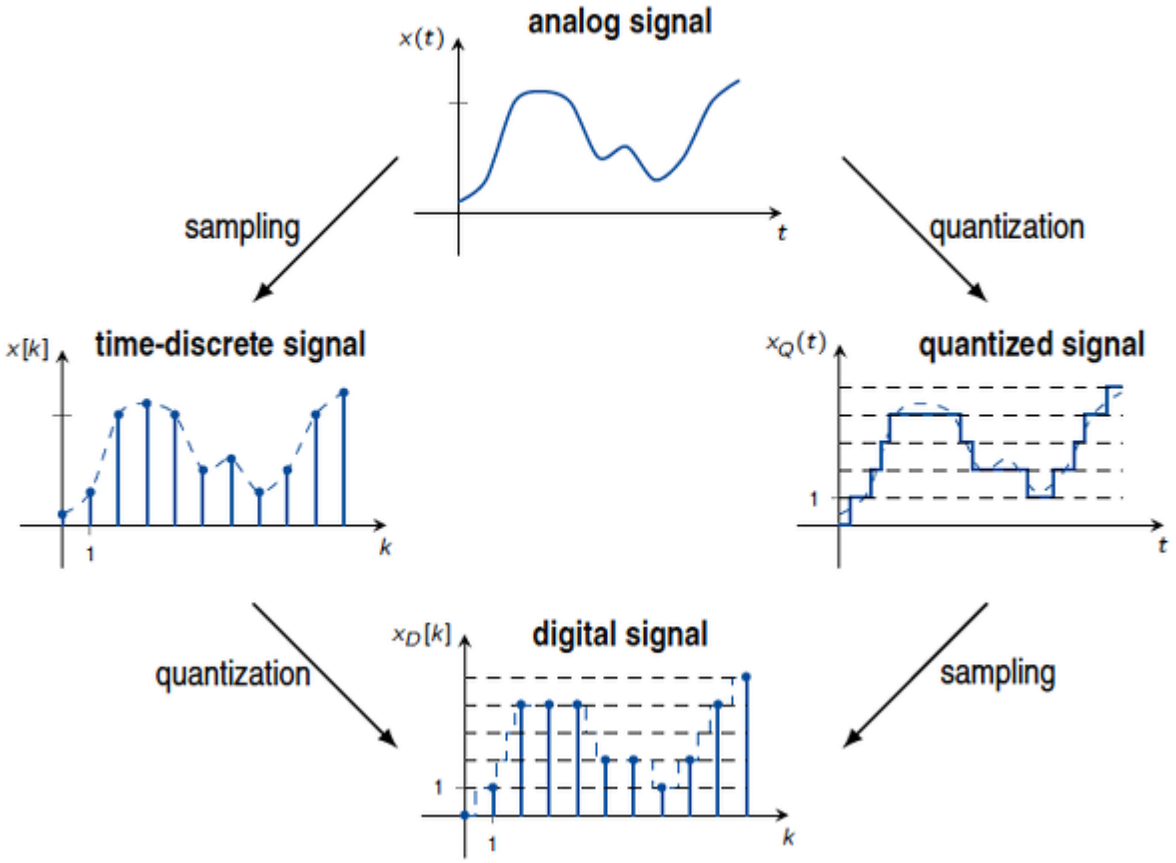
In downsampling, the range of values on the x-axis is always less.

Quantization

It is a process of image processing, in which continuous and time-varying values of analog signals are divided into non-overlapping discrete and unique values assigned to each subrange.

Sampling and quantization are opposite to each other. Sampling is done along the x-axis but quantization is done along the y-axis.

In the image processing, the sampled image is considered as a digital value. When there is a transition of states between time-varying values of image function and its digital equivalent signifies quantization.



(conversion of analog signals to digital signals).

The main problem in the image is the continuous occurrence of false contours which can be quantized later with inadequate brightness levels. The fine shading of the image depends on the level of quantization.

Noiseless Channel

An ideal channel in which no frames are lost, duplicated or corrupted is regarded as Noiseless Channel.

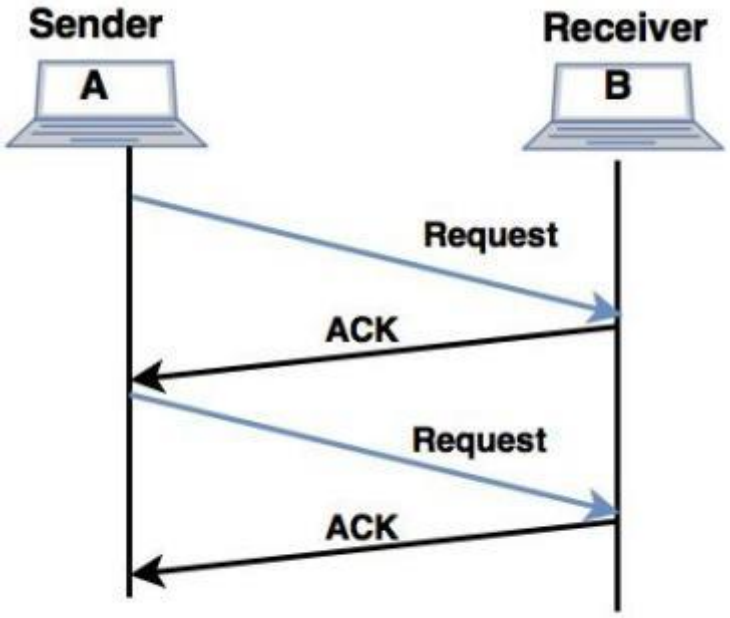
Simplest Protocol

- In simplest protocol, there is no flow control and error control mechanism. It is a unidirectional protocol in which data frames travel in only one direction (from sender to receiver).
- Also, the receiver can immediately handle any received frame with a processing time that is small enough to be negligible.
- The protocol consists of two distinct procedures :a sender and receiver. The sender runs in the data link layer of the source machine and the receiver runs in the data link layer of the destination machine. No sequence number or acknowledgements are used here.

Stop and Wait Protocol

- The simplest retransmission protocol is stop-and-wait.
- Transmitter (Station A) sends a frame over the communication line and then waits for a positive or negative acknowledgement from the receiver (station B).
- If no error occurs in the transmission, station B sends a positive acknowledgement (ACK) to station A.
- Now, the transmitter starts to send the next frame. If frame is received at station B with errors, then a negative acknowledgement(NAK) is sent to station A. In this case, station 'A' must retransmit the old packet in a new frame.
- There is also a possibility that the information frames or ACKs may get lost.
- Then, the sender is equipped with a timer. If no recognizable acknowledgement is received when the timer expires at the end of time out interval, the same frame is sent again.
- The sender which sends one frame and then waits for an acknowledgement before process is known as **stop and wait.**

DIWAKAR EDUCATION HUB



Stop and Wait

Noisy Channels

Consider the normal situation of a communication channel that makes errors. Frames may be either damaged or lost completely.

1. Stop and Wait Automatic Repeat Request

- In a noisy communication channel, if a frame is damaged in transit, the receiver hardware will detect this when it computes the checksum.
- If a damaged frame is received, it will be discarded and transmitter will retransmit the same frame after receiving a proper acknowledgement.
- If the acknowledgement frame gets lost and data link layer on 'A' eventually times out. Not having received an ACK, it assumes that its data frame was lost or damaged and sends the frame containing packet 1 again. This duplicate frame also arrives at data link layer on 'B', thus part of file will be duplicated and protocol is said to be failed.

DIWAKAR EDUCATION HUB

- A typical approach to solve this problem is the provision of a sequence number in the header of the message.
- The receiver can then check the sequence number determine if the message is a duplicate since only message is transmitted at any time.
- The sending and receiving station needs only 1-bit alternating sequence of '0' or '1' to maintain the relationship of the transmitted message and its ACK/ NAK.
- A modulo-2 numbering scheme is used where the frames are alternatively label with '0' or '1' and positive acknowledgements are of the form ACK 0 and ACK 1.

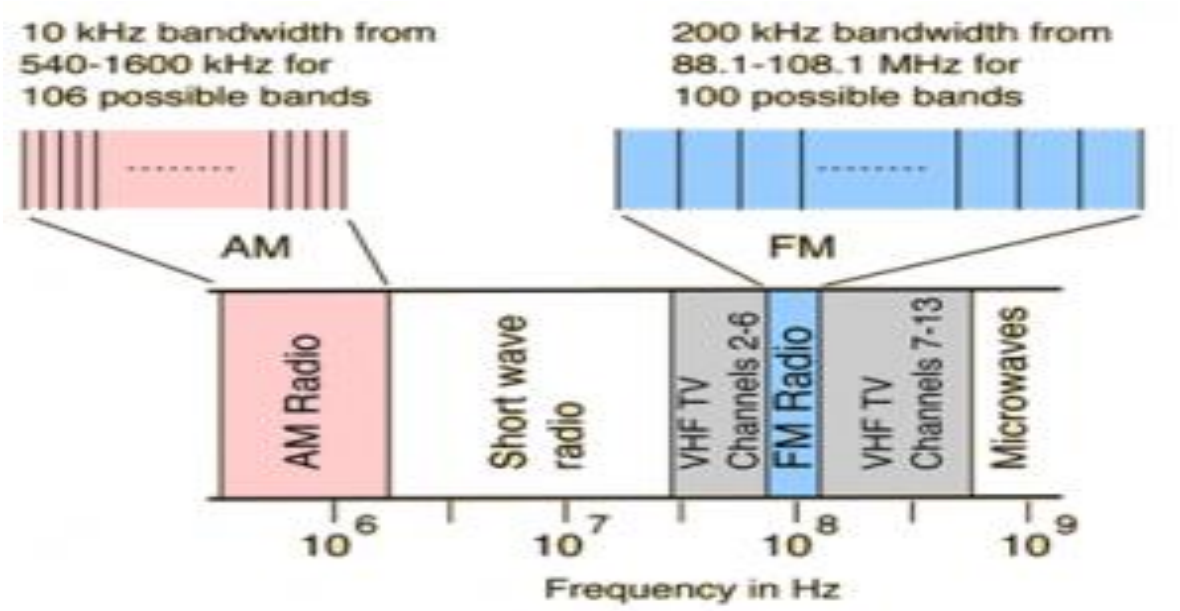
2. Sequence numbers

- The protocol specifies that frames need to be numbered. This is done by using sequence number. A field is added to the data frame to hold the sequence number of that frame.
- The sequence numbers are based on modulo-2 arithmetic.
- Stop-and-wait ARQ is the simplest mechanism for error and flow control.

Bandwidth

Bandwidth is a range of frequencies within a continuous set of frequencies. It is measured in Hertz. The purpose of a communication system is to transfer information from the transmitter which is located in one place to a receiver which is usually far away from the transmitter. When we send an email, we are sending it as bits of information to the receiver. This information is transported over the air or wire at a certain frequency depending on the mode chosen. Another factor at play is that the information can be in many forms; voice, video, photo, word document, etc. Luckily there is a very large spectrum of frequencies waiting for our bidding.

DIWAKAR EDUCATION HUB



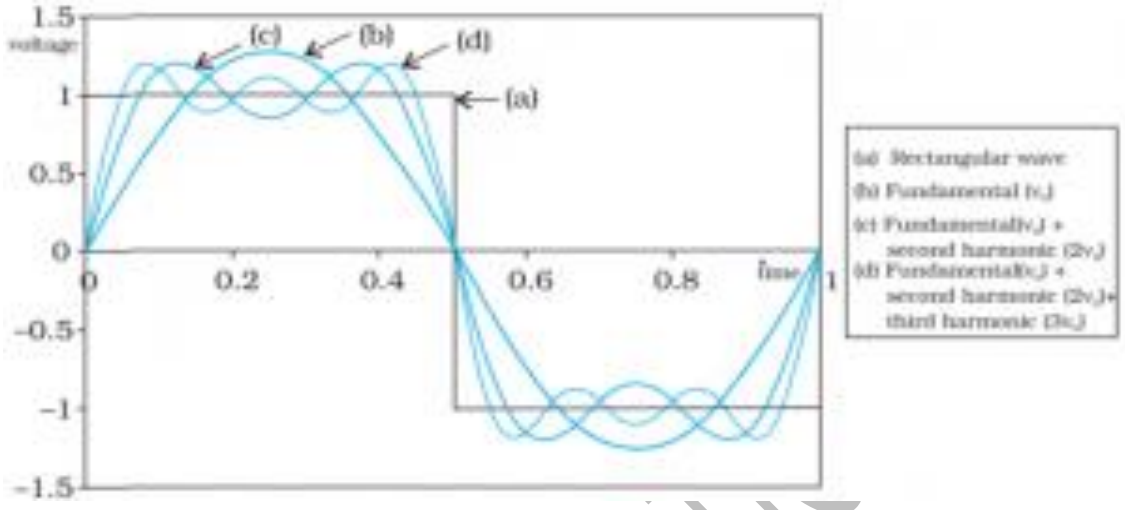
The smaller frequencies are used for long-distance communication and can travel unaffected over large distances, ie, less attenuation. Larger frequencies have greater energy and can carry more information but they are very inefficient and cannot be transmitted over long distances. One such set of frequencies are used for a very different purpose than others, ie the microwaves. For transmitting sounds or speech, the frequency range of 300 Hz to 3100 Hz is sufficient and hence the current telephones operate at a bandwidth of 2800 Hz. Transmission of music requires a bandwidth of the signal of 20 kHz because of the various instruments with a variety of pitches.

The audible range of a human is from 20 Hz to 20 kHz whereas a dog can hear from 50 Hz to 46 kHz. The key characteristic of bandwidth is that any band of a given width can carry the same amount of information, regardless of where the band is located in the frequency spectrum. For example, a 4kHz signal bandwidth can transmit a telephone conversation whether it is through lower frequency, like a wired telephone or modulated to a higher frequency, ie cell phone.

What we discussed till now was with respect to analog signals. Digital signals are in rectangular form, either on or off, ie 1 or 0. The sine wave is the fundamental waveform and every other kind of waveform (triangular, rectangular as in digital)

DIWAKAR EDUCATION

can be written as a combination of the fundamental sine wave. We get digital pulses when we superimpose sine waves of different harmonics.



Bandwidth of Transmission Medium

There are various methods of transmission, yes lots of them. From smoke signals and beating drums to the current fiber optics. The amount of data these various methods can transfer differ hugely. During the 1990's and the early 2000's, India had dial-up internet which was really slow but now with infrastructure changes we have faster internet. Wires are the most commonly used transmission media. A wire offers a bandwidth of approximately 750 MHz. The transmission over the air and free space range from a few hundred kHz to a few GHz. An optical fiber can offer a signal bandwidth of over 100 GHz. The bandwidths are allocated to radios, televisions and cellular communication companies by the government of the country.

Measurement of the Bandwidth of a Signal

Bandwidth is a key concept in several technological fields. In signal processing, it describes the difference between upper and lower frequencies in transmission signals like radio signals, etc. The **measurement of the bandwidth** of a signal is done in hertz (Hz). Depending on the context, the bandwidth may specifically be referred to passband bandwidth or base bandwidth.

DIWAKAR EDUCATION

A signal processing system works efficiently over a finite range of frequencies. Within this band of frequencies, the response of a system is flat. Outside this band, the frequency response gradually drops off. The boundary in a system's frequency response at which the energy flowing through a system reduces rather than passing through is known as the cutoff frequency. A passband bandwidth is a difference between the upper and lower cut off frequency and a baseband bandwidth equals the highest frequency of a system. Bandwidth in hertz is a central concept in many fields like electronics, radio communications, digital communications, information theory, etc.

Latency

Latency is the time it takes for a packet to get across the network, from source to destination. It is measured in units of time — ms (millisecond, or 1/1,000 of a second).

The time taken for a packet to be transferred across a network. We can measure this as one-way to its destination or as a round trip.

What Causes Network Latency?

Network latency can be caused by a range of issues but generally, it comes down to the state of routers and the distance between our network devices. **The more routers a packet has to travel through the more latency** there is because each router has to process the packet. In most cases, this latency isn't noticeable but when traffic travels across the internet it can be more pronounced (because the number of routers the packet passes through increases).

The distance that a packet travels can also have a significant influence on the amount of latency within a network. **A packet that travels around the world would have at least 250 ms of latency**. In enterprise-level networks, latency is present to a lesser extent. When packets travel across a network to their destination, they rarely travel to the node in a straight line. As such the amount of latency is dependent on the route that the packet takes.

DIWAKAR EDUCATION HUB

On a well-designed network, efficient routes should be available so that packets arrive promptly at their destination. If the network is poorly-designed with indirect network paths then latency is going to be much more pronounced.

Throughput

The quantity of data being sent and received within a unit of time.

Throughput is the actual amount of data that is successfully sent/received over the communication link. Throughput is presented as kbps, Mbps or Gbps, and can differ from bandwidth due to a range of technical issues, including latency, packet loss, jitter and more.

Throughput is the actual speed with which data gets transferred over the network. Besides transmitting the actual data, network bandwidth is used for transmitting error messages, acknowledgement frames, etc.

Throughput is a better measurement of network speed, efficiency and capacity utilization rather than bandwidth.

What Causes Poor Network Throughput?

Poor network throughput can be caused by several factors. One of the main culprits is **poor hardware performance**. If devices like routers are experiencing performance degradation, faults, or are simply outdated then our can end up with low throughput. Likewise, if computer networks are congested with lots of traffic then packet loss will occur. Packet loss is where data packets are lost in transit. Low network throughput is often caused when packets are lost in transit.

Why are Network Latency and Throughput Important?

Both network latency and throughput are important because they have an effect on how well our network is performing. If latency is too high then packets will take a longer amount of time to reach their destination. The more time it takes for packets to reach their destination, the slower devices, services, and applications will operate within the network. Likewise, the lower the amount of

DIWAKAR EDUCATION HUB

throughput, the lower the number of packets being processed in a specific time period.

The moment latency gets too high or throughput falls, then our network is going to grind to a halt. This is the point at which services will start to perform sluggishly as packets fail to reach their destination at a speed that can sustain the full operation of our network.

It is **important to measure network latency and throughput** because it allows us to check that our network isn't falling victim to poor performance. There are many ways that we can measure latency and throughput but the simplest way is to use a network monitoring tool. This type of tool will be able to tell us when latency and throughput have reached problematic levels.

Protocol

Protocol is a set of rules and regulations used by devices to communicate over the network. Just like humans, computers also need rules to ensure successful communication. If two people start speaking at the same time or in different languages when no interpreter is present, no meaningful exchange of information can occur.

Similarly, devices connected on the network need to follow rules defining situations like when and how to transmit data, when to receive data, how to give error-free message, etc.

Some common protocols used over the Internet are –

- Transmission Control Protocol
- Internet Protocol
- Point to Point Protocol
- File Transfer Protocol
- Hypertext Transfer Protocol

DIWAKAR EDUCATION HUB

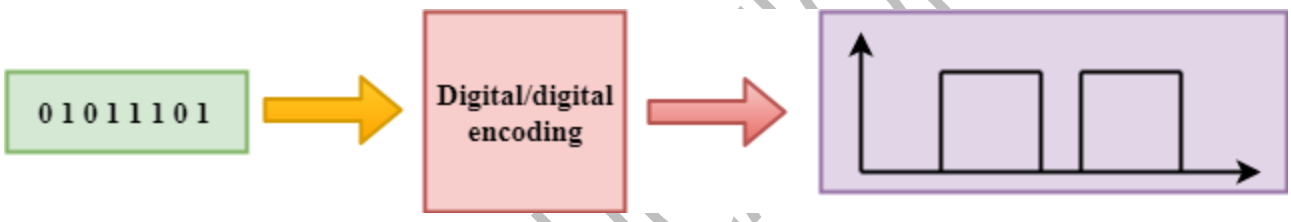
- Internet Message Access Protocol

Digital Transmission

Data can be represented either in analog or digital form. The computers used the digital form to store the information. Therefore, the data needs to be converted in digital form so that it can be used by a computer.

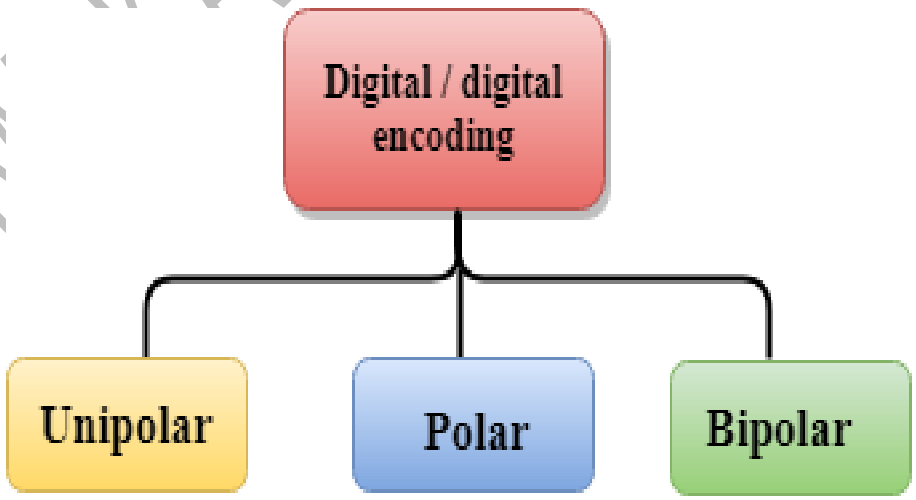
DIGITAL-TO-DIGITAL CONVERSION

Digital-to-digital encoding is the representation of digital information by a digital signal. When binary 1s and 0s generated by the computer are translated into a sequence of voltage pulses that can be propagated over a wire, this process is known as digital-to-digital encoding.



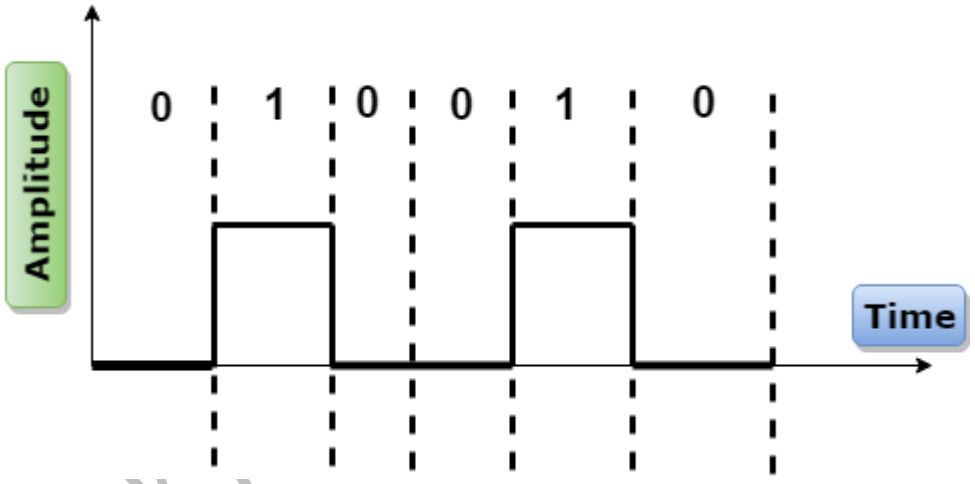
Digital-to-digital encoding is divided into three categories:

- Unipolar Encoding
- Polar Encoding
- Bipolar Encoding



Unipolar

- Digital transmission system sends the voltage pulses over the medium link such as wire or cable.
- In most types of encoding, one voltage level represents 0, and another voltage level represents 1.
- The polarity of each pulse determines whether it is positive or negative.
- This type of encoding is known as Unipolar encoding as it uses only one polarity.
- In Unipolar encoding, the polarity is assigned to the 1 binary state.
- In this, 1s are represented as a positive value and 0s are represented as a zero value.
- In Unipolar Encoding, '1' is considered as a high voltage and '0' is considered as a zero voltage.
- Unipolar encoding is simpler and inexpensive to implement.

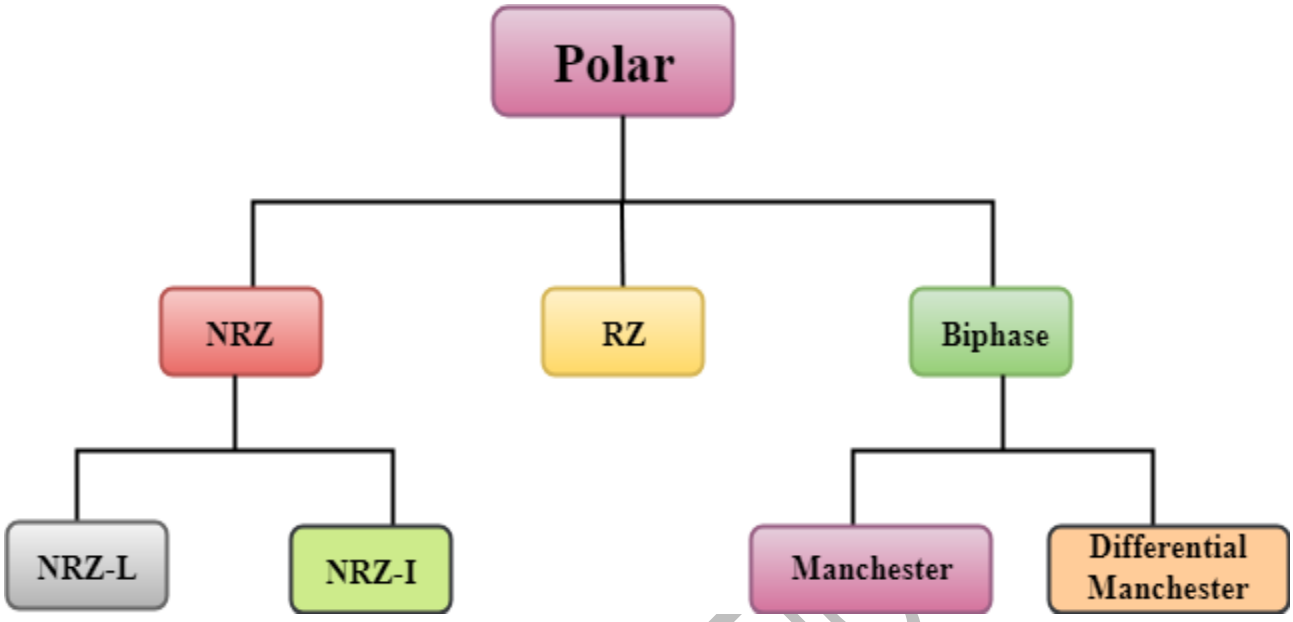


Unipolar encoding has two problems that make this scheme less desirable:

- DC Component
- Synchronization

Polar

- Polar encoding is an encoding scheme that uses two voltage levels: one is positive, and another is negative.
- By using two voltage levels, an average voltage level is reduced, and the DC component problem of unipolar encoding scheme is alleviated.



NRZ

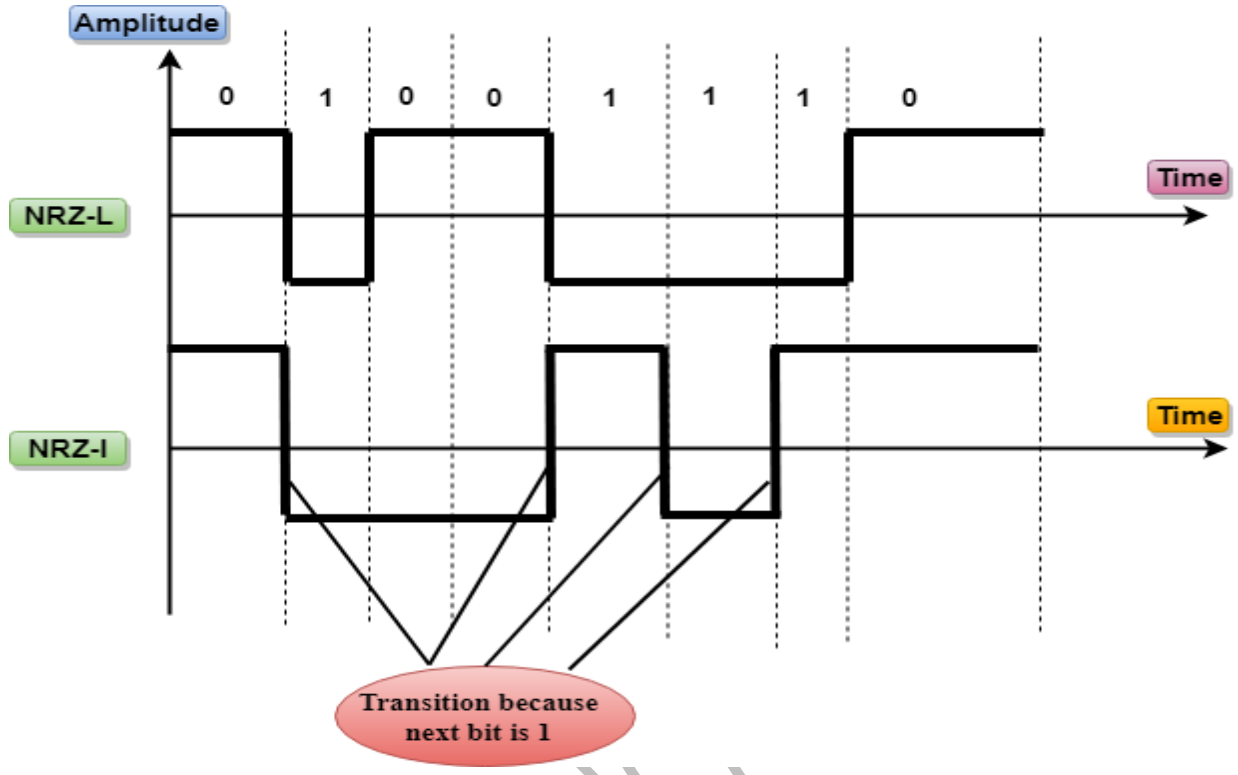
- NRZ stands for Non-return zero.
- In NRZ encoding, the level of the signal can be represented either positive or negative.

The two most common methods used in NRZ are:

NRZ-L: In NRZ-L encoding, the level of the signal depends on the type of the bit that it represents. If a bit is 0 or 1, then their voltages will be positive and negative respectively. Therefore, we can say that the level of the signal is dependent on the state of the bit.

NRZ-I: NRZ-I is an inversion of the voltage level that represents 1 bit. In the NRZ-I encoding scheme, a transition occurs between the positive and negative voltage that represents 1 bit. In this scheme, 0 bit represents no change and 1 bit represents a change in voltage level.

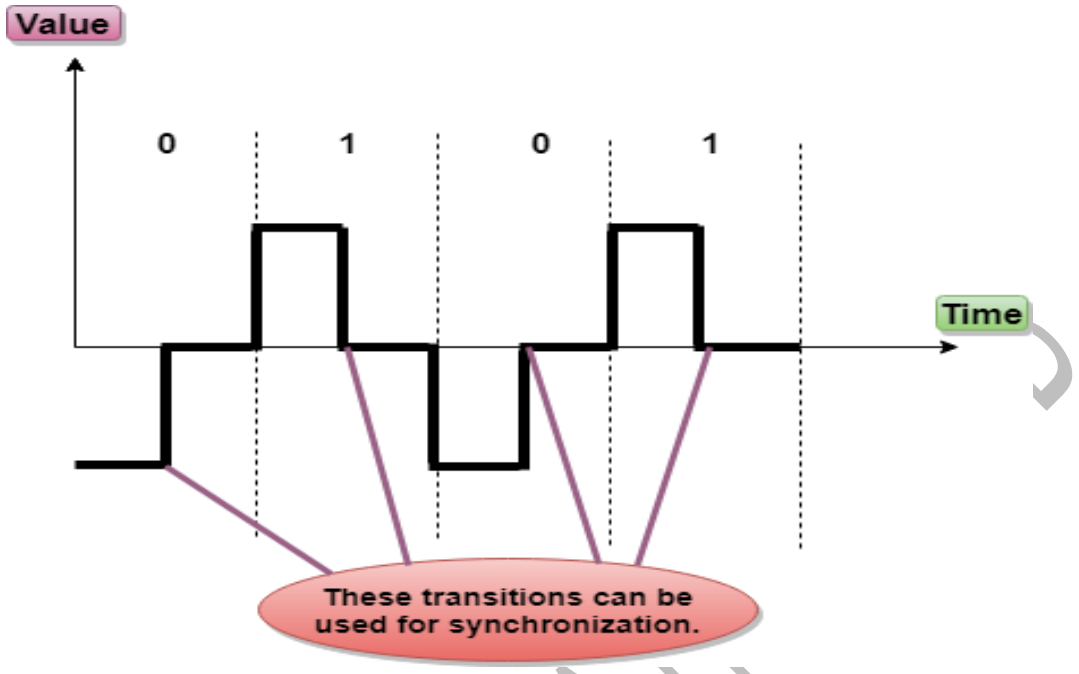
DIWAKAR EDUCATION



RZ

- RZ stands for Return to zero.
- There must be a signal change for each bit to achieve synchronization. However, to change with every bit, we need to have three values: positive, negative and zero.
- RZ is an encoding scheme that provides three values, positive voltage represents 1, the negative voltage represents 0, and zero voltage represents none.
- In the RZ scheme, halfway through each interval, the signal returns to zero.
- In RZ scheme, 1 bit is represented by positive-to-zero and 0 bit is represented by negative-to-zero.

DIWAKAR EDUC



Disadvantage of RZ:

It performs two signal changes to encode one bit that acquires more bandwidth.

Biphase

- Biphase is an encoding scheme in which signal changes at the middle of the bit interval but does not return to zero.

Biphase encoding is implemented in two different ways:

Manchester

- It changes the signal at the middle of the bit interval but does not return to zero for synchronization.
- In Manchester encoding, a negative-to-positive transition represents binary 1, and positive-to-negative transition represents 0.
- Manchester has the same level of synchronization as RZ scheme except that it has two levels of amplitude.

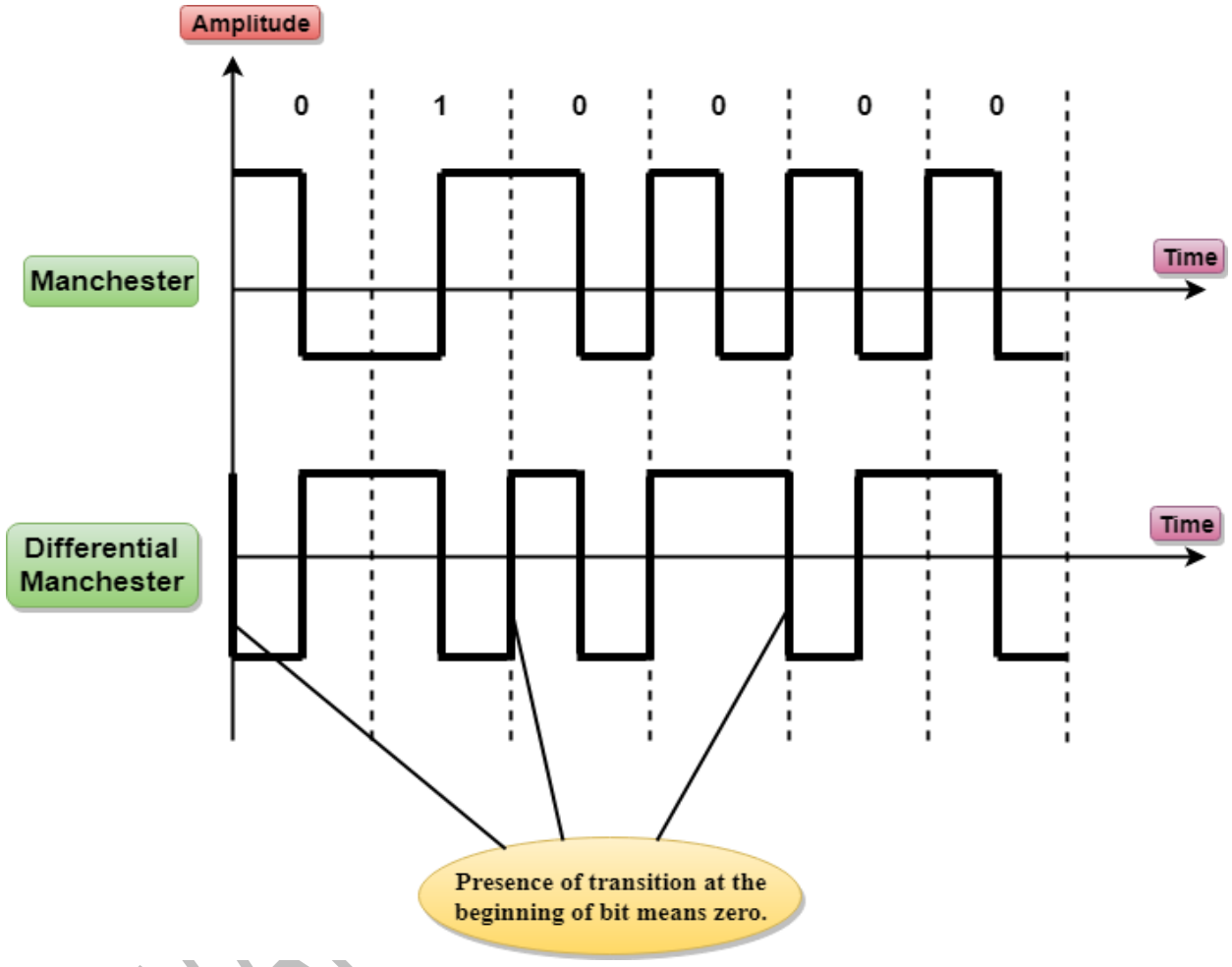
Differential Manchester

- It changes the signal at the middle of the bit interval for synchronization, but the presence or absence of the transition at the beginning of the

DIWAKAR EDUCATION

interval determines the bit. A transition means binary 0 and no transition means binary 1.

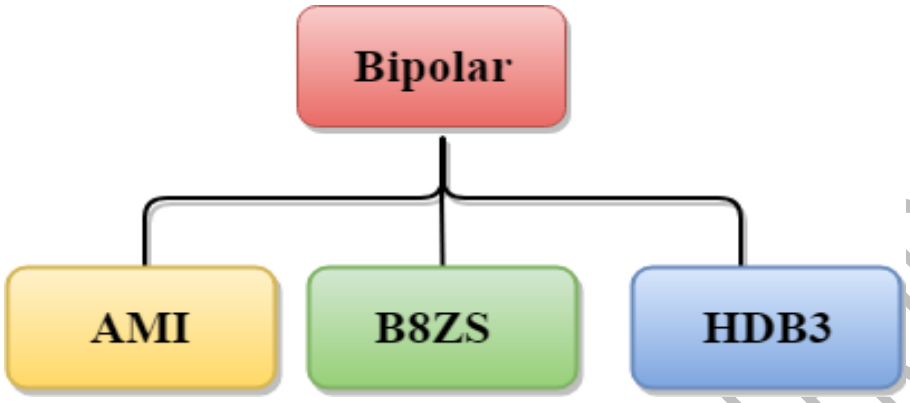
- In Manchester Encoding scheme, two signal changes represent 0 and one signal change represent 1.



Bipolar

- Bipolar encoding scheme represents three voltage levels: positive, negative, and zero.
- In Bipolar encoding scheme, zero level represents binary 0, and binary 1 is represented by alternating positive and negative voltages.
- If the first 1 bit is represented by positive amplitude, then the second 1 bit is represented by negative voltage, third 1 bit is represented by the positive amplitude and so on. This alternation can also occur even when the 1bits are not consecutive.

Bipolar can be classified as:



AMI

- AMI stands for **alternate mark inversion** where mark work comes from telegraphy which means 1. So, it can be redefined as **alternate 1 inversion**.
- In Bipolar AMI encoding scheme, 0 bit is represented by zero level and 1 bit is represented by alternating positive and negative voltages.

Advantage:

- DC component is zero.
- Sequence of 1s bits are synchronized.

Disadvantage:

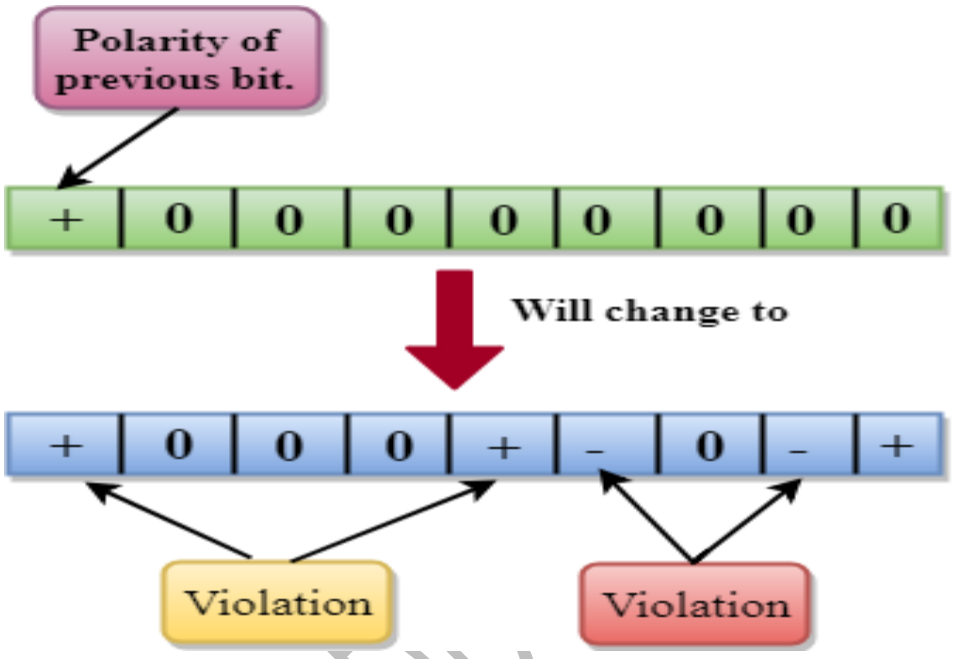
- This encoding scheme does not ensure the synchronization of a long string of 0s bits.

B8ZS

- B8ZS stands for **Bipolar 8-Zero Substitution**.
- This technique is adopted in North America to provide synchronization of a long sequence of 0s bits.
- In most of the cases, the functionality of B8ZS is similar to the bipolar AMI, but the only difference is that it provides the synchronization when a long sequence of 0s bits occur.
- B8ZS ensures synchronization of a long string of 0s by providing force artificial signal changes called violations, within 0 string pattern.

DIWAKAR EDUCATION HUB

- When eight 0 occurs, then B8ZS implements some changes in 0s string pattern based on the polarity of the previous 1 bit.
- If the polarity of the previous 1 bit is positive, the eight 0s will be encoded as zero, zero, zero, positive, negative, zero, negative, positive.

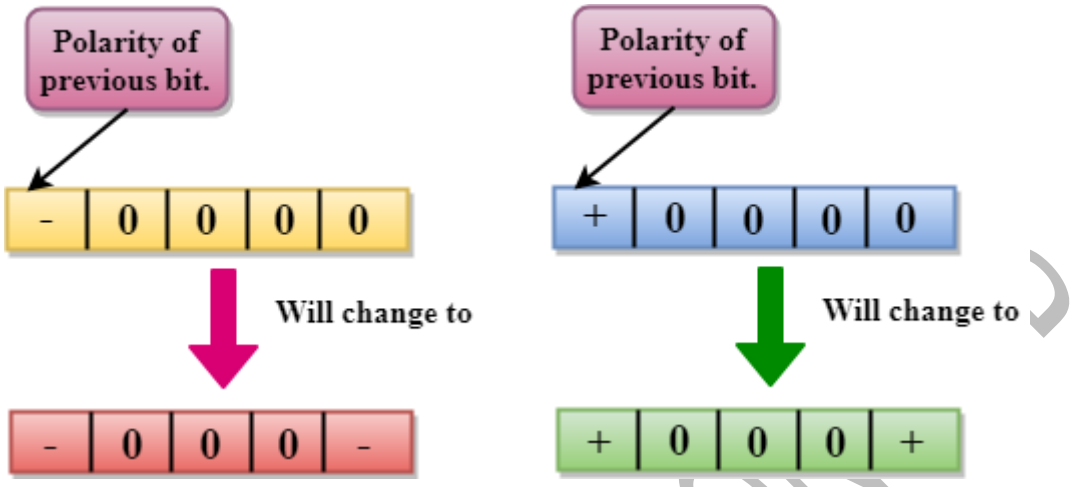


- If the polarity of previous 1 bit is negative, then the eight 0s will be encoded as zero, zero, zero, negative, positive, zero, positive, negative.

HDB3

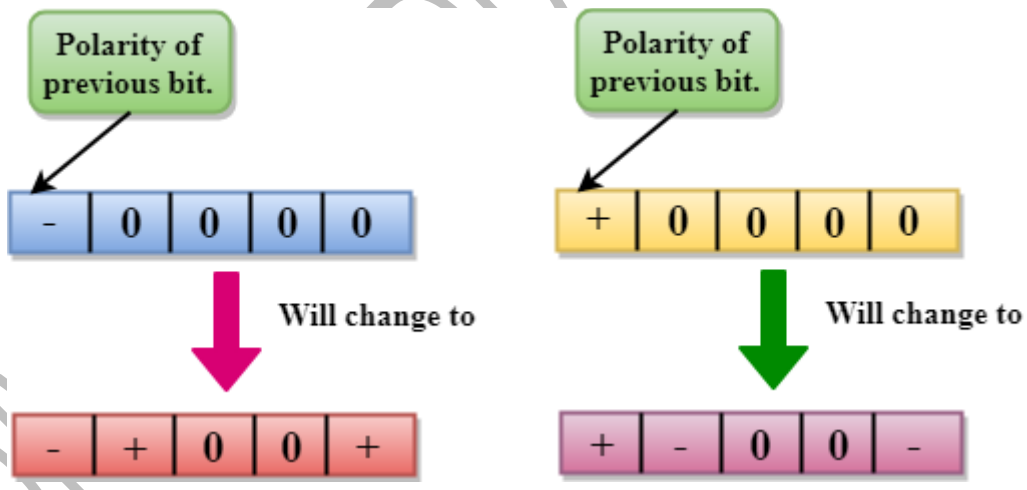
- HDB3 stands for **High-Density Bipolar 3**.
- HDB3 technique was first adopted in Europe and Japan.
- HDB3 technique is designed to provide the synchronization of a long sequence of 0s bits.
- In the HDB3 technique, the pattern of violation is based on the polarity of the previous bit.
- When four 0s occur, HDB3 looks at the number of 1s bits occurred since the last substitution.
- If the number of 1s bits is odd, then the violation is made on the fourth consecutive of 0. If the polarity of the previous bit is positive, then the violation is positive. If the polarity of the previous bit is negative, then the violation is negative.

If the number of 1s bits since the last substitution is odd.



If the number of 1s bits is even, then the violation is made on the place of the first and fourth consecutive 0s. If the polarity of the previous bit is positive, then violations are negative, and if the polarity of the previous bit is negative, then violations are positive.

If the number of 1s bits since the last substitution is even.



ANALOG-TO-DIGITAL CONVERSION

- When an analog signal is digitalized, this is called an analog-to-digital conversion.
- Suppose human sends a voice in the form of an analog signal, we need to digitalize the analog signal which is less prone to noise. It requires a

reduction in the number of values in an analog message so that they can be represented in the digital stream.

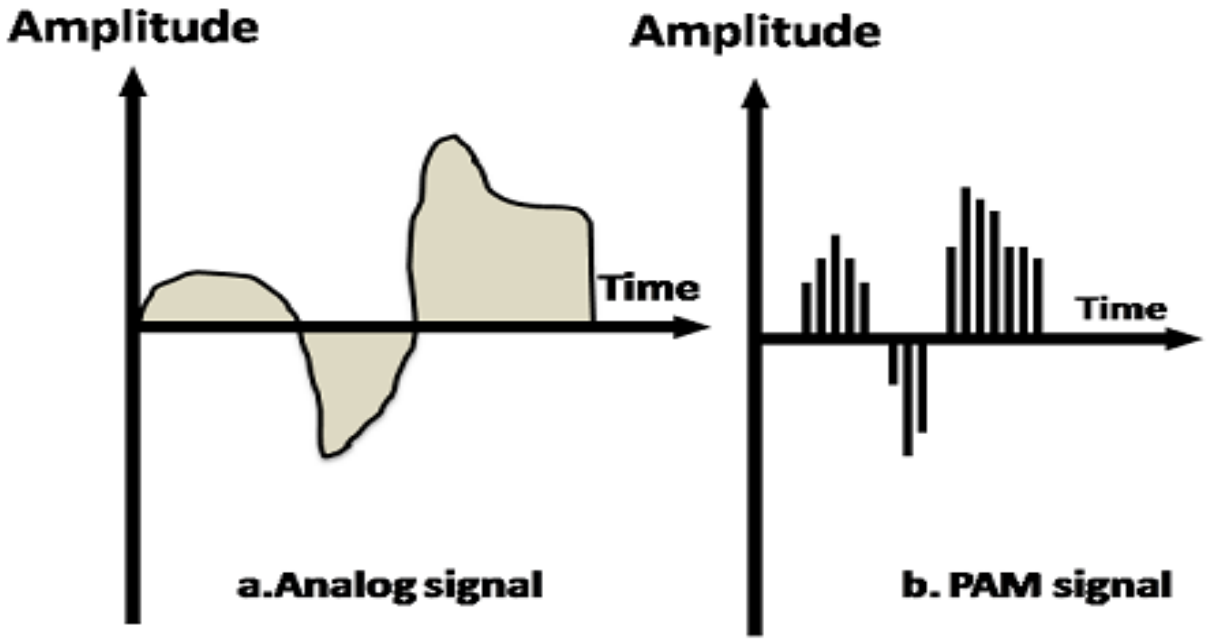
- In analog-to-digital conversion, the information contained in a continuous wave form is converted in digital pulses.

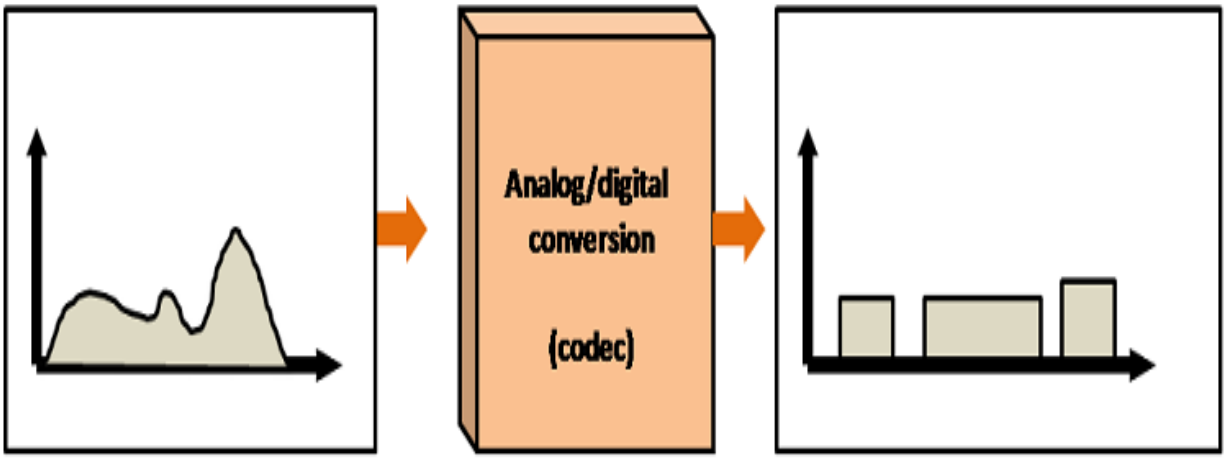
Techniques for Analog-To-Digital Conversion

PAM

- PAM stands for **pulse amplitude modulation**.
- PAM is a technique used in analog-to-digital conversion.
- PAM technique takes an analog signal, samples it, and generates a series of digital pulses based on the result of sampling where sampling means measuring the amplitude of a signal at equal intervals.
- PAM technique is not useful in data communication as it translates the original wave form into pulses, but these pulses are not digital. To make them digital, PAM technique is modified to PCM technique.

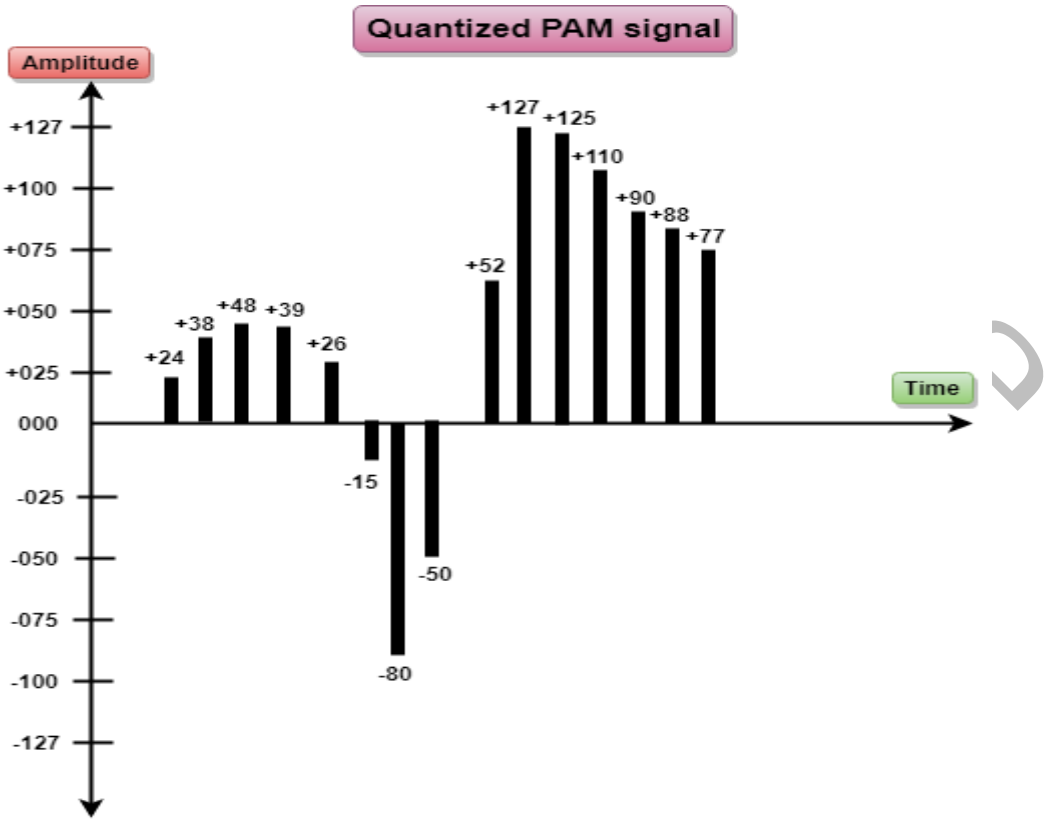
DIWAKAR EDUCATION HUB



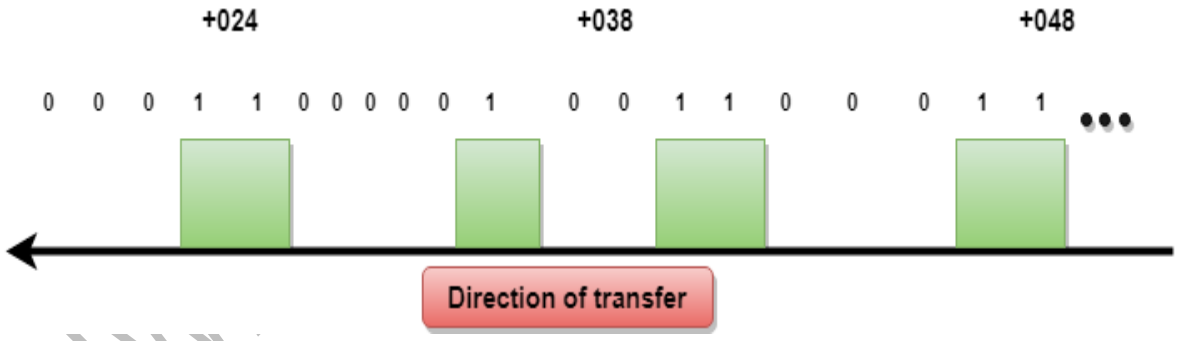


PCM

- PCM stands for **Pulse Code Modulation**.
- PCM technique is used to modify the pulses created by PAM to form a digital signal. To achieve this, PCM quantizes PAM pulses. Quantization is a process of assigning integral values in a specific range to sampled instances.
- PCM is made of four separate processes: PAM, quantization, binary encoding, and digital-to-digital encoding.



PCM



Analog Transmission

To send the digital data over an analog media, it needs to be converted into analog signal.There can be two cases according to data formatting.

Bandpass: The filters are used to filter and pass frequencies of interest. A bandpass is a band of frequencies which can pass the filter.

Low-pass: Low-pass is a filter that passes low frequencies signals.

When digital data is converted into a bandpass analog signal, it is called digital-to-analog conversion. When low-pass analog signal is converted into bandpass analog signal, it is called analog-to-analog conversion.

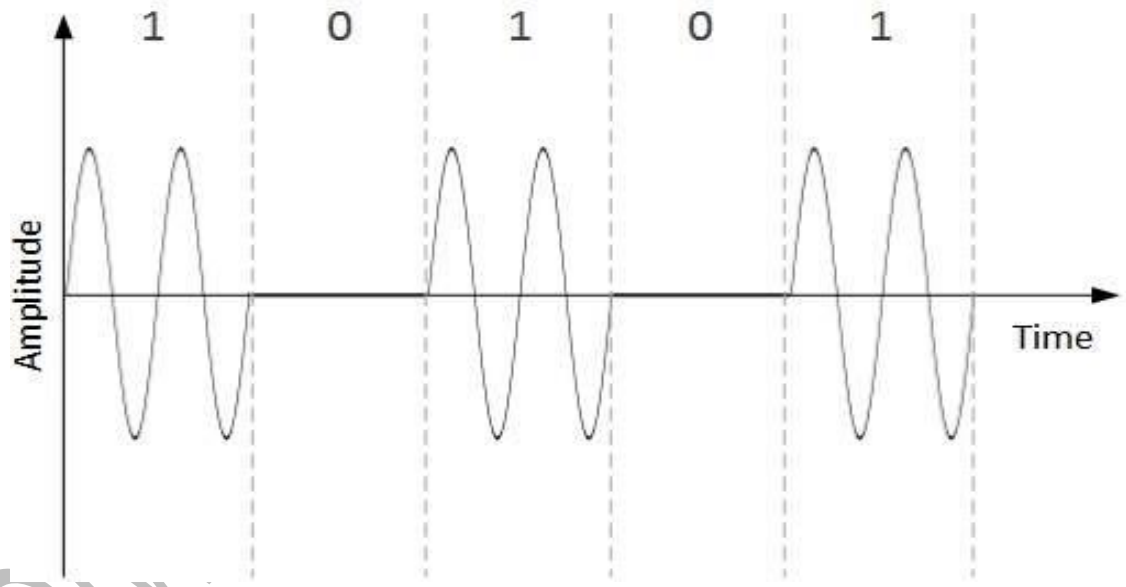
Digital-to-Analog Conversion

When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data.

An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions:

Amplitude Shift Keying

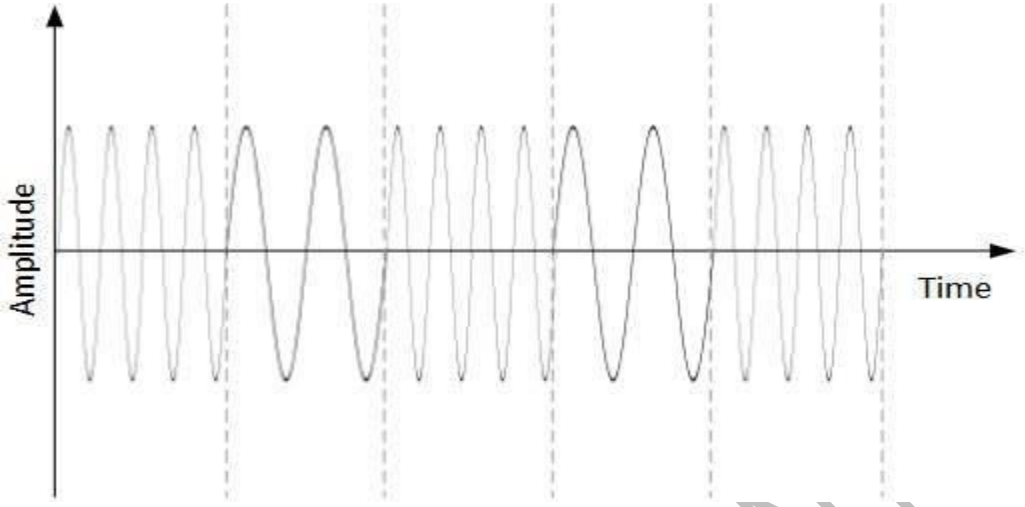
In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data.



When binary data represents digit 1, the amplitude is held; otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal.

Frequency Shift Keying

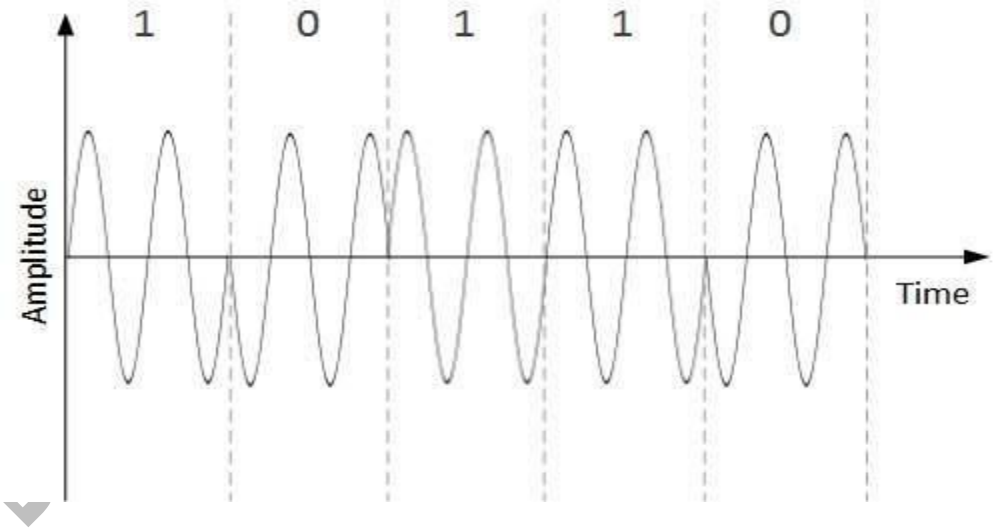
In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.



This technique uses two frequencies, f1 and f2. One of them, for example f1, is chosen to represent binary digit 1 and the other one is used to represent binary digit 0. Both amplitude and phase of the carrier wave are kept intact.

Phase Shift Keying

In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.



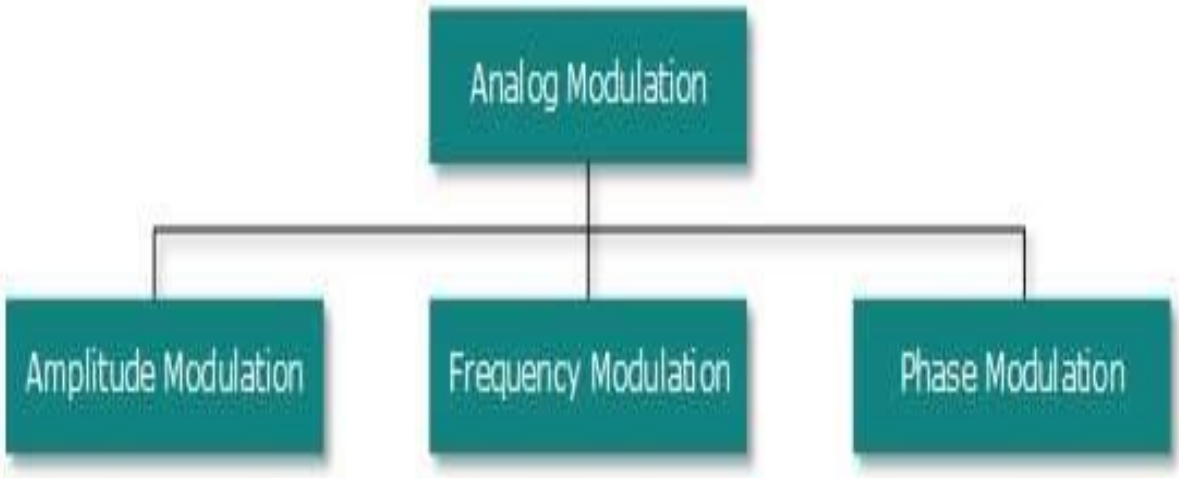
When a new binary symbol is encountered, the phase of the signal is altered. Amplitude and frequency of the original carrier signal is kept intact.

Quadrature Phase Shift Keying

QPSK alters the phase to reflect two binary digits at once. This is done in two different phases. The main stream of binary data is divided equally into two sub-streams. The serial data is converted in to parallel in both sub-streams and then each stream is converted to digital signal using NRZ technique. Later, both the digital signals are merged together.

Analog-to-Analog Conversion

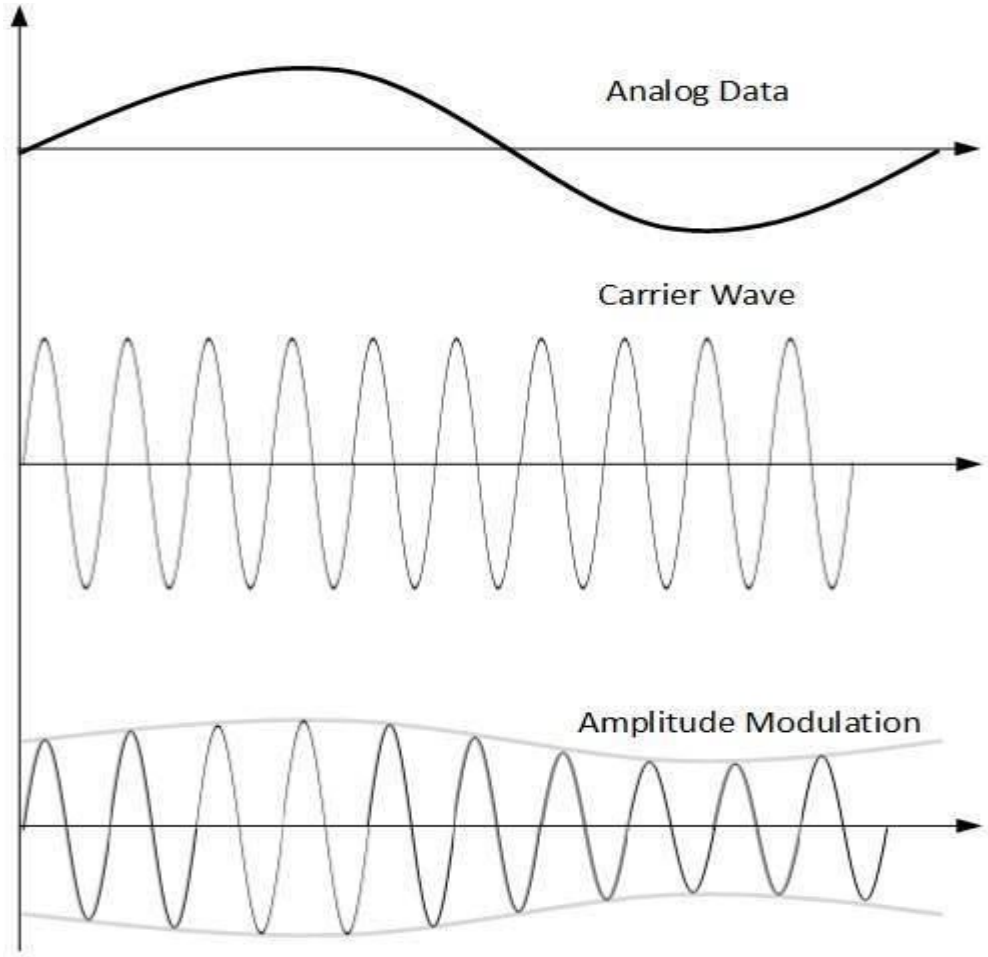
Analog signals are modified to represent analog data. This conversion is also known as Analog Modulation. Analog modulation is required when bandpass is used. Analog to analog conversion can be done in three ways:



Amplitude Modulation

In this modulation, the amplitude of the carrier signal is modified to reflect the analog data.

DIWAKAR



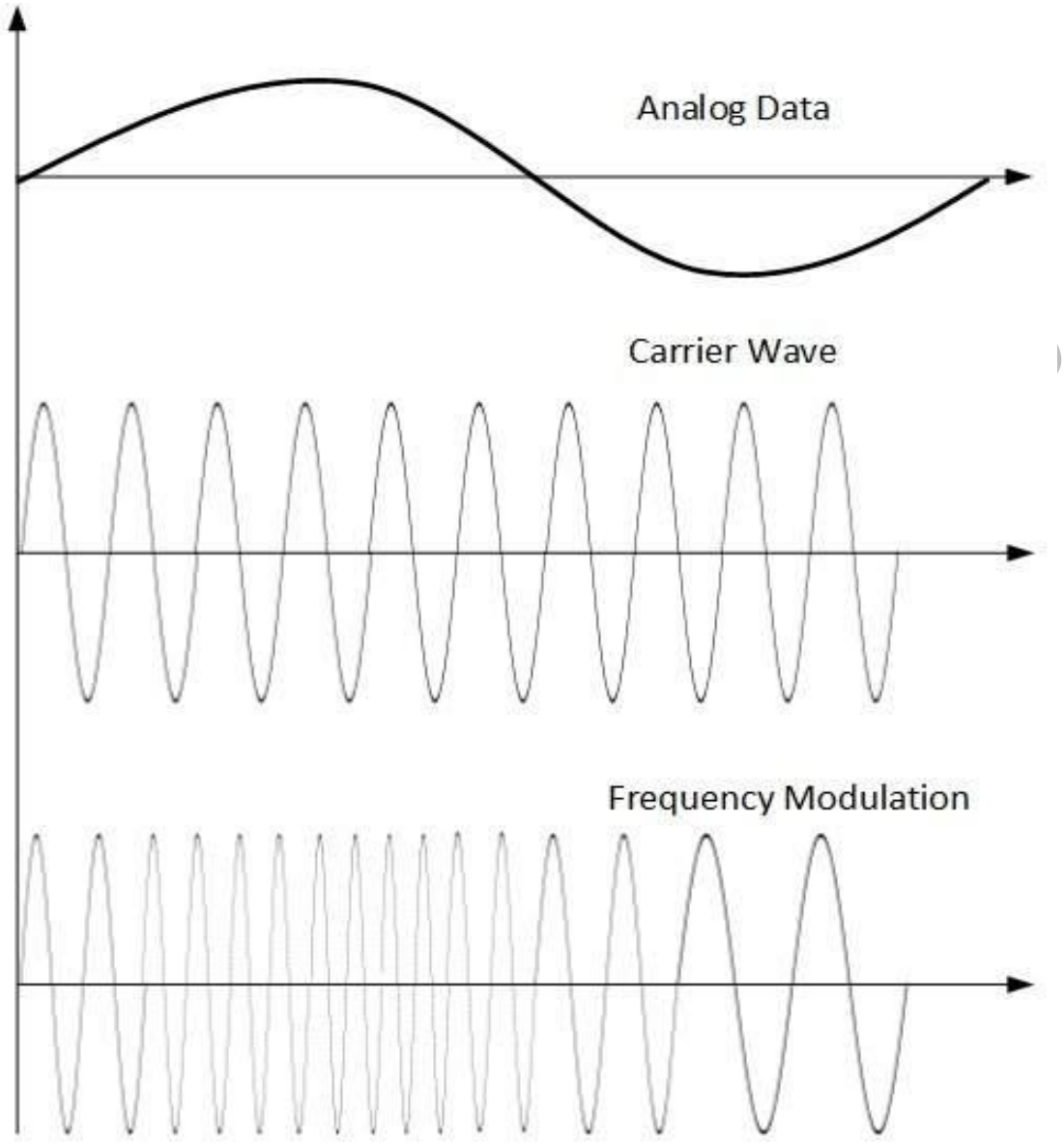
Amplitude modulation is implemented by means of a multiplier. The amplitude of modulating signal (analog data) is multiplied by the amplitude of carrier frequency, which then reflects analog data.

The frequency and phase of carrier signal remain unchanged.

Frequency Modulation

In this modulation technique, the frequency of the carrier signal is modified to reflect the change in the voltage levels of the modulating signal (analog data).

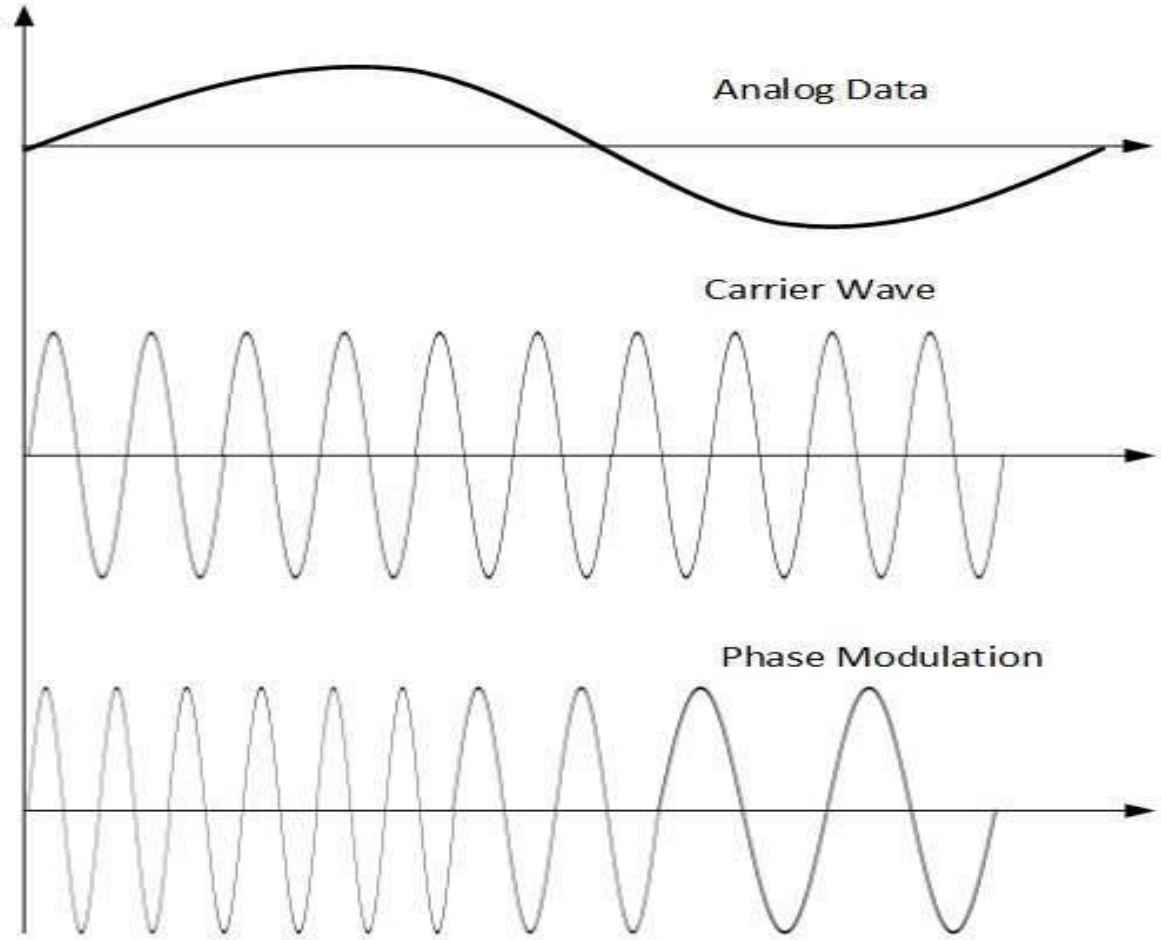
DIWAKAR



The amplitude and phase of the carrier signal are not altered.

Phase Modulation

In the modulation technique, the phase of carrier signal is modulated in order to reflect the change in voltage (amplitude) of analog data signal.



Phase modulation is practically similar to Frequency Modulation, but in Phase modulation frequency of the carrier signal is not increased. Frequency of carrier is signal is changed (made dense and sparse) to reflect voltage change in the amplitude of modulating signal.

Data Encoding Techniques

Encoding is the process of converting the data or a given sequence of characters, symbols, alphabets etc., into a specified format, for the secured transmission of data. **Decoding** is the reverse process of encoding which is to extract the information from the converted format.

Data Encoding

Encoding is the process of using various patterns of voltage or current levels to represent **1s** and **0s** of the digital signals on the transmission link.

The common types of line encoding are Unipolar, Polar, Bipolar, and Manchester.

Encoding Techniques

The data encoding technique is divided into the following types, depending upon the type of data conversion.

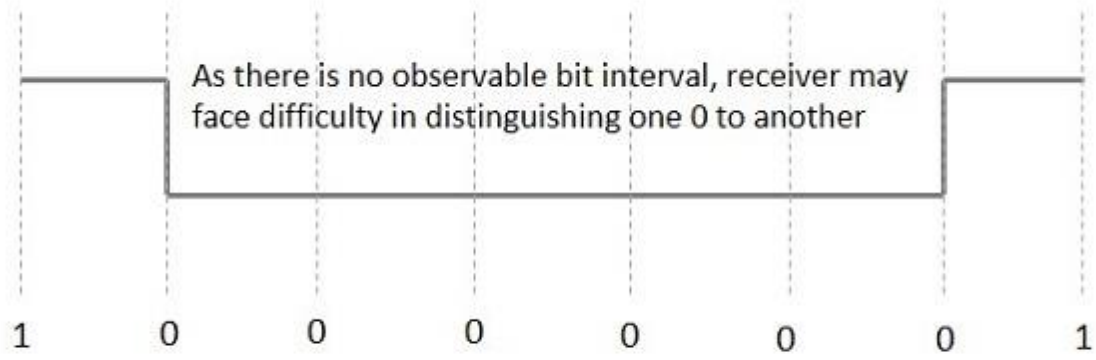
- **Analog data to Analog signals** − The modulation techniques such as Amplitude Modulation, Frequency Modulation and Phase Modulation of analog signals, fall under this category.
- **Analog data to Digital signals** − This process can be termed as digitization, which is done by Pulse Code Modulation PCMPCM. Hence, it is nothing but digital modulation. As we have already discussed, sampling and quantization are the important factors in this. Delta Modulation gives a better output than PCM.
- **Digital data to Analog signals** − The modulation techniques such as Amplitude Shift Keying ASKASK, Frequency Shift Keying FSKFSK, Phase Shift Keying PSKPSK, etc., fall under this category. These will be discussed in subsequent chapters.
- **Digital data to Digital signals** − These are in this section. There are several ways to map digital data to digital signals. Some of them are −

Non Return to Zero NRZNRZ

NRZ Codes has **1** for High voltage level and **0** for Low voltage level. The main behavior of NRZ codes is that the voltage level remains constant during bit interval. The end or start of a bit will not be indicated and it will maintain the same voltage state, if the value of the previous bit and the value of the present bit are same.

The following figure explains the concept of NRZ coding.

DIWAKAR EDUCATION HUB



NRZ Coding

If the above example is considered, as there is a long sequence of constant voltage level and the clock synchronization may be lost due to the absence of bit interval, it becomes difficult for the receiver to differentiate between 0 and 1.

There are two variations in NRZ namely –

NRZ - L NRZ–LEVELNRZ–LEVEL

There is a change in the polarity of the signal, only when the incoming signal changes from 1 to 0 or from 0 to 1. It is the same as NRZ, however, the first bit of the input signal should have a change of polarity.

NRZ - I NRZ–INVERTEDNRZ–INVERTED

If a **1** occurs at the incoming signal, then there occurs a transition at the beginning of the bit interval. For a **0** at the incoming signal, there is no transition at the beginning of the bit interval.

NRZ codes has a **disadvantage** that the synchronization of the transmitter clock with the receiver clock gets completely disturbed, when there is a string of **1s** and **0s**. Hence, a separate clock line needs to be provided.

Bi-phase Encoding

The signal level is checked twice for every bit time, both initially and in the middle. Hence, the clock rate is double the data transfer rate and thus the

DIWAKAR EDUCATION

modulation rate is also doubled. The clock is taken from the signal itself. The bandwidth required for this coding is greater.

There are two types of Bi-phase Encoding.

- Bi-phase Manchester
- Differential Manchester

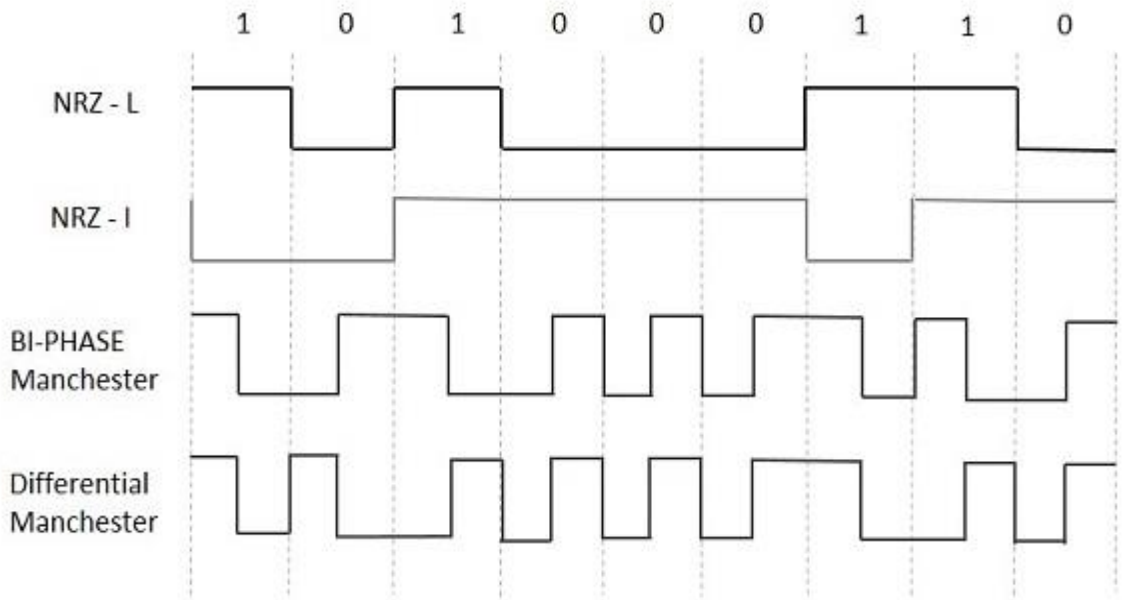
Bi-phase Manchester

In this type of coding, the transition is done at the middle of the bit-interval. The transition for the resultant pulse is from High to Low in the middle of the interval, for the input bit 1. While the transition is from Low to High for the input bit **0**.

Differential Manchester

In this type of coding, there always occurs a transition in the middle of the bit interval. If there occurs a transition at the beginning of the bit interval, then the input bit is **0**. If no transition occurs at the beginning of the bit interval, then the input bit is **1**.

The following figure illustrates the waveforms of NRZ-L, NRZ-I, Bi-phase Manchester and Differential Manchester coding for different digital inputs.



Block Coding

Among the types of block coding, the famous ones are 4B/5B encoding and 8B/6T encoding. The number of bits are processed in different manners, in both of these processes.

4B/5B Encoding

In Manchester encoding, to send the data, the clocks with double speed is required rather than NRZ coding. Here, as the name implies, 4 bits of code is mapped with 5 bits, with a minimum number of **1** bits in the group.

The clock synchronization problem in NRZ-I encoding is avoided by assigning an equivalent word of 5 bits in the place of each block of 4 consecutive bits. These 5-bit words are predetermined in a dictionary.

The basic idea of selecting a 5-bit code is that, it should have **one leading 0** and it should have **no more than two trailing 0s**. Hence, these words are chosen such that two transactions take place per block of bits.

8B/6T Encoding

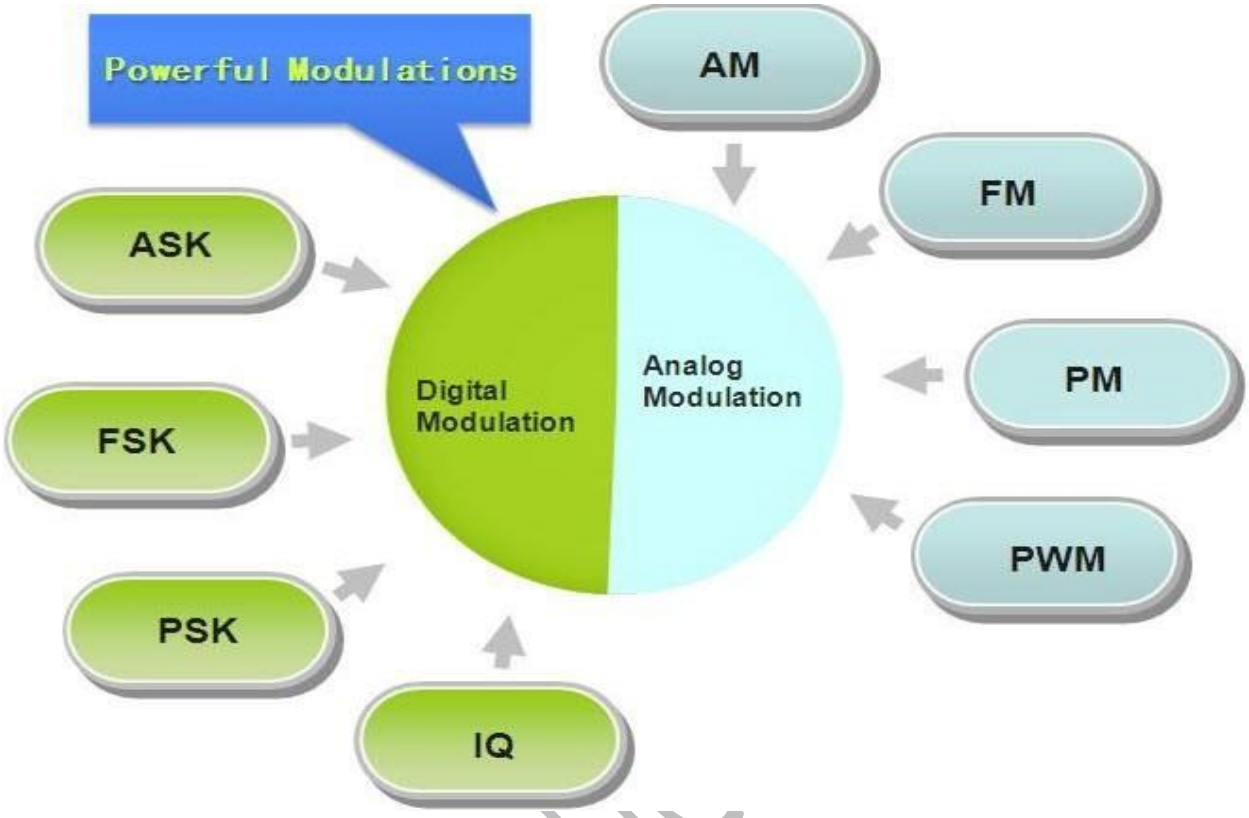
We have used two voltage levels to send a single bit over a single signal. But if we use more than 3 voltage levels, we can send more bits per signal.

For example, if 6 voltage levels are used to represent 8 bits on a single signal, then such encoding is termed as 8B/6T encoding. Hence in this method, we have as many as 729 3636 combinations for signal and 256 2828 combinations for bits.

These are the techniques mostly used for converting digital data into digital signals by compressing or coding them for reliable transmission of data.

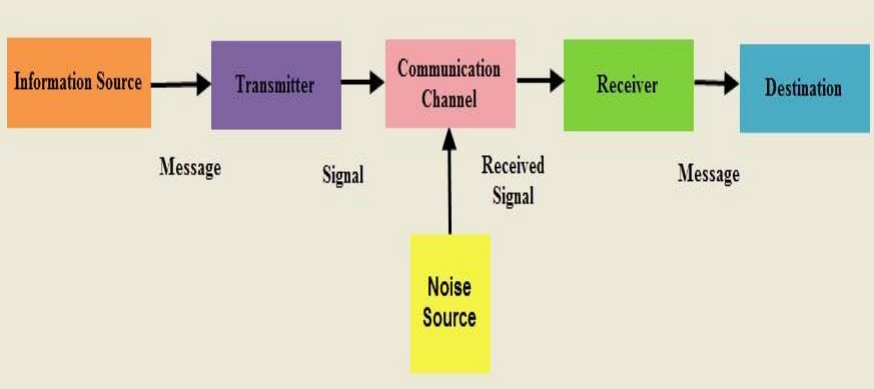
Modulation Techniques

DIWAKAR EDUCATION HUB



Communication is the basic attraction of mankind as it gives the knowledge of what is going on around us. In our daily life, we communicate with many people and use the entertainment media like television, radio, internet and newspaper to get ourselves involved. These entertainment media act as a source of communication. Electronic communication comprises TV, radio, internet, etc. When we want to transmit a signal from one location to another, we have to strengthen the signal. After undergoing strenghthening process the signal travels to a long distance. This is called as modulation, and this article gives an overview of the modulation and types of modulation techniques.

Communication is nothing but, the process of exchanging (two way communication) or passing (one way communication) information from one person to another. The basic electronic communication system consists of these components: transmitter, receiver and communication channel.



Communication System

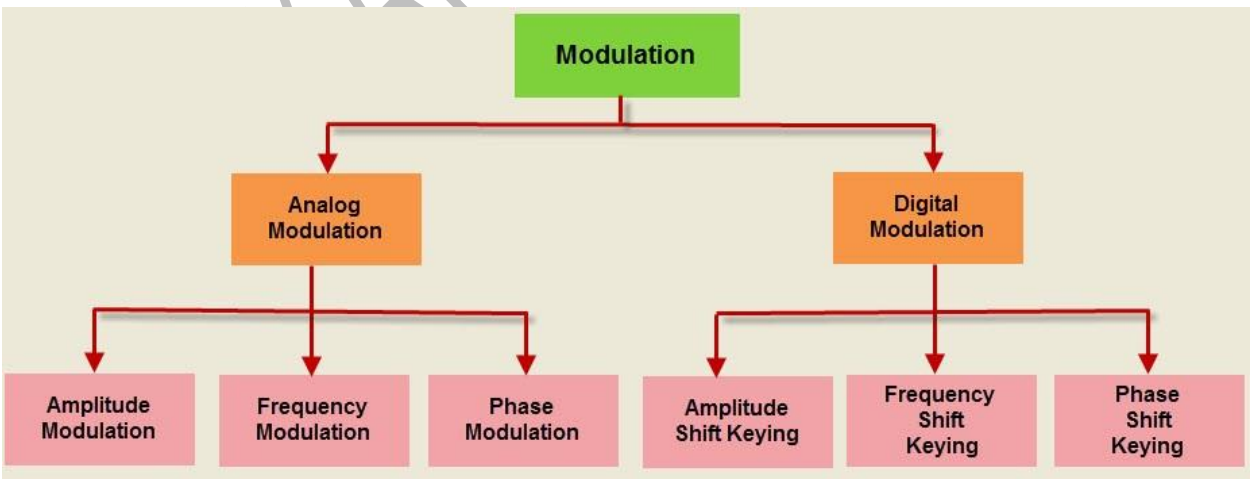
A **transmitter** is a group of electronic circuits designed to convert the information into a signal for transmission over a given communication medium.

A **receiver** is a group of electronic circuits designed to convert the signal back to the original information.

The communication channel is the medium which is designed to transmit the electronic signal from one place to another.

What is Modulation?

Modulation is nothing but, a carrier signal that varies in accordance with the message signal. Modulation technique is used to change the signal characteristics. Basically, the modulation is of following two types:



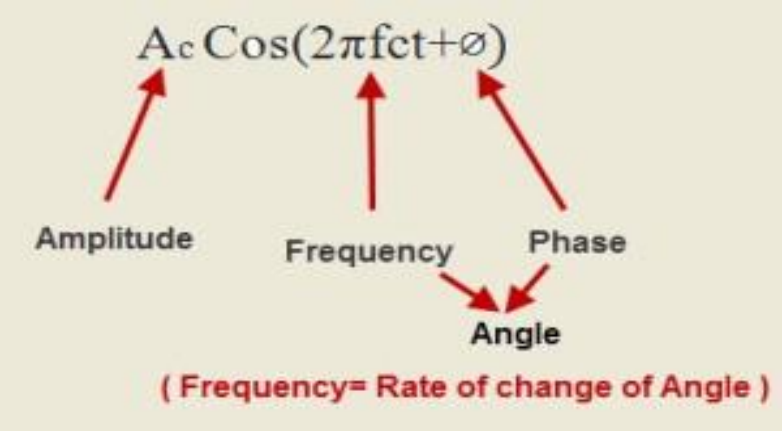
Modulation Techniques

AREDUCATION HUB

- Analog Modulation
- Digital Modulation

Analog Modulation

In analog modulation, analog signal (sinusoidal signal) is used as a carrier signal that modulates the message signal or data signal. The general function Sinusoidal wave's is shown in the figure below, in which, three parameters can be altered to get modulation – they are amplitude, frequency and phase; so, the types of analog modulation are:



Analog Modulation

- Amplitude Modulation (AM)
- Frequency Modulation (FM)
- Phase Modulation (PM)

Amplitude Modulation

Amplitude modulation was developed in the beginning of the 20th century. It was the earliest modulation technique used to transmit voice by radio. This type of modulation technique is used in electronic communication. In this modulation, the amplitude of the carrier signal varies in accordance with the message signal, and other factors like phase and frequency remain constant.

The modulated signal is shown in the below figure, and its spectrum consists of the lower frequency band, upper frequency band and carrier frequency components. This type of modulation requires more power and greater

bandwidth; filtering is very difficult. Amplitude modulation is used in computer modems, VHF aircraft radio, and in portable two-way radio

Frequency Modulation

In this type of modulation, the frequency of the carrier signal varies in accordance with the message signal, and other parameters like amplitude and phase remain constant. Frequency modulation is used in different applications like radar, radio and telemetry, seismic prospecting and monitoring newborns for seizures via EEG, etc.

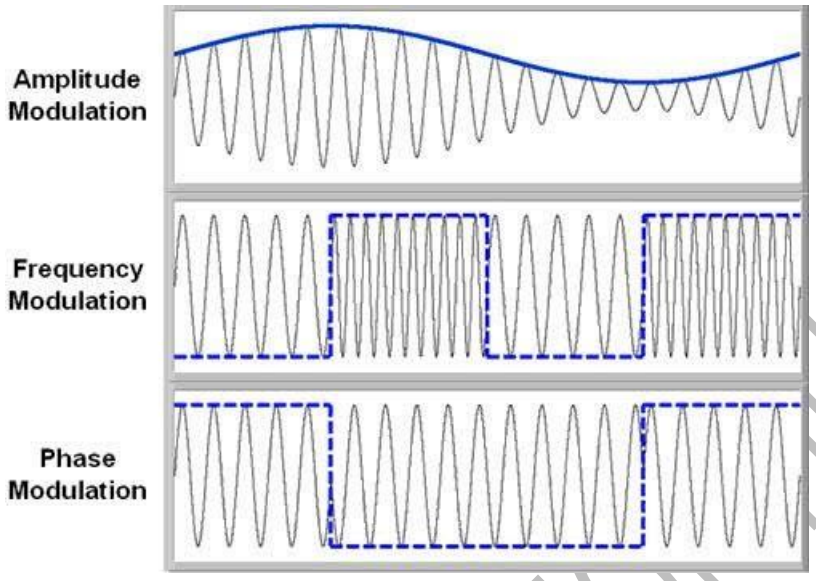
This type of modulation is commonly used for broadcasting music and speech, magnetic tape recording systems, two way radio systems and video transmission systems. When noise occurs naturally in radio systems, frequency modulation with sufficient bandwidth provides an advantage in cancelling the noise.

Phase Modulation

In this type of modulation, the phase of the carrier signal varies in accordance with the message signal. When the phase of the signal is changed, then it affects the frequency. So, for this reason, this modulation is also comes under the frequency modulation.

Generally, phase modulation is used for transmitting waves. It is an essential part of many digital transmission coding schemes that underlie a wide range of technologies like GSM, WiFi, and satellite television. This type of modulation is used for signal generation in al synthesizers, such as the Yamaha DX7 to implement FM synthesis.

DIWAKAR EDUCATION HUB



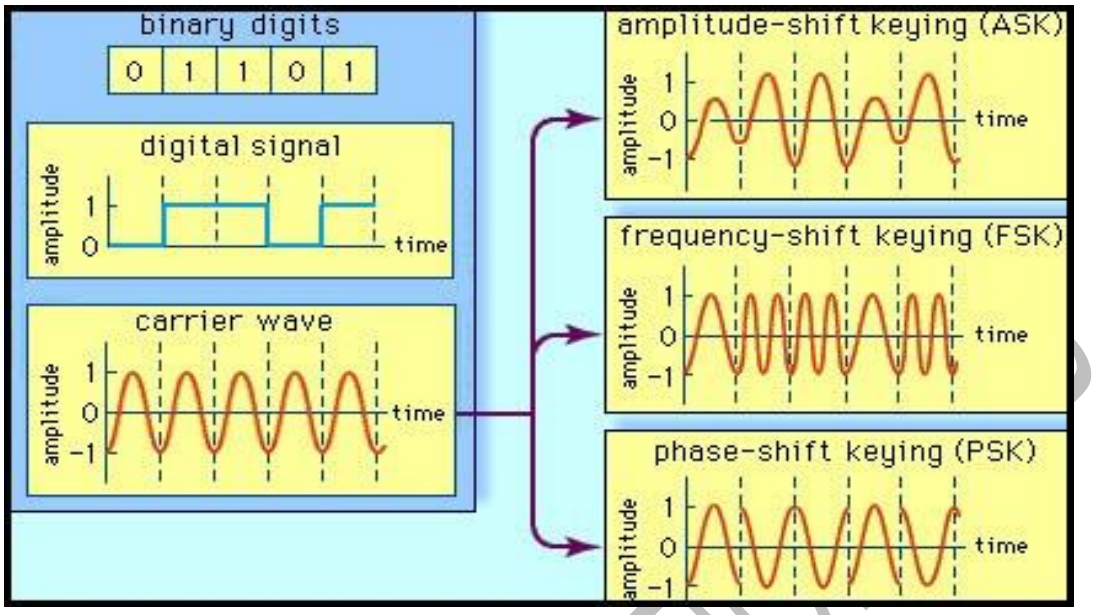
Types of Analog Modulation

Therefore, Analog modulation includes AM, FM and PM and these are more sensitive to noise. If noise enters into a system, it persists and gets carried up to the end receiver. So, this drawback can be overcome by the digital modulation technique.

Digital Modulation

For a better quality and efficient communication, digital modulation technique is employed. The main advantages of the digital modulation over analog modulation include available bandwidth , high noise immunity and permissible power. In digital modulation, a message signal is converted from analog to digital message, and then modulated by using a carrier wave.

DIWAKAR EDUCATION HUB



Digital Modulation

The carrier wave is switched on and off to create pulses such that the signal is modulated. Similar to the analog, in this system, the type of the digital modulation is decided by the variation of the carrier wave parameters like amplitude, phase and frequency.

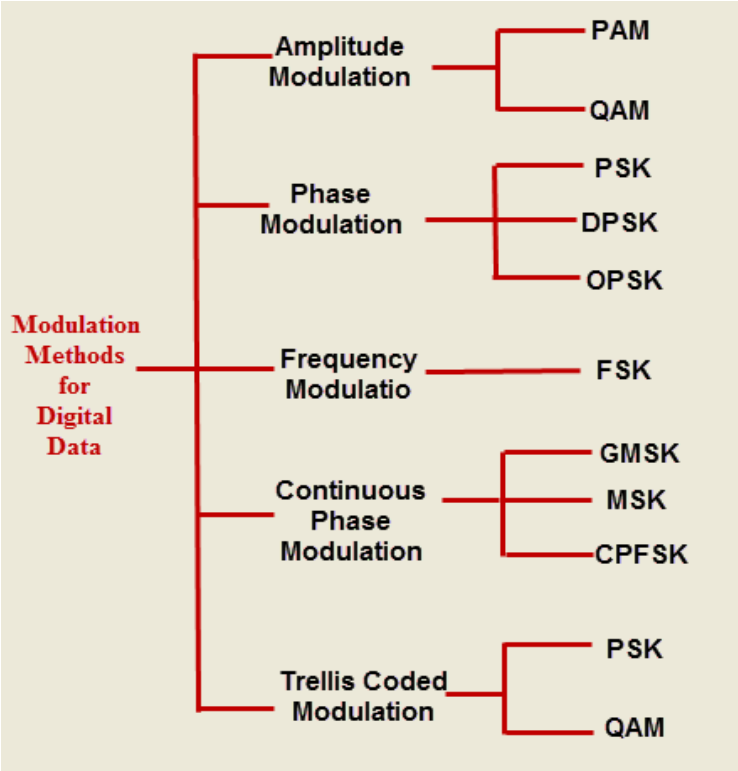
The most important digital modulation techniques are based on keying such as

Amplitude Shift Keying, Frequency Shift Keying, Phase Shift Keying, Differential Phase Shift Keying, Quadrature Phase Shift Keying, Minimum Shift Keying, Gaussian Minimum Shift Keying, Orthogonal Frequency Division Multiplexing, etc., as shown in the figure.

In an Amplitude shift keying, the amplitude of the carrier wave changes based on the message signal or on the base-band signal, which is in digital format. It is sensitive to noise and used for low-band requirements.

In frequency shift keying, the frequency of the carrier wave is varied for each symbol in the digital data. It needs larger bandwidths as shown in the figure. Similarly, the phase shift keying changes the phase of the carrier for each symbol and it is less sensitive to noise.

DIWAKAR EDUCATION



Types of Digital Modulation

Multiplexing

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

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

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

Why Multiplexing?

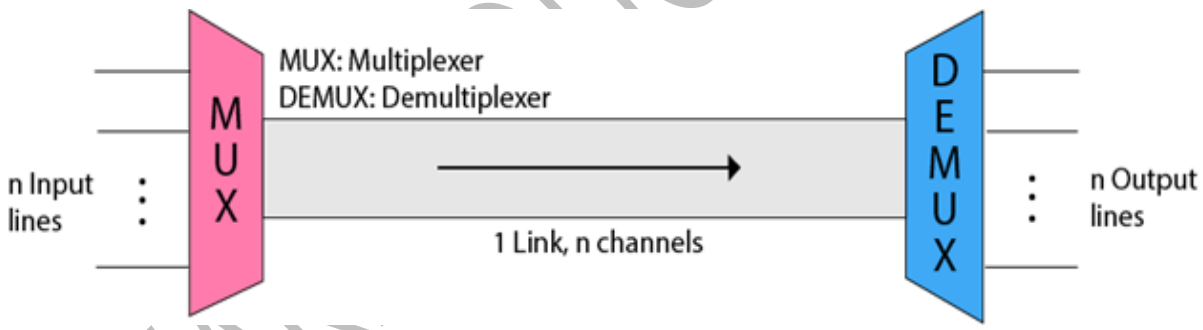
- The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.

- If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.
- When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.
- Transmission services are very expensive.

History of Multiplexing

- Multiplexing technique is widely used in telecommunications in which several telephone calls are carried through a single wire.
- Multiplexing originated in telegraphy in the early 1870s and is now widely used in communication.
- George Owen Squier developed the **telephone carrier multiplexing** in 1910.

Concept of Multiplexing



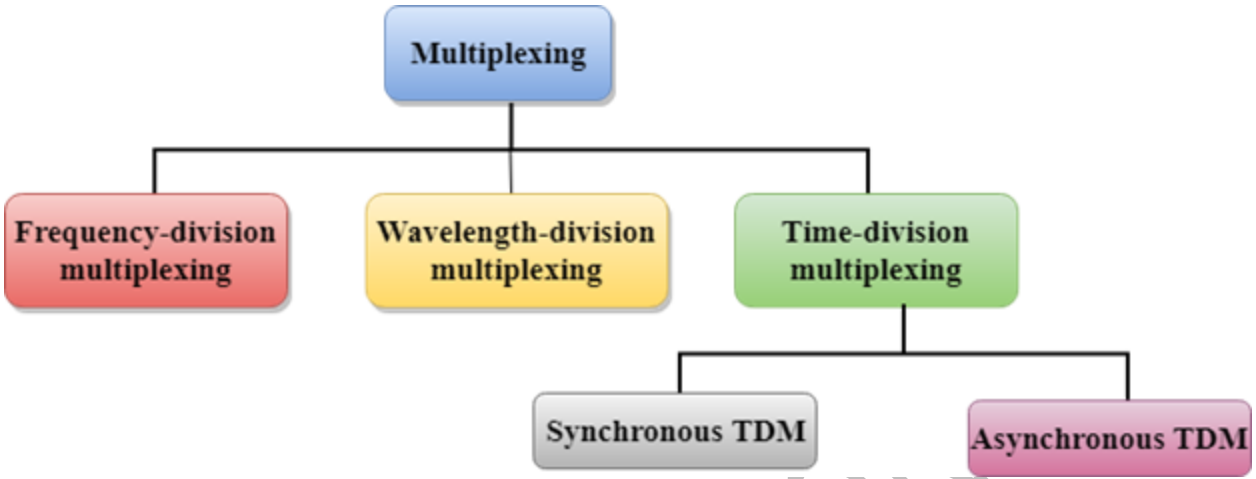
- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

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

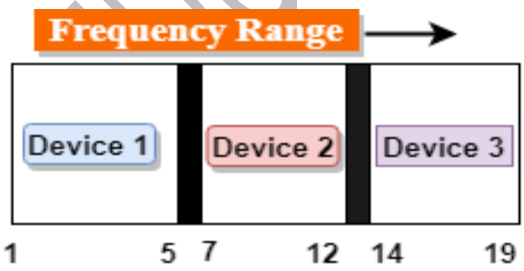
Multiplexing Techniques

Multiplexing techniques can be classified as:



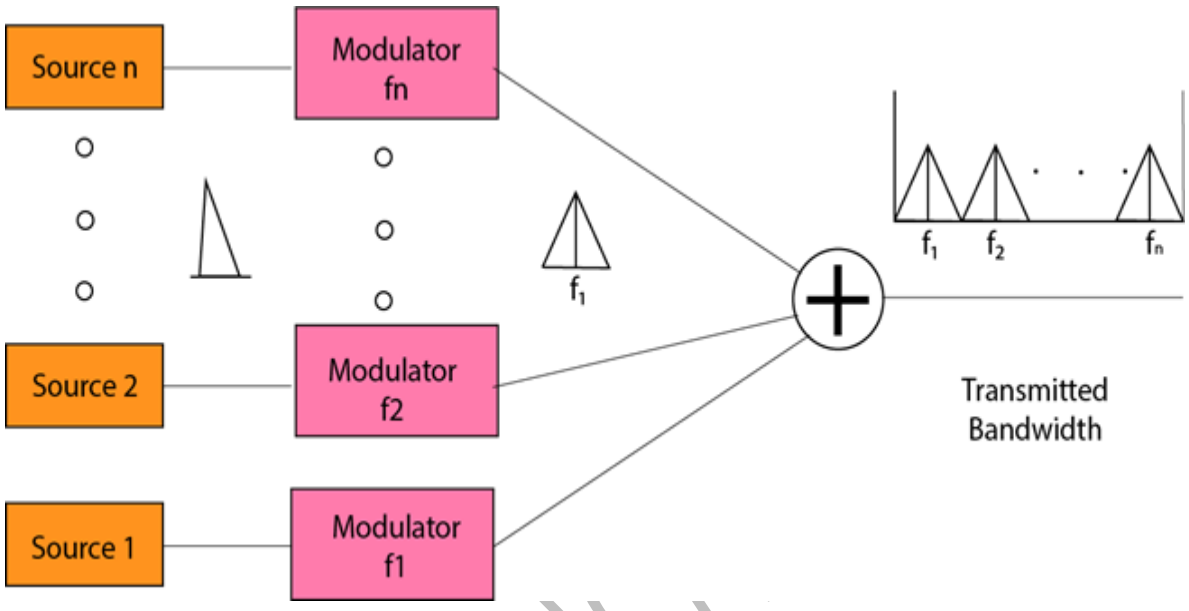
Frequency-division Multiplexing (FDM)

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



- In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.
- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.

- The carriers which are used for modulating the signals are known as **sub-carriers**. They are represented as f1,f2..fn.
- **FDM** is mainly used in radio broadcasts and TV networks.



Advantages Of FDM:

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

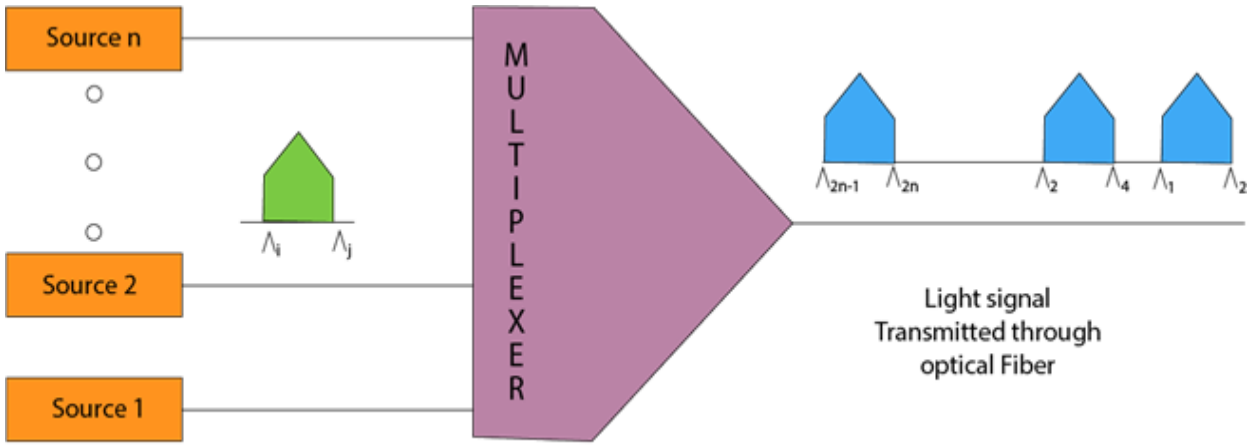
Disadvantages Of FDM:

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

Applications Of FDM:

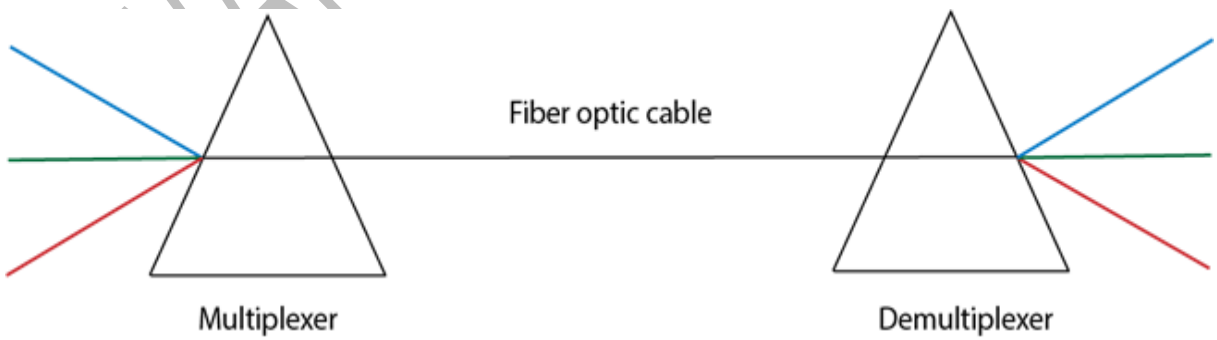
- FDM is commonly used in TV networks.
- It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Wavelength Division Multiplexing (WDM)



WDM Transmitter

- Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.
- WDM is used on fibre optics to increase the capacity of a single fibre.
- It is used to utilize the high data rate capability of fibre optic cable.
- It is an analog multiplexing technique.
- Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.
- Multiplexing and Demultiplexing can be achieved by using a prism.
- Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.
- Prism also performs a reverse operation, i.e., demultiplexing the signal.



Time Division Multiplexing

- It is a digital technique.

- In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
- In **Time Division Multiplexing technique**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.
- It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

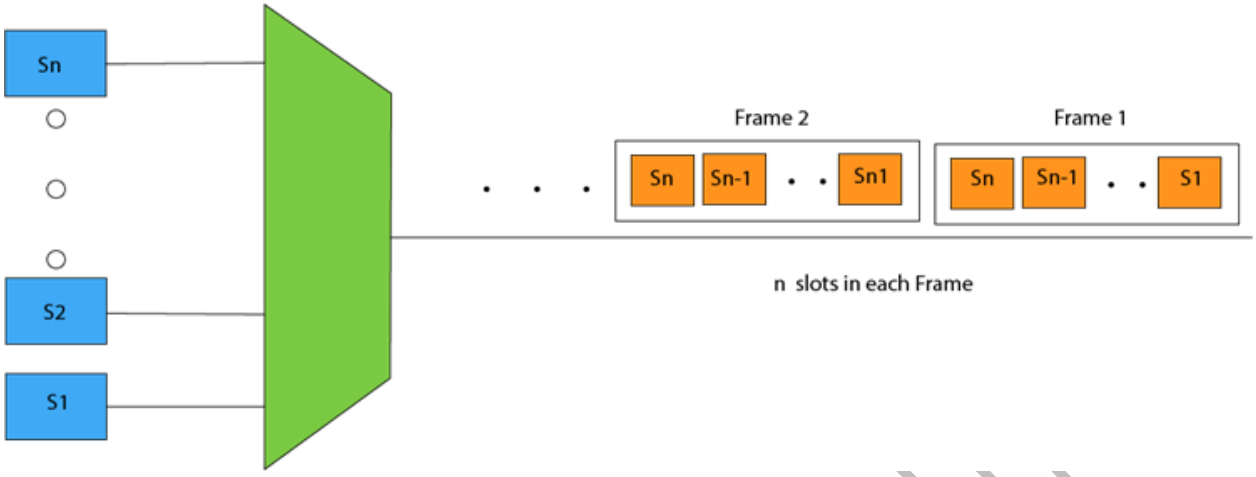
There are two types of TDM:

- Synchronous TDM
- Asynchronous TDM

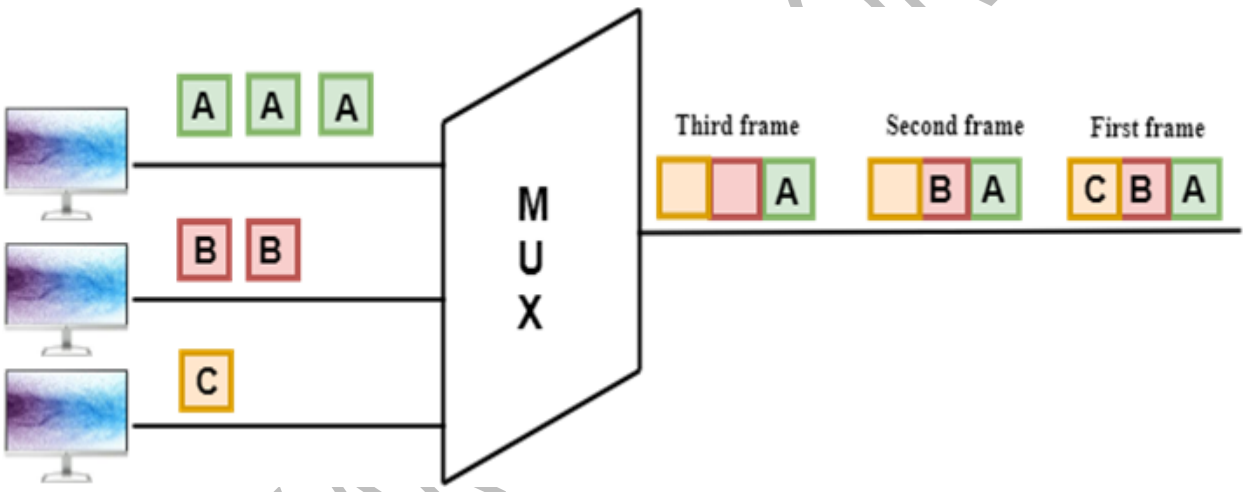
Synchronous TDM

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

DIWAKAR EDUCATION HUB



Concept Of Synchronous TDM



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

Disadvantages Of Synchronous TDM:

- The capacity of the channel is not fully utilized as the empty slots are also transmitted which is having no data. In the above figure, the first frame is completely filled, but in the last two frames, some slots are empty. Therefore, we can say that the capacity of the channel is not utilized efficiently.

- The speed of the transmission medium should be greater than the total speed of the input lines. An alternative approach to the Synchronous TDM is Asynchronous Time Division Multiplexing.

Asynchronous TDM

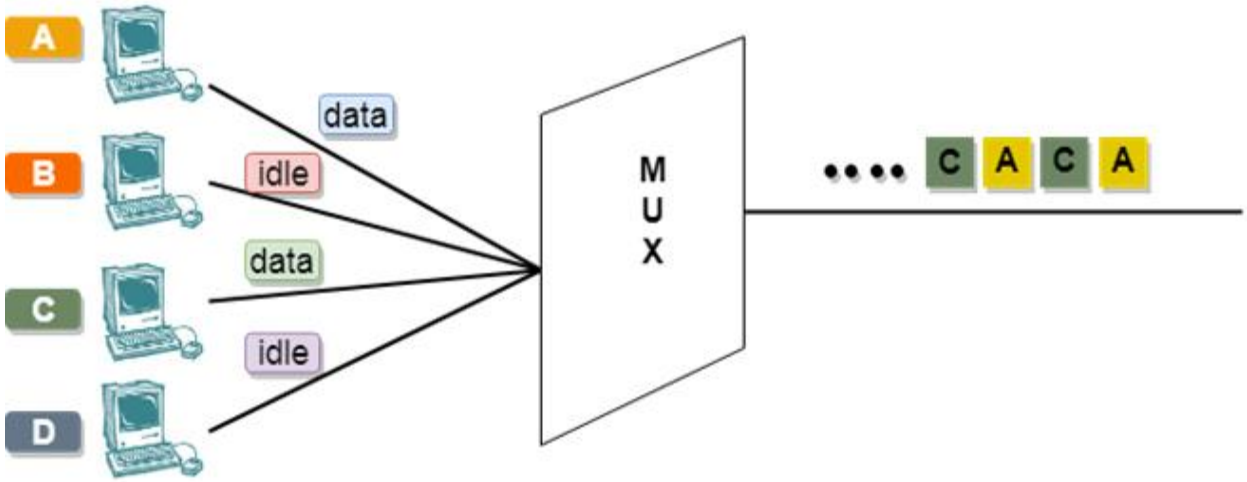
- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.
- An asynchronous TDM technique dynamically allocates the time slots to the devices.
- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.



- 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.

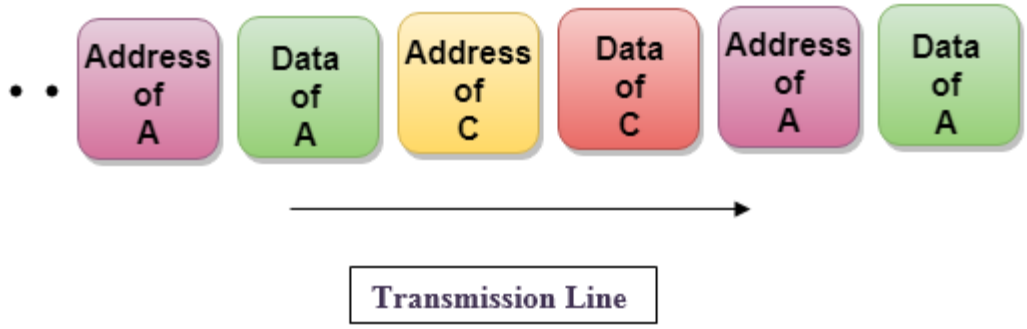
Concept Of Asynchronous TDM

DIWAKAR EDUCATION HUB



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

Frame of above diagram can be represented as:



The above figure shows that the data part contains the address to determine the source of the data.

What is Transmission media?

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).

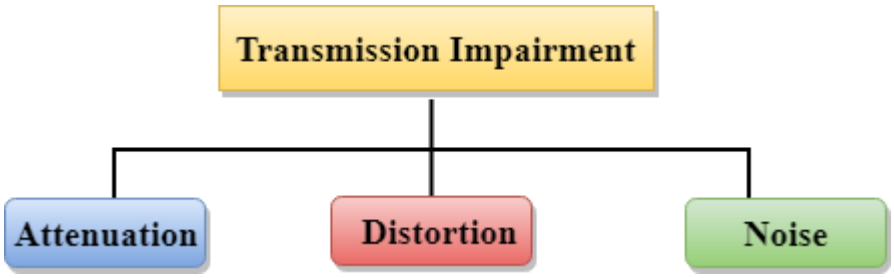
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre based network, the bits in the form of light pulses.
- In **OSI**(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
- The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

Some factors need to be considered for designing the transmission media:

- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

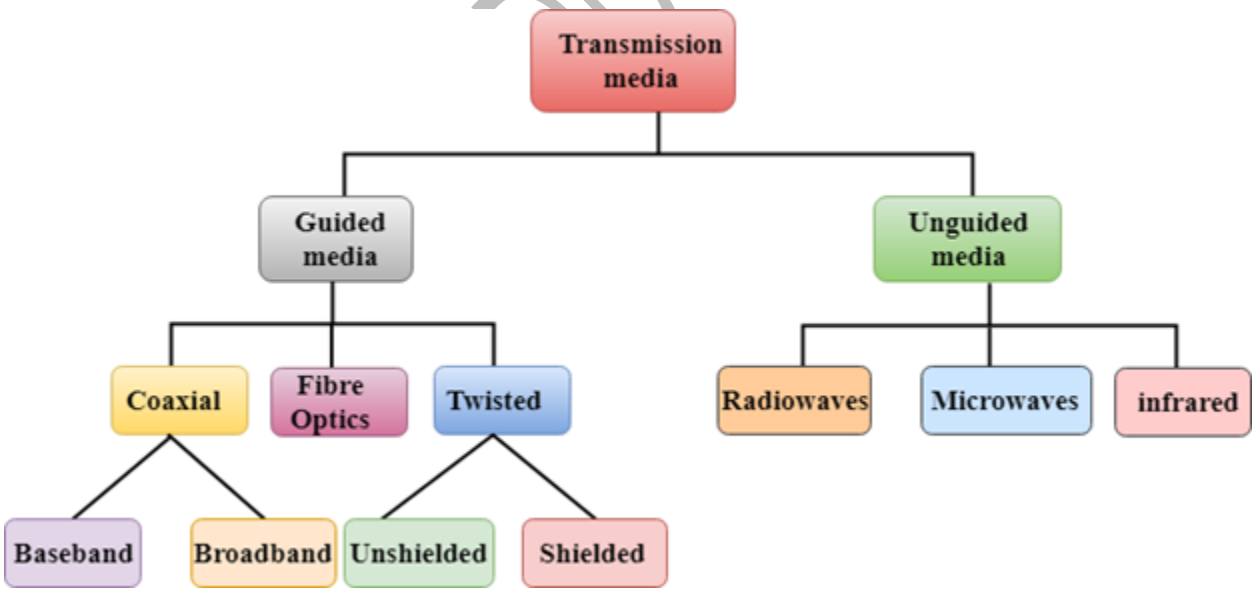
Causes Of Transmission Impairment:

DIWAKAR EDUCATION HUB



- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Classification Of Transmission Media:



- Guided Transmission Media
- UnGuided Transmission Media

EDUCATION HUB

Guided Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

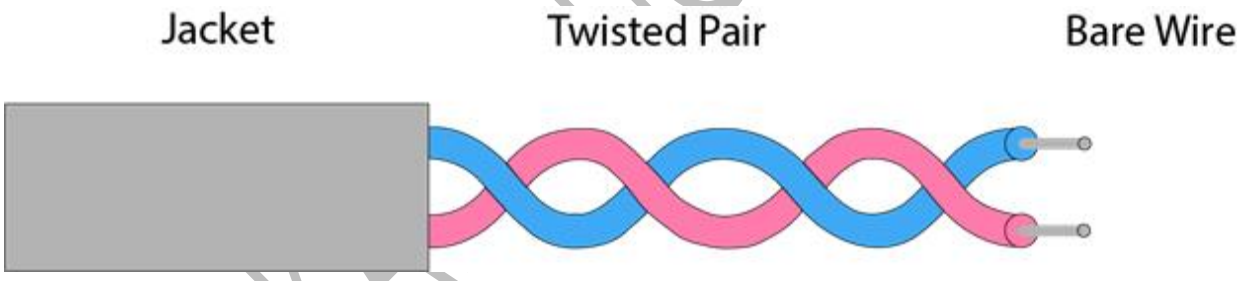
Types Of Guided media:

Twisted pair:

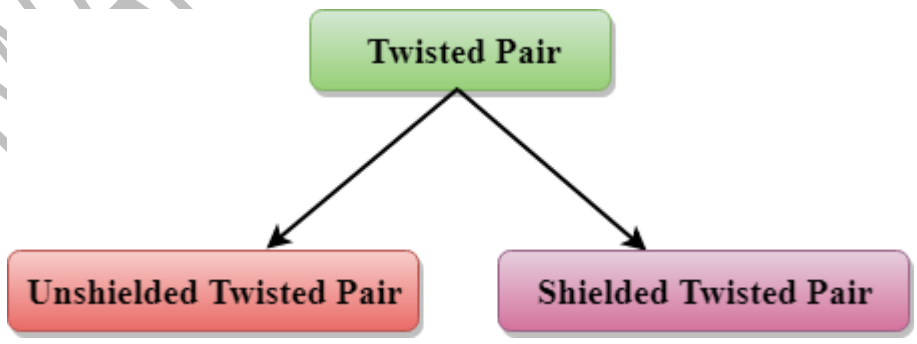
Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Types of Twisted pair:



Unshielded Twisted Pair:

DIVAKAR EDUCATION HUB

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support upto 4Mbps.
- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support upto 200Mbps.

Advantages Of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

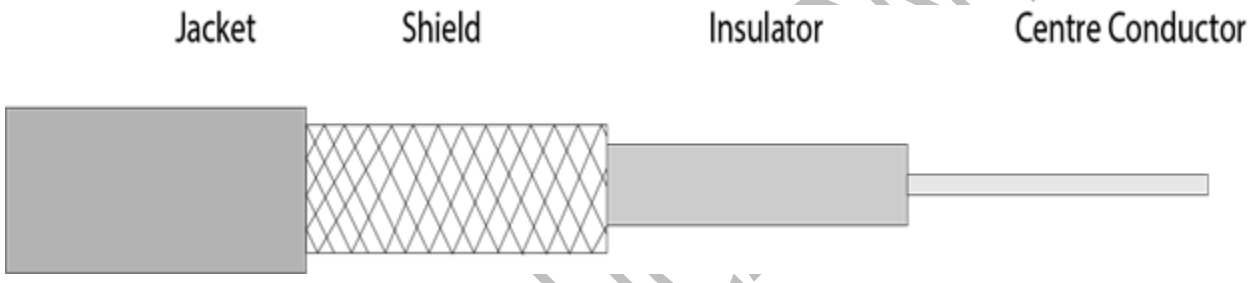
Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

Coaxial Cable

DIWAKAR EDUCATION HUB

- 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:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **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:

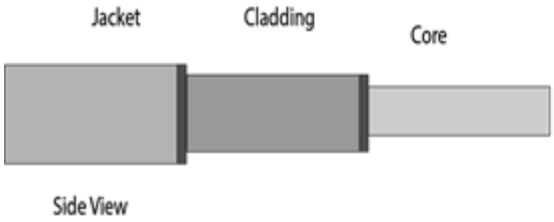
- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

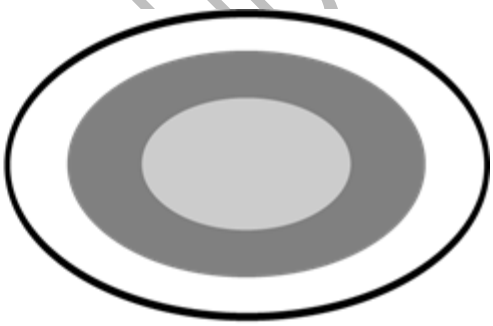
Fibre Optic

DIWAKAR EDUCATION HUB

- 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 fibre 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.

UnGuided Transmission

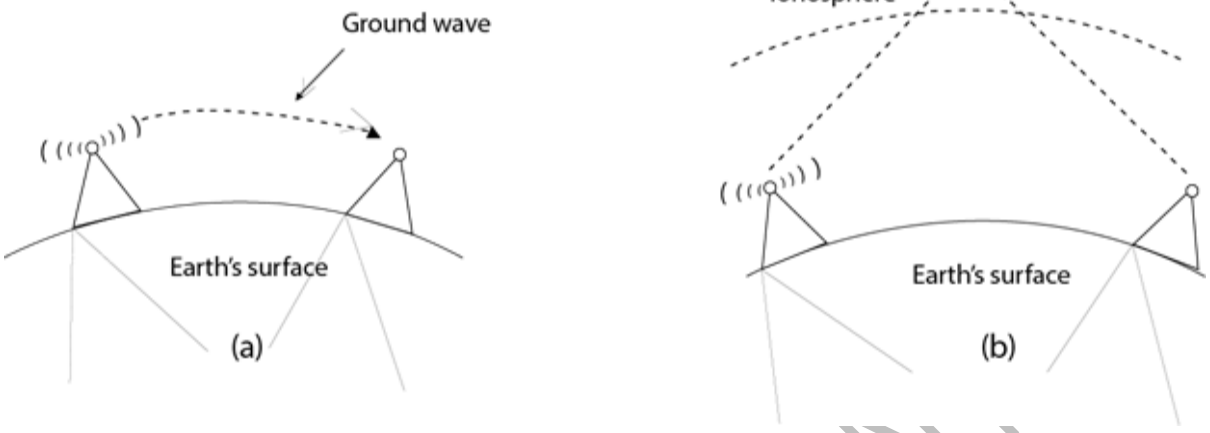
- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

Radio waves

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**.

DIWAKAR EDUCATION HUB



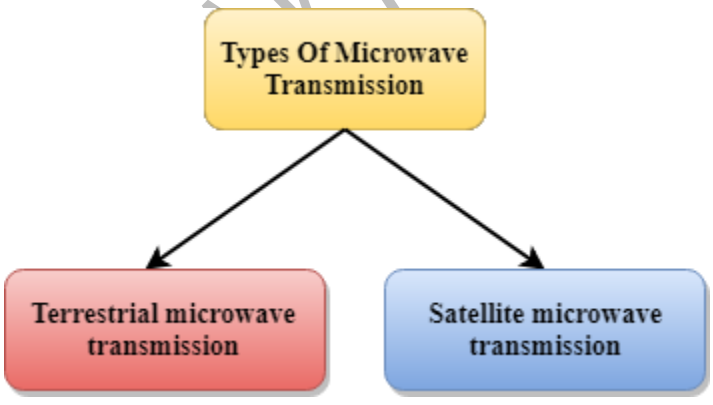
Applications Of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Radio transmission:

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

Microwaves



Microwaves are of two types:

- Terrestrial microwave

KARE EDUCATION

- Satellite microwave communication.

Terrestrial Microwave Transmission

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
- **Short distance:** It is inexpensive for short distance.
- **Long distance:** It is expensive as it requires a higher tower for a longer distance.
- **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

DIWAKAR EDUCATION HUB

- **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.
- **Susceptible to weather condition:** A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

- A satellite is a physical object that revolves around the earth at a known height.
- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using satellite communication.

How Does Satellite work?

The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages Of Satellite Microwave Communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.
- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.

DIWAKAR EDUCATION HUB

- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

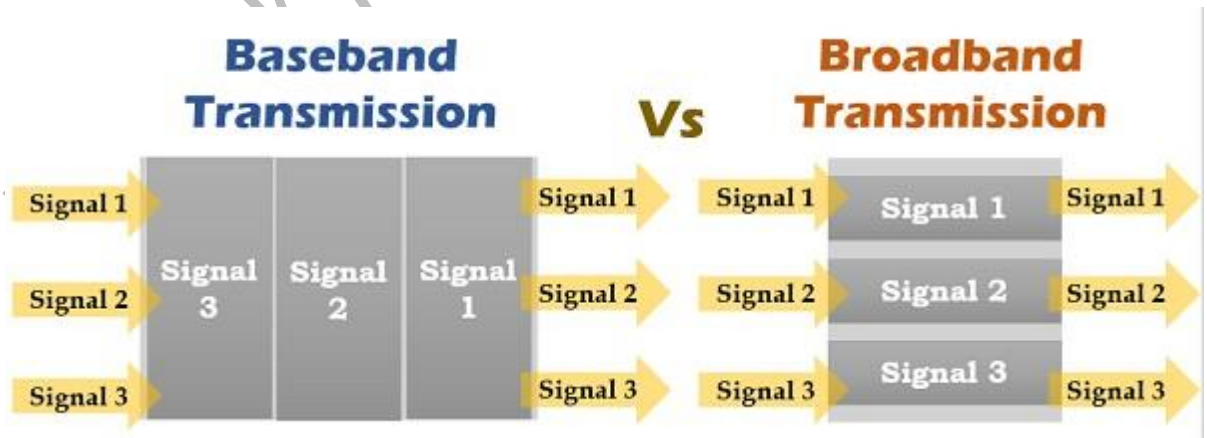
Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics Of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

Broadband and Baseband Transmission



VAREDUCATIONHUB

The baseband and broadband are the types of signalling techniques. These terminologies were developed to categorise different types of signals depending on particular kind of signal formats or modulation technique.

The prior difference between baseband transmission and broadband transmission is that in the baseband transmission the whole bandwidth of the cable is utilized by a single signal. Conversely, in the broadband transmission, multiple signals are sent on multiple frequencies simultaneously using a single channel.

Comparison Chart

BASIS FOR COMPARISON	BASEBAND TRANSMISSION	BROADBAND TRANSMISSION
Type of signalling used	Digital	Analog
Application	Work well with bus topology.	Used with a bus as well as tree topology.
Encoding Used	Manchester and Differential Manchester encoding.	PSK encoding.

BASIS FOR COMPARISON	BASEBAND TRANSMISSION	BROADBAND TRANSMISSION
Transmission	Bidirectional	Unidirectional
Signal range	Signals can be travelled over short distances	Signals can be travelled over long distances without being attenuated.

Broadband

Broadband system use modulation techniques to reduce the effect of noise in the environment. Broadband transmission employs multiple channel unidirectional transmission using combination of phase and amplitude modulation.

The **Broadband transmission** employs analog signals which include optical or electromagnetic wave form of signal. The signals are sent into multiple frequencies permitting multiple signals to be sent simultaneously. Frequency division multiplexing is possible in which the frequency spectrum is divided into multiple sections of bandwidth. The distinct channels can support different types of signals of varying frequency ranges to travel simultaneously (at the same instance).

The signals propagated at any point are unidirectional in nature, in simple words the signal can be travelled at only one direction, unlike baseband transmission. It requires two data path that are connected at a point in the network refer to as headend. The first path is used for signal transmission from the station to the headend. And the other path is used for receiving propagated signals.

DIWAKAR EDUCA

Baseband

Baseband is a digital signal is transmitted on the medium using one of the signal codes like NRZ, RZ Manchester biphase-M code etc. is called baseband transmission.

Baseband transmission uses whole frequency spectrum of the medium for the transmission. That is the reason frequency division multiplexing cannot be used in the transmission but time division multiplexing is used in this transmission as in TDM the link is not divided into multiple channels instead it provides each input signal with a time slot, in which the signal utilize whole bandwidth for a given time slot. The signals are carried by wires in the form of electrical pulse.

Signals transmitted at point propagated in both the directions hence it is bidirectional. The expansion of baseband signal is limited to shorter distances because at high frequency the attenuation of the signal is most strong and the pulse blur out, causing the large distance communication completely impractical.

These are following differences between Broadband and Baseband transmission.

Baseband transmission –

1. Digital signalling.
2. Frequency division multiplexing is not pssible.
3. Baseband is bi-directional transmission.
4. Short distance signal travelling.
5. Entire bandwidth is for single signal transmission.
6. Example: Ethernet is using Basebands for LAN.

Broadband transmission –

1. Analog signalling.
2. Transmission of data is unidirectional.
3. Signal travelling distance is long.
4. Frequency division multiplexing possible.

DIWAKAR EDUCATION HUB

5. Simultaneous transmission of multiple signals over different frequencies.
6. Example : Used to transmit cable TV to premise

Key Differences Between Baseband and Broadband Transmission

1. Baseband transmission utilizes digital signalling while broadband transmission uses analog signalling.
2. Bus and tree topologies, both work well with the broadband transmission. On the other hand, for the baseband transmission bus topology is suitable.
3. Baseband involves manchester and differential manchester encoding. In contrast, broadband does not make use of any digital encoding instead it uses PSK (Phase shift keying) encoding.
4. The signals can be travelled in both the direction in baseband transmission whereas in broadband transmission the signals can travel in only one direction.
5. In baseband transmission, the signals cover shorter distances because at higher frequencies the attenuation is most pronounced which make a signal to travel short distances without reducing its power. As against, in broadband signals, the signals can be travelled at longer distances.

Transmission Errors

There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing.Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

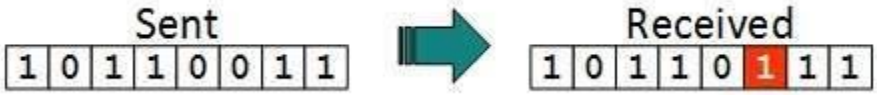
Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

Types of Errors

DIWAKAR EDUCATION HUB

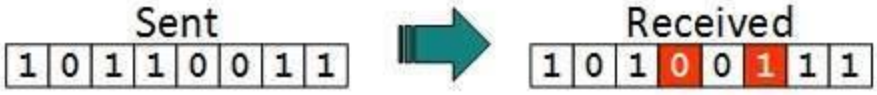
There may be three types of errors:

Single bit error



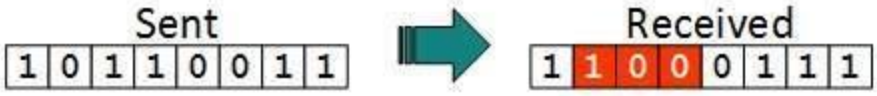
In a frame, there is only one bit, anywhere though, which is corrupt.

Multiple bits error



Frame is received with more than one bits in corrupted state.

Burst error



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.

DIWAKAR EDUCATION HUB

The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even.If the number of 1s is odd, to make it even a bit with value 1 is added.



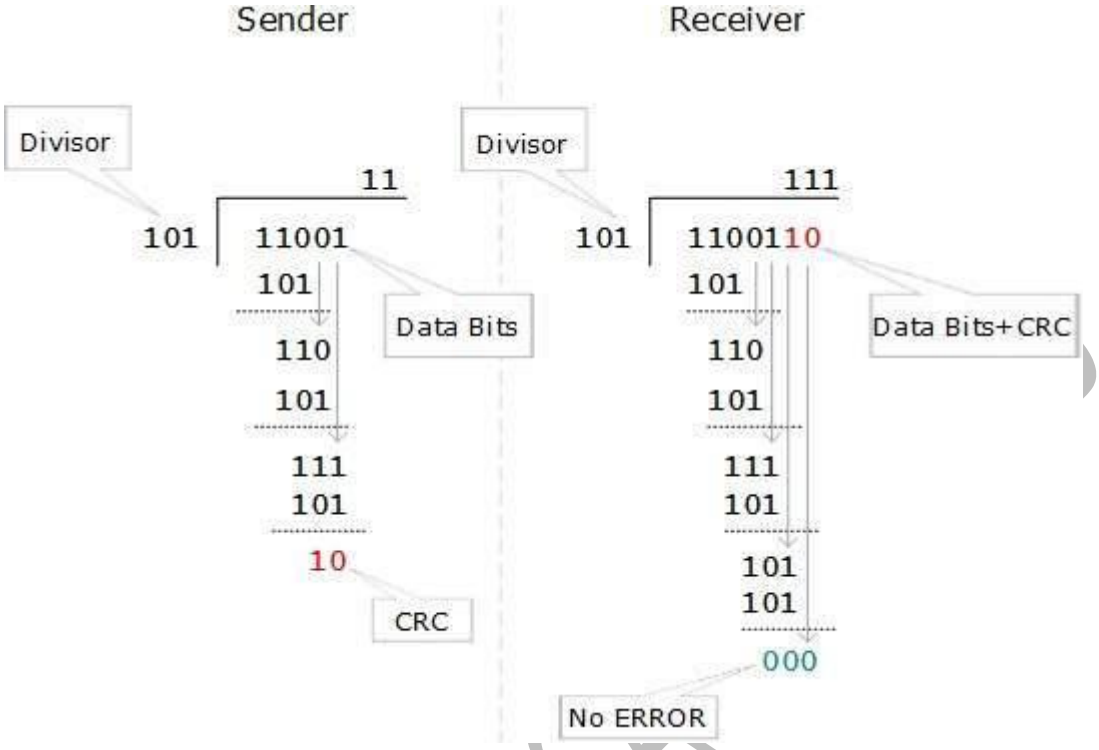
The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are erro neous, then it is very hard for the receiver to detect the error.

Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.

DIWAKAR EDUCATION HUB



At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.

Error Correction

In the digital world, error correction can be done in two ways:

Backward Error Correction When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.

Feedback or (backward) error control Along with each character, little additional information is added only for error detection. The receiver performs no error correction. If the received data contains error, then the entire data is retransmitted. Hence, the feedback techniques perform error detection and retransmission.

Forward Error Correction When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

DWAKAR EDUCA

Forward error control Additional redundant information is transmitted along with the useful data. Hence, the receiver not only detects the error, but also determines the location of the error in the data. This method is not widely used, because of the number of additional redundant information.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection.For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.

For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.

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

Computer Network

A computer network is a set of devices connected through links. A node can be computer, printer, or any other device capable of sending or receiving the data. The links connecting the nodes are known as communication channels.

- **Computer Network** is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.
- The aim of the computer network is the sharing of resources among various devices.
- In the case of computer network technology, there are several types of networks that vary from simple to complex level.

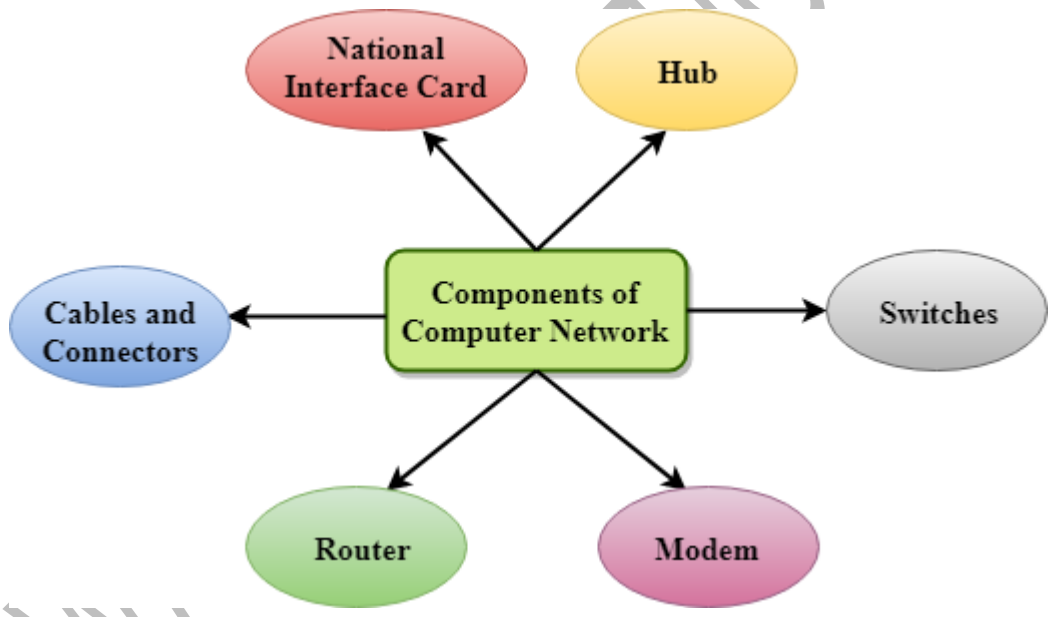
Computer Network uses distributed processing in which task is divided among several computers. Instead, a single computer handles an entire task, each separate computer handles a subset.

DIWAKAR EDUCATION HUB

Following are the advantages of Distributed processing:

- **Security:** It provides limited interaction that a user can have with the entire system. For example, a bank allows the users to access their own accounts through an ATM without allowing them to access the bank's entire database.
- **Faster problem solving:** Multiple computers can solve the problem faster than a single machine working alone.
- **Security through redundancy:** Multiple computers running the same program at the same time can provide the security through redundancy. For example, if four computers run the same program and any computer has a hardware error, then other computers can override it.

Components Of Computer Network:



Major components of a computer network

NIC(National interface card)

NIC is a device that helps the computer to communicate with another device. The network interface card contains the hardware addresses, the data-link layer protocol use this address to identify the system on the network so that it transfers the data to the correct destination.

There are two types of NIC: wireless NIC and wired NIC.

- **Wireless NIC:** All the modern laptops use the wireless NIC. In Wireless NIC, a connection is made using the antenna that employs the **radio wave technology**.
- **Wired NIC:** Cables use the **wired NIC** to transfer the data over the medium.

Hub

Hub is a central device that splits the network connection into multiple devices. When computer requests for information from a computer, it sends the request to the Hub. Hub distributes this request to all the interconnected computers.

Switches

Switch is a networking device that groups all the devices over the network to transfer the data to another device. A switch is better than Hub as it does not broadcast the message over the network, i.e., it sends the message to the device for which it belongs to. Therefore, we can say that switch sends the message directly from source to the destination.

Cables and connectors

Cable is a transmission media that transmits the communication signals. **There are three types of cables:**

- **Twisted pair cable:** It is a high-speed cable that transmits the data over **1Gbps** or more.
- **Coaxial cable:** Coaxial cable resembles like a TV installation cable. Coaxial cable is more expensive than twisted pair cable, but it provides the high data transmission speed.
- **Fibre optic cable:** Fibre optic cable is a high-speed cable that transmits the data using light beams. It provides high data transmission speed as compared to other cables. It is more expensive as compared to other cables, so it is installed at the government level.

Router

Router is a device that connects the LAN to the internet. The router is mainly used to connect the distinct networks or connect the internet to multiple computers.

Modem

DIWAKAR EDUCATION HUB

Modem connects the computer to the internet over the existing telephone line. A modem is not integrated with the computer motherboard. A modem is a separate part on the PC slot found on the motherboard.

Uses Of Computer Network

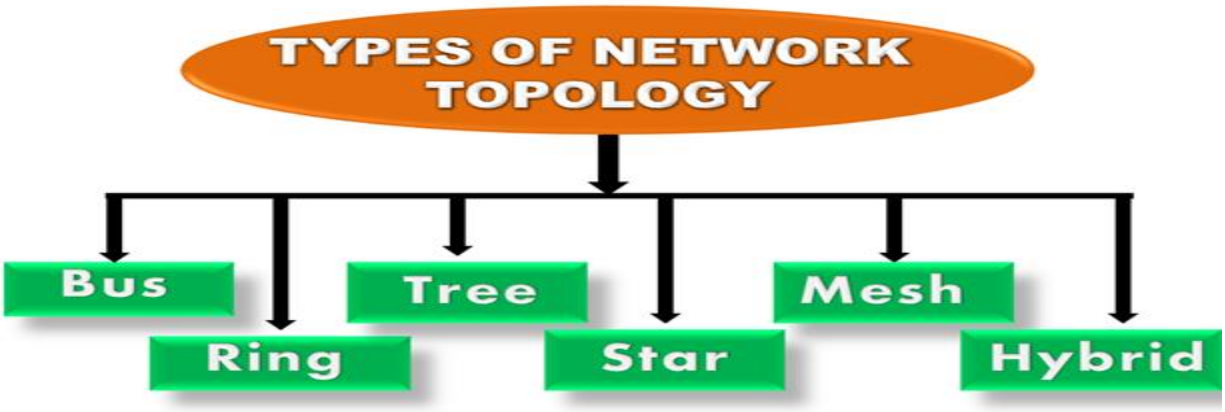
- **Resource sharing:** Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
- **Server-Client model:** Computer networking is used in the **server-client model**. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.
- **Communication medium:** Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.
- **E-commerce:** Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

Topology

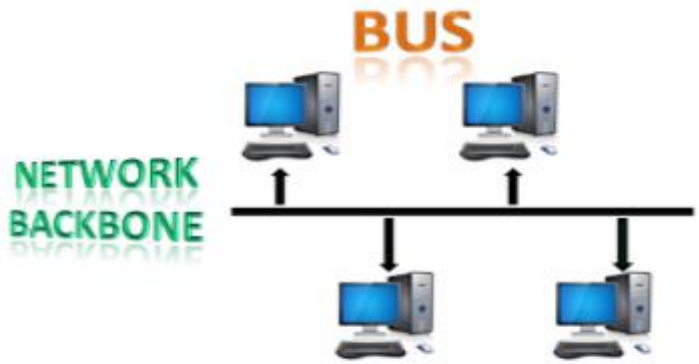
Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

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

DIWAKAR EDUCATION HUB



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.

- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

CSMA: It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

- **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
- **CSMA CA: CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

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.

DIWAKAR EDUCATION HUB

- **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.

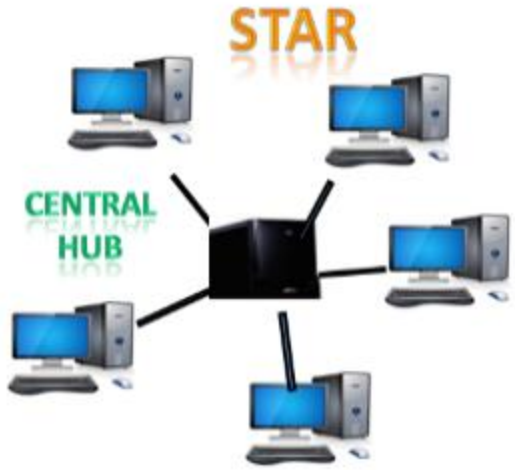
Disadvantages of Ring topology:

- **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.

DIWAKAR EDUCATION HUB

- **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.

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



DIWAKAR EDUCATION HUB

- 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.

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.

DIWAKAR EDUCATION HUB

- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

Mesh topology



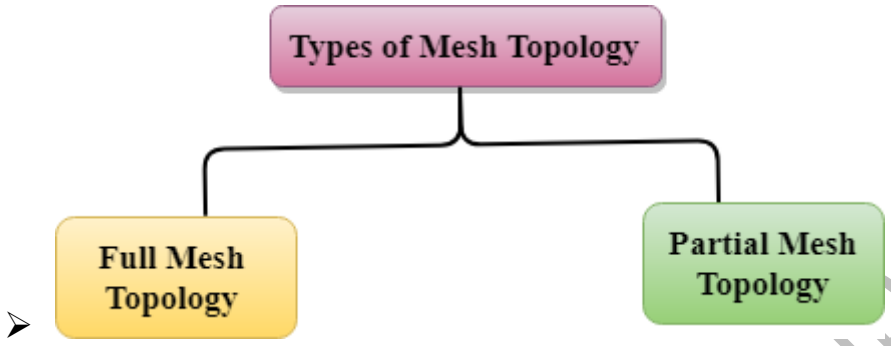
- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- 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

DIWAKAR EDUCATION HUB



- **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.

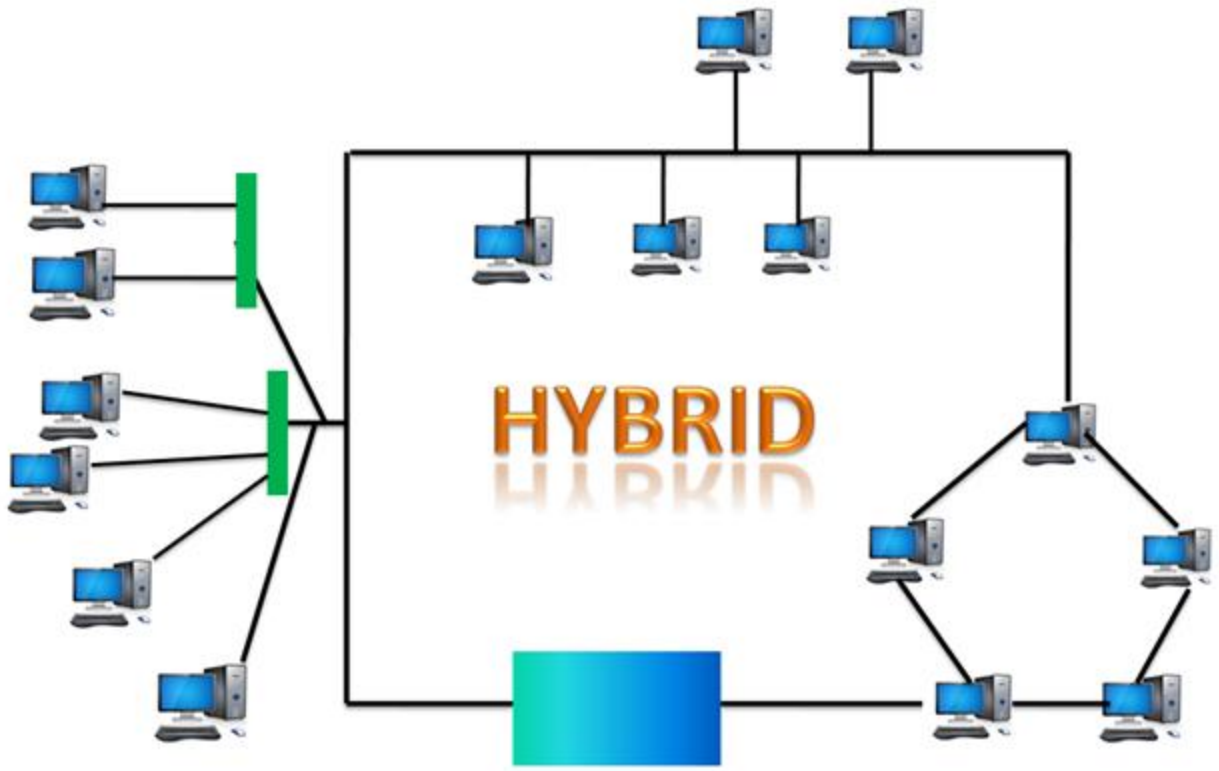
Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.

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

DIWAKAR EDUCATION HUB



- 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.

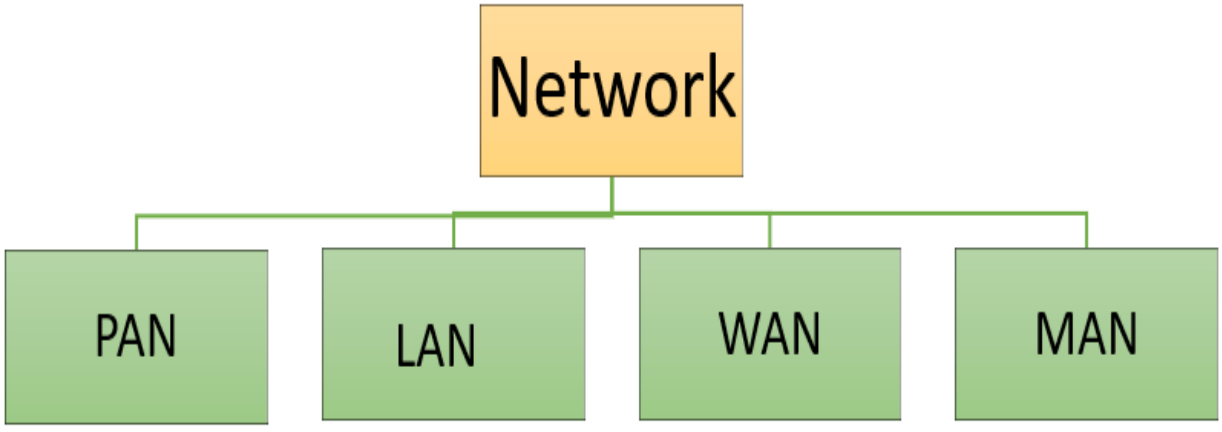
Disadvantages of Hybrid topology

- **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.

Types of Computer Networks: LAN, MAN, WAN, VPN

There are various types of computer networks available. We can categorize them according to their size as well as their purpose.

The size of a network should be expressed by the geographic area and number of computers, which are a part of their networks. It includes devices housed in a single room to millions of devices spread across the world.



VARE DUCATION HUB

Some of the most popular network types are:

- PAN
- LAN
- MAN
- WAN

PAN (Personal Area Network)

PAN is a computer network formed around a person. It generally consists of a computer, mobile, or personal digital assistant. PAN can be used for establishing communication among these personal devices for connecting to a digital network and the internet.

Characteristics of PAN

- It is mostly personal devices network equipped within a limited area.
- Allows you to handle the interconnection of IT devices at the surrounding of a single user.
- PAN includes mobile devices, tablet, and laptop.
- It can be wirelessly connected to the internet called WPAN.
- Appliances use for PAN: cordless mice, keyboards, and Bluetooth systems.

Advantages of PAN

Here, are important pros/benefits of using PAN network:

- PAN networks are relatively secure and safe
- It offers only short-range solution up to ten meters
- Strictly restricted to a small area

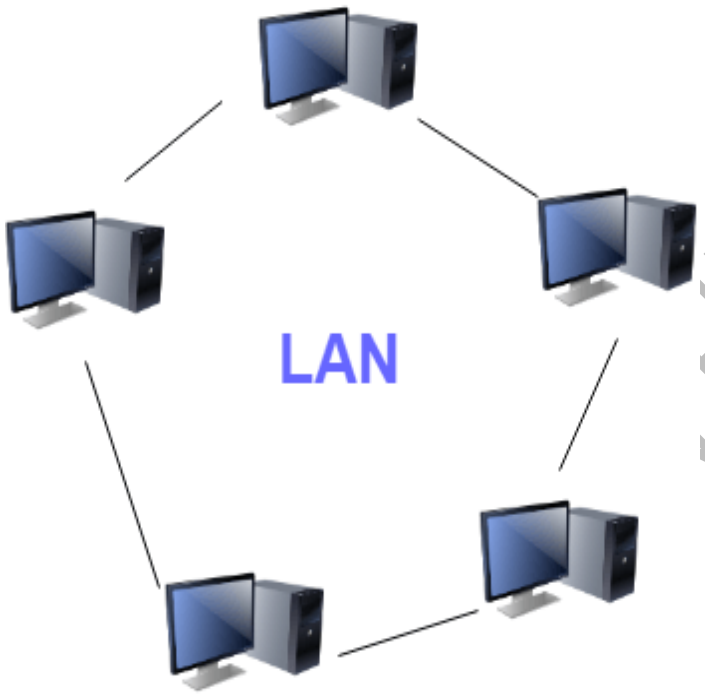
Disadvantages of PAN

Here are important cons/ drawback of using PAN network:

- It may establish a bad connection to other networks at the same radio bands.
- Distance limits.

DIWAKAR EDUCATION HUB

LAN(Local Area Network)



A **L**ocal **A**rea **N**etwork (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application. The simplest type of LAN network is to connect computers and a printer in someone's home or office. In general, LAN will be used as one type of transmission medium.

It is a network which consists of less than 5000 interconnected devices across several buildings.

Characteristics of LAN

Here are important characteristics of a LAN network:

- It is a private network, so an outside regulatory body never controls it.
- LAN operates at a relatively higher speed compared to other WAN systems.
- There are various kinds of media access control methods like token ring and ethernet.

Advantages of LAN

Here are pros/benefits of using LAN:

- Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.
- You can use the same software over the network instead of purchasing the licensed software for each client in the network.
- Data of all network users can be stored on a single hard disk of the server computer.
- You can easily transfer data and messages over networked computers.
- It will be easy to manage data at only one place, which makes data more secure.
- Local Area Network offers the facility to share a single internet connection among all the LAN users.

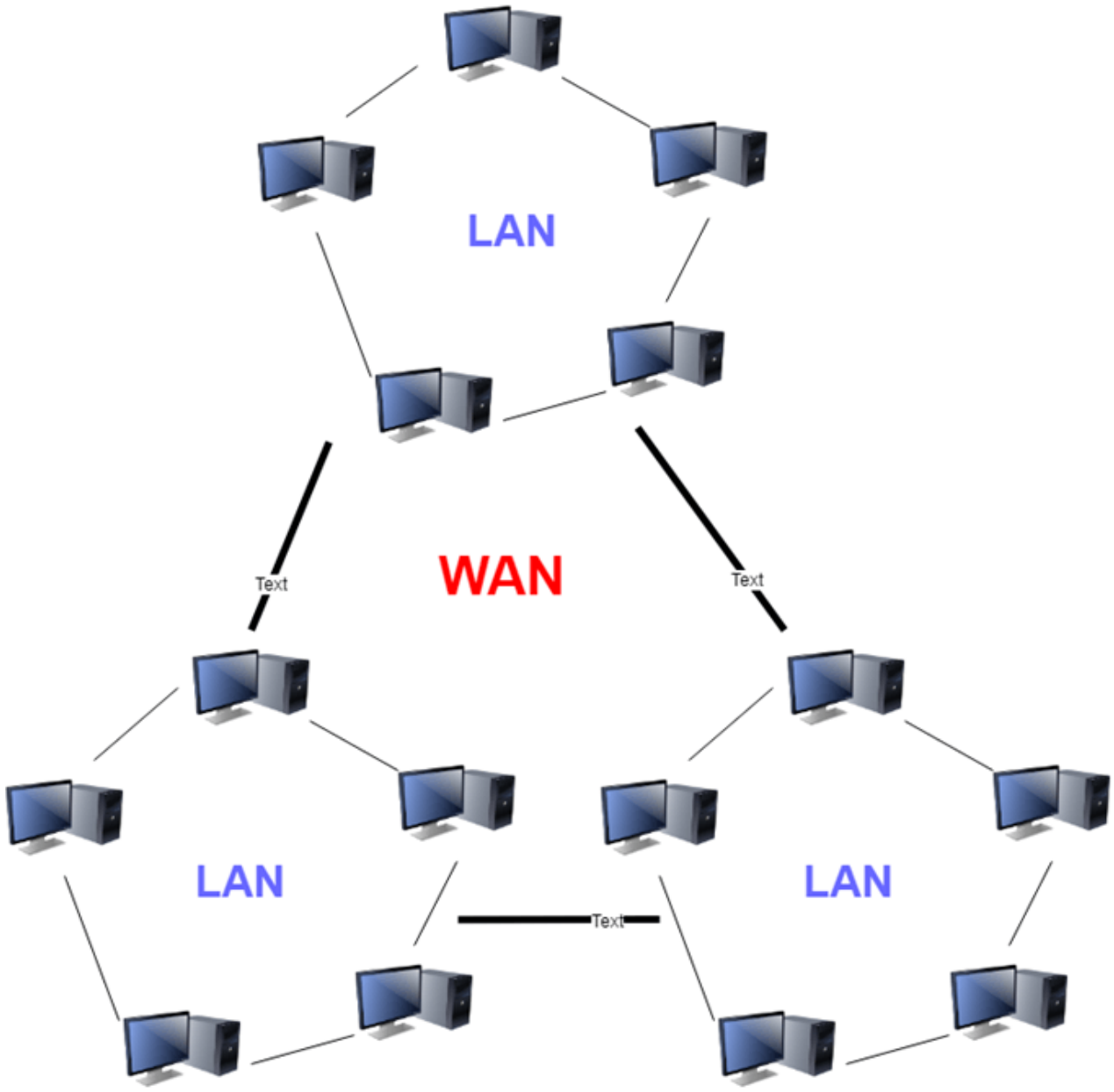
Disadvantages of LAN

Here are the important cons/ drawbacks of LAN:

- LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
- The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.
- Unauthorized users can access critical data of an organization in case LAN admin is not able to secure centralized data repository.
- Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

WAN(Wide Area Network)

DIWAKAR EDUCATION HUB



WAN (Wide Area Network) is another important computer network that which is spread across a large geographical area. WAN network system could be a connection of a LAN which connects with other LAN's using telephone lines and radio waves. It is mostly limited to an enterprise or an organization.

Characteristics of LAN:

- The software files will be shared among all the users; therefore, all can access to the latest files.

- Any organization can form its global integrated network using WAN.

Advantages of WAN

Here are the benefits/ pros of using WAN:

- WAN helps you to cover a larger geographical area. Therefore business offices situated at longer distances can easily communicate.
- Contains devices like mobile phones, laptop, tablet, computers, gaming consoles, etc.
- WLAN connections work using radio transmitters and receivers built into client devices.

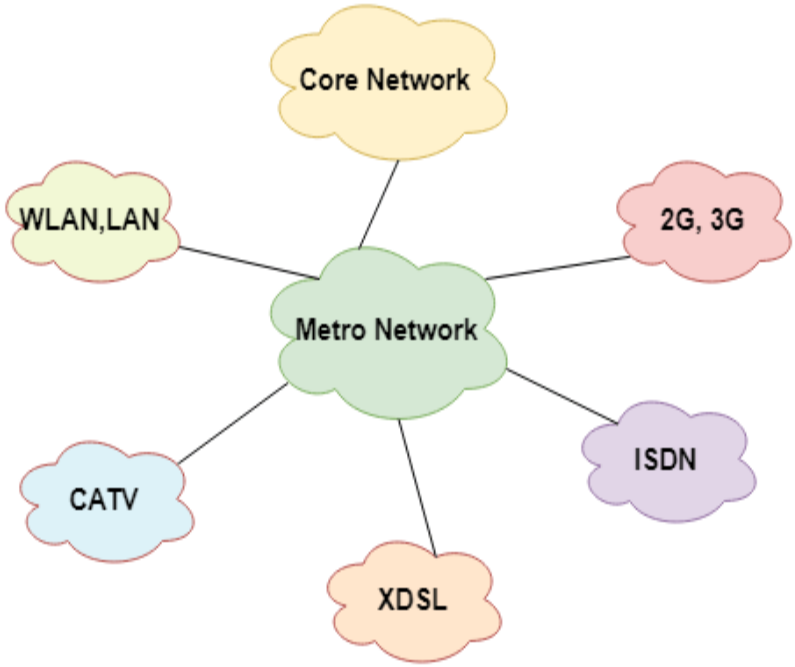
Disadvantage of WAN

Here are drawbacks/cons of using WAN:

- The initial setup cost of investment is very high.
- It is difficult to maintain the WAN network. You need skilled technicians and network administrators.
- There are more errors and issues because of the wide coverage and the use of different technologies.
- It requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.
- Offers lower security compared to other types of networks.

MAN(Metropolitan Area Network)

DIWAKAR EDUCATION HUB



A Metropolitan Area Network or MAN is consisting of a computer network across an entire city, college campus, or a small region. This type of network is large than a LAN, which is mostly limited to a single building or site. Depending upon the type of configuration, this type of network allows you to cover an area from several miles to tens of miles.

Characteristics of MAN

Here are important characteristics of the MAN network:

- It mostly covers towns and cities in a maximum 50 km range
- Mostly used medium is optical fibers, cables
- Data rates adequate for distributed computing applications.

Advantages of MAN

Here are pros/benefits of using MAN system:

- It offers fast communication using high-speed carriers, like fiber optic cables.
- It provides excellent support for an extensive size network and greater access to WANs.

- The dual bus in MAN network provides support to transmit data in both directions concurrently.
- A MAN network mostly includes some areas of a city or an entire city.

Disadvantages of MAN

Here are drawbacks/ cons of using the MAN network:

- You need more cable to establish MAN connection from one place to another.
- In MAN network it is tough to make the system secure from hackers

Other Types of Networks

Apart from above mentioned here, are some other important types of networks:

- WLAN (Wireless Local Area Network)
- Storage Area Network
- System Area Network
- Home Area Network
- POLAN- Passive Optical LAN
- Enterprise private network
- Campus Area Network
- Virtual Area Network

1) WLAN

WLAN (Wireless Local Area Network) helps you to link single or multiple devices using wireless communication within a limited area like home, school, or office building. It gives users an ability to move around within a local coverage area which may be connected to the network. Today most modern day's WLAN systems are based on IEEE 802.11 standards.

2) Storage-Area Network (SAN)

DIWAKAR EDUCATION HUB

A Storage Area Network is a type of network which allows consolidated, block-level data storage. It is mainly used to make storage devices, like disk arrays, optical jukeboxes, and tape libraries.

3) System-Area Network

System Area Network is used for a local network. It offers high-speed connection in server-to-server and processor-to-processor applications. The computers connected on a SAN network operate as a single system at quite high speed.

4) Passive Optical Local Area Network

POLAN is a networking technology which helps you to integrate into structured cabling. It allows you to resolve the issues of supporting Ethernet protocols and network apps.

POLAN allows you to use optical splitter which helps you to separate an optical signal from a single-mode optical fiber. It converts this single signal into multiple signals.

5) Home Area Network (HAN):

A Home Area Network is always built using two or more interconnected computers to form a local area network (LAN) within the home. For example, in the United States, about 15 million homes have more than one computer.

This type of network helps computer owners to interconnect with multiple computers. This network allows sharing files, programs, printers, and other peripherals.

6) Enterprise Private Network :

Enterprise private network (EPN) networks are build and owned by businesses that want to securely connect numerous locations in order to share various computer resources.

7) Campus Area Network (CAN):

A Campus Area Network is made up of an interconnection of LANs within a specific geographical area. For example, a university campus can be linked with a variety of campus buildings to connect all the academic departments.

DWAKAR EDUCATION HUB

8) Virtual Private Network:

A VPN is a private network which uses a public network to connect remote sites or users together. The VPN network uses "virtual" connections routed through the internet from the enterprise's private network or a third-party VPN service to the remote site.

It is a free or paid service that keeps our web browsing secure and private over public WiFi hotspots.

Computer Network Models

Introduction

A communication subsystem is a complex piece of Hardware and software. Early attempts for implementing the software for such subsystems were based on a single, complex, unstructured program with many interacting components. The resultant software was very difficult to test and modify. To overcome such problem, the ISO has developed a layered approach. In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task. Therefore, we can say that networking tasks depend upon the layers.

- For data communication to take place and two or more users can transmit data from one to other, a systematic approach is required. This approach enables users to communicate and transmit data through efficient and ordered path. It is implemented using models in computer networks and are known as computer network models.
- Computer network models are responsible for establishing a connection among the sender and receiver and transmitting the data in a smooth manner respectively.
- There are two computer network models i.e. OSI Model and TCP/IP Model on which the whole data communication process relies.

Layered Architecture

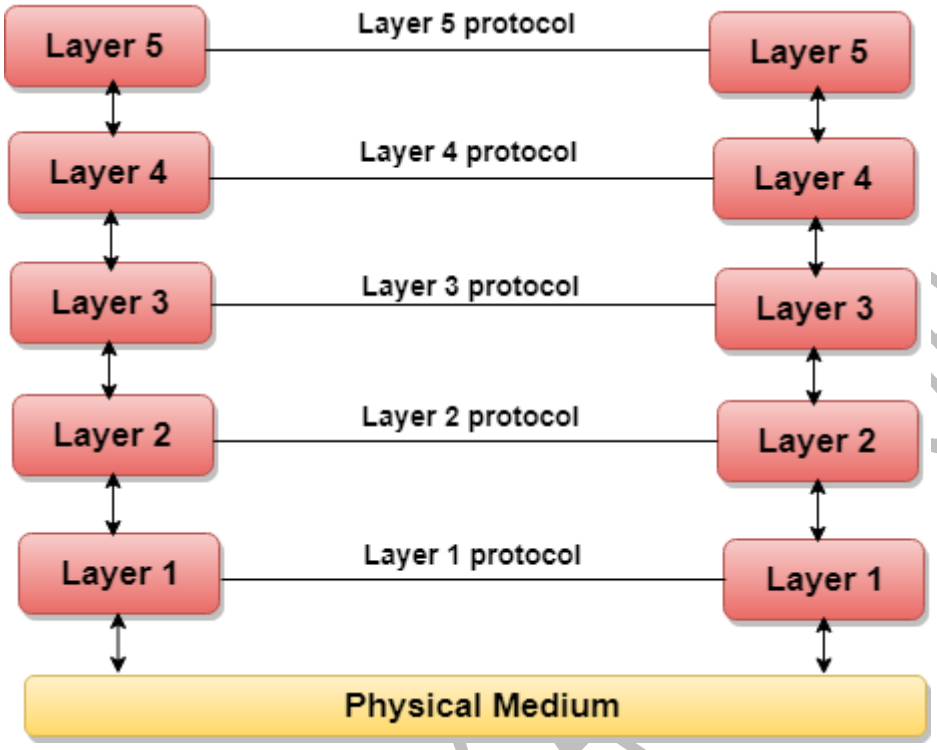
- The main aim of the layered architecture is to divide the design into small pieces.

DIWAKAR EDUCATION HUB

- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.
- The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a higher layer and hiding the details from the layers of how the services are implemented.
- The basic elements of layered architecture are services, protocols, and interfaces.
    - **Service:** It is a set of actions that a layer provides to the higher layer.
    - **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
    - **Interface:** It is a way through which the message is transferred from one layer to another layer.
- In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.

An example of the five-layered architecture.

DIWAKAR EDUCATION HUB



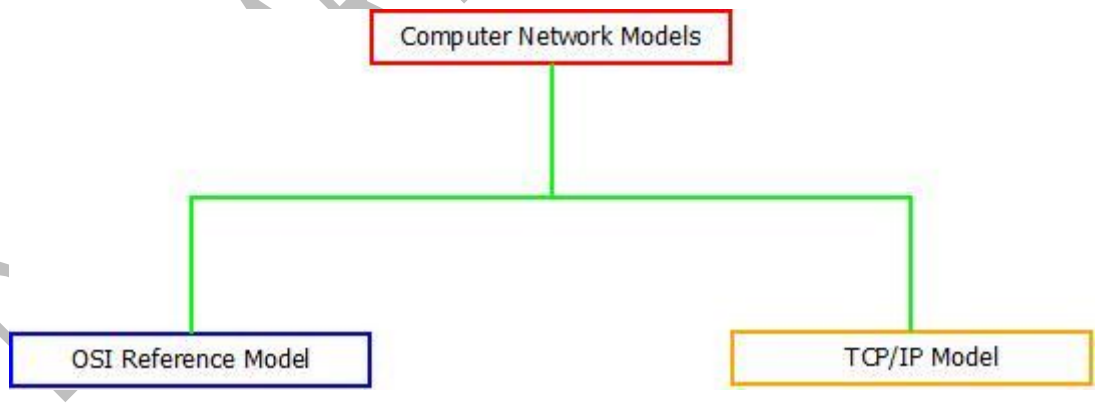
- In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which the actual communication takes place.
- In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
- A set of layers and protocols is known as network architecture.

Why do we require Layered architecture?

- **Divide-and-conquer approach:** Divide-and-conquer approach makes a design process in such a way that the unmanageable tasks are divided into

small and manageable tasks. In short, we can say that this approach reduces the complexity of the design.

- **Modularity:** Layered architecture is more modular. Modularity provides the independence of layers, which is easier to understand and implement.
- **Easy to modify:** It ensures the independence of layers so that implementation in one layer can be changed without affecting other layers.
- **Easy to test:** Each layer of the layered architecture can be analyzed and tested individually.
  - For data communication to take place and two or more users can transmit data from one to other, a systematic approach is required. This approach enables users to communicate and transmit data through efficient and ordered path. It is implemented using models in computer networks and are known as computer network models.
  - Computer network models are responsible for establishing a connection among the sender and receiver and transmitting the data in a smooth manner respectively.
  - There are two computer network models i.e. OSI Model and TCP/IP Model on which the whole data communication process relies.



Computer Network Models

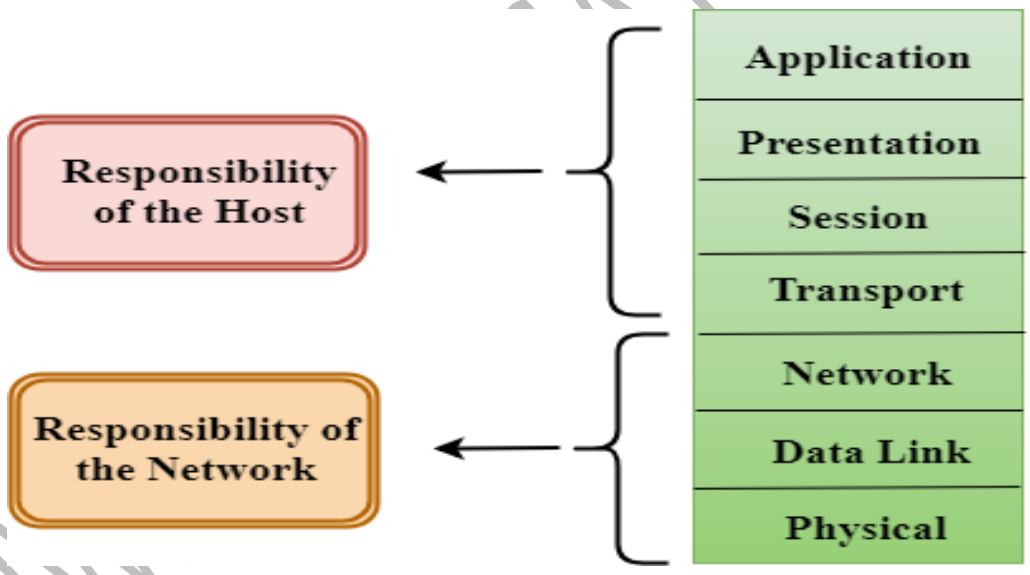
OSI Model

- 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.

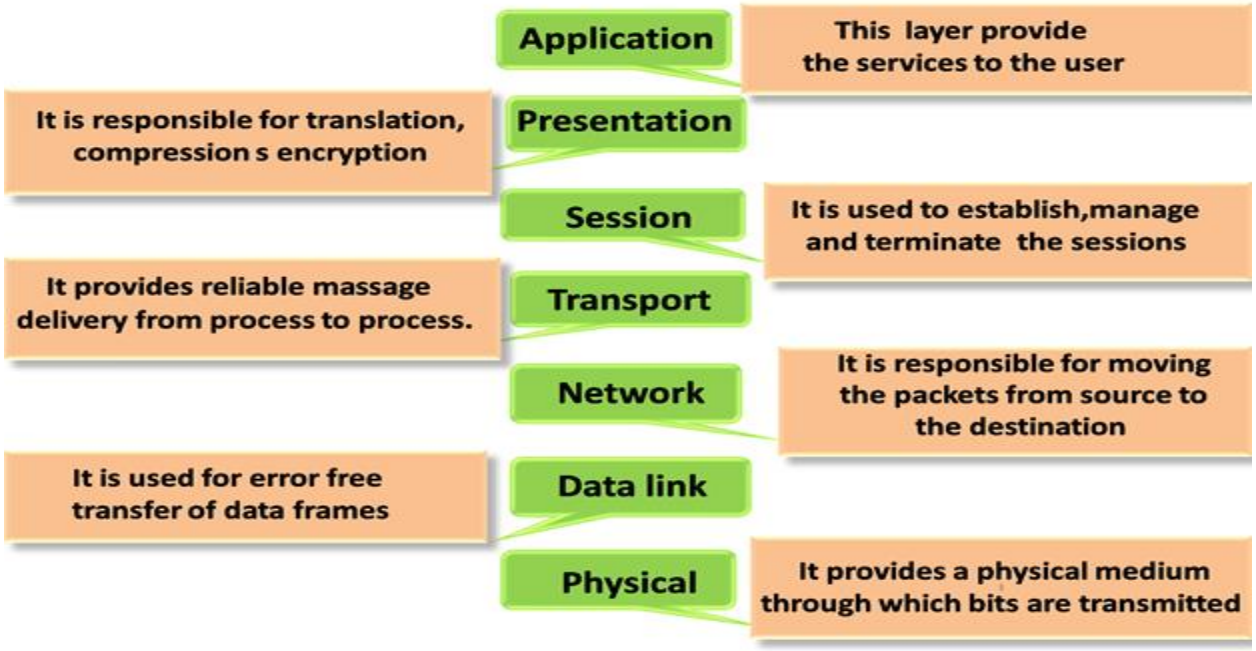
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing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

Functions of the OSI Layers

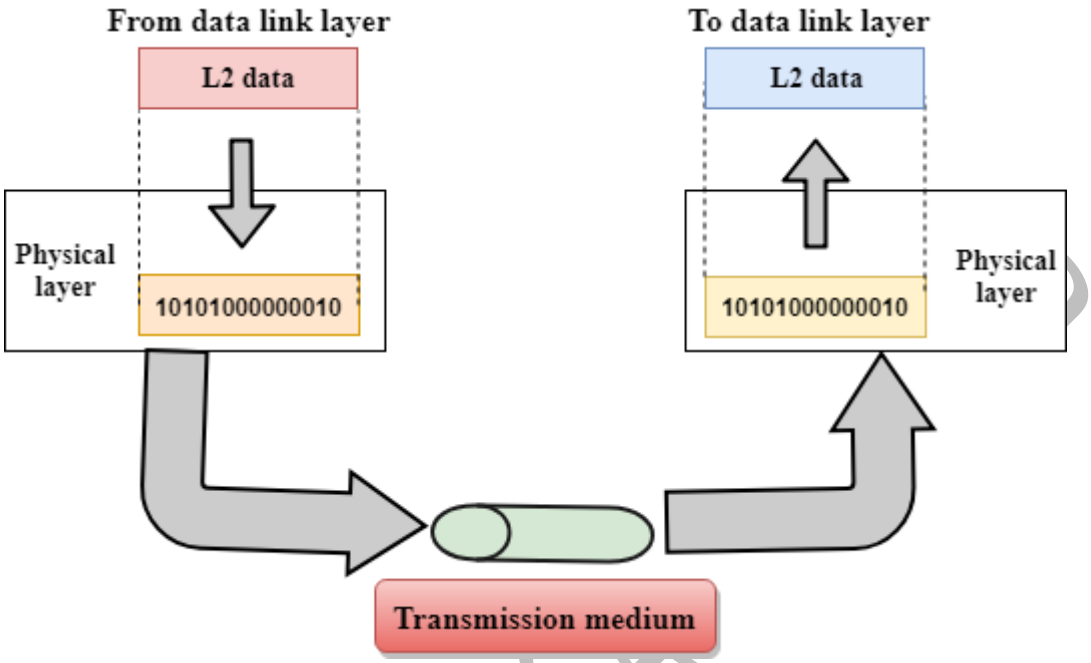
There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

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

EDUCATION HUB



Physical layer

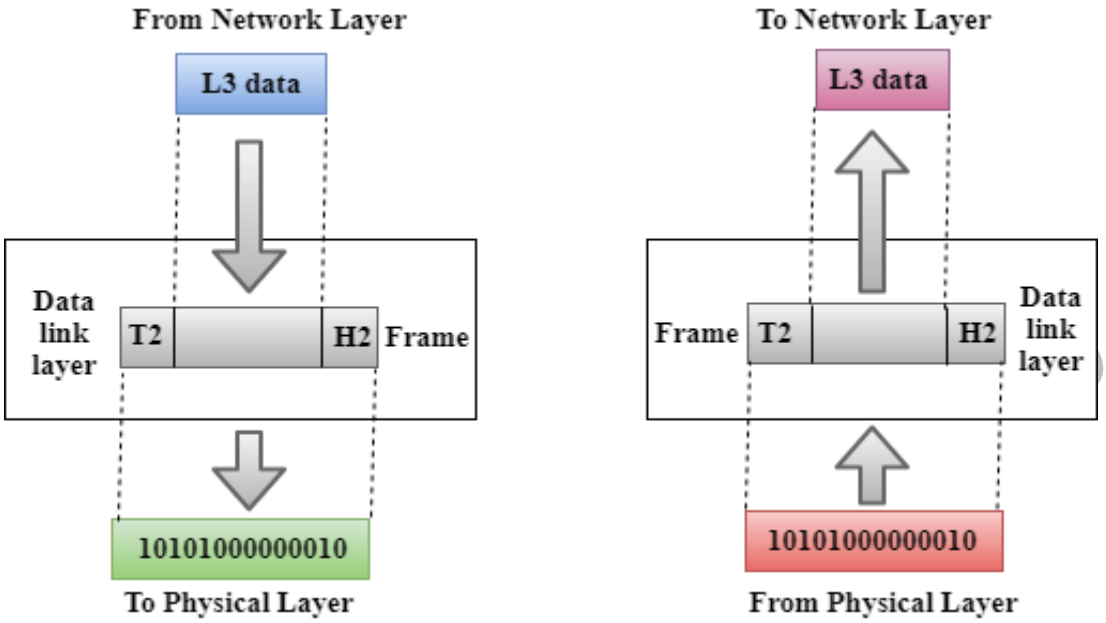


- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

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

DIWAKAR EDUCATION

- It is used for transferring the packets over the network.

Functions of the Data-link layer

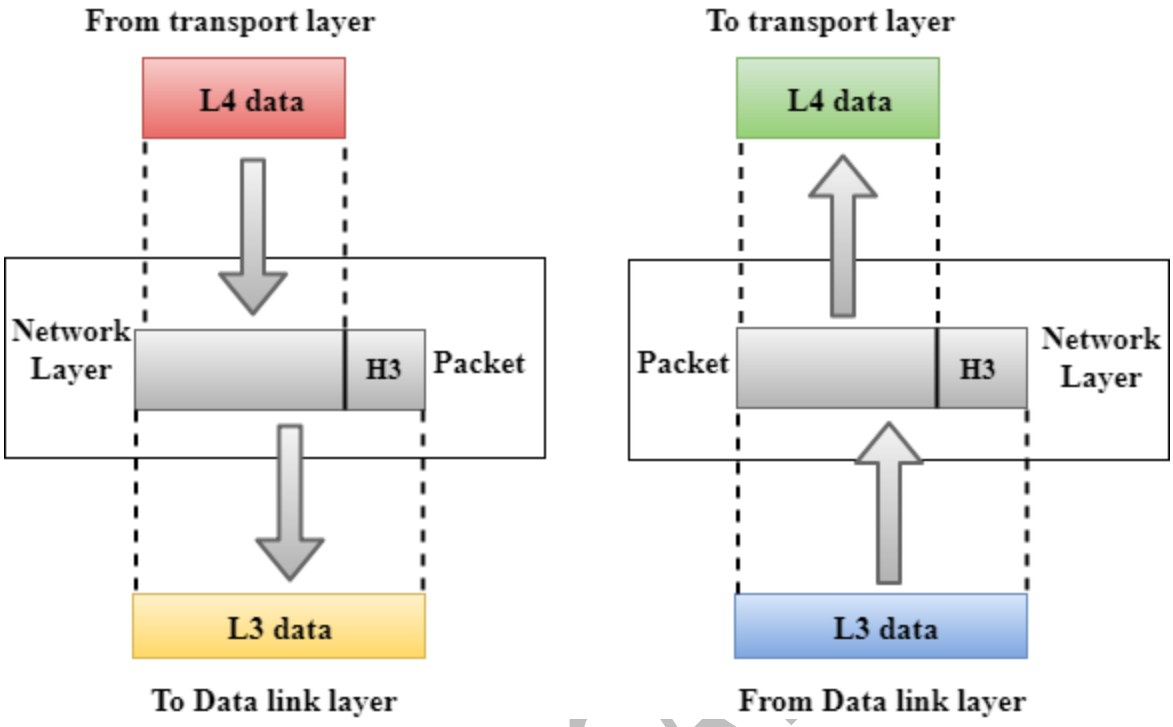
- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.



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

Network Layer

DIWAKAR EDUCATION HUB



- 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.

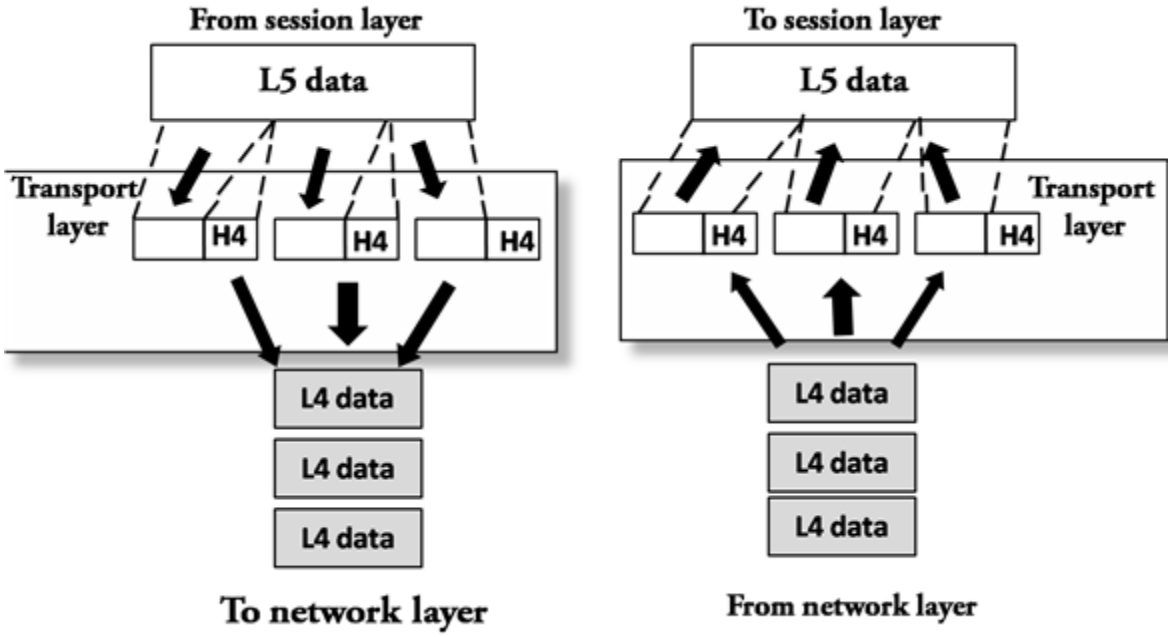
Functions of Network Layer:

- **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.

DIWAKAR EDUCATION

- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Transport Layer



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

The two protocols used in this layer are:

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

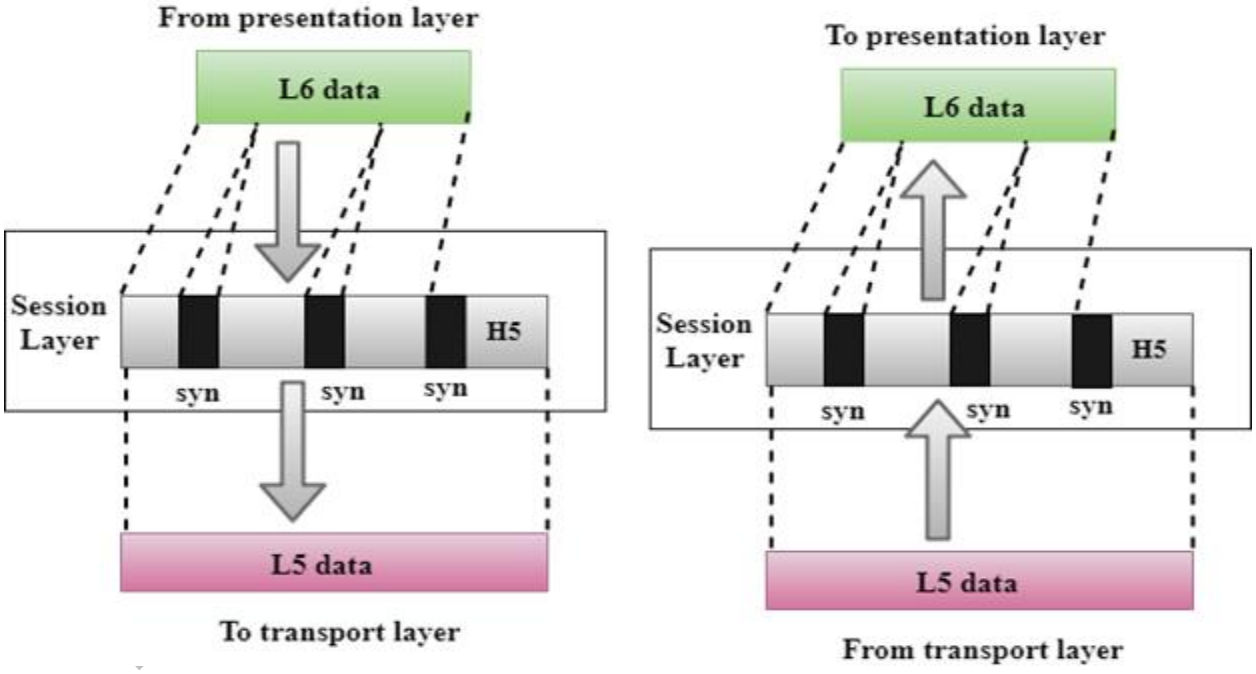
Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

DIWAKAR EDUCATION HUB

- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer

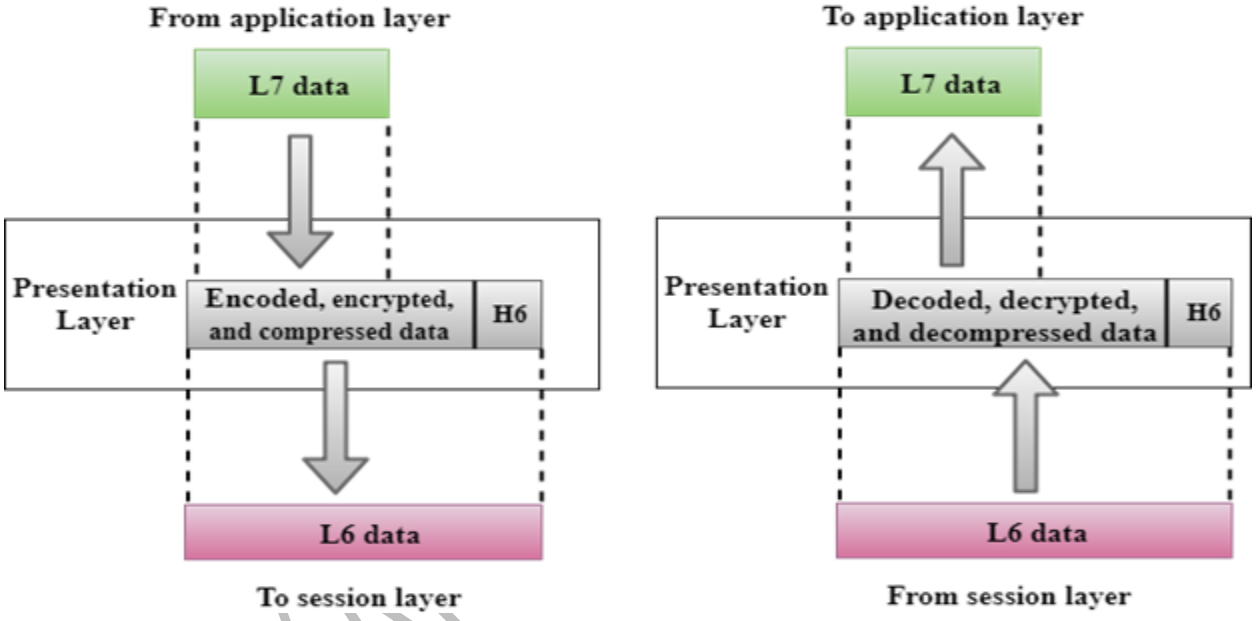


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

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

Presentation Layer



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

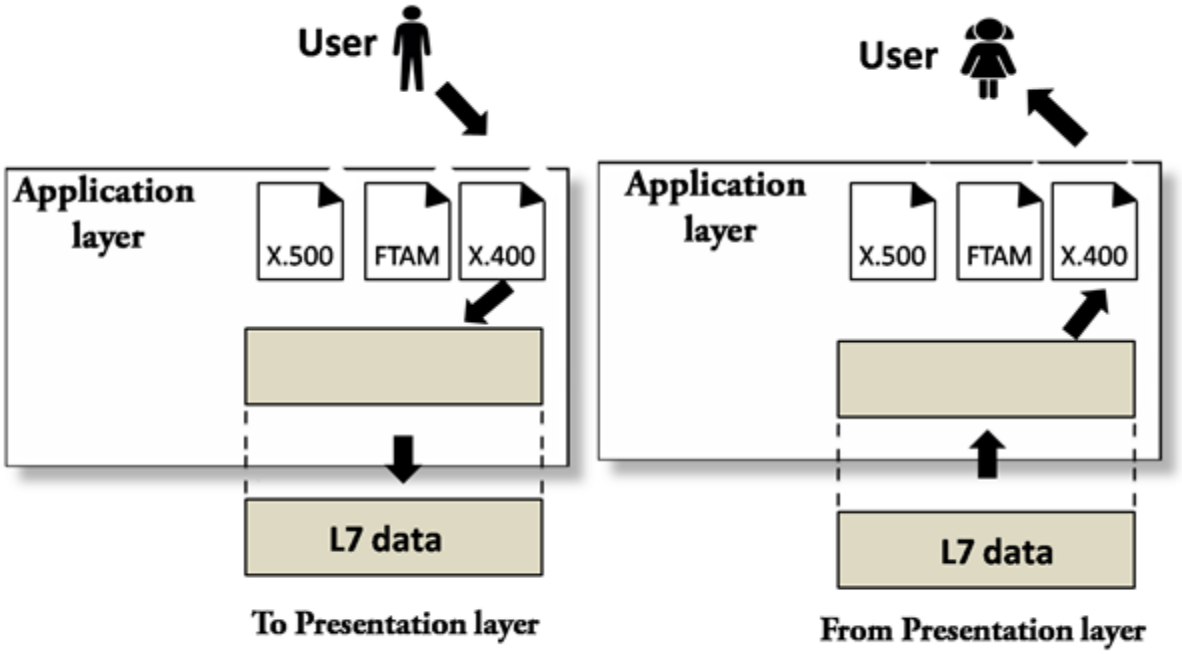
Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the

interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

Application Layer



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

Functions of Application layer:

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

What does OSI Protocols mean?

OSI protocols are a family of standards for information exchange. They consist of a set of rules that should represent a standard for physical connections, cabling, data formats, transmission models, as well as means to ensure correction of errors and missing data.

These protocols were developed and designed by the International Organization of Standardization (ISO). In 1977 the ISO model was introduced, which consisted of seven different layers. This model has been criticized because of its technicality and limited features and never met the goal of becoming universal standard.

Each layer of the ISO model has its own protocols and functions. The OSI protocol stack was later adapted into the TCP/IP stack.

In some networks, protocols are still popular using only the data link and network layers of the OSI model.

OSI Protocols

The OSI protocol stack works on a hierarchical form, from the hardware physical layer to the software application layer. There are a total of seven layers. Data and information are received by each layer from an upper layer.

After the required processing, this layer then passes the information on to the next lower layer. A header is added to the forwarded message for the convenience of the next layer. Each header consists of information such as source and destination addresses, protocol used, sequence number and other flow-control related data.

DIWAKAR EDUCATION HUB

The following are the OSI protocols used in the seven layers of the OSI Model:

Layer 1, the Physical Layer

This layer deals with the hardware of networks such as cabling. It defines the mechanical and electrical standards of interface devices and the types of cables used to transmit digital signals (e.g. optical fiber, coaxial cable, wireless, etc.).

The major protocols used by this layer include Bluetooth, PON, OTN, DSL, IEEE.802.11, IEEE.802.3, L431 and TIA 449.

Layer 2, the Data Link Layer

This layer receives data from the physical layer and compiles it into a transform form called framing or frame. The principal purpose of this layer is to detect transfer errors by adding headers to data packets.

The protocols are used by the Data Link Layer include: ARP, CSLIP, HDLC, IEEE.802.3, PPP, X-25, SLIP, ATM, SDLS and PLIP.

Layer 3, the Network Layer

This is the most important layer of the OSI model, which performs real time processing and transfers data from nodes to nodes. Routers and switches are the devices used for this layer that connects the notes in the network to transmit and control data flow.

The network layer assists the following protocols: Internet Protocol (IPv4), Internet Protocol (IPv6), IPX, AppleTalk, ICMP, IPSec and IGMP.

Layer 4, the Transport Layer

The transport layer works on two determined communication modes: Connection oriented and connectionless. This layer transmits data from source to destination node.

It uses the most important protocols of OSI protocol family, which are: Transmission Control Protocol (TCP), UDP, SPX, DCCP and SCTP.

Layer 5, the Session Layer

DIWAKAR EDUCATION HUB

The session layer creates a session between the source and the destination nodes and terminates sessions on completion of the communication process.

The protocols used are: PPTP, SAP, L2TP and NetBIOS.

Layer 6, the Presentation Layer

The functions of encryption and decryption are defined on this layer. It ensures that data is transferred in standardized formats by converting data formats into a format readable by the application layer.

The following are the presentation layer protocols: XDR, TLS, SSL and MIME.

Layer 7, the Application Layer

This layer works at the user end to interact with user applications. QoS (quality of service), file transfer and email are the major popular services of the application layer.

This layer uses following protocols: HTTP, SMTP, DHCP, FTP, Telnet, SNMP and SMPP.

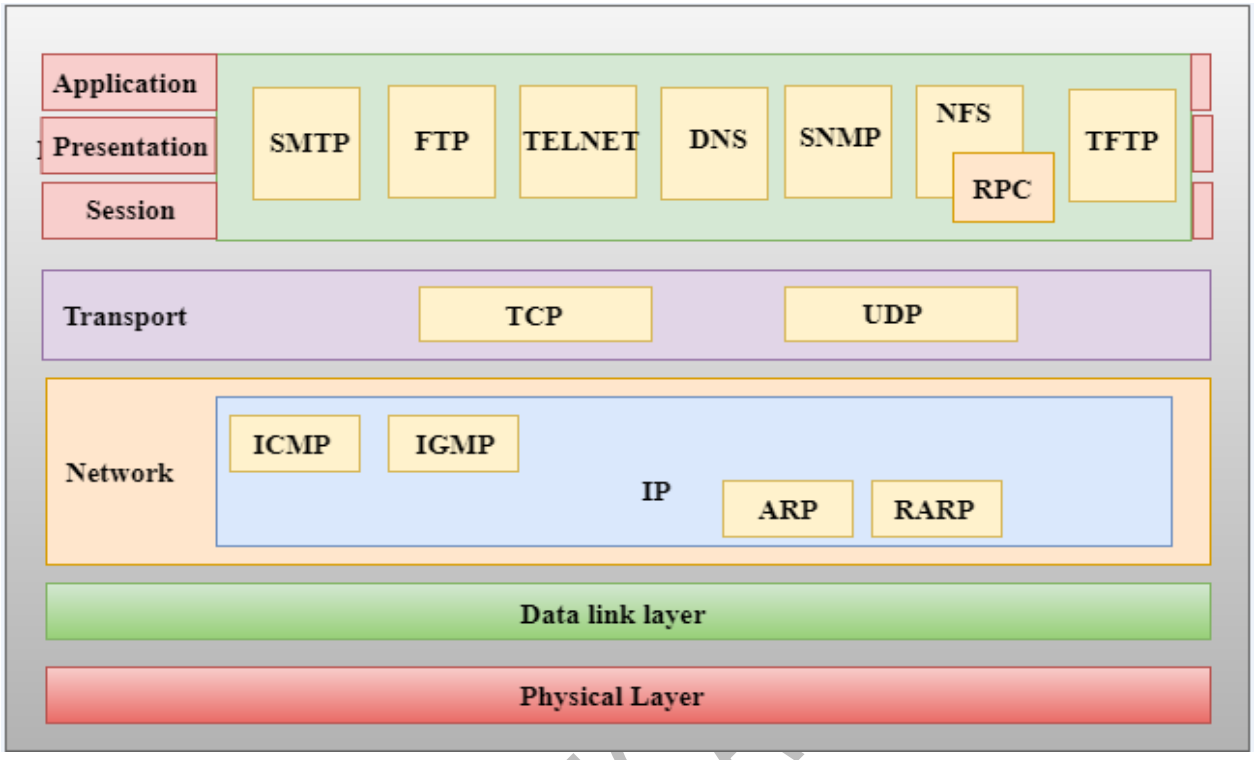
TCP/IP model

- 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:

DIWAKAR EDUCATION HUB



Network Access Layer

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

Internet Layer

- An internet layer is the second layer of the TCP/IP model.

DIWAKAR EDUCA

- 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

DIWAKAR EDUCATION HUB

- 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.

DIWAKAR EDUCATION HUB

Transport Layer

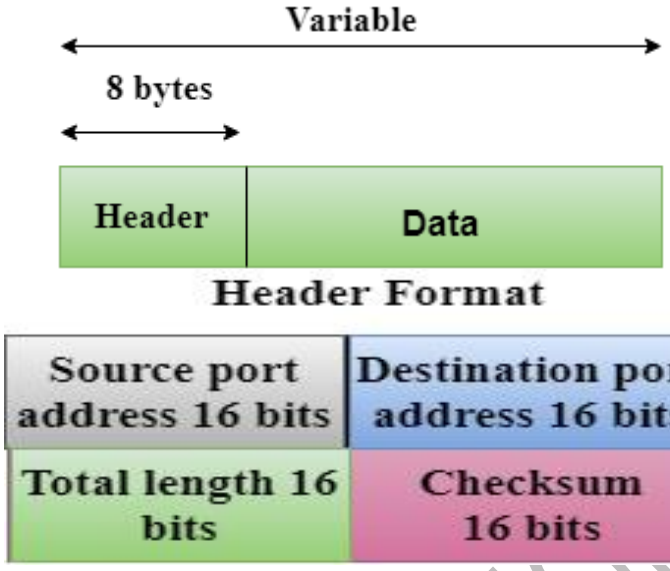
The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

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.

DIWAKAR EDUCATION HUB



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.

DIWAKAR EDUCATION HUB

- 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.

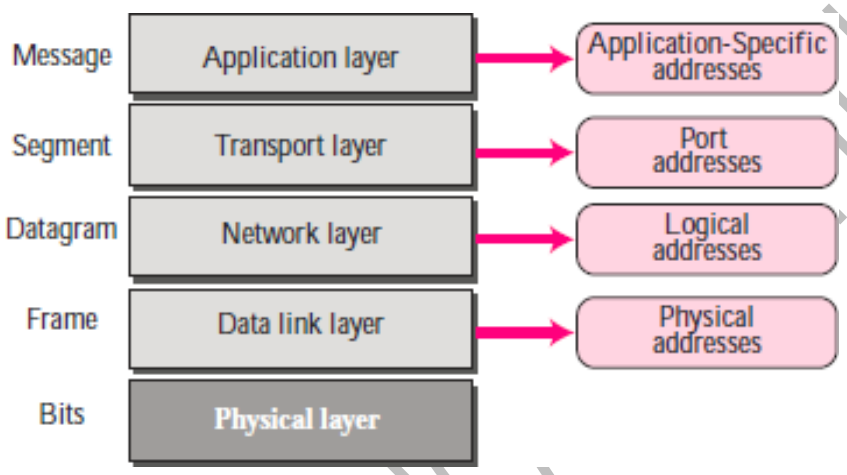
Following are the main protocols used in the application layer:

- **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.

ADDRESSING

DIWAKAR EDUCATION HUB

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical address, logical address, port address, and application-specific address. Each address is related to a one layer in the TCP/IP architecture, as shown in the following Figure.



Physical Addresses

The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address. The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).

Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below.

07:01:02:01:2C:4B

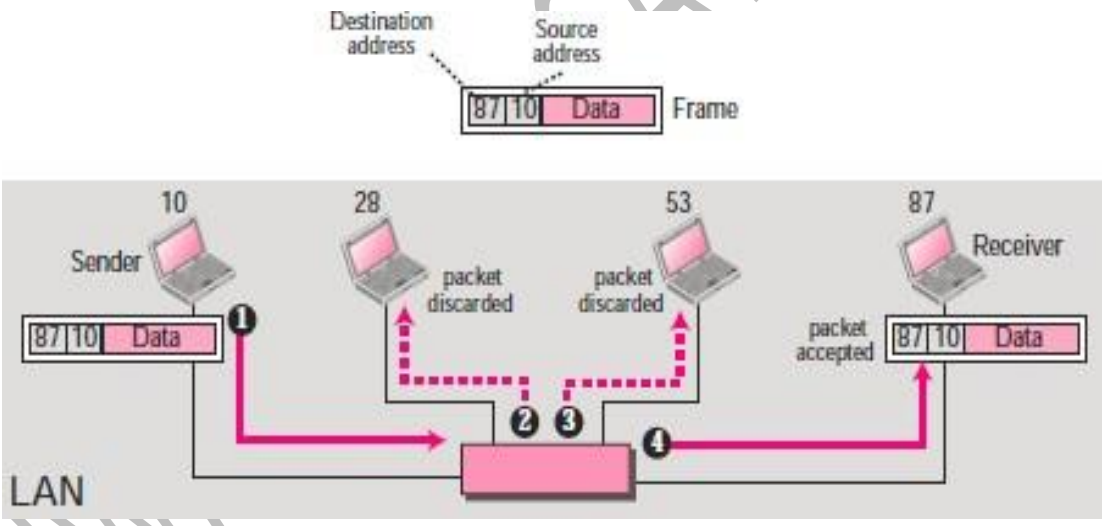
A 6-byte (12 hexadecimal digits) physical address

Example (1)

In Figure below a node with physical address 10 sends a frame to a node with physical address

The two nodes are connected by a link (a LAN). At the data link layer, this frame contains physical (link) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection. The data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. The header, among other pieces of information, carries the receiver and the sender physical (link) addresses.

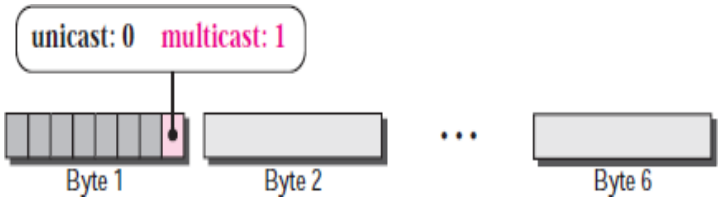
Note that in most data link protocols, the destination address 87 in this case, comes before the source address (10 in this case). The frame is propagated through the LAN. Each station with a physical address other than 87 drops the frame because the destination address in the frame does not match its own physical address. The intended destination computer, however, finds a match between the destination address in the frame and its own physical address. The frame is checked, the header and trailer are dropped, and the data part is decapsulated and delivered to the upper layer.



Unicast, Multicast, and Broadcast Physical Addresses

Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network). Some networks support all three addresses.

A source address is always a unicast address—the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. The least significant bit of the first byte defines the type of address.



Q: Define the type of the following destination addresses:

1. 4A:30:10:21:10:1A

2. 47:20:1B:2E:08:EE

3. FF:FF:FF:FF:FF:FF

Logical Addresses

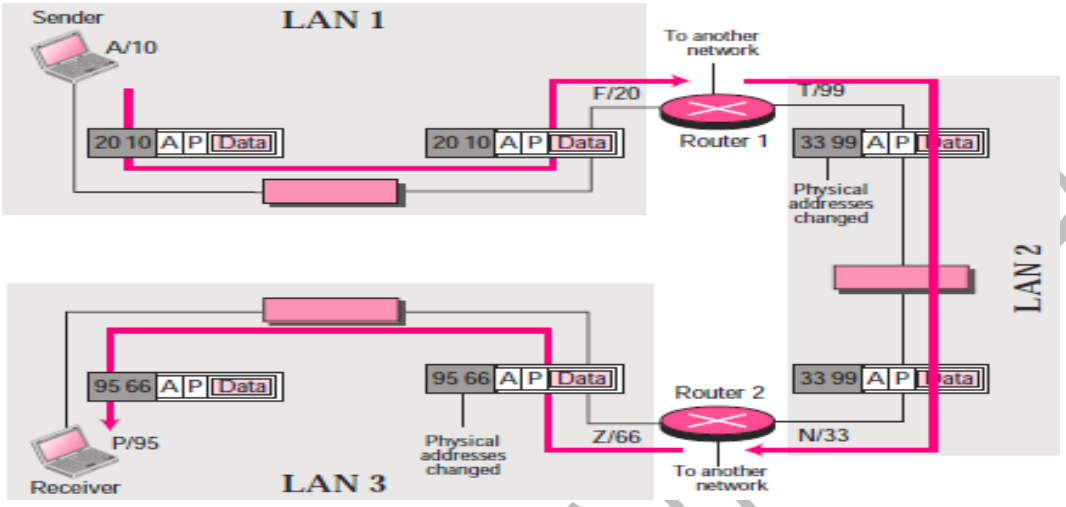
Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32- bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

Example (2)

The Figure below shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection. Although it may be obvious that each router must have a separate physical address for each connection, it may. The computer with logical address **A** and physical address **10** needs to send a packet to the computer with logical address **P** and physical address **95**. The sender encapsulates its data in a packet at the network layer and adds two logical addresses (A and P). Note that in most protocols, the logical source address comes before the logical destination address (contrary to the order of physical addresses). The network layer, however, needs to find the physical address of the

DIWAKAR EDUCATION HUB

next hop before the packet can be delivered. The network layer consults its routing table and finds the logical address of the next hop (router 1) to be F.



Another protocol, Address Resolution Protocol (ARP) finds the physical address of router 1 that corresponds to its logical address (20). Now the network layer passes this address to the data link layer, which in turn, encapsulates the packet with physical destination address 20 and physical source address 10. The router decapsulates the packet from the frame to read the logical destination address P. Since the logical destination address does not match the router's logical address, the router knows that the packet needs to be forwarded. The router consults its routing table and ARP to find the physical destination address of the next hop (router 2), creates a new frame, encapsulates the packet, and sends it to router 2.

Note the physical addresses in the frame. The source physical address changes from 10 to 99. The destination physical address changes from 20 (router 1 physical address) to 33 (router 2 physical address). The logical source and destination addresses must remain the same; otherwise the packet will be lost. At router 2 we have a similar scenario. The physical addresses are changed, and a new frame is sent to the destination computer. When the frame reaches the destination, the packet is decapsulated. The destination logical address P matches the logical address of the computer. The data are decapsulated from the packet and delivered to the upper layer. Note that although physical addresses will change from hop to hop, logical addresses remain the same from the source to destination.

The physical addresses will change from hop to hop, but the logical addresses remain the same.

Unicast, Multicast, and Broadcast Addresses

The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network).

Port Addresses

The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. Computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes.

In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A port address in TCP/IP is 16 bits in length.

753

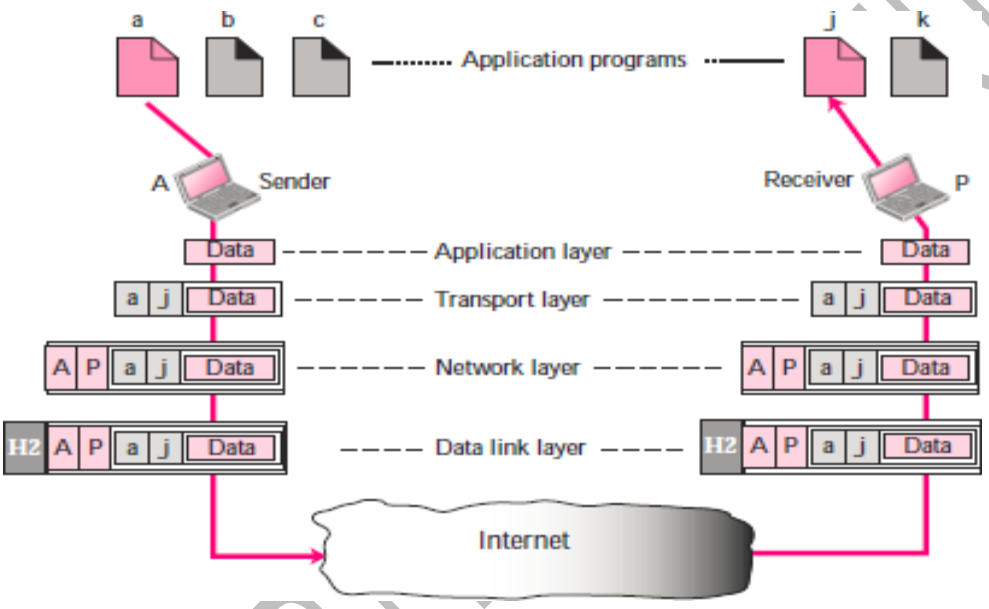
A 16-bit port address represented as one single number

A port address is a 16-bit address represented by one decimal number as shown.

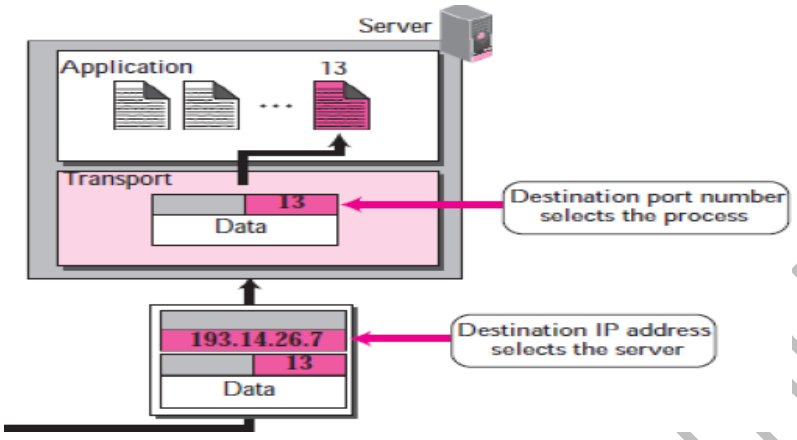
Example (3)

DIWAKAR EDUCATION HUB

The following Figure shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses **a**, **b**, and **c**. The receiving computer is running two processes at this time with port addresses **j** and **k**. Process **a** in the sending computer needs to communicate with process **j** in the receiving computer. Note that although both computers are using the same application, FTP, for example, the port addresses are different because one is a client program and the other is a server program.



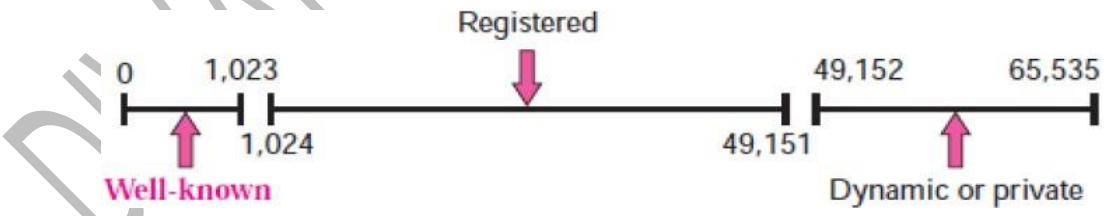
To show that data from process **a** need to be delivered to process **j**, and not **k**, the transport layer encapsulates data from the application layer in a packet and adds two port addresses (**a** and **j**), source and destination. The packet from the transport layer is then encapsulated in another packet at the network layer with logical source and destination addresses (**A** and **P**). Finally, this packet is encapsulated in a frame with the physical source and destination addresses of the next hop. We have not shown the physical addresses because they change from hop to hop inside the cloud designated as the Internet. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.



- In the TCP/IP protocol suite, the port numbers are integers between 0 and 65,535.
- The client program defines itself with a port number, called the **ephemeral port number** (chosen randomly). The word ephemeral means short lived.
- The server process must also define itself with a port number (called well-known port numbers). This port number, however, cannot be chosen randomly.

ICANN Ranges (Internet Corporation for Assigned Names and Numbers)

ICANN has divided the port numbers into three ranges: well-known, registered, and dynamic (or private)



- **Well-known ports:** The ports ranging from 0 to 1,023 are assigned and controlled by ICANN..

- **Registered ports:** The ports ranging from 1,024 to 49,151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.
- **Dynamic ports:** The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used as temporary or private port numbers. The original recommendation was that the ephemeral port numbers for clients be chosen from this range. However, most systems do not follow this recommendation.

Application-Specific Addresses

Some applications have user-friendly addresses that are designed for that specific application. Examples include the e-mail address (for example, co_sci@yahoo.com) and the Universal Resource Locator (URL) (for example, www.mhhe.com). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web. These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.

Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.

DIWAKAR EDUCATION HUB

- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

Why is Switching Concept required?

Switching concept is developed because of the following reasons:

- **Bandwidth:** It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.
- **Collision:** Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.

Advantages of Switching:

- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

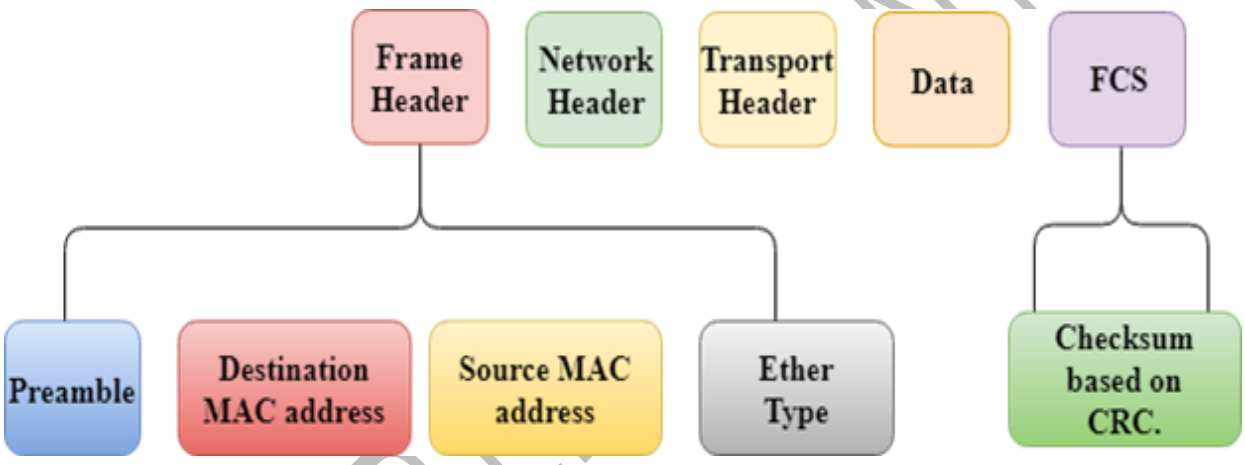
Disadvantages of Switching:

- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

Switching Modes

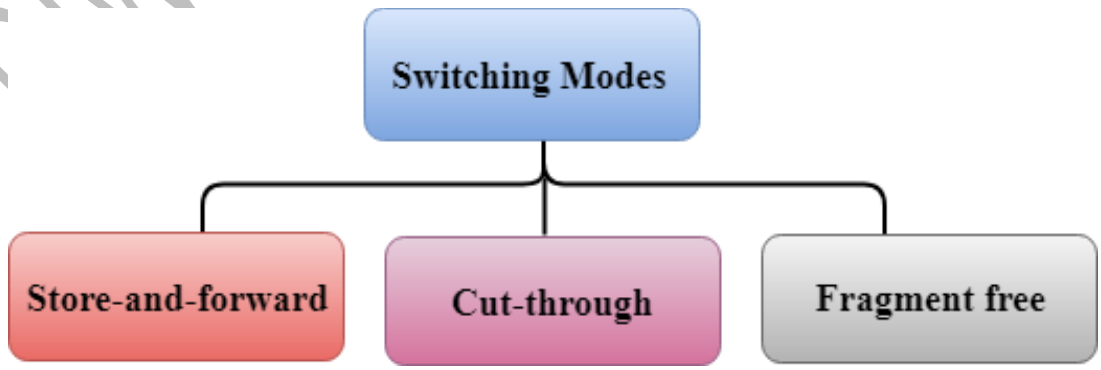
DIWAKAR EDUCATION HUB

- The layer 2 switches are used for transmitting the data on the data link layer, and it also performs error checking on transmitted and received frames.
- The layer 2 switches forward the packets with the help of MAC address.
- Different modes are used for forwarding the packets known as **Switching modes**.
- In **switching mode**, Different parts of a frame are recognized. The frame consists of several parts such as preamble, destination MAC address, source MAC address, user's data, FCS.

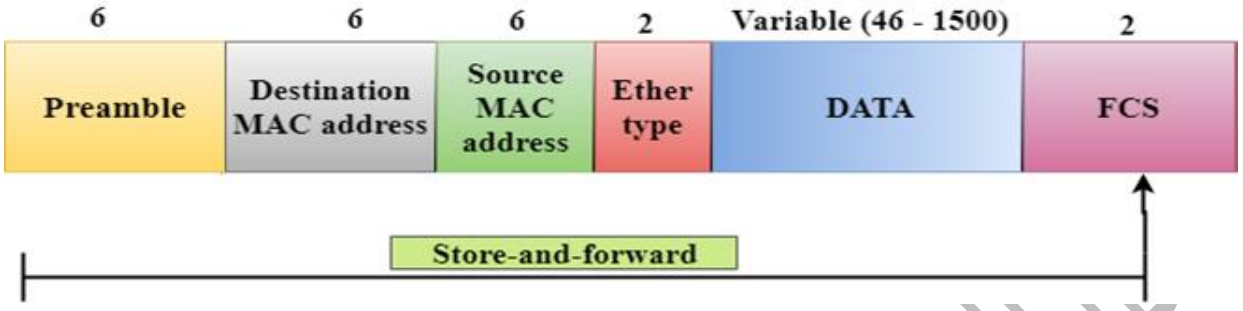


There are three types of switching modes:

- Store-and-forward
- Cut-through
- Fragment-free

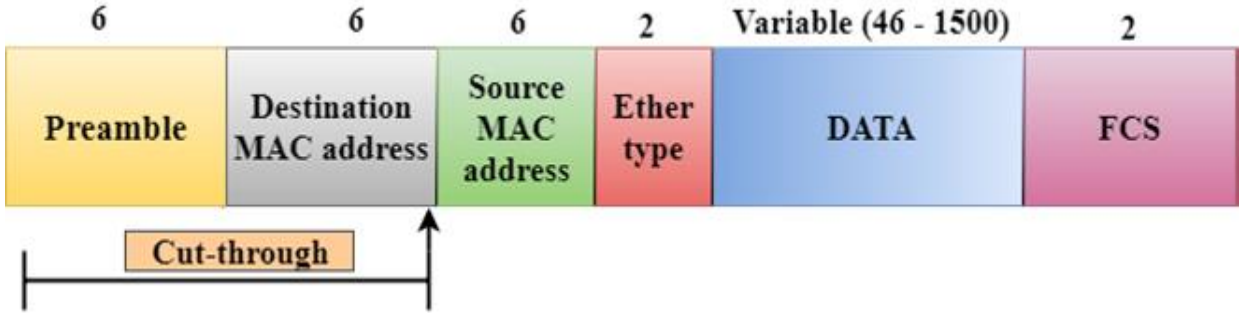


Store-and-forward



- Store-and-forward is a technique in which the intermediate nodes store the received frame and then check for errors before forwarding the packets to the next node.
- The layer 2 switch waits until the entire frame has received. On receiving the entire frame, switch store the frame into the switch buffer memory. This process is known as **storing the frame**.
- When the frame is stored, then the frame is checked for the errors. If any error found, the message is discarded otherwise the message is forwarded to the next node. This process is known as **forwarding the frame**.
- CRC (Cyclic Redundancy Check) technique is implemented that uses a number of bits to check for the errors on the received frame.
- The store-and-forward technique ensures a high level of security as the destination network will not be affected by the corrupted frames.
- Store-and-forward switches are highly reliable as it does not forward the collided frames.

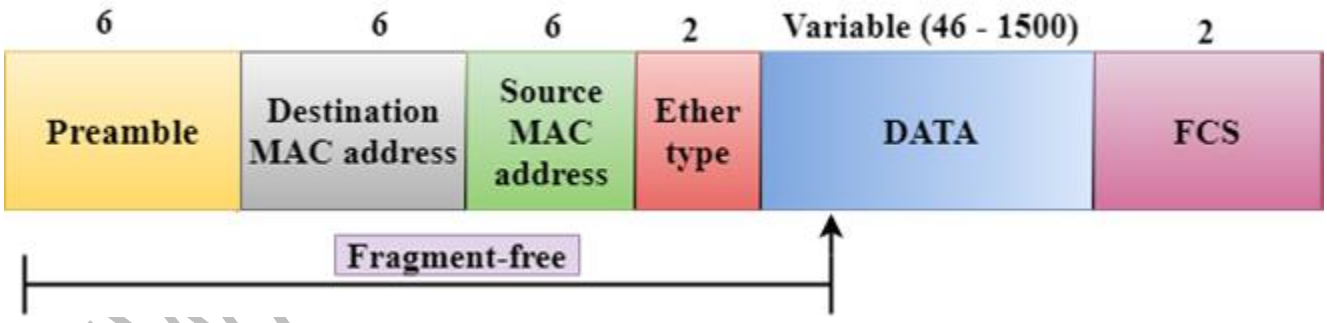
Cut-through Switching



DIWAKAR EDUCATION HUB

- Cut-through switching is a technique in which the switch forwards the packets after the destination address has been identified without waiting for the entire frame to be received.
- Once the frame is received, it checks the first six bytes of the frame following the preamble, the switch checks the destination in the switching table to determine the outgoing interface port, and forwards the frame to the destination.
- It has **low latency** rate as the switch does not wait for the entire frame to be received before sending the packets to the destination.
- It has no **error checking technique**. Therefore, the errors can be sent with or without errors to the receiver.
- A Cut-through switching technique has **low wait time** as it forwards the packets as soon as it identifies the destination MAC address.
- In this technique, collision is not detected, if frames have collided will also be forwarded.

Fragment-free Switching



- A Fragment-free switching is an advanced technique of the Cut-through Switching.
- A Fragment-free switching is a technique that reads atleast 64 bytes of a frame before forwarding to the next node to provide the error-free transmission.
- It combines the speed of Cut-through Switching with the error checking functionality.

- This technique checks the 64 bytes of the ethernet frame where addressing information is available.
- A collision is detected within 64 bytes of the frame, the frames which are collided will not be forwarded further.

Differences b/w Store-and-forward and Cut-through Switching.

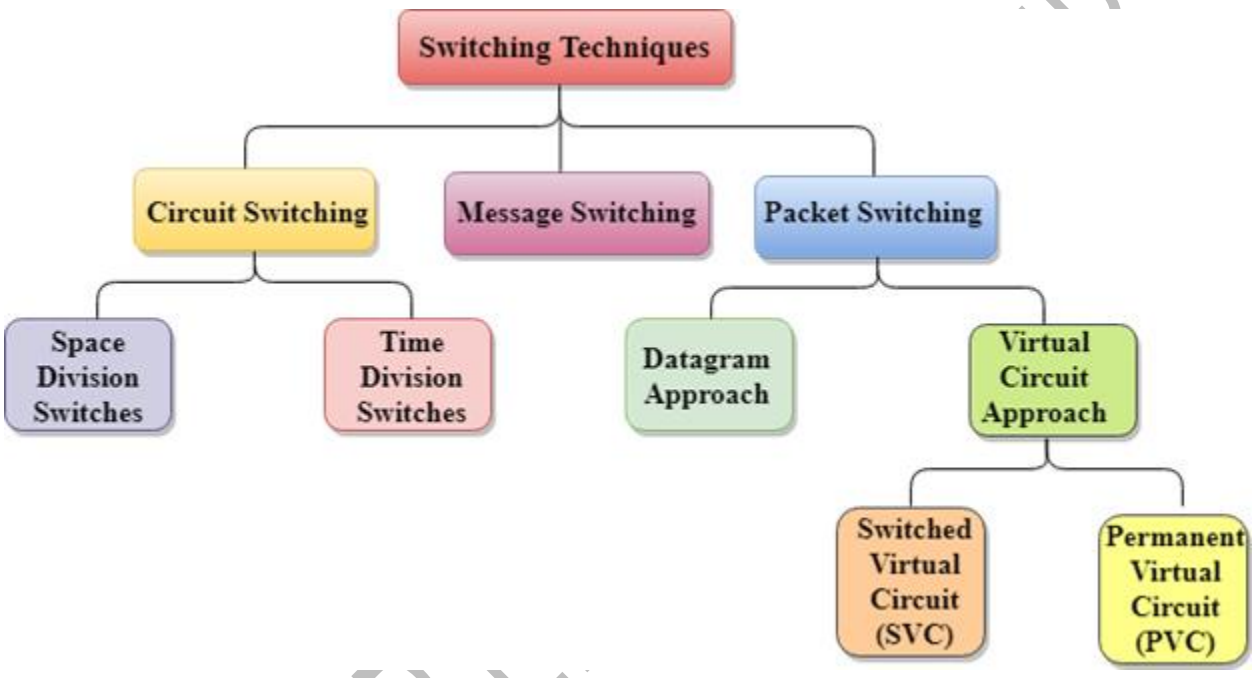
Store-and-forward Switching	Cut-through Switching
Store-and-forward Switching is a technique that waits until the entire frame is received.	Cut-through Switching is a technique that checks the first 6 bytes following the preamble to identify the destination address.
It performs error checking functionality. If any error is found in the frame, the frame will be discarded otherwise forwarded to the next node.	It does not perform any error checking. The frame with or without errors will be forwarded.
It has high latency rate as it waits for the entire frame to be received before forwarding to the next node.	It has low latency rate as it checks only six bytes of the frame to determine the destination address.
It is highly reliable as it forwards only error-free packets.	It is less reliable as compared to Store-and-forward technique as it forwards error prone packets as well.
It has a high wait time as it waits for the entire frame to be received before taking any forwarding decisions.	It has low wait time as cut-through switches do not store the whole frame or packets.

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

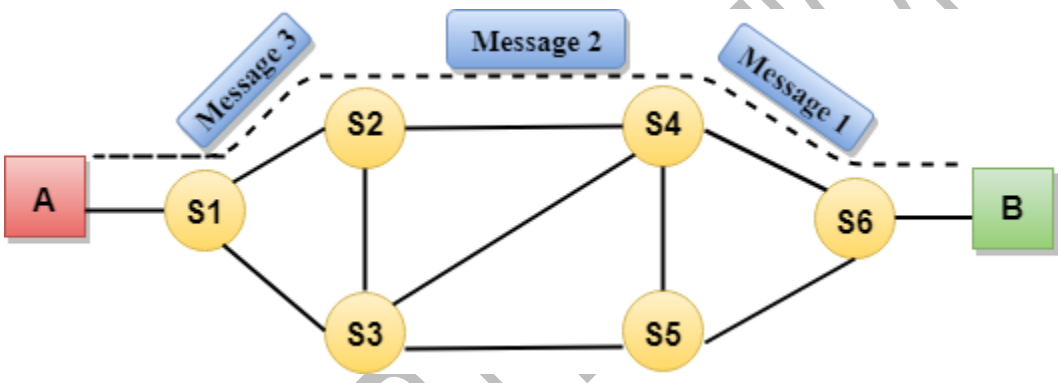
- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates 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.

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 crosspoints.
- Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic crosspoint 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 nonblocking switches.

DIWAKAR EDUCATION HUB

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:

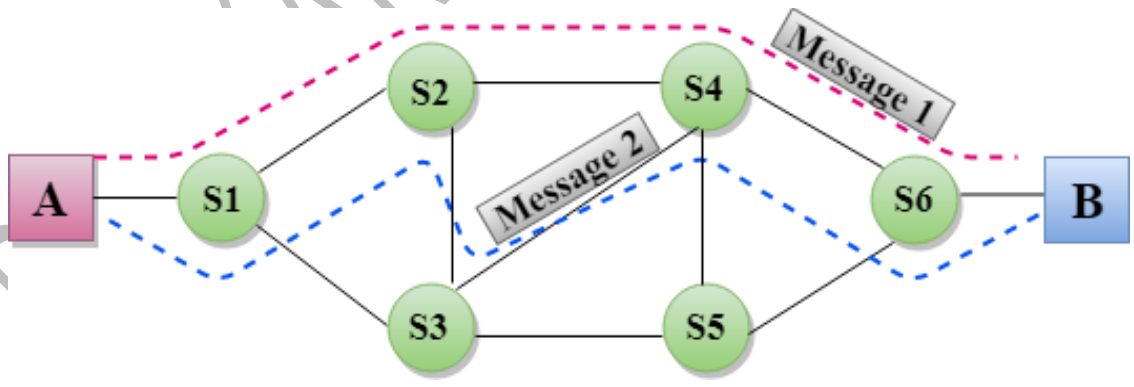
- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.

DIWAKAR EDUCATION HUB

- 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.

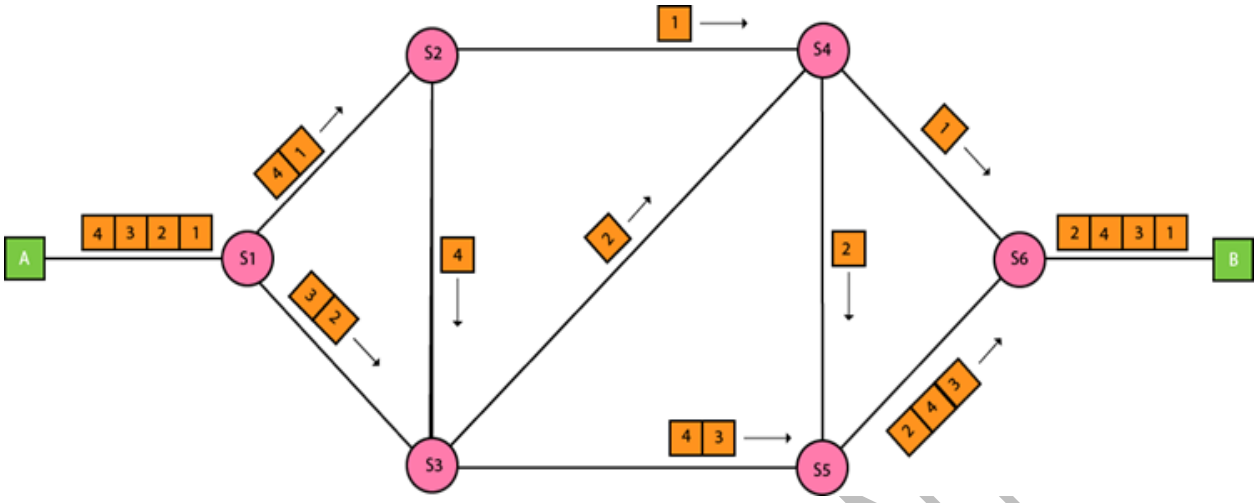
Disadvantages Of Message Switching

- 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.

DIWAKAR EDUCATION HUB



Approaches Of Packet Switching:

There are two approaches to Packet Switching:

Datagram Packet switching:

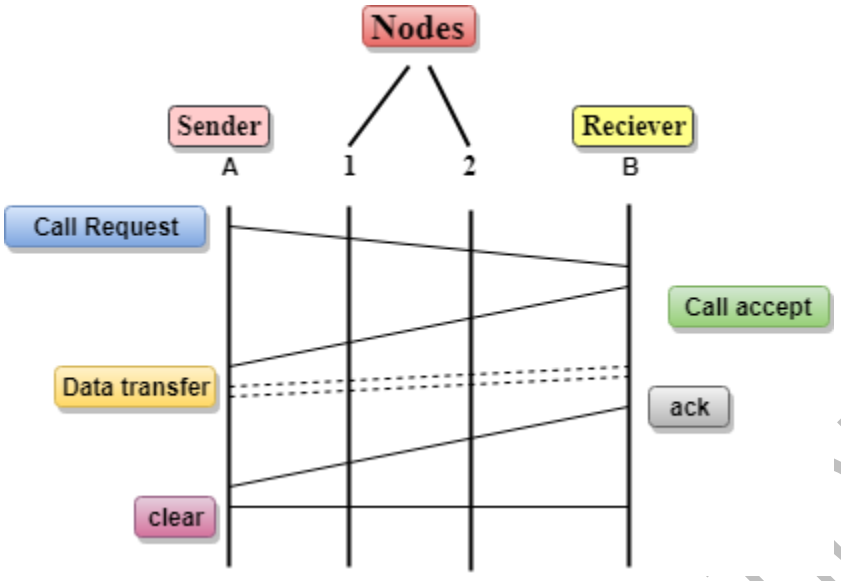
- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving 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.

DIWAKAR EDUCATION

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.

DIWAKAR EDUCATION HUB

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.

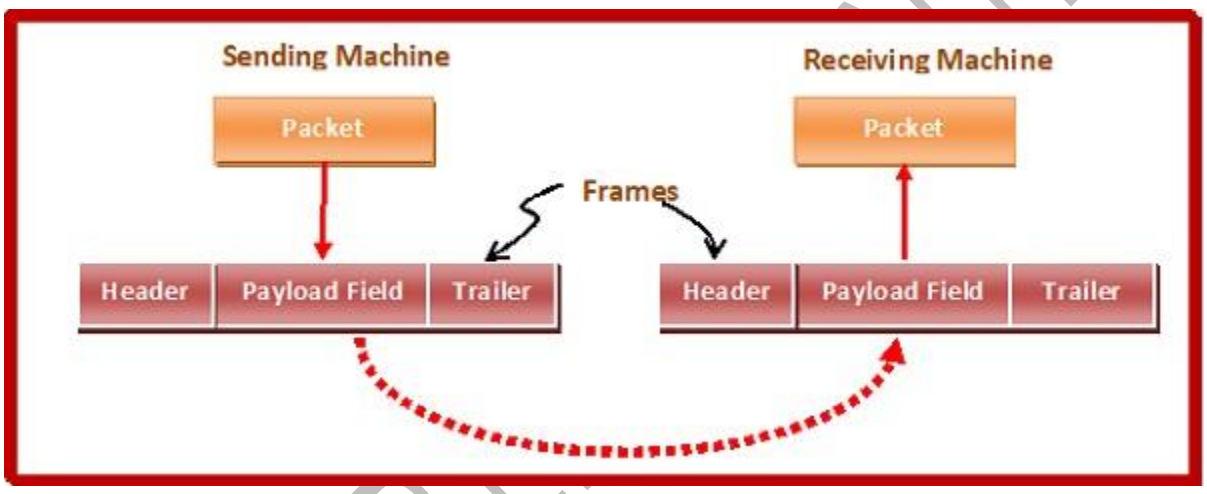
Framing in Data Link Layer

DIWAKAR EDUCATION HUB

In the physical layer, data transmission involves synchronised transmission of bits from the source to the destination. The data link layer packs these bits into frames.

Data-link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. Smaller sized frames makes flow control and error control more efficient.

Then, it sends each frame bit-by-bit on the hardware. At receiver's end, data link layer picks up signals from hardware and assembles them into frames.



Parts of a Frame

A frame has the following parts −

- Frame Header − It contains the source and the destination addresses of the frame.
- Payload field − It contains the message to be delivered.
- Trailer − It contains the error detection and error correction bits.
- Flag − It marks the beginning and end of the frame.



Types of Framing

Framing can be of two types, fixed sized framing and variable sized framing.

Fixed-sized Framing

Here the size of the frame is fixed and so the frame length acts as delimiter of the frame. Consequently, it does not require additional boundary bits to identify the start and end of the frame.

Example − ATM cells.

Variable – Sized Framing

Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame.

It is used in local area networks.

Two ways to define frame delimiters in variable sized framing are −

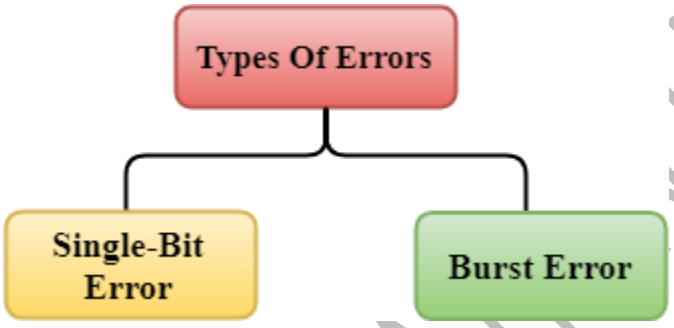
- **Length Field** − Here, a length field is used that determines the size of the frame. It is used in Ethernet (IEEE 802.3).
- **End Delimiter** − Here, a pattern is used as a delimiter to determine the size of frame. It is used in Token Rings. If the pattern occurs in the message, then two approaches are used to avoid the situation −
    - **Byte – Stuffing** − A byte is stuffed in the message to differentiate from the delimiter. This is also called character-oriented framing.
    - **Bit – Stuffing** − A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit – oriented framing.

DIWAKAR EDUCATION HUB

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

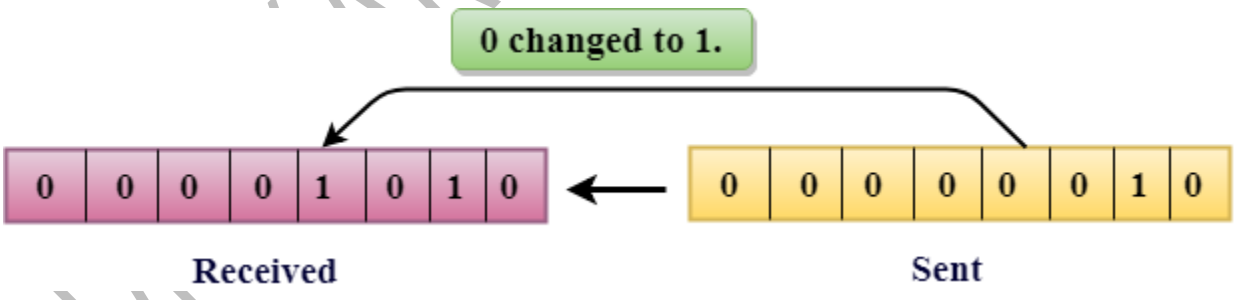


Errors can be classified into two categories:

- 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.

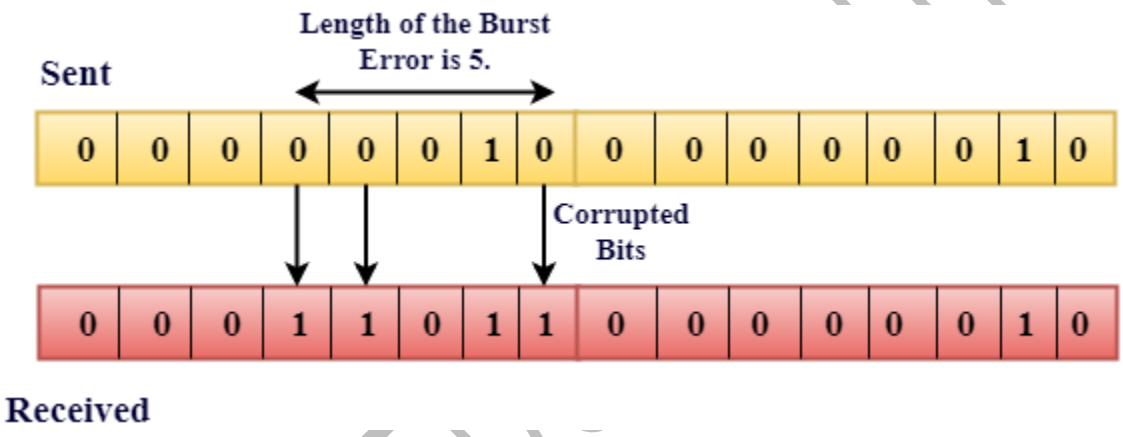
Single-Bit Error does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.

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 occurr in Serial Data Transmission.

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

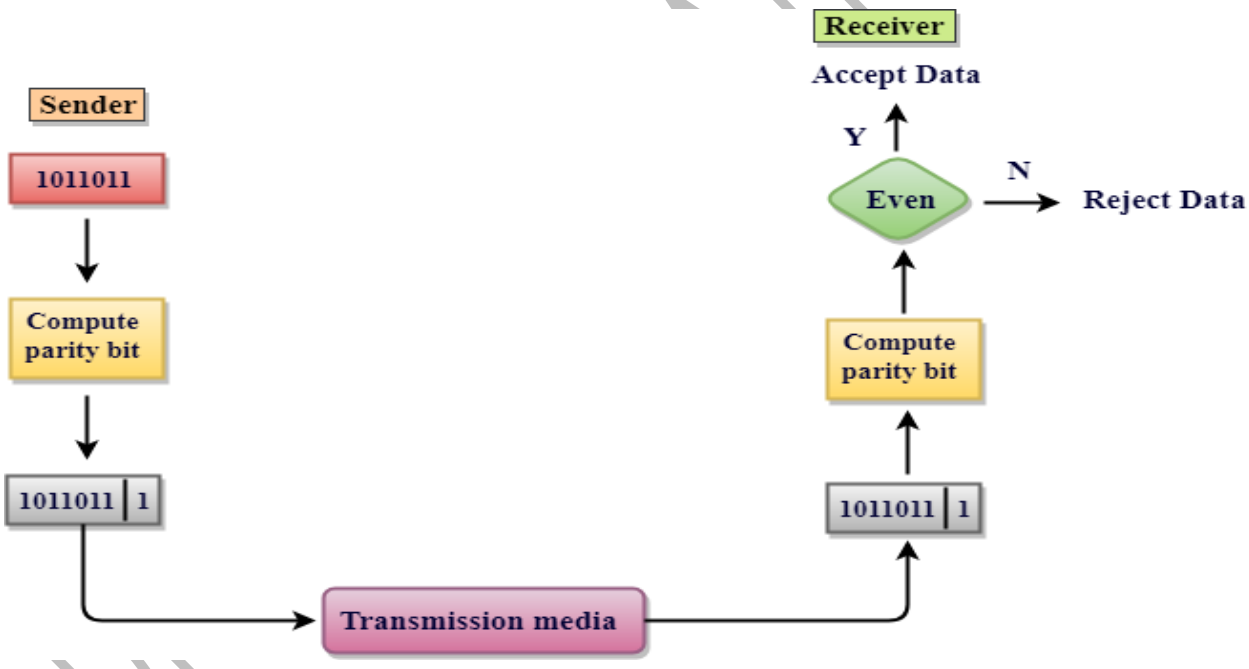
Error Detecting Techniques:

The most popular Error Detecting Techniques are:

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

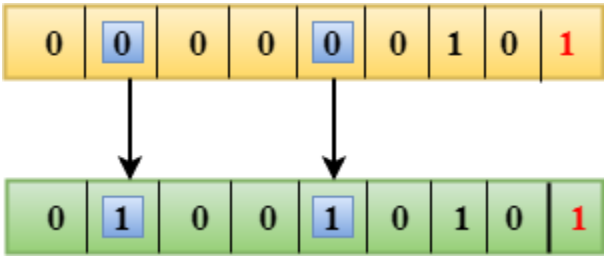
Single Parity Check

- 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.



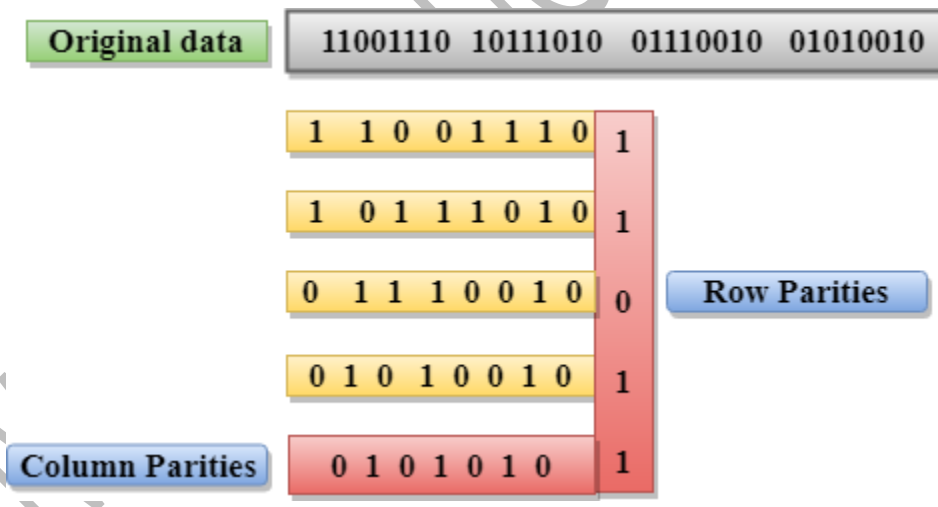
Drawbacks Of Single Parity Checking

- 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 are 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

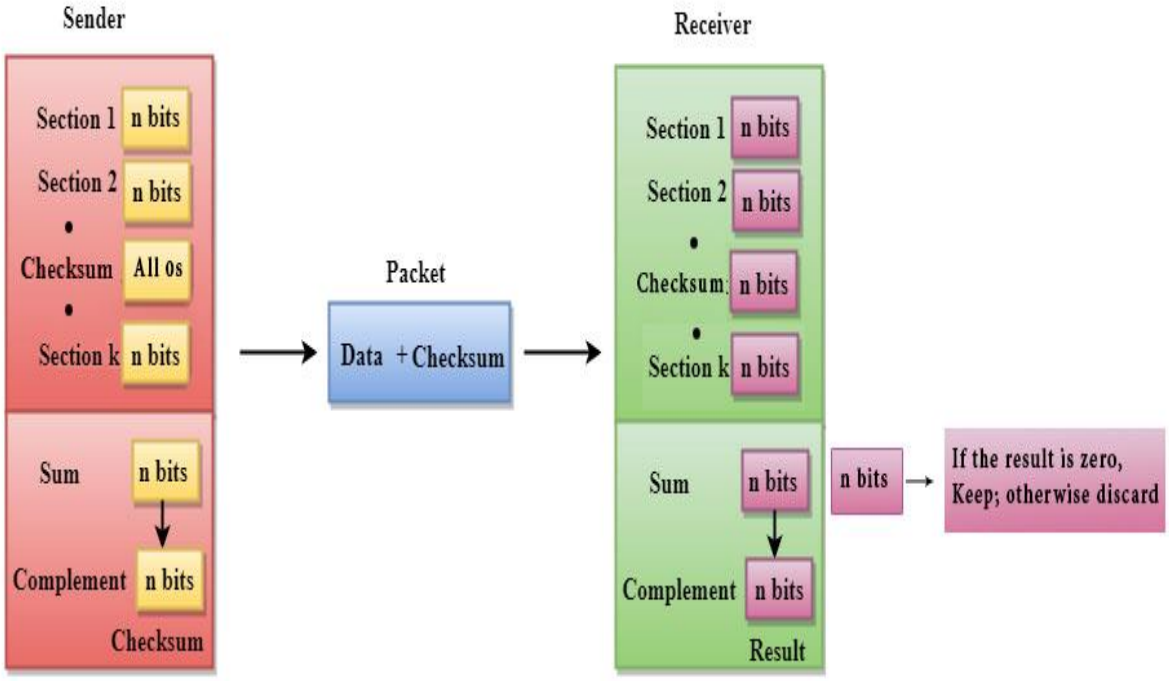
A Checksum is an error detection technique based on the concept of redundancy.

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



1. The Sender follows the given steps:
2. The block unit is divided into k sections, and each of n bits.
3. All the k sections are added together by using one's complement to get th e sum.

4. The sum is complemented and it becomes the checksum field.
5. 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.

1. The Receiver follows the given steps:
2. The block unit is divided into k sections and each of n bits.
3. All the k sections are added together by using one's complement algorith m to get the sum.
4. The sum is complemented.
5. If the result of the sum is zero, then the data is accepted otherwise the dat a is discarded.

Cyclic Redundancy Check (CRC)

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

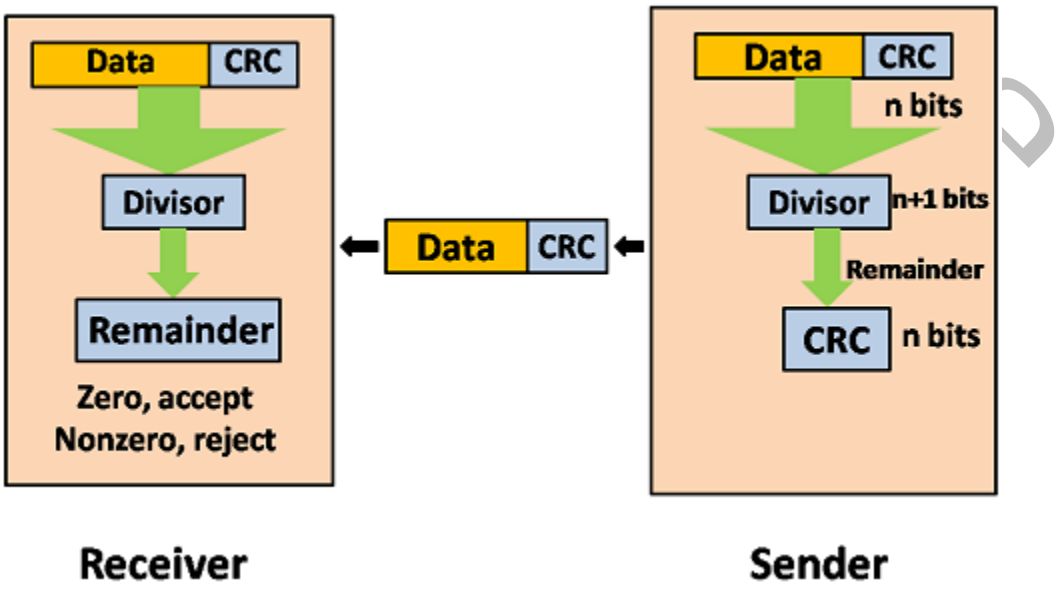
Following are the steps used in CRC for error detection:

- 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.

DIWAKAR EDUCATION HUB

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.

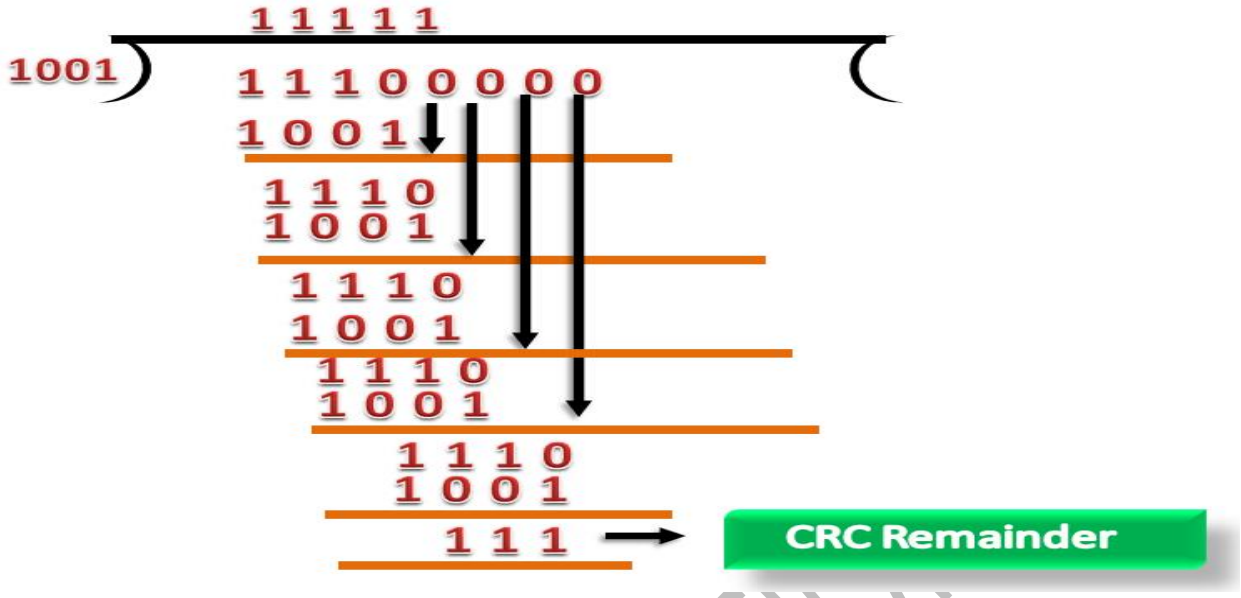


this concept through an example:

Suppose the original data is 11100 and divisor is 1001.

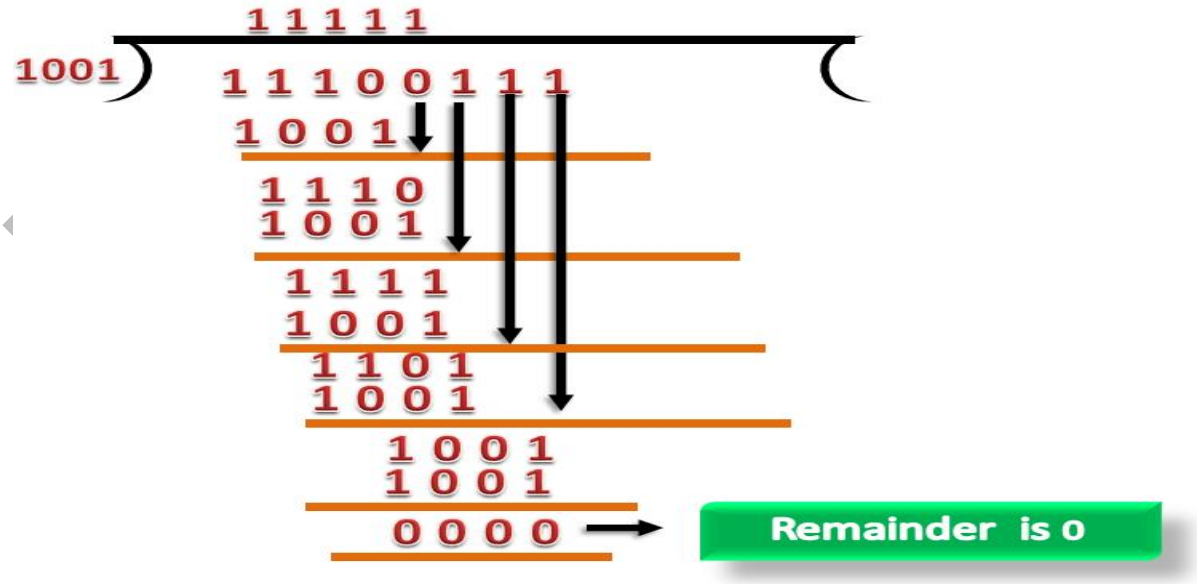
CRC Generator

- 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.

DIWAKAR EDUCATION HUB

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

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.

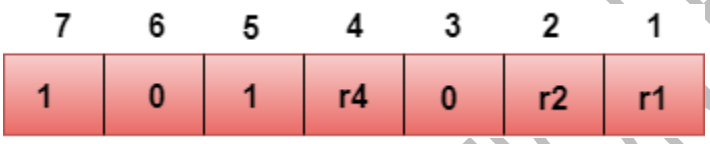
Total number of bits = d+r = 4+3 = 7;

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**.

1. The position of r1 = 1
2. The position of r2 = 2
3. The position of r4 = 4

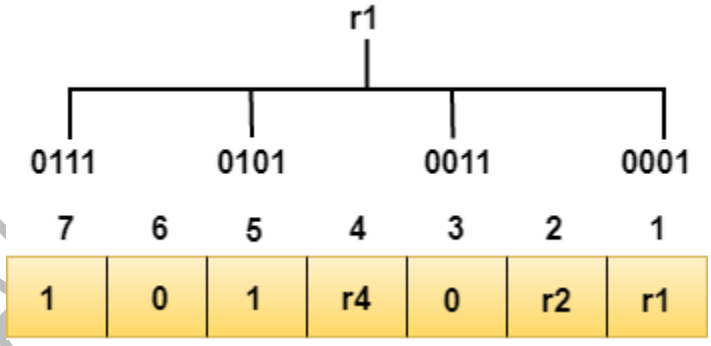
Representation of Data on the addition of parity bits:



Determining the Parity bits

Determining the r1 bit

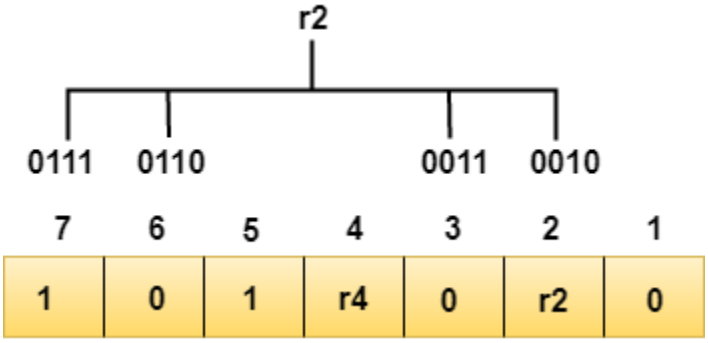
The r1 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the first position.



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

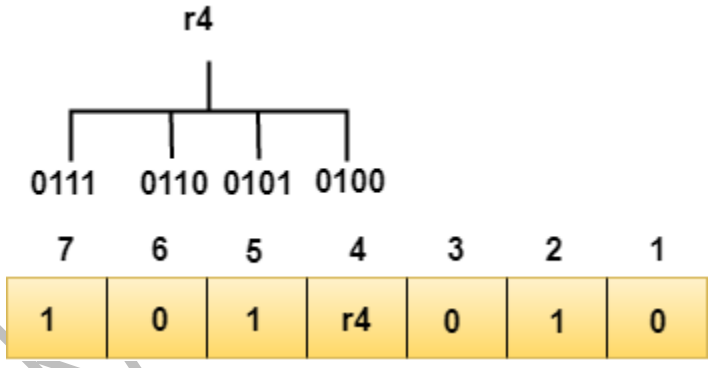
The r2 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the second position.



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**.

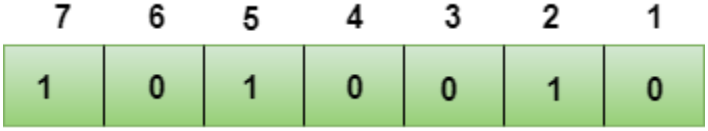
Determining r4 bit

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**.

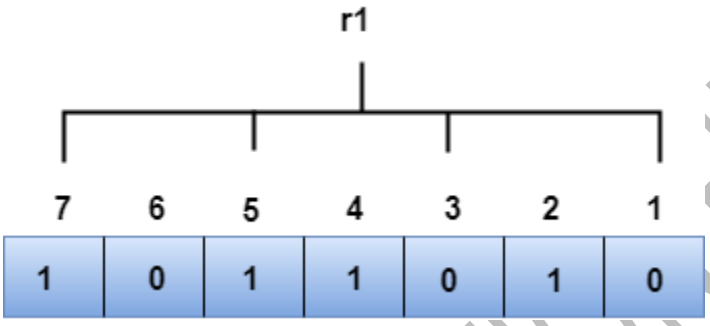
Data transferred is given below:



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

R1 bit

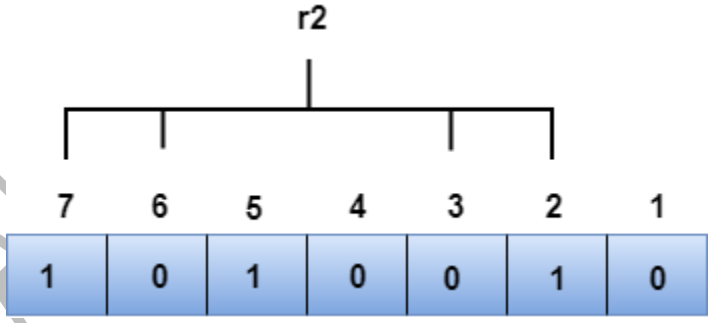
The bit positions of the r1 bit are 1,3,5,7



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

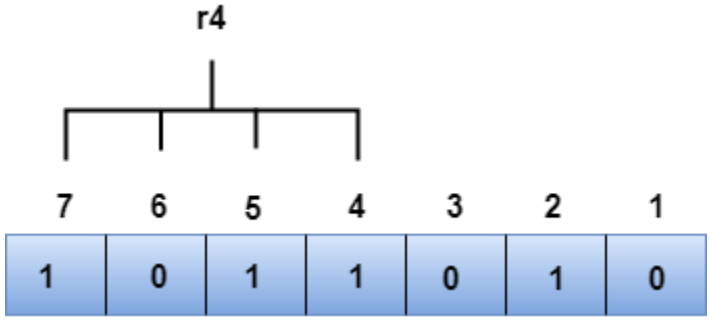
The bit positions of r2 bit are 2,3,6,7.



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.

- The binary representation of redundant bits, i.e., r4r2r1 is 100, and its corresponding decimal value is 4. Therefore, the error occurs in a 4th bit position. The bit value must be changed from 1 to 0 to correct the error.

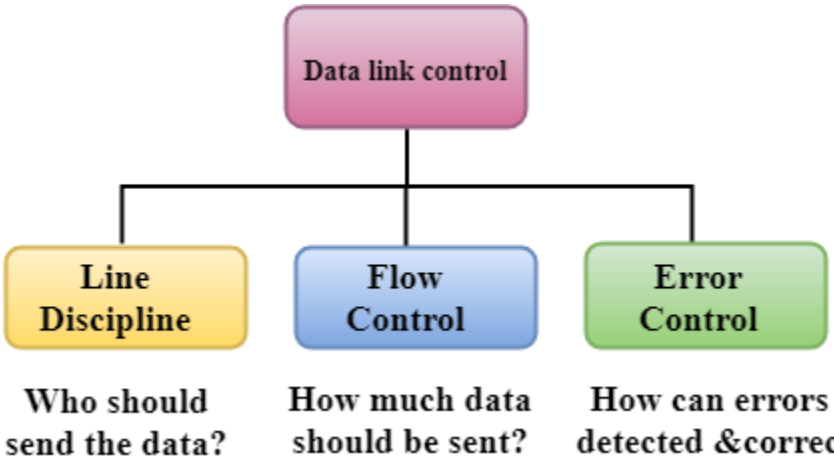
Data Link Controls

Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium. For example, In the half-duplex transmission mode, one device can only transmit the data at a time. If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs.

The Data link layer provides three functions:

- Line discipline
- Flow Control
- Error Control

DIWAKAR EDUCATION HUB



Line Discipline

- Line Discipline is a functionality of the Data link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.

Line Discipline can be achieved in two ways:

- ENQ/ACK
- Poll/select

END/ACK

END/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one.

END/ACK coordinates which device will start the transmission and whether the recipient is ready or not.

Working of END/ACK

The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.

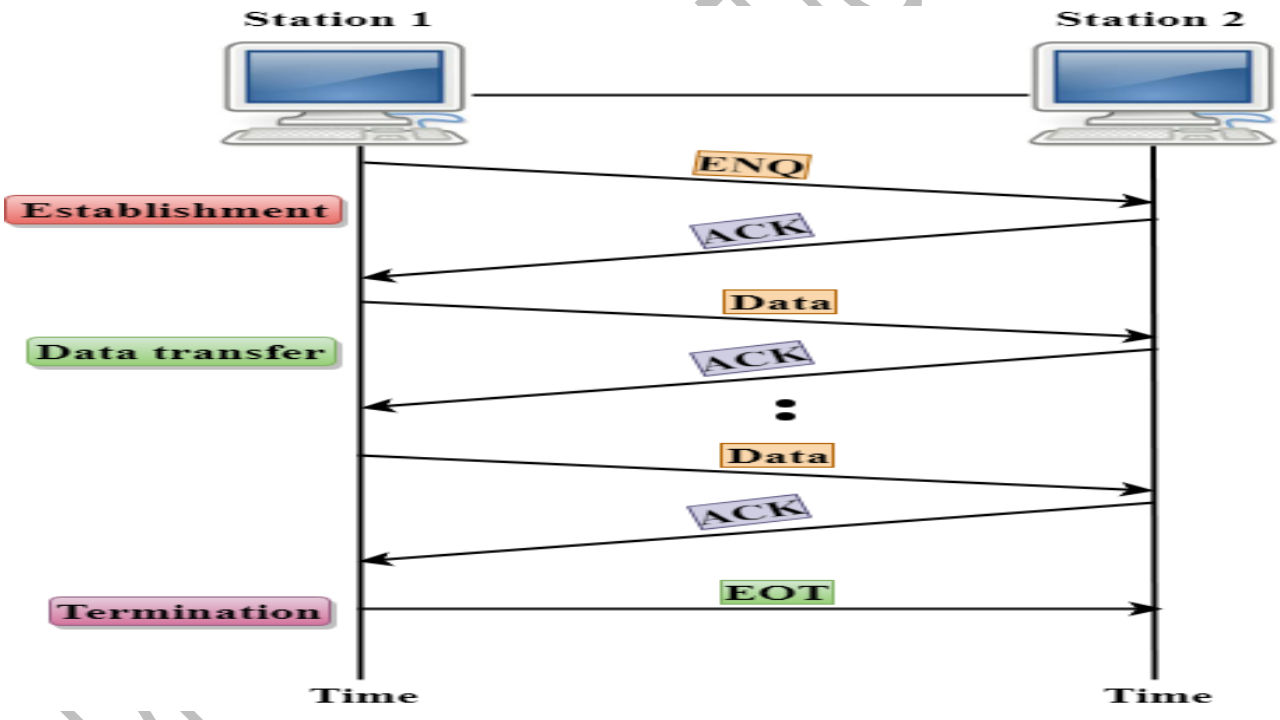
The receiver responses either with the positive acknowledgement(ACK) or with the negative acknowledgement(NACK) where positive acknowledgement means

DIWAKAR EDUCATION HUB

that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

Following are the responses of the receiver:

- If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (END-of-Transmission) frame.
- If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.
- If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.



Poll/Select

The Poll/Select method of line discipline works with those topologies where one device is designated as a primary station, and other devices are secondary stations.

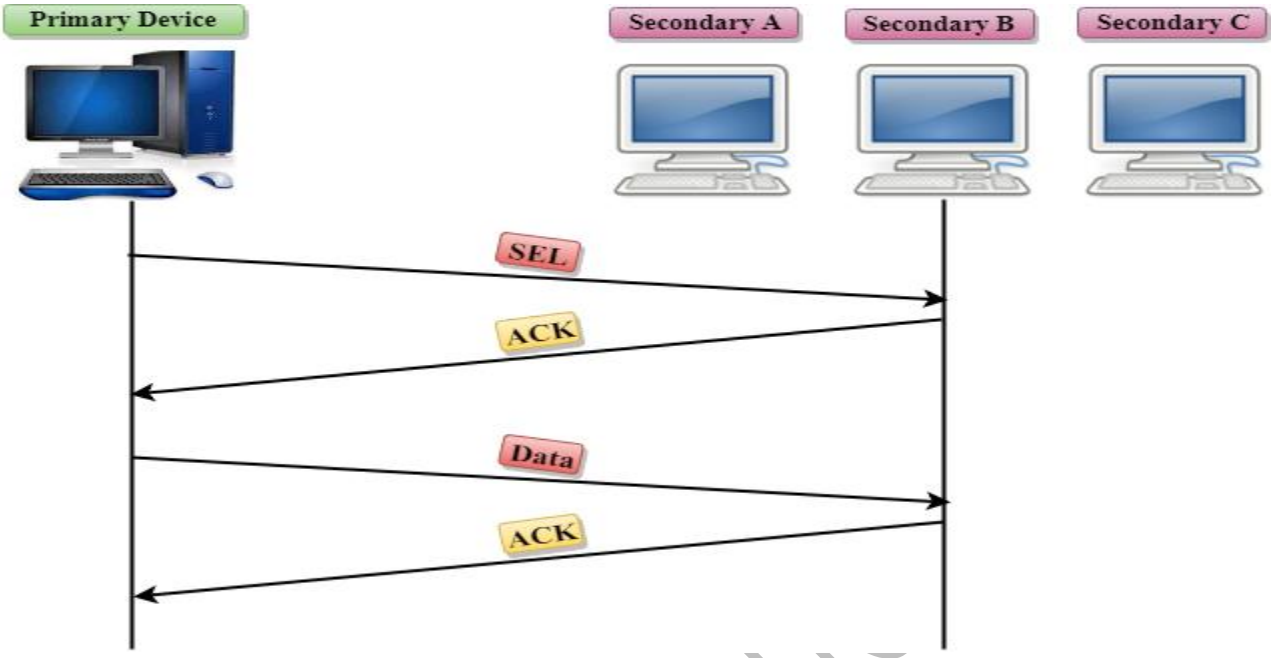
Working of Poll/Select

- In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.
- The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.
- The primary device determines which device is allowed to use the communication channel. Therefore, we can say that it is an initiator of the session.
- If the primary device wants to receive the data from the secondary device, it asks the secondary device that they anything to send, this process is known as polling.
- If the primary device wants to send some data to the secondary device, then it tells the target secondary to get ready to receive the data, this process is known as selecting.

Select

- The select mode is used when the primary device has something to send.
- When the primary device wants to send some data, then it alerts the secondary device for the upcoming transmission by transmitting a Select (SEL) frame, one field of the frame includes the address of the intended secondary device.
- When the secondary device receives the SEL frame, it sends an acknowledgement that indicates the secondary ready status.
- If the secondary device is ready to accept the data, then the primary device sends two or more data frames to the intended secondary device. Once the data has been transmitted, the secondary sends an acknowledgement specifies that the data has been received.

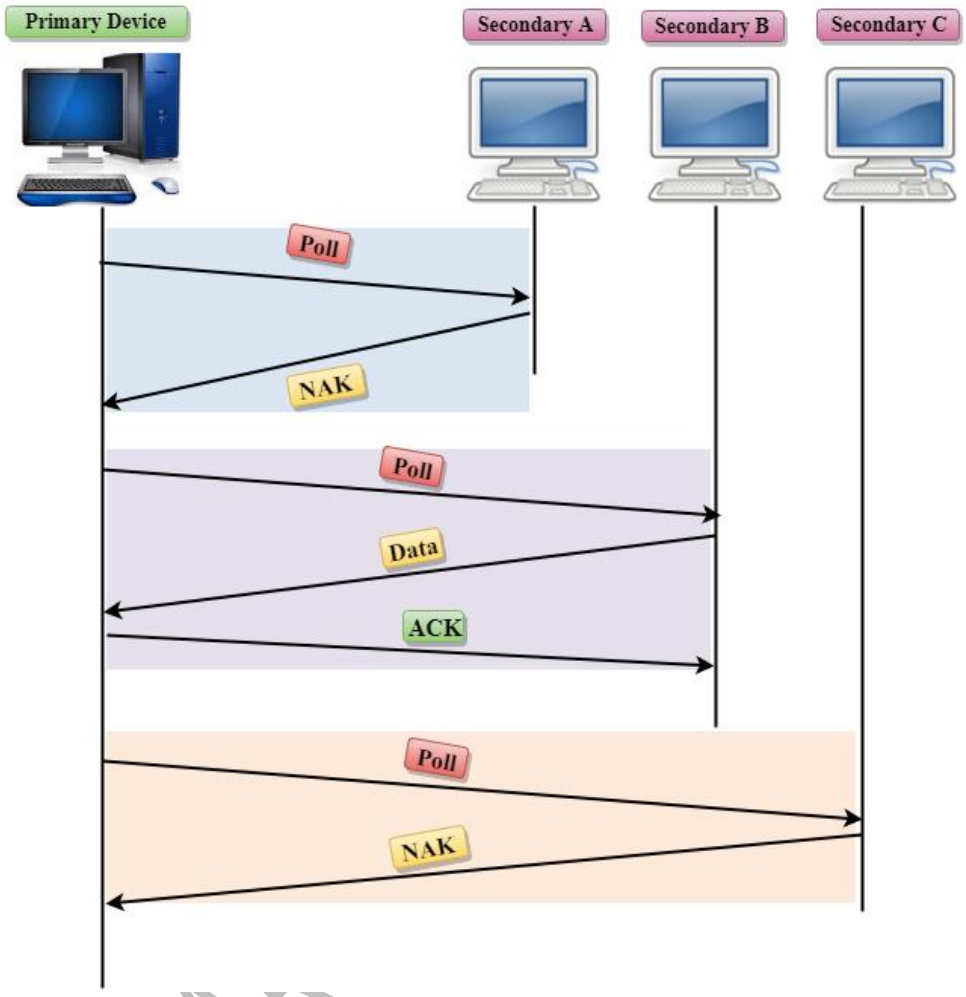
DIWAKAR EDUCATION HUB



Poll

- The Poll mode is used when the primary device wants to receive some data from the secondary device.
- When a primary device wants to receive the data, then it asks each device whether it has anything to send.
- Firstly, the primary asks (poll) the first secondary device, if it responds with the NACK (Negative Acknowledgement) means that it has nothing to send. Now, it approaches the second secondary device, it responds with the ACK means that it has the data to send. The secondary device can send more than one frame one after another or sometimes it may be required to send ACK before sending each one, depending on the type of the protocol being used.

DIWAKAR EDUCATION



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.

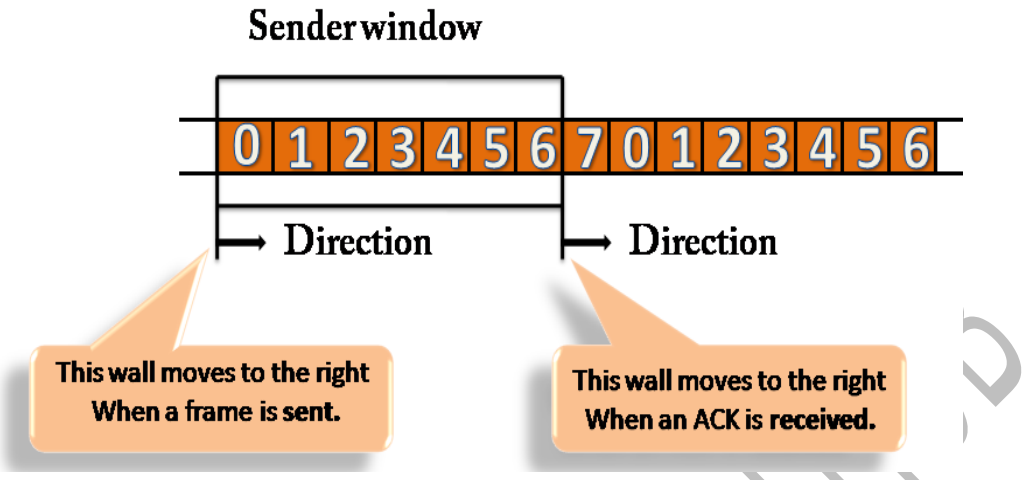
DIWAKAR EDUCATION HUB

- 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).

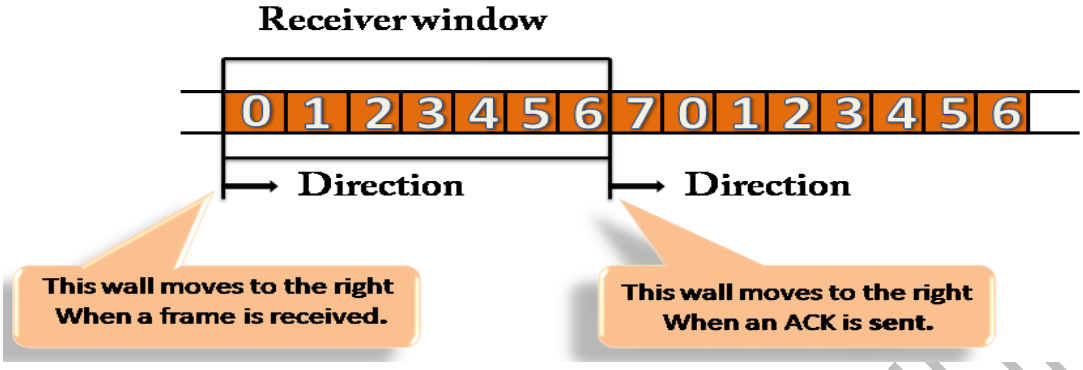
DIWAKAR EDUCATION HUB



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.

DIWAKAR EDUCATION HUB



Error Control

Error Control is a technique of error detection and retransmission.

Categories of Error Control:



Stop-and-wait ARQ

Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.

This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

Four features are required for the retransmission:

- The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly.
- Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame

DIWAKAR EDUCATION HUB

acknowledges the data 0 frame means that the data 0 frame has been arrived correctly and expects to receive data 1 frame.

- If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data.
- It works with the timer. If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.

Two possibilities of the retransmission:

- **Damaged Frame:** When the receiver receives a damaged frame, i.e., the frame contains an error, then it returns the NAK frame. For example, when the data 0 frame is sent, and then the receiver sends the ACK 1 frame means that the data 0 has arrived correctly, and transmits the data 1 frame. The sender transmits the next frame: data 1. It reaches undamaged, and the receiver returns ACK 0. The sender transmits the next frame: data 0. The receiver reports an error and returns the NAK frame. The sender retransmits the data 0 frame.
- **Lost Frame:** Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it can be acknowledged neither positively nor negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.

Sliding Window ARQ

SlidingWindow ARQ is a technique used for continuous transmission error control.

Three Features used for retransmission:

- In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly.
- The receiver can send either NAK or ACK depending on the conditions. The NAK frame tells the sender that the data have been received damaged.

DIWAKAR EDUCATION HUB

Since the sliding window is a continuous transmission mechanism, both ACK and NAK must be numbered for the identification of a frame. The ACK frame consists of a number that represents the next frame which the receiver expects to receive. The NAK frame consists of a number that represents the damaged frame.

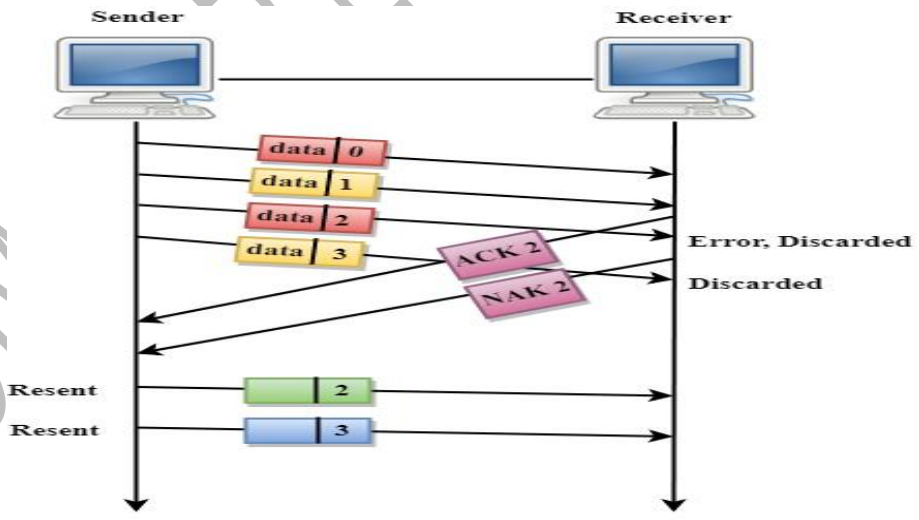
- The sliding window ARQ is equipped with the timer to handle the lost acknowledgements. Suppose then n-1 frames have been sent before receiving any acknowledgement. The sender waits for the acknowledgement, so it starts the timer and waits before sending any more. If the allotted time runs out, the sender retransmits one or all the frames depending upon the protocol used.

Two protocols used in sliding window ARQ:

- **Go-Back-n ARQ:** In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.

Three possibilities can occur for retransmission:

- **Damaged Frame:** When the frame is damaged, then the receiver sends a NAK frame.



In the above figure, three frames have been transmitted before an error discovered in the third frame. In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error. The receiver

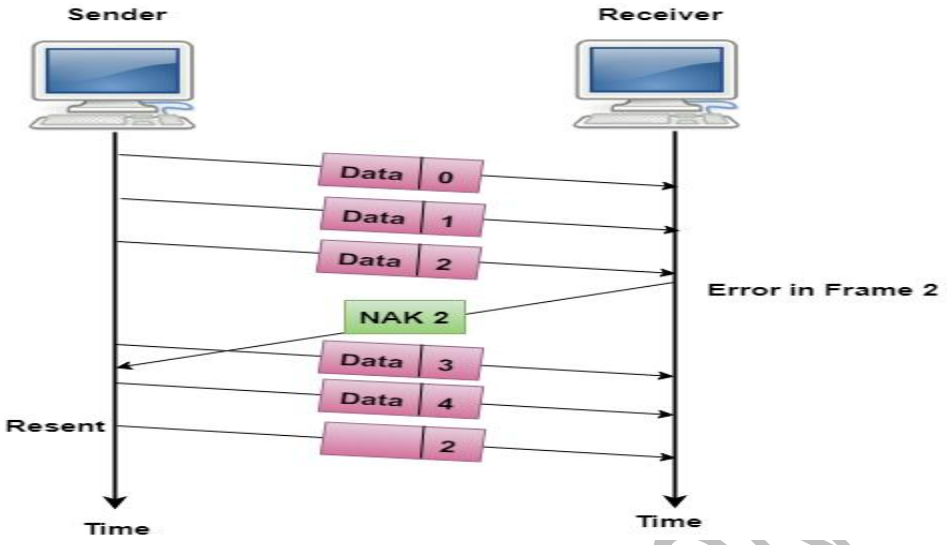
discovers the error in data 2 frame, so it returns the NAK 2 frame. The frame 3 is also discarded as it is transmitted after the damaged frame. Therefore, the sender retransmits the frames 2,3.

- **Lost Data Frame:** In Sliding window protocols, data frames are sent sequentially. If any of the frames is lost, then the next frame arrive at the receiver is out of sequence. The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame. The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame.
- **Lost Acknowledgement:** The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

Selective-Reject ARQ

- Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ.
- In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.
- The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
- The receiver must have an appropriate logic for reinserting the frames in a correct order.
- The sender must consist of a searching mechanism that selects only the requested frame for retransmission.

DIWAKAR EDUCATION HUB



Sliding Window Protocol

Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames. The sliding window is also used in Transmission Control Protocol.

In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.

Working Principle

In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.

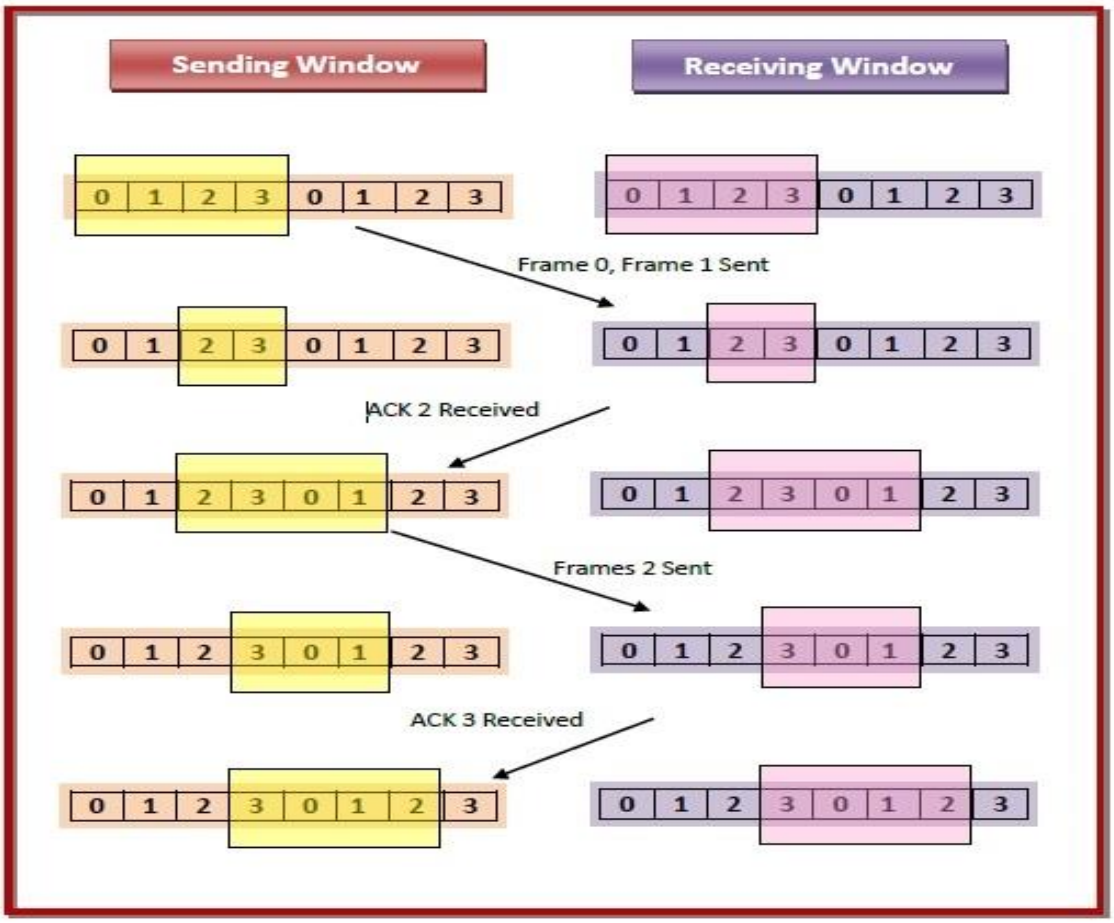
The size of the sending window determines the sequence number of the outbound frames. If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2^n–1. Consequently, the size of the sending window is 2^n–1. Thus in order to accommodate a sending window size of 2^n–1, a n-bit sequence number is chosen.

The sequence numbers are numbered as modulo-n. For example, if the sending window size is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on. The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.

The size of the receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum number of frames that the sender can send before receiving acknowledgment.

Example

Suppose that we have sender window and receiver window each of size 4. So the sequence numbering of both the windows will be 0,1,2,3,0,1,2 and so on. The following diagram shows the positions of the windows after sending the frames and receiving acknowledgments.



Types of Sliding Window Protocols

The Sliding Window ARQ (Automatic Repeat reQuest) protocols are of two categories −



Go – Back – N ARQ

Go – Back – N ARQ provides for sending multiple frames before receiving the acknowledgment for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgment of a frame is not received within the time period, all frames starting from that frame are retransmitted.

Selective Repeat ARQ

This protocol also provides for sending multiple frames before receiving the acknowledgment for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

High-level Data Link Control (HDLC)

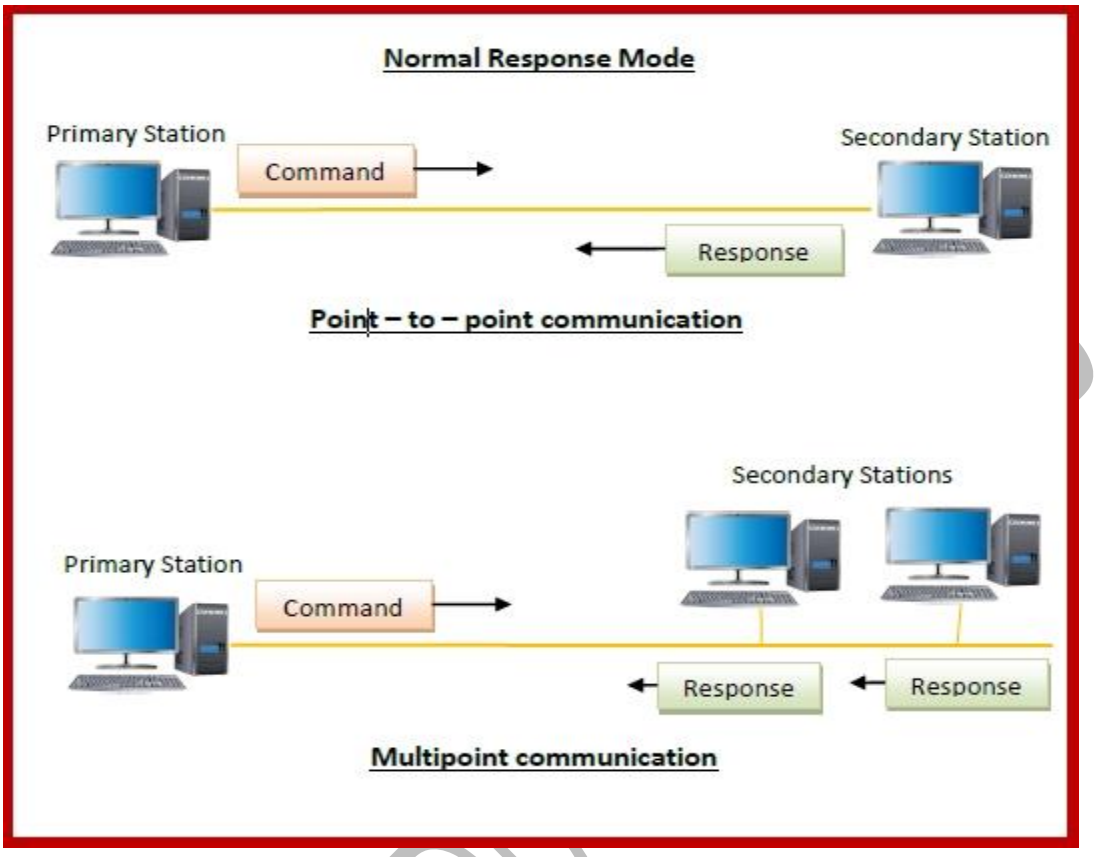
High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

Transfer Modes

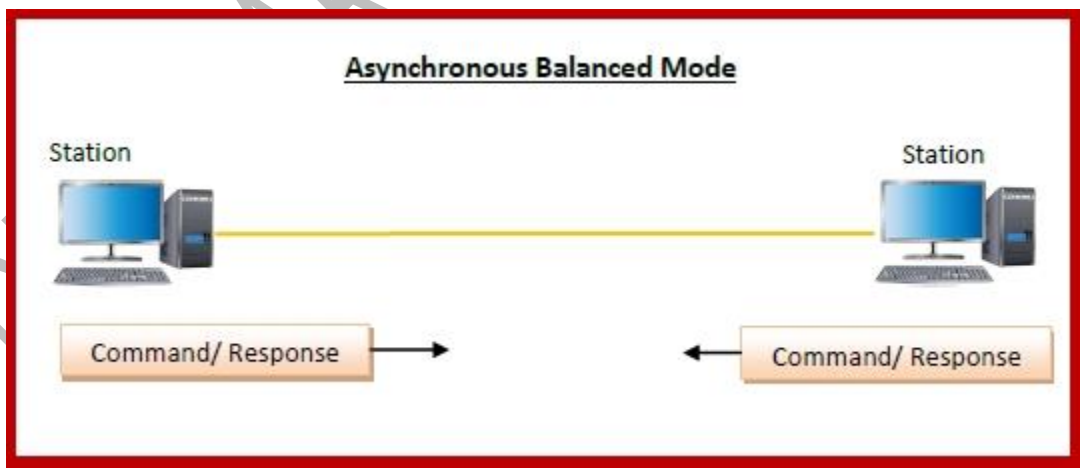
HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

- **Normal Response Mode (NRM)** – Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.

DIWAKAR EDUCATION HUB



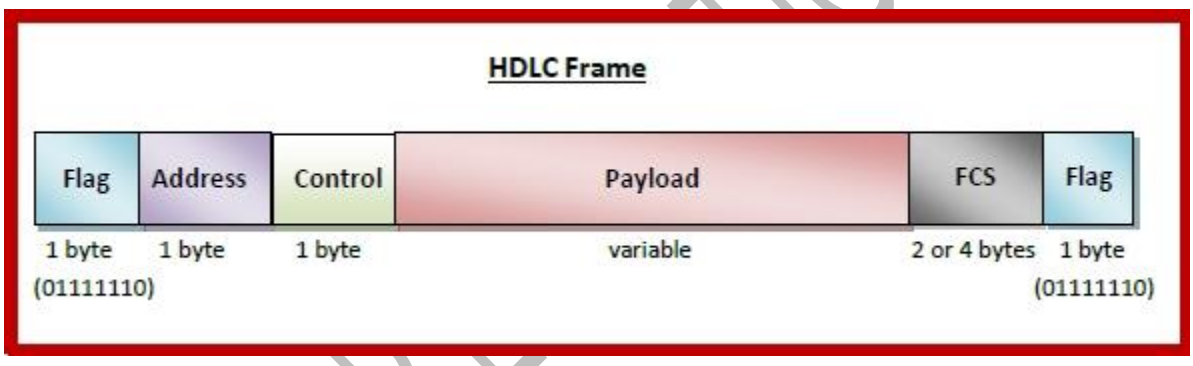
- **Asynchronous Balanced Mode (ABM)** − Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.



HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are −

- **Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control** − It is 1 or 2 bytes containing flow and error control information.
- **Payload** − This carries the data from the network layer. Its length may vary from one network to another.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)

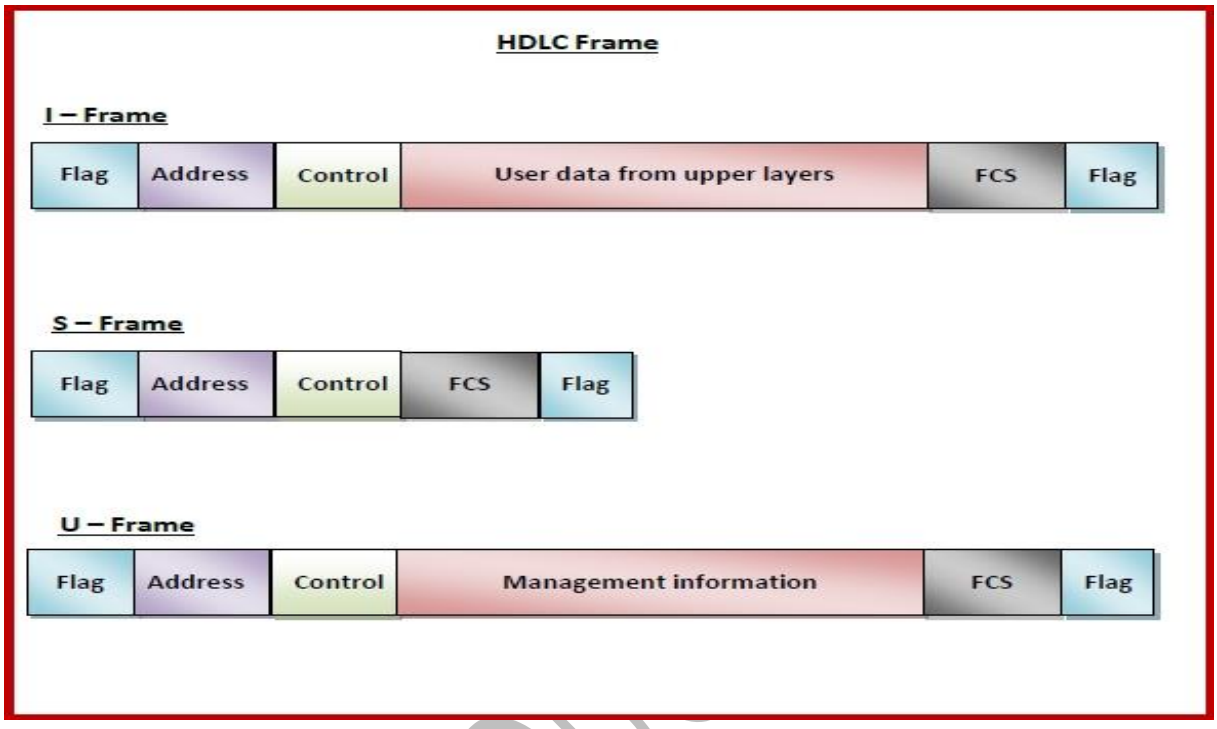


Types of HDLC Frames

There are three types of HDLC frames. The type of frame is determined by the control field of the frame –

- **I-frame** − I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.
- **S-frame** − S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.
- **U-frame** − U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an

information field, if required. The first two bits of control field of U-frame is 11.



Multiple Access

Multiple access schemes are used to allow many mobile users to share simultaneously a finite amount of radio spectrum.

Multiple Access Techniques

In wireless communication systems, it is often desirable to allow the subscriber to send information simultaneously from the mobile station to the base station while receiving information from the base station to the mobile station.

A cellular system divides any given area into cells where a mobile unit in each cell communicates with a base station. The main aim in the cellular system design is to be able to **increase the capacity of the channel**, i.e., to handle as many calls as possible in a given bandwidth with a sufficient level of quality of service.

There are several different ways to allow access to the channel. These includes mainly the following −

- Frequency division multiple-access (FDMA)

- Time division multiple-access (TDMA)
- Code division multiple-access (CDMA)
- Space division multiple access (SDMA)

Depending on how the available bandwidth is allocated to the users, these techniques can be classified as **narrowband** and **wideband** systems.

Narrowband Systems

Systems operating with channels substantially narrower than the coherence bandwidth are called as Narrow band systems. Narrow band TDMA allows users to use the same channel but allocates a unique time slot to each user on the channel, thus separating a small number of users in time on a single channel.

Wideband Systems

In wideband systems, the transmission bandwidth of a single channel is much larger than the coherence bandwidth of the channel. Thus, multipath fading doesn't greatly affect the received signal within a wideband channel, and frequency selective fades occur only in a small fraction of the signal bandwidth.

Frequency Division Multiple Access (FDMA)

FDMA is the basic technology for advanced mobile phone services. The features of FDMA are as follows.

- FDMA allots a different sub-band of frequency to each different user to access the network.
- If FDMA is not in use, the channel is left idle instead of allotting to the other users.
- FDMA is implemented in Narrowband systems and it is less complex than TDMA.
- Tight filtering is done here to reduce adjacent channel interference.
- The base station BS and mobile station MS, transmit and receive simultaneously and continuously in FDMA.

Time Division Multiple Access (TDMA)

DIWAKAR EDUCATION HUB

In the cases where continuous transmission is not required, there TDMA is used instead of FDMA. The features of TDMA include the following.

- TDMA shares a single carrier frequency with several users where each users makes use of non-overlapping time slots.
- Data transmission in TDMA is not continuous, but occurs in bursts. Hence handsoff process is simpler.
- TDMA uses different time slots for transmission and reception thus duplexers are not required.
- TDMA has an advantage that is possible to allocate different numbers of time slots per frame to different users.
- Bandwidth can be supplied on demand to different users by concatenating or reassigning time slot based on priority.

Code Division Multiple Access (CDMA)

Code division multiple access technique is an example of multiple access where several transmitters use a single channel to send information simultaneously. Its features are as follows.

- In CDMA every user uses the full available spectrum instead of getting allotted by separate frequency.
- CDMA is much recommended for voice and data communications.
- While multiple codes occupy the same channel in CDMA, the users having same code can communicate with each other.
- CDMA offers more air-space capacity than TDMA.
- The hands-off between base stations is very well handled by CDMA.

Space Division Multiple Access (SDMA)

Space division multiple access or spatial division multiple access is a technique which is MIMO (multiple-input multiple-output) architecture and used mostly in wireless and satellite communication. It has the following features.

- All users can communicate at the same time using the same channel.

DIWAKAR EDUCATION HUB

- SDMA is completely free from interference.
- A single satellite can communicate with more satellites receivers of the same frequency.
- The directional spot-beam antennas are used and hence the base station in SDMA, can track a moving user.
- Controls the radiated energy for each user in space.

Spread Spectrum Multiple Access

Spread spectrum multiple access (SSMA) uses signals which have a transmission bandwidth whose magnitude is greater than the minimum required RF bandwidth.

There are two main types of spread spectrum multiple access techniques −

- Frequency hopped spread spectrum (FHSS)
- Direct sequence spread spectrum (DSSS)

Frequency Hopped Spread Spectrum (FHSS)

This is a digital multiple access system in which the carrier frequencies of the individual users are varied in a pseudo random fashion within a wideband channel. The digital data is broken into uniform sized bursts which is then transmitted on different carrier frequencies.

Direct Sequence Spread Spectrum (DSSS)

This is the most commonly used technology for CDMA. In DS-SS, the message signal is multiplied by a Pseudo Random Noise Code. Each user is given his own code word which is orthogonal to the codes of other users and in order to detect the user, the receiver must know the code word used by the transmitter.

The combinational sequences called as **hybrid** are also used as another type of spread spectrum. **Time hopping** is also another type which is rarely mentioned.

Since many users can share the same spread spectrum bandwidth without interfering with one another, spread spectrum systems become **bandwidth efficient** in a multiple user environment.

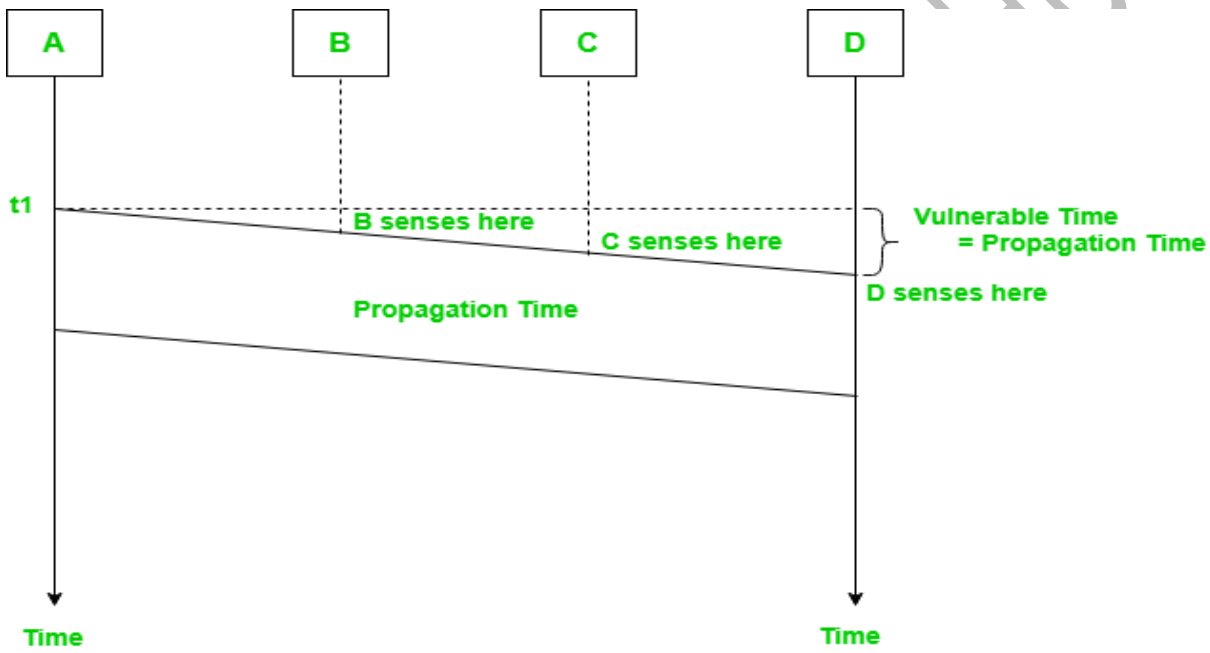
DIWAKAR EDUCATION HUB

Carrier Sense Multiple Access (CSMA)

This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the datalink layer. Carrier Sense multiple access requires that each station **first check the state of the medium** before sending.

Vulnerable Time –

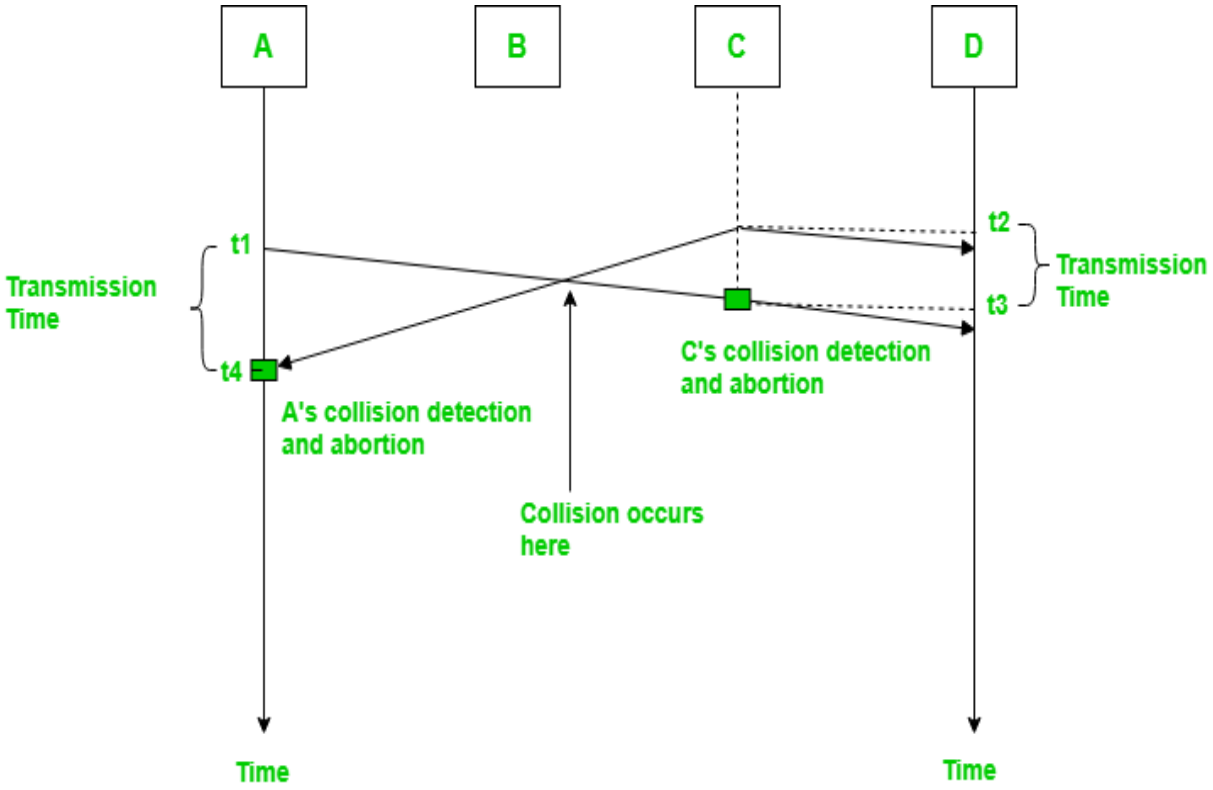
Vulnerable time = Propagation time (Tp)



The persistence methods can be applied to help the station take action when the channel is busy/idle.

1. Carrier Sense Multiple Access with Collision Detection (CSMA/CD) –

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If successful, the station is finished, if not, the frame is sent again.

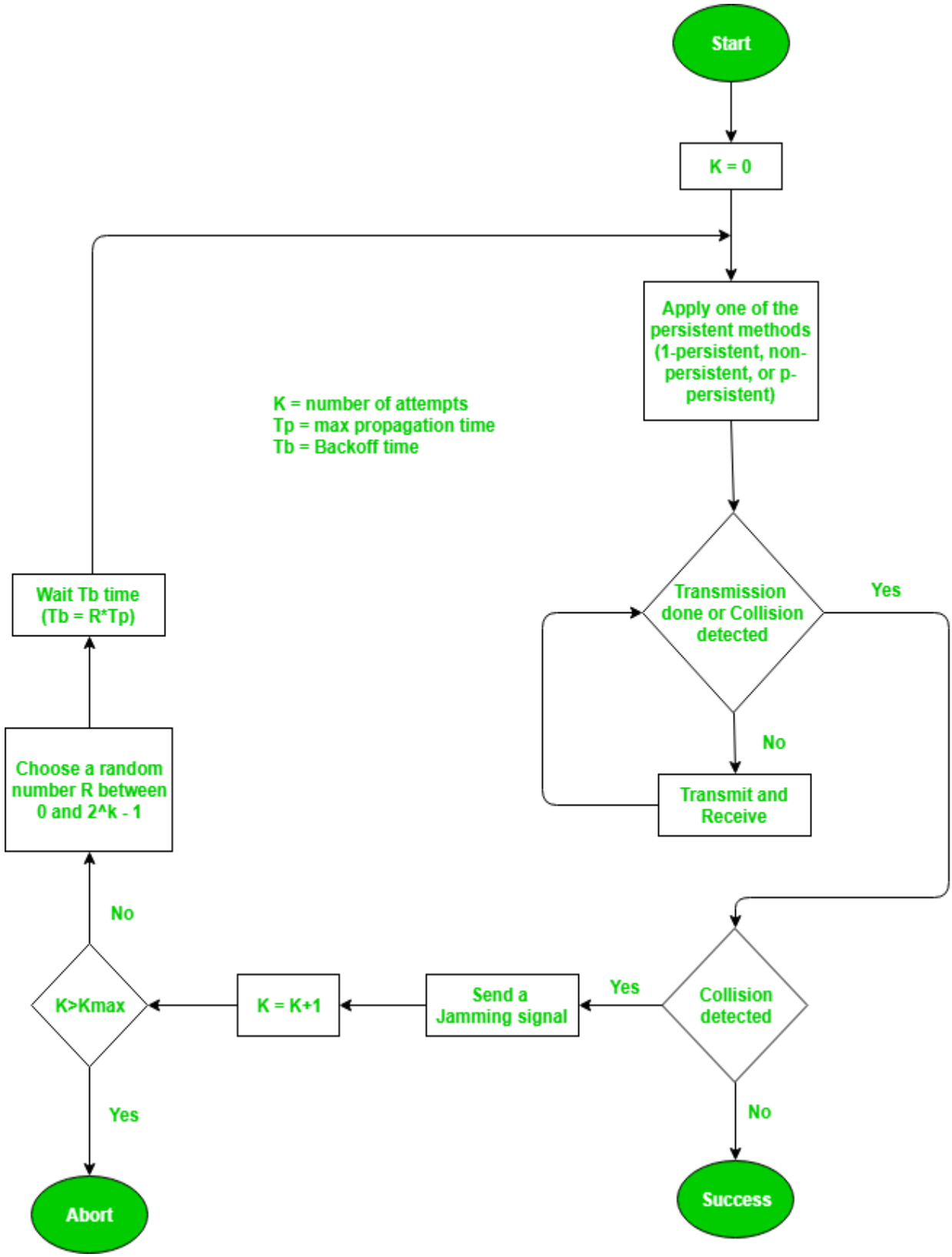


In the diagram, A starts send the first bit of its frame at t1 and since C sees the channel idle at t2, starts sending its frame at t2. C detects A's frame at t3 and aborts transmission. A detects C's frame at t4 and aborts its transmission. Transmission time for C's frame is therefore and for A's frame is .

So, the **frame transmission time (Tfr) should be at least twice the maximum propagation time (Tp)**. This can be deduced when the two stations involved in collision are maximum distance apart.

Process –
The entire process of collision detection can be explained as follows:

DIWAKAR EDUC


Start
K = 0
Apply one of the persistent methods (1-persistent, non-persistent, or p-persistent)
K = number of attempts
Tp = max propagation time
Tb = Backoff time
Transmission done or Collision detected
Yes
No
Transmit and Receive
Wait Tb time (Tb = R*Tp)
Choose a random number R between 0 and 2^k - 1
No
K>Kmax
K = K+1
Send a Jamming signal
Yes
Collision detected
Yes
No
Abort
Success

Throughput and Efficiency – The throughput of CSMA/CD is much greater than pure or slotted ALOHA.

- For 1-persistent method throughput is 50% when G=1.
- For non-persistent method throughput can go upto 90%.

2. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) –

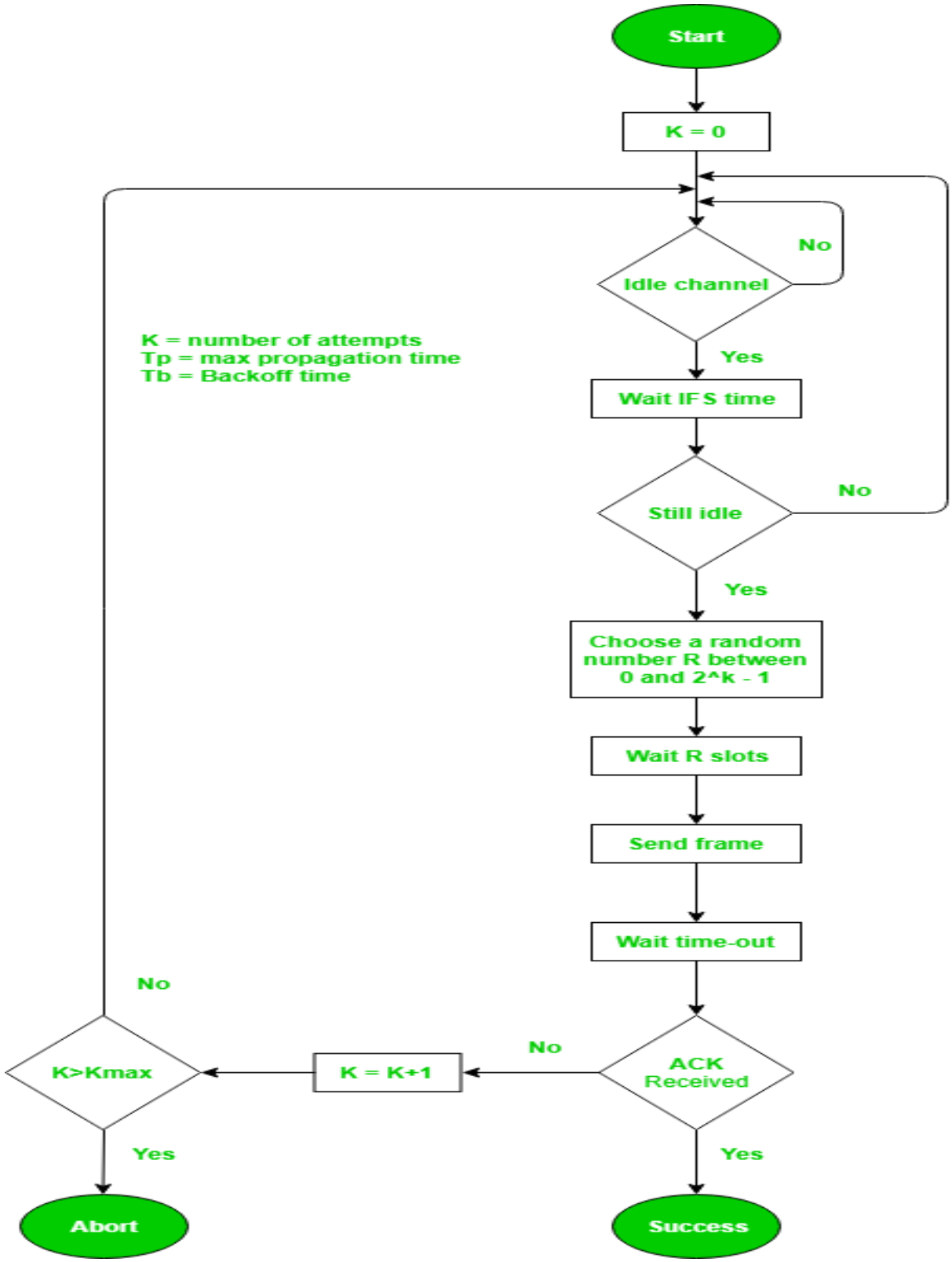
The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of received signal almost doubles and the station can sense the possibility of collision. In case of wireless networks, most of the energy is used for transmission and the energy of received signal increases by only 5-10% if a collision occurs. It can't be used by the station to sense collision. Therefore **CSMA/CA has been specially designed for wireless networks**.

These are three types of strategies:

1. **InterFrame Space (IFS) –** When a station finds the channel busy, it waits for a period of time called IFS time. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.
2. **Contention Window –** It is the amount of time divided into slots.A station which is ready to send frames chooses random number of slots as **wait time**.
3. **Acknowledgements –** The positive acknowledgements and time-out timer can help guarantee a successful transmission of the frame.

Process –
The entire process for collision avoidance can be explained as follows:

DIWAKAR EDUCATION HUB


Start
K = 0
No
Idle channel
K = number of attempts
Tp = max propagation time
Tb = Backoff time
Yes
Wait IFS time
No
Still idle
Yes
Choose a random number R between 0 and 2^k - 1
Wait R slots
Send frame
Wait time-out
No
ACK Received
No
K = K+1
K>Kmax
Yes
Abort
Yes
Success

Packet Reservation Multiple Access (PRMA) means:

Packet Reservation Multiple Access (PRMA) refers to a multiple access strategy with frames of a fixed number of slots. In case a terminal contains a set of data packets or speech segments to deliver, it competes to gain access in any free slot.

If it can successfully capture the base station (BS), the terminal acquires reservation in the associated slots of the next frames, right until it releases the reservation. In PRMA, adjacent cells make use of distinct carrier frequencies in line with a cellular reuse plan. The fundamental process of PRMA includes occupying a time slot only at the time of speech talkspurts and releasing the channel at the time of silence periods.

Packet Reservation Multiple Access (PRMA)

Although PRMA was previously widely used for speech traffic, it can be used for data users as well because of its bandwidth efficiency, random access, and reservation qualities. The flexibility in receiving various traffic bit rates makes PRMA a fine candidate for multi-rate data traffic.

A benefit of PRMA is that it demands minimal central control. As hand-overs call for minimum intervention from the base station, an active voice terminal which moves into another cell drops its slot reservations. Therefore, it has to re-contend with other terminals to broadcast the left-over voice packets. In addition, the terminal demands registration with the new base station. The resulting delay can compel the terminal to lose voice packets, thus degrading its overall performance.

One key benefit of the PRMA protocol is that it can be used in combination with existing CDMA or TDMA-based systems. It can also be incorporated with the next-gen WCDMA systems. PRMA-centered protocol is ideal for multimedia traffic due to its dynamic and flexible bandwidth-allocation process.

PRMA facts:

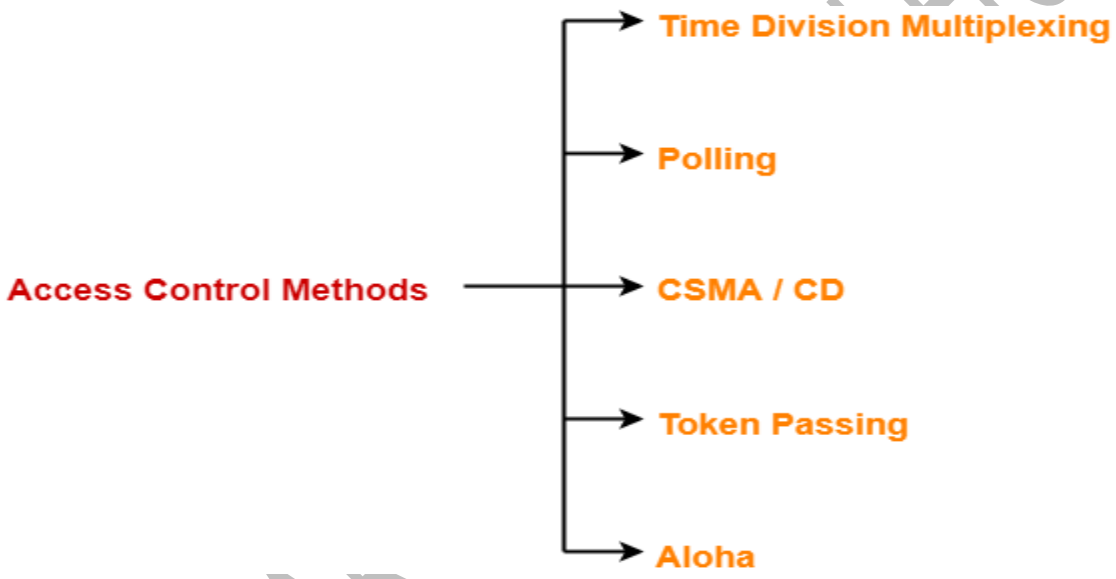
- TDMA with slotted ALOHA reservation system
- Source rates are 32 kbit/sec
- Frame Duration is 16 msec (62.5 frames/sec)
- 20 slots per frame
- Channel bit rate is 720 kbit/sec and bandwidth is 720 khz
- 576 bits per slot (contains 64 bit overhead)

DIWAKAR EDUCATION HUB

- Packet dropping rate is 1%
- Supports data and voice

Access Control in Networking-

- Access Control is a mechanism that controls the access of stations to the transmission link.
- Broadcast links require the access control mechanism.
- There are various access control methods-

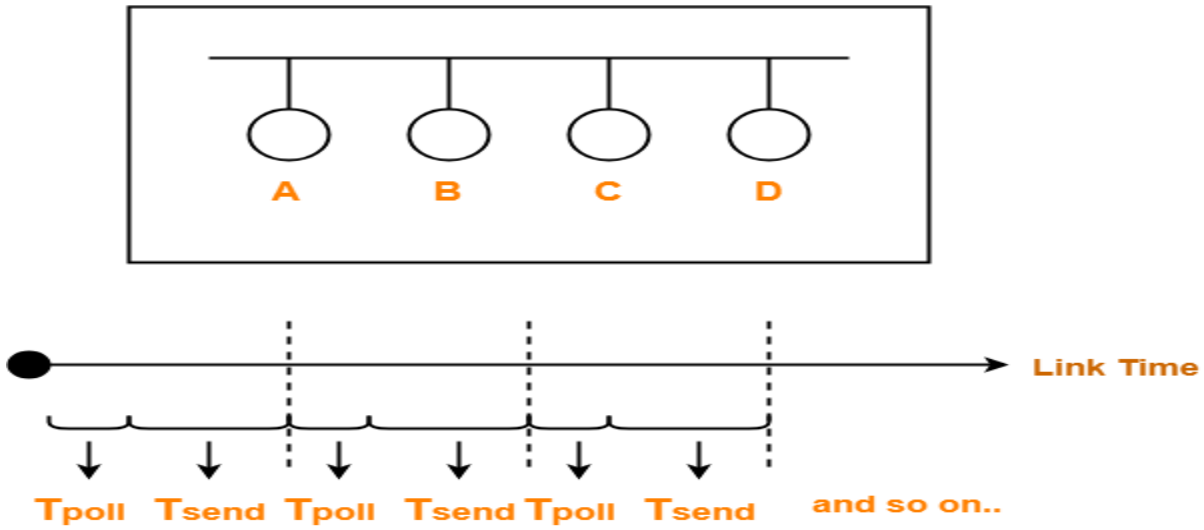


Polling-

In this access control method,

- A polling is conducted in which all the stations willing to send data participates.
- The polling algorithm chooses one of the stations to send the data.
- The chosen station sends the data to the destination.
- After the chosen station has sent the data, the cycle repeats.

Example-



Polling Access Control Method

Here-

- T_{poll} = Time taken for polling
- T_{send} = Time taken for sending the data = Transmission delay + Propagation delay = $T_t + T_p$

Efficiency-

Efficiency (η) = Useful Time / Total Time

- Useful time = Transmission delay of data packet = T_t
- Useless time = Time wasted during polling + Propagation delay of data packet = $T_{poll} + T_p$

Thus,

$$\text{Efficiency } (\eta) = \frac{T_t}{T_{poll} + T_t + T_p}$$

DIWAKAR EDUCATION

Advantages-

- Unlike in Time Division Multiplexing, no slot is ever wasted.
- It leads to maximum efficiency and bandwidth utilization.

Disadvantages-

- Time is wasted during polling.
- Link sharing is not fair since each station has the equal probability of winning in each round.
- Few stations might starve for sending the data.

Important Formulas-

- Efficiency (η) = T_t / (T_{poll} + T_t + T_p)
- Effective Bandwidth / Bandwidth Utilization / Throughput = Efficiency(η) x Bandwidth
- Maximum Available Effective Bandwidth = Total number of stations x Bandwidth requirement of 1 station

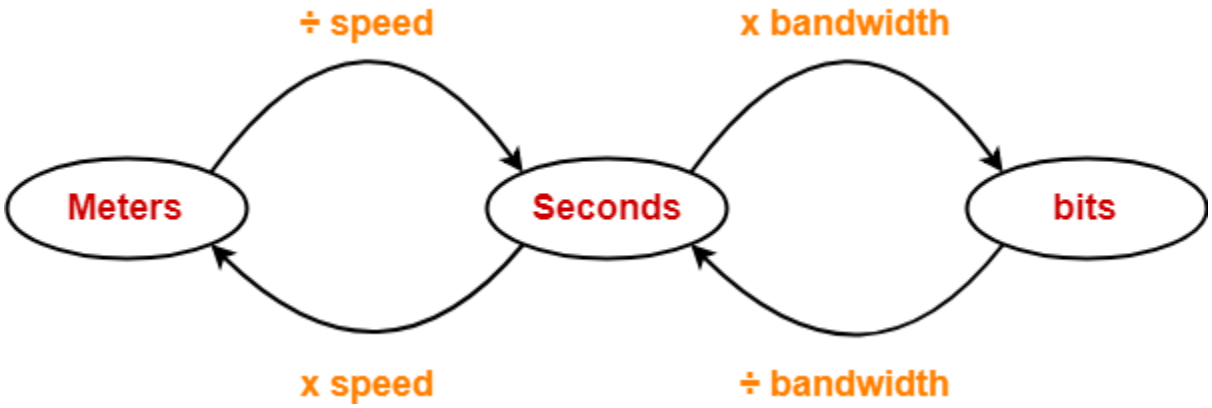
Token Passing

Time Conversions-

In token passing,

- Time may be expressed in seconds, bits or meters.
- To convert the time from one unit to another, we use the following conversion chart-

EDUCATION HUB



Conversion Chart

Token Passing Terminology-

The following terms are frequently used-

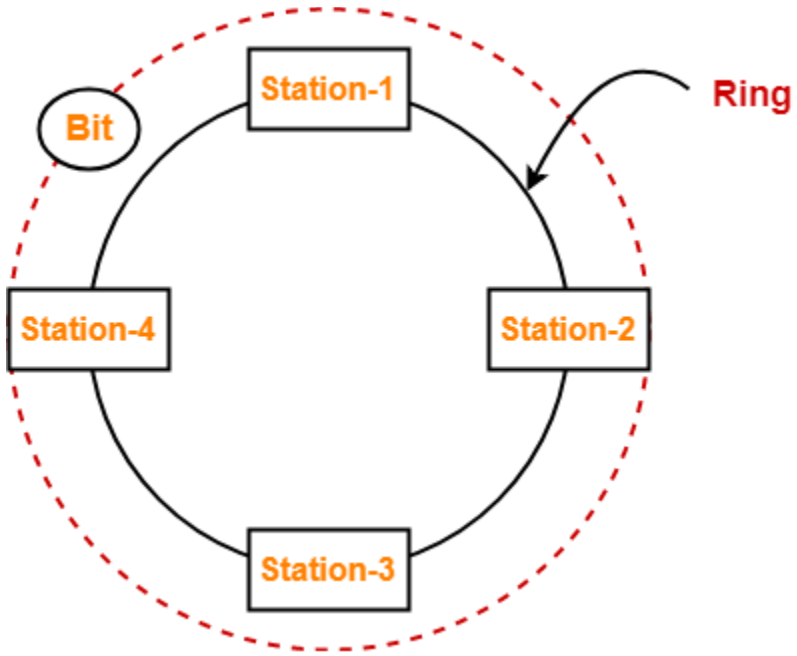
1. Token
2. Ring Latency
3. Cycle Time

1. Token-

- A token is a small message composed of a special bit pattern.
- It represents the permission to send the data packet.
- A station is allowed to transmit a data packet if and only if it possess the token otherwise not.

2. Ring Latency-

Time taken by a bit to complete one revolution of the ring is called as **ring latency**.



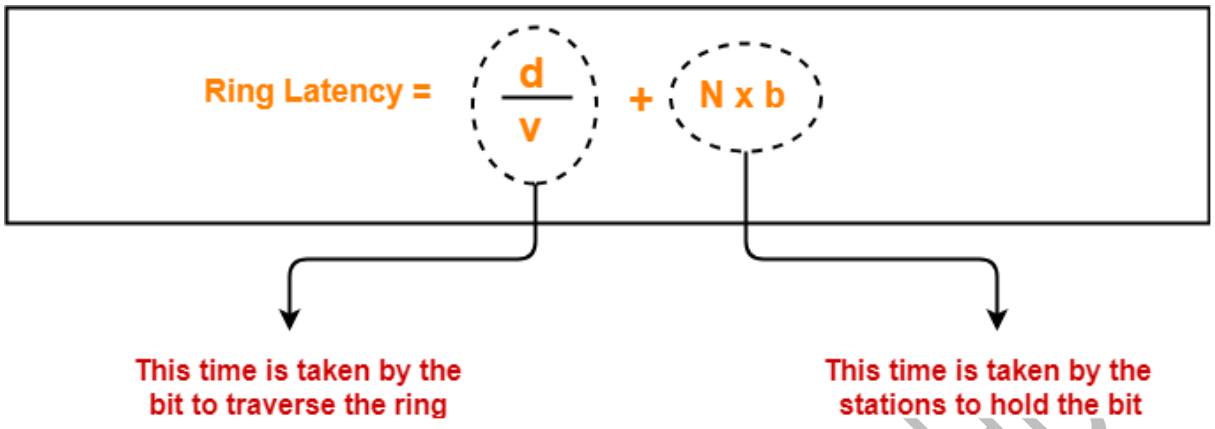
the expression for ring latency.

If-

- Length of the ring = d
- Speed of the bit = v
- Number of stations = N
- Bit delay at each station = b

  (Bit delay is the time for which a station holds the bit before transmitting to the other side)

Then-



Notes-

- d / v is the propagation delay (T_p) expressed in seconds.
- Generally, bit delay is expressed in bits.
- So, both the terms (d / v and N x b) have different units.
- While calculating the ring latency, both the terms are brought into the same unit.
- The above conversion chart is used for conversion.

After conversion, we have-

$$\text{Ring Latency} = \left(\frac{d}{v} + \frac{N \times b}{B}\right) \text{ sec}$$

$$= \left(T_p + \frac{N \times b}{B}\right) \text{ sec}$$

OR

$$\text{Ring Latency} = \left(\frac{d \times B}{v} + N \times b\right) \text{ bits}$$

$$= \left(T_p \times B + N \times b\right) \text{ bits}$$

3. Cycle Time-

Time taken by the token to complete one revolution of the

ring is called as cycle time.

If-

- Length of the ring = d
- Speed of the bit = v
- Number of stations = N
- Token Holding Time = THT

(Token Holding Time is the time for which a station holds the token before transmitting to the other side)

Then-

$$\text{Cycle Time} = \frac{d}{v} + N \times THT$$

$$= T_p + N \times THT$$

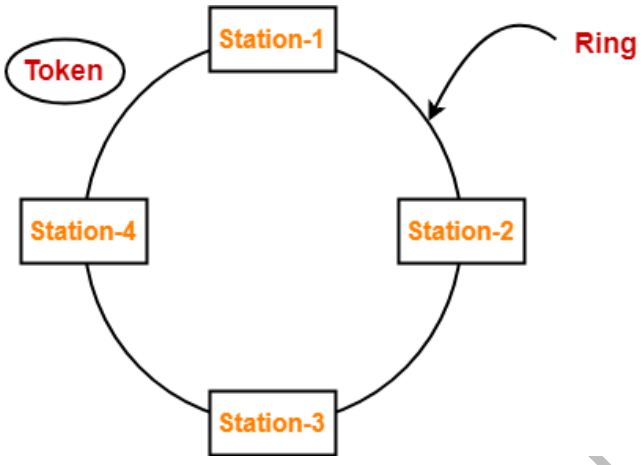
Token Passing Access Control Method.

Token Passing-

In this access control method,

- All the stations are logically connected to each other in the form of a ring.
- The access of stations to the transmission link is governed by a token.
- A station is allowed to transmit a data packet if and only if it possess the token otherwise not.
- Each station passes the token to its neighboring station either clockwise or anti-clockwise.

DIWAKAR EDUCATION HUB



Assumptions-

Token passing method assumes-

- Each station in the ring has the data to send.
- Each station sends exactly one data packet after acquiring the token.

Efficiency-

Efficiency (η) = Useful Time / Total Time

In one cycle,

- Useful time = Sum of transmission delay of N stations since each station sends 1 data packet = N x T_t
- Total Time = Cycle time = T_p + N x THT

Thus,

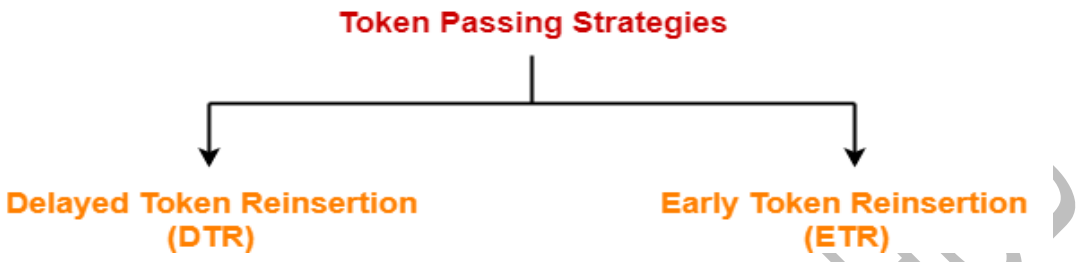
$$\text{Efficiency } (\eta) = \frac{N \times T_t}{T_p + N \times THT}$$

Token Holding Time depends on the strategy implemented.

DIWAKAR EDUCATION HUB

Token Passing Strategies-

The following 2 strategies are used in token passing-



1. Delayed Token Reinsertion (DTR)
2. Early Token Reinsertion (ETR)

1. Delayed Token Reinsertion-

In this strategy,

- Station keeps holding the token until the last bit of the data packet transmitted by it takes the complete revolution of the ring and comes back to it.

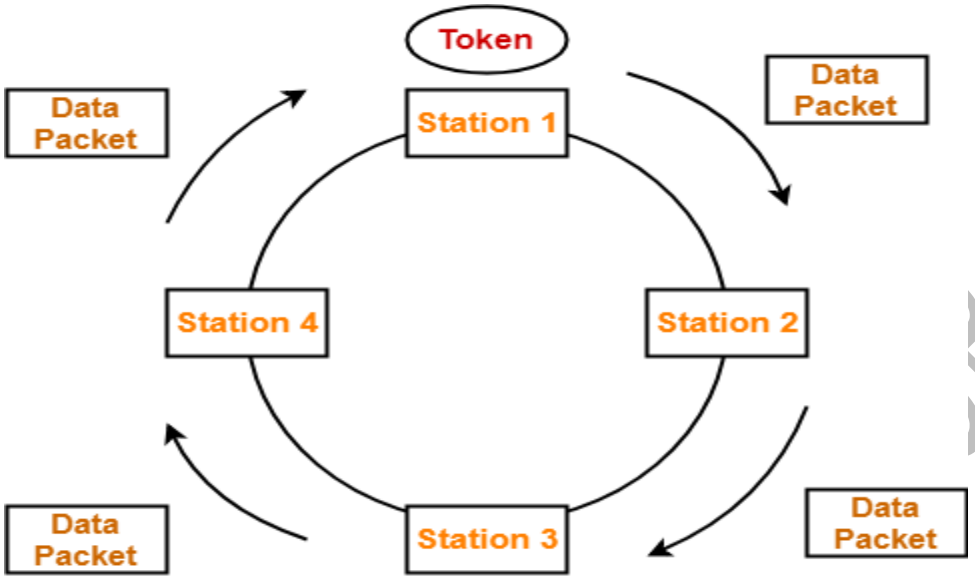
Working-

After a station acquires the token,

- It transmits its data packet.
- It holds the token until the data packet reaches back to it.
- After data packet reaches to it, it discards its data packet as its journey is completed.
- It releases the token.

The following diagram illustrates these steps for station-1. Same procedure is repeated at every station.

DIWAKAR EDUCATION HUB



Delayed Token Reinsertion Token Passing

Token Holding Time-

Token Holding Time (THT) = Transmission delay + Ring Latency

We know,

- Ring Latency = T_p + N x bit delay
- Assuming bit delay = 0 (in most cases), we get-

Token Holding Time = $T_t + T_p$

Efficiency-

Substituting THT = $T_t + T_p$ in the efficiency expression, we get-

$$\text{Efficiency } (\eta) = \frac{N \times T_t}{T_p + N \times (T_t + T_p)}$$

OR

$$\text{Efficiency } (\eta) = \frac{1}{\frac{a}{N} + (1 + a)}$$

OR

$$\text{Efficiency } (\eta) = \frac{1}{1 + \left(1 + \frac{1}{N}\right) a}$$

OR

$$\text{Efficiency } (\eta) = \frac{1}{1 + \left(\frac{N + 1}{N}\right) a}$$

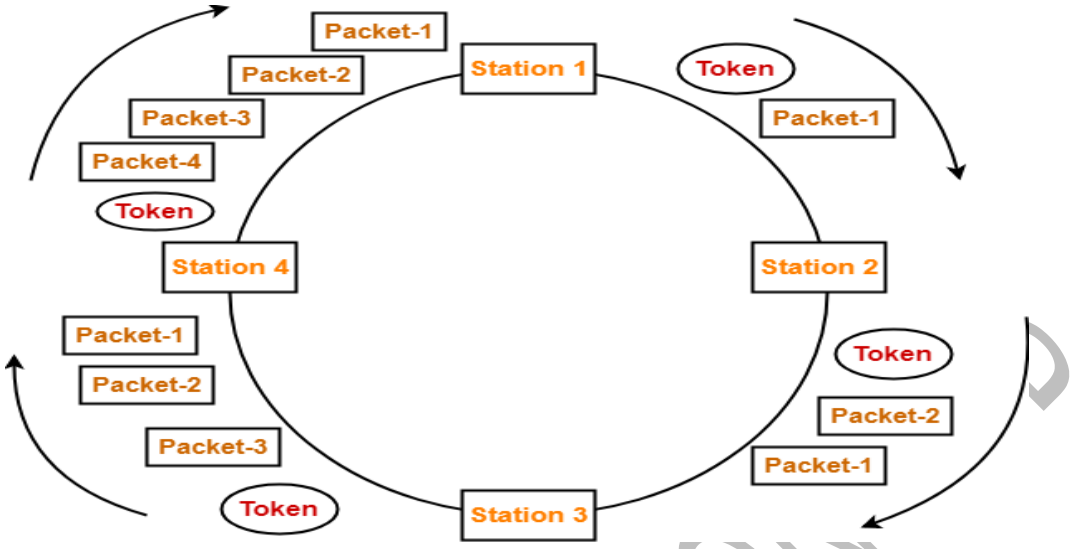
2. Early Token Reinsertion-

In this strategy,

- Station releases the token immediately after putting its data packet to be transmitted on the ring.

Working-

DIWAKAR EDUCATION HUB



Step-01: At Station-1:

Station-1

- Acquires the token
- Transmits packet-1
- Releases the token

Step-02: At Station-2:

Station-2

- Receives packet-1
- Transmits packet-1
- Acquires the token
- Transmits packet-2
- Releases the token

Step-03: At Station-3:

Station-3

- Receives packet-1
- Transmits packet-1

DIWAKAR EDUCATION

- Receives packet-2
- Transmits packet-2
- Acquires the token
- Transmits packet-3
- Releases the token

Step-04: At Station-4:

Station-4

- Receives packet-1
- Transmits packet-1
- Receives packet-2
- Transmits packet-2
- Receives packet-3
- Transmits packet-3
- Acquires the token
- Transmits packet-4
- Releases the token

Step-05: At Station-1:

- Receives packet-1
- Discards packet-1 (as its journey is completed)
- Receives packet-2
- Transmits packet-2
- Receives packet-3
- Transmits packet-3
- Receives packet-4
- Transmits packet-4
- Acquires the token
- Transmits packet-1 (new)
- Releases the token

In this manner, the cycle continues.

Token Holding Time-

DIWAKAR EDUCATION HUB

Token Holding Time (THT) = Transmission delay of data packet = T_t

Efficiency-

Substituting THT = T_t in the efficiency expression, we get-

$$\text{Efficiency } (\eta) = \frac{N \times T_t}{T_p + N \times T_t}$$

OR

$$\text{Efficiency } (\eta) = \frac{1}{1 + \frac{a}{N}}$$

Differences between DTR and ETR-

Delay Token Retransmission (DTR)	Early Token Retransmission (ETR)
Each station holds the token until its data packet reaches back to it.	Each station releases the token immediately after putting its data packet on the ring.
There exists only one data packet on the ring at any given instance.	There exists more than one data packet on the ring at any given instance.

It is more reliable than ETR.	It is less reliable than DTR.
It has low efficiency as compared to ETR.	It has high efficiency as compared to ETR.

Important Notes-

Note-01:

In token passing,

- It is the responsibility of each transmitting station to remove its own data packet from the ring.

Note-02:

While solving questions,

- If the strategy used is not mentioned, then consider Early Token Retransmission strategy.

Multi-Access Networks

Developed in the mid-1970s by researchers at the Xerox Palo Alto Research Center (PARC), the Ethernet eventually became the dominant local area networking technology, emerging from a pack of competing technologies. Today, it competes mainly with 802.11 wireless networks but remains extremely popular in campus networks and data centers. The more general name for the technology behind the Ethernet is Carrier Sense, Multiple Access with Collision Detect (CSMA/CD).

As indicated by the CSMA name, the Ethernet is a multiple-access network, meaning that a set of nodes sends and receives frames over a shared link. You can, therefore, think of an Ethernet as being like a bus that has multiple stations plugged into it. The “carrier sense” in CSMA/CD means that all the nodes can

distinguish between an idle and a busy link, and "collision detect" means that a node listens as it transmits and can therefore detect when a frame it is transmitting has interfered (collided) with a frame transmitted by another node.

The Ethernet has its roots in an early packet radio network, called Aloha, developed at the University of Hawaii to support computer communication across the Hawaiian Islands. Like the Aloha network, the fundamental problem faced by the Ethernet is how to mediate access to a shared medium fairly and efficiently (in Aloha, the medium was the atmosphere, while in the Ethernet the medium was originally a coax cable). The core idea in both Aloha and the Ethernet is an algorithm that controls when each node can transmit.

Modern Ethernet links are now largely point to point; that is, they connect one host to an Ethernet switch, or they interconnect switches. As a consequence, the "multiple access" algorithm is not used much in today's wired Ethernets, but a variant is now used in wireless networks, such as 802.11 networks (also known as Wi-Fi). Due to the enormous influence of Ethernet, we chose to describe its classic algorithm here, and then explain how it has been adapted to Wi-Fi in the next section. We will also discuss Ethernet switches elsewhere. For now, we'll focus on how a single Ethernet link works.

Digital Equipment Corporation and Intel Corporation joined Xerox to define a 10-Mbps Ethernet standard in 1978. This standard then formed the basis for IEEE standard 802.3, which additionally defines a much wider collection of physical media over which an Ethernet can operate, including 100-Mbps, 1-Gbps, 10-Gbps, 40-Gbps, and 100-Gbps versions.

Physical Properties

Ethernet segments were originally implemented using coaxial cable of length up to 500 m. (Modern Ethernets use twisted copper pairs, usually a particular type known as "Category 5," or optical fibers, and in some cases can be quite a lot longer than 500 m.) This cable was similar to the type used for cable TV. Hosts connected to an Ethernet segment by tapping into it. A transceiver, a small device directly attached to the tap, detected when the line was idle and drove the signal when the host was transmitting. It also received incoming signals. The transceiver,

in turn, connected to an Ethernet adaptor, which was plugged into the host. This configuration is shown in Figure 39.

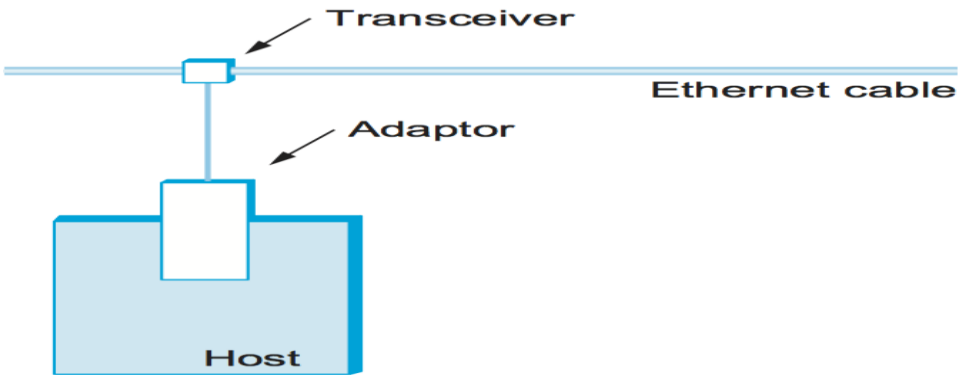


Figure 39. Ethernet transceiver and adaptor.

Multiple Ethernet segments can be joined together by repeaters (or a multi-port variant of a repeater, called a hub). A repeater is a device that forwards digital signals, much like an amplifier forwards analog signals; repeaters do not understand bits or frames. No more than four repeaters could be positioned between any pair of hosts, meaning that a classical Ethernet had a total reach of only 2500 m. For example, using just two repeaters between any pair of hosts supports a configuration similar to the one illustrated in Figure 40; that is, a segment running down the spine of a building with a segment on each floor.

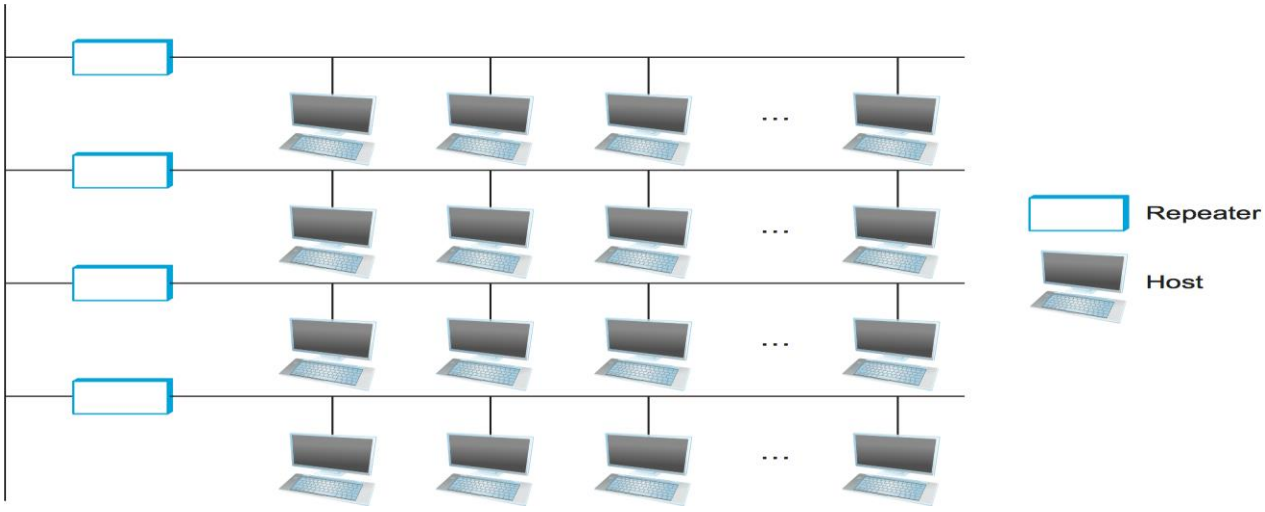


Figure 40. Ethernet repeater, interconnecting segments to form a larger collision domain.

Any signal placed on the Ethernet by a host is broadcast over the entire network; that is, the signal is propagated in both directions, and repeaters and hubs forward the signal on all outgoing segments. Terminators attached to the end of each segment absorb the signal and keep it from bouncing back and interfering with trailing signals. The original Ethernet specifications used the Manchester encoding scheme described in an earlier section, while 4B/5B encoding (or the similar 8B/10B) scheme is used today on higher speed Ethernets.

It is important to understand that whether a given Ethernet spans a single segment, a linear sequence of segments connected by repeaters, or multiple segments connected in a star configuration, data transmitted by any one host on that Ethernet reaches all the other hosts. This is the good news. The bad news is that all these hosts are competing for access to the same link, and, as a consequence, they are said to be in the same collision domain. The multi-access part of the Ethernet is all about dealing with the competition for the link that arises in a collision domain.

Access Protocol

We now turn our attention to the algorithm that controls access to a shared Ethernet link. This algorithm is commonly called the Ethernet's media access control (MAC). It is typically implemented in hardware on the network adaptor. We will not describe the hardware per se, but instead focus on the algorithm it implements. First, however, we describe the Ethernet's frame format and addresses.

Frame Format

Each Ethernet frame is defined by the format given in Figure 41. The 64-bit preamble allows the receiver to synchronize with the signal; it is a sequence of alternating 0s and 1s. Both the source and destination hosts are identified with a 48-bit address. The packet type field serves as the demultiplexing key; it identifies to which of possibly many higher-level protocols this frame should be delivered. Each frame contains up to 1500 bytes of data. Minimally, a frame must contain at least 46 bytes of data, even if this means the host has to pad the frame before transmitting it. The reason for this minimum frame size is that the frame must be long enough to detect a collision; we discuss this more below. Finally, each frame

includes a 32-bit CRC. Like the HDLC protocol described in an earlier section, the Ethernet is a bit-oriented framing protocol. Note that from the host's perspective, an Ethernet frame has a 14-byte header: two 6-byte addresses and a 2-byte type field. The sending adaptor attaches the preamble and CRC before transmitting, and the receiving adaptor removes them.

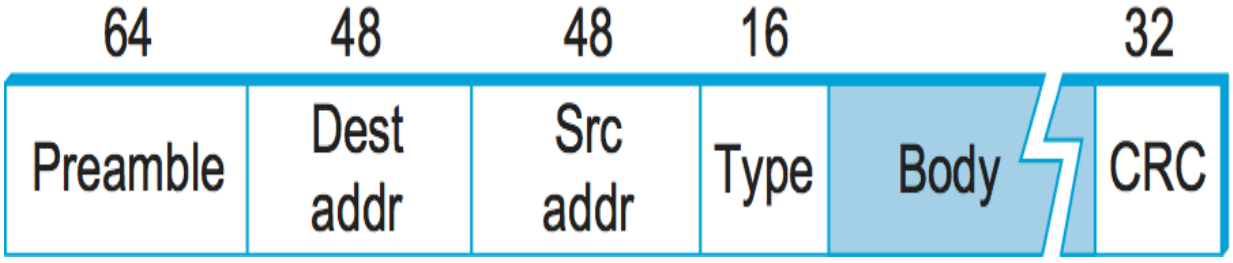


Figure 41. Ethernet frame format.

Addresses

Each host on an Ethernet—in fact, every Ethernet host in the world—has a unique Ethernet address. Technically, the address belongs to the adaptor, not the host; it is usually burned into ROM. Ethernet addresses are typically printed in a form humans can read as a sequence of six numbers separated by colons. Each number corresponds to 1 byte of the 6-byte address and is given by a pair of hexadecimal digits, one for each of the 4-bit nibbles in the byte; leading 0s are dropped. For example, 8:0:2b:e4:b1:2 is the human-readable representation of Ethernet address

00001000 00000000 00101011 11100100 10110001 00000010

To ensure that every adaptor gets a unique address, each manufacturer of Ethernet devices is allocated a different prefix that must be prepended to the address on every adaptor they build. For example, Advanced Micro Devices has been assigned the 24-bit prefix 080020 (or 8:0:20). A given manufacturer then makes sure the address suffixes it produces are unique.

Each frame transmitted on an Ethernet is received by every adaptor connected to that Ethernet. Each adaptor recognizes those frames addressed to its address and passes only those frames on to the host. (An adaptor can also be programmed to run in promiscuous mode, in which case it delivers all received frames to the host,

but this is not the normal mode.) In addition to these unicast addresses, an Ethernet address consisting of all 1s is treated as a broadcast address; all adaptors pass frames addressed to the broadcast address up to the host. Similarly, an address that has the first bit set to 1 but is not the broadcast address is called a multicast address. A given host can program its adaptor to accept some set of multicast addresses. Multicast addresses are used to send messages to some subset of the hosts on an Ethernet (e.g., all file servers). To summarize, an Ethernet adaptor receives all frames and accepts

- Frames addressed to its own address
- Frames addressed to the broadcast address
- Frames addressed to a multicast address, if it has been instructed to listen to that address
- All frames, if it has been placed in promiscuous mode

It passes to the host only the frames that it accepts.

Transmitter Algorithm

As we have just seen, the receiver side of the Ethernet protocol is simple; the real smarts are implemented at the sender's side. The transmitter algorithm is defined as follows.

When the adaptor has a frame to send and the line is idle, it transmits the frame immediately; there is no negotiation with the other adaptors. The upper bound of 1500 bytes in the message means that the adaptor can occupy the line for only a fixed length of time.

When an adaptor has a frame to send and the line is busy, it waits for the line to go idle and then transmits immediately. (To be more precise, all adaptors wait 9.6 µs after the end of one frame before beginning to transmit the next frame. This is true for both the sender of the first frame as well as those nodes listening for the line to become idle.) The Ethernet is said to be a 1-persistent protocol because an adaptor with a frame to send transmits with probability 1 whenever a busy line goes idle. In general, a p-persistent algorithm transmits with probability $0 \le p \le 10 \le p \le 1$ after a line becomes idle and defers with probability q = 1

- p. The reasoning behind choosing a p<1 is that there might be multiple adaptors waiting for the busy line to become idle, and we don't want all of them to begin transmitting at the same time. If each adaptor transmits immediately with a probability of, say, 33%, then up to three adaptors can be waiting to transmit and the odds are that only one will begin transmitting when the line becomes idle. Despite this reasoning, an Ethernet adaptor always transmits immediately after noticing that the network has become idle and has been very effective in doing so.

To complete the story about p-persistent protocols for the case when p<1, you might wonder how long a sender that loses the coin flip (i.e., decides to defer) has to wait before it can transmit. The answer for the Aloha network, which originally developed this style of protocol, was to divide time into discrete slots, with each slot corresponding to the length of time it takes to transmit a full frame. Whenever a node has a frame to send and it senses an empty (idle) slot, it transmits with probability p and defers until the next slot with probability q = 1 - p. If that next slot is also empty, the node again decides to transmit or defer, with probabilities p and q, respectively. If that next slot is not empty—that is, some other station has decided to transmit—then the node simply waits for the next idle slot and the algorithm repeats.

Returning to our discussion of the Ethernet, because there is no centralized control it is possible for two (or more) adaptors to begin transmitting at the same time, either because both found the line to be idle or because both had been waiting for a busy line to become idle. When this happens, the two (or more) frames are said to collide on the network. Each sender, because the Ethernet supports collision detection, is able to determine that a collision is in progress. At the moment an adaptor detects that its frame is colliding with another, it first makes sure to transmit a 32-bit jamming sequence and then stops the transmission. Thus, a transmitter will minimally send 96 bits in the case of a collision: 64-bit preamble plus 32-bit jamming sequence.

One way that an adaptor will send only 96 bits—which is sometimes called a runt frame—is if the two hosts are close to each other. Had the two hosts been farther apart, they would have had to transmit longer, and thus send more bits, before detecting the collision. In fact, the worst-case scenario happens when the two hosts are at opposite ends of the Ethernet. To know for sure that the frame it just

sent did not collide with another frame, the transmitter may need to send as many as 512 bits. Not coincidentally, every Ethernet frame must be at least 512 bits (64 bytes) long: 14 bytes of header plus 46 bytes of data plus 4 bytes of CRC.

Why 512 bits? The answer is related to another question you might ask about an Ethernet: Why is its length limited to only 2500 m? Why not 10 or 1000 km? The answer to both questions has to do with the fact that the farther apart two nodes are, the longer it takes for a frame sent by one to reach the other, and the network is vulnerable to a collision during this time.

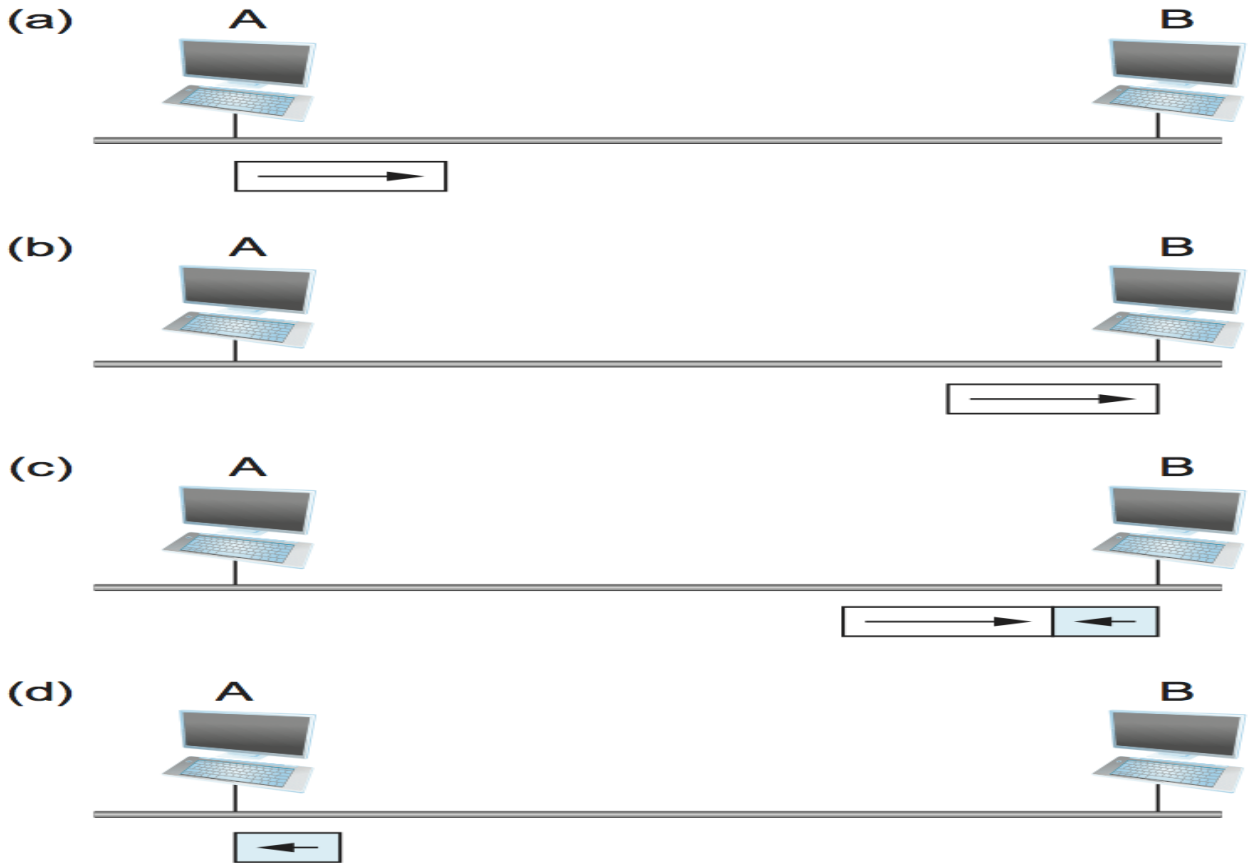


Figure 42. Worst-case scenario: (a) A sends a frame at time t; (b) A's frame arrives at B at time t+d; (c) B begins transmitting at time t+d and collides with A's frame; (d) B's runt (32-bit) frame arrives at A at time t+2×d.

Figure 42 illustrates the worst-case scenario, where hosts A and B are at opposite ends of the network. Suppose host A begins transmitting a frame at time t, as

shown in (a). It takes it one link latency (let's denote the latency as d) for the frame to reach host B. Thus, the first bit of A's frame arrives at B at time t+d, as shown in (b). Suppose an instant before host A's frame arrives (i.e., B still sees an idle line), host B begins to transmit its own frame. B's frame will immediately collide with A's frame, and this collision will be detected by host B (c). Host B will send the 32-bit jamming sequence, as described above. (B's frame will be a runt.) Unfortunately, host A will not know that the collision occurred until B's frame reaches it, which will happen one link latency later, at time t+2×d, as shown in (d). Host A must continue to transmit until this time in order to detect the collision. In other words, host A must transmit for 2×d to be sure that it detects all possible collisions. Considering that a maximally configured Ethernet is 2500 m long, and that there may be up to four repeaters between any two hosts, the round-trip delay has been determined to be 51.2 µs, which on a 10-Mbps Ethernet corresponds to 512 bits. The other way to look at this situation is that we need to limit the Ethernet's maximum latency to a fairly small value (e.g., 51.2 µs) for the access algorithm to work; hence, an Ethernet's maximum length must be something on the order of 2500 m.

Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again. Each time it tries to transmit but fails, the adaptor doubles the amount of time it waits before trying again. This strategy of doubling the delay interval between each retransmission attempt is a general technique known as exponential backoff. More precisely, the adaptor first delays either 0 or 51.2 µs, selected at random. If this effort fails, it then waits 0, 51.2, 102.4, or 153.6 µs (selected randomly) before trying again; this is k × 51.2 for k=0..3. After the third collision, it waits k × 51.2 for $k = 0.2^3 - 1$, again selected at random. In general, the algorithm randomly selects a k between 0 and $2^n - 1$ and waits k × 51.2 µs, where n is the number of collisions experienced so far. The adaptor gives up after a given number of tries and reports a transmit error to the host. Adaptors typically retry up to 16 times, although the backoff algorithm caps n in the above formula at 10.

Longevity of Ethernet

Ethernet has been the dominant local area network technology for over 30 years. Today it is typically deployed point-to-point rather than tapping into a coax cable, it often runs at speeds of 1 or 10 Gbps rather than 10 Mbps, and it allows jumbo

packets with up to 9000 bytes of data rather than 1500 bytes. But, it remains backwards compatible with the original standard. This makes it worth saying a few words about why Ethernets have been so successful, so that we can understand the properties we should emulate with any technology that tries to replace it.

First, an Ethernet is extremely easy to administer and maintain: There is no routing or configuration tables to be kept up-to-date, and it is easy to add a new host to the network. It is hard to imagine a simpler network to administer. Second, it is inexpensive: cable/fiber is relatively cheap, and the only other cost is the network adaptor on each host. Ethernet became deeply entrenched for these reasons, and any switch-based approach that aspired to displace it required additional investment in infrastructure (the switches), on top of the cost of each adaptor. The switch-based variant of Ethernet did eventually succeed in replacing multi-access Ethernet, but this is primarily because it could be deployed incrementally—with some hosts connected by point-to-point links to switches while others remained tapped into coax and connected to repeaters or hubs—all the while retaining the simplicity of network administration.

Backbone

Backbone is most important part of a system which provides the central support to the rest system, for example backbone of a human body that balance and hold all the body parts. Similarly in Computer Networks a **Backbone Network** is as a Network containing a high capacity connectivity infrastructure that backbone to the different part of the network.

Actually a backbone network allows multiple LANs to get connected in a backbone network, not a single station is directly connected to the backbone but the stations are part of LAN, and backbone connect those LANs.

Backbone LANs:

Because of increasing use of distributed applications and PCs, a new flexible strategy for LANs has been introduced. if a premises wide data communication system is to be supported then we need a networking system which can span over the required distance and which capable of interconnecting all the equipment in a single building or in a group of buildings.

DWARKA EDU

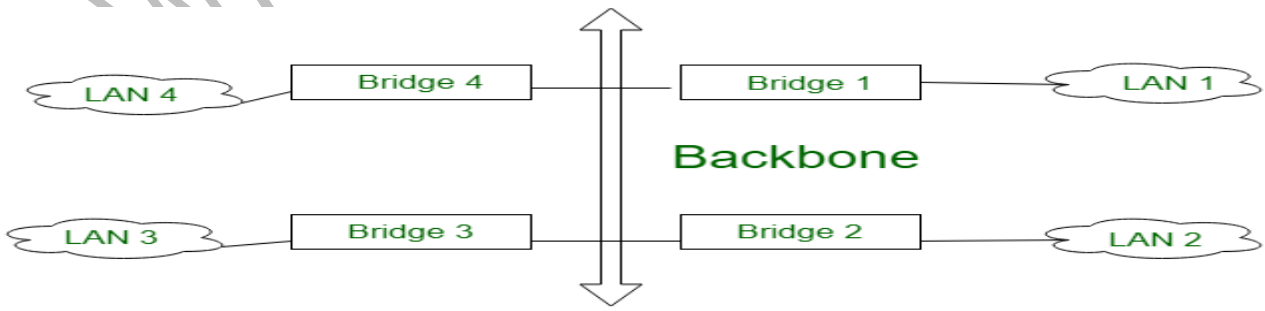
It is possible to develop a single LAN for this purpose but practically this scheme faces the following drawbacks:

1. **Poor Reliability:**
   With a single LAN, the reliability will be poor since a service interruption even for a short duration can cause major problem to the user.
2. **Capacity:**
   There is a possibility that a single LAN may be saturated due to increase in number of devices beyond a certain number
3. **Cost:**
   A single LAN can not give its optimum performance for the diverse requirements of communication and interconnection.

So the alternative for using a single LAN is to use low cost low capacity LANs in each building or department and then interconnection all these LANs with high capacity LAN. such a network is called as **Backbone LAN**. the backbone network allows several LANs to be connected. in the backbone network, no station is directly connected with backbone, instead each station is a part a LAN, and the LANs are connected to the backbone.

The backbone itself is a LAN, it uses a LAN protocol such as ethernet, Hence each connection in the backbone is itself another LAN. The two very common used architectures are: Bus backbone, Star backbone. These are explained as following below.

1. **Bus Backbone:**
   In Bus backbone the topology used for the backbone is bus topology.



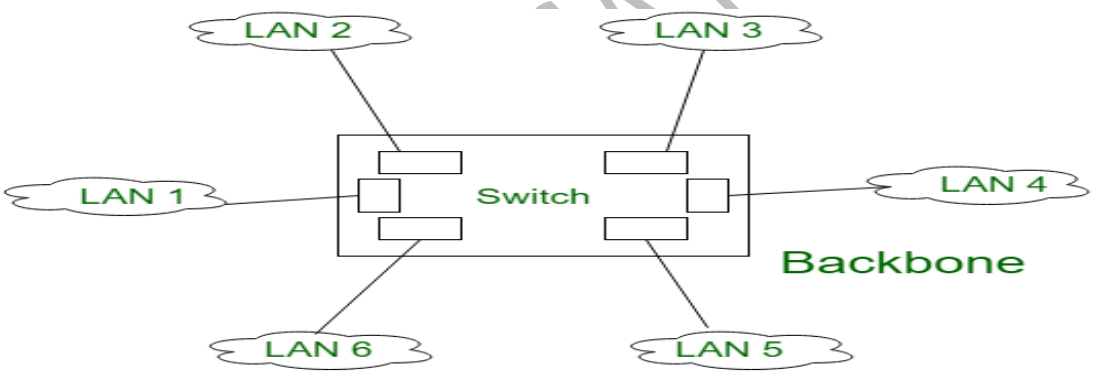
Structure of a Bus backbone

VAKAR EDUCATION HUB

In above the Bus backbone structure is used as a distribution backbone for connecting different buildings in an organization. each building may have either a single LAN or another backbone which comes in star backbone. the structure is a bridge based (bridge is the connecting device) backbone with four LANs.

Working:
In above structure if a station in LAN 2 wants to send a frame to some other station in Same LAN then Bridge 2 will not allow the frame to pass to any other LAN, hence this frame will not reach the backbone. If a station from LAN 1 wants to send a frame to a station in LAN 4 then Bridge 1 passes this frame to the backbone. This frame is then received by Bridge 4 and delivered to the destination.

2. **Star Backbone:**
   The topology of this backbone is star topology.



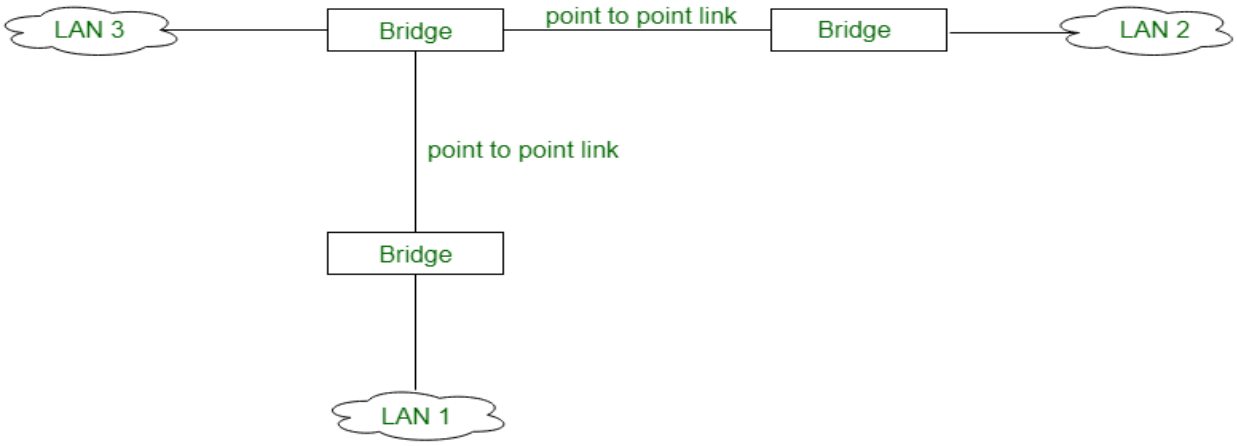
Star Backbone

Above figure shows the Star backbone in this configuration, the backbone is simply a switch which is used to connect various LANs. The switch does the job of backbone and connect the LANs as well. This type of backbone are basically used as distribution backbone inside a building.

There is one more category of backbone network is Interconnecting of Remote LANs:

3. **Interconnection of Remote control:**
   In this type of backbone network the connection are done through the

bridge called remote bridges which acts as connecting devices in connect LANs as point to point network link.



Connecting remote LANs to each other

Example of point to point networks are leased telephone lines or ADLS lines. Such a point to point network can be considered as being equivalent ta a LAN without stations.

Virtual LAN (VLAN)

Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divides broadcast domain but broadcast domain can be divided by switches using the concept of VLAN.

A broadcast domain is a network segment in which if a device broadcast a packet then all the devices in the same broadcast domain will receive it. The devices in the same broadcast domain will receive all the broadcast packet but it is limited to switches only as routers don't forward out the broadcast packet.To forward out the packets to different VLAN (from one VLAN to another) or broadcast domain, inter Vlan routing is needed. Through VLAN, different small size sub networks are created which are comparatively easy to handle.

VLAN ranges –

- **VLAN 0, 4095:**These are reserved VLAN which cannot be seen or used.

DIWAKAR EDUCA

- **VLAN 1:**It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can't be deleted or edit but can be used.
- **VLAN 2-1001:** This is a normal VLAN range. We can create, edit and delete these VLAN.
- **VLAN 1002-1005:** These are CISCO defaults for fddi and token rings. These VLAN can't be deleted.
- **Vlan 1006-4094:** This is the extended range of Vlan.

Configuration –
We can simply create VLANs by simply assigning the vlan-id and Vlan name.

```
#switch1(config)#vlan 2
#switch1(config-vlan)#vlan accounts
```

Here, 2 is the Vlan I'd and accounts is the Vlan name. Now, we assign Vlan to the switch ports.e.g-

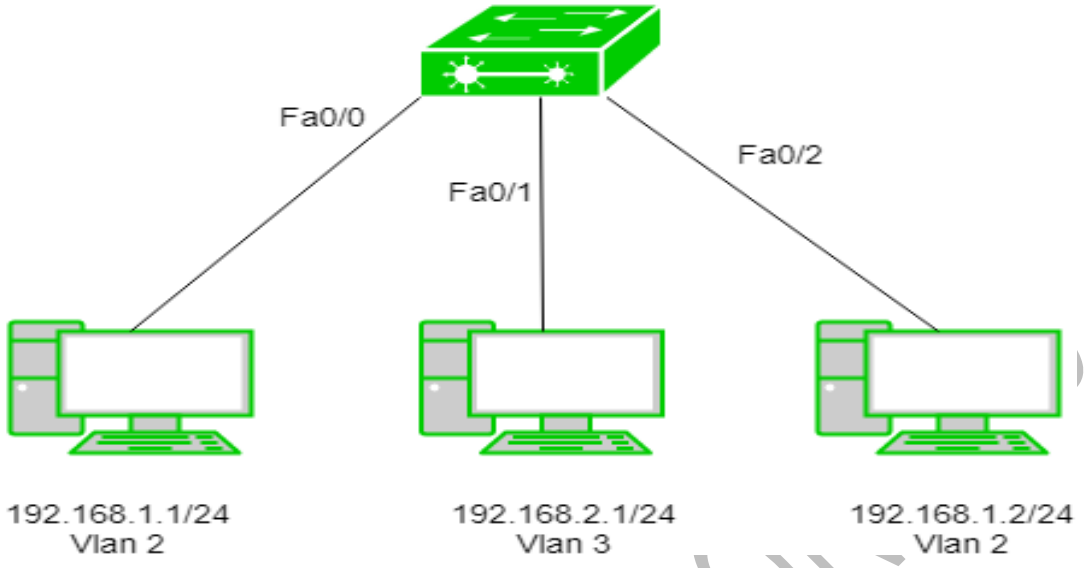
```
Switch(config)#int fa0/0
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access Vlan 2
```

Also, switchport range can be assigned to required vlans.

```
Switch(config)#int range fa0/0-2
Switch(config-if)#switchport mode access
Switch(config-if) #switchport access Vlan 2
```

By this, switchport fa0/0, fa0/1, fa0-2 will be assigned Vlan 2.
Example –

DIWAKAR EDUCATION HUB



Assigning IP address 192.168.1.1/24, 192.168.1.2/24 and 192.168.2.1/24 to the PC's. Now, we will create Vlan 2 and 3 on switch.

- Switch(config)#vlan 2
- Switch(config)#vlan 3

We have made VLANs but the most important part is to assign switch ports to the VLANs .

- Switch(config)#int fa0/0
- Switch(config-if)#switchport mode access
- Switch(config-if) #switchport access Vlan 2

- Switch(config)#int fa0/1
- Switch(config-if)#switchport mode access
- Switch(config-if) #switchport access Vlan 3

- Switch(config)#int fa0/2
- Switch(config-if)#switchport mode access
- Switch(config-if) #switchport access Vlan 2

As seen, we have assigned Vlan 2 to fa0/0, fa0/2 and Vlan 3 to fa0/1.

Advantages –

- **performance –**The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destination.e.g-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain therefore all will receive the traffic i.e wastage of bandwidth but if we make VLANs, then the broadcast or mulicast packet will go to the intended users only.
- **formation of virtual groups –** As there are different departments in every organisation namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.
- **security –** In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.
- **Flexibility –** VLAN provide flexibility to add, remove the number of host we want.
- **Cost reduction –** VLANs can be used to create broadcast domains which eliminate the need for expensive routers.
- By using Vlan, the number of small size broadcast domain can be increased which are easy to handle as compared to a bigger broadcast domain.

There are 5 main types of VLANs depending on the type of the network they carry:

1. **Default VLAN –**
   When the switch initially starts up, all switch ports become a member of the default VLAN (generally all switches have default VLAN named as **VLAN 1**), which makes them all part of the same broadcast domain. Using default VLAN allows any network device connected to any of the switch port to connect with other devices on other switch ports. One unique feature of Default VLAN is that it can't be rename or delete.
2. **Data VLAN –**
   Data VLAN is used to divide the whole network into 2 groups. One group of

DIWAKAR EDUCATION HUB

users and other group of devices. This VLAN also known as a user VLAN, the data VLAN is used only for user-generated data. This VLAN carrying data only. It is not used for carrying management traffic or voice.

3. **Voice VLAN –**
   Voice VLAN is configured to carry voice traffic. Voice VLANs are mostly given high transmission priority over other types of network traffic. To ensure voice over IP (VoIP) quality (delay of less than 150 milliseconds (ms) across the network), we must have separate voice VLAN as this will preserve bandwidth for other applications.
4. **Management VLAN –**
   A management VLAN is configured to access the management capabilities of a switch (traffic like system logging, monitoring). VLAN 1 is the management VLAN by default (VLAN 1 would be a bad choice for the management VLAN). Any of a switch VLAN could be define as the management VLAN if admin as not configured a unique VLAN to serve as the management VLAN. This VLAN ensures that bandwidth for management will be available even when user traffic is high.
5. **Native VLAN –**
   This VLAN identifies traffic coming from each end of a trunk link. A native VLAN is allocated only to an 802.1Q trunk port. The 802.1Q trunk port places untagged traffic (traffic that does not come from any VLAN) on the native VLAN. It is a best to configure the native VLAN as an unused VLAN.

IPv4 vs IPv6

What is IP?

An IP stands for internet protocol. An IP address is assigned to each device connected to a network. Each device uses an IP address for communication. It also behaves as an identifier as this address is used to identify the device on a network. It defines the technical format of the packets. Mainly, both the networks, i.e., IP and TCP, are combined together, so together, they are referred to as a TCP/IP. It creates a virtual connection between the source and the destination.

We can also define an IP address as a numeric address assigned to each device on a network. An IP address is assigned to each device so that the device on a

DIWAKAR EDUCATION HUB

network can be identified uniquely. To facilitate the routing of packets, TCP/IP protocol uses a 32-bit logical address known as IPv4(Internet Protocol version 4).

An IP address consists of two parts, i.e., the first one is a network address, and the other one is a host address.

There are two types of IP addresses:

- IPv4
- IPv6

IPv4

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.

For example, **66.94.29.13**

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

Each bit in an octet can be either 1 or 0. If the bit the 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.

Representation of 8 Bit Octet

128	64	32	16	8	4	2	1

DIWAKAR EDUCATION HUB

The above representation shows the structure of 8- bit octet.

Now, we will see how to obtain the binary representation of the above IP address, i.e., 66.94.29.13

Step 1: First, we find the binary number of 66.

128	64	32	16	8	4	2	1
0	1	0	0	0	0	1	0

To obtain 66, we put 1 under 64 and 2 as the sum of 64 and 2 is equal to 66 (64+2=66), and the remaining bits will be zero, as shown above. Therefore, the binary bit version of 66 is 01000010.

Step 2: Now, we calculate the binary number of 94.

128	64	32	16	8	4	2	1
0	1	0	1	1	1	1	0

To obtain 94, we put 1 under 64, 16, 8, 4, and 2 as the sum of these numbers is equal to 94, and the remaining bits will be zero. Therefore, the binary bit version of 94 is 01011110.

Step 3: The next number is 29.

128	64	32	16	8	4	2	1
0	0	0	1	1	1	0	0

To obtain 29, we put 1 under 16, 8, 4, and 1 as the sum of these numbers is equal to 29, and the remaining bits will be zero. Therefore, the binary bit version of 29 is 00011101.

Step 4: The last number is 13.

128	64	32	16	8	4	2	1
0	0	0	0	1	1	0	1

To obtain 13, we put 1 under 8, 4, and 1 as the sum of these numbers is equal to 13, and the remaining bits will be zero. Therefore, the binary bit version of 13 is 00001101.

Drawback of IPv4

Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet. As we know that IPv4 produces 4 billion addresses, which are not enough for each device connected to the internet on a planet. Although the various techniques were invented, such as variable- length mask, network address translation, port address translation, classes, inter-domain translation, to conserve the bandwidth of IP address and slow down the depletion of an IP address. In these techniques, public IP is converted into a private IP due to which the user having public IP can also use the internet. But still, this was not so efficient, so it gave rise to the development of the next generation of IP addresses, i.e., IPv6.

IPv6

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

- **Dual stacking:** It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.

DIWAKAR EDUCATION HUB

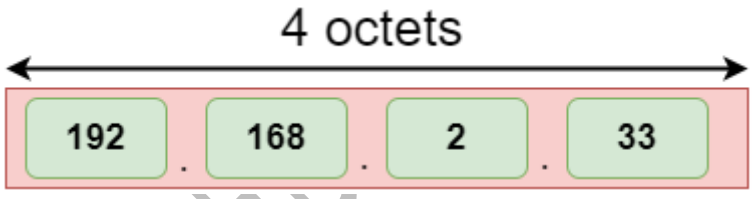
- **Tunneling:** In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.
- **Network Address Translation:** The translation allows the communication between the hosts having a different version of IP.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion ($3.4*10^{38}$) addresses.

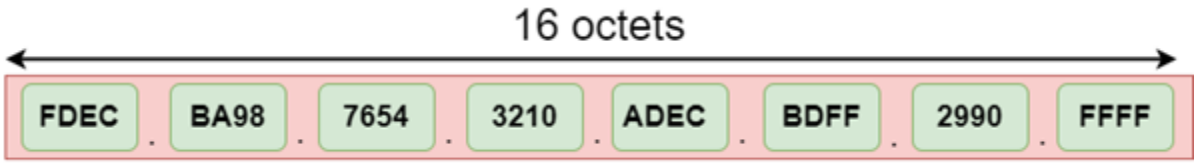
IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time

Address format

The address format of IPv4:



The address format of IPv6:



The above diagram shows the address format of IPv4 and IPv6. An IPv4 is a 32-bit decimal address. It contains 4 octets or fields separated by 'dot', and each field is 8-bit in size. The number that each field contains should be in the range of 0-255. Whereas an IPv6 is a 128-bit hexadecimal address. It contains 8 fields separated by a colon, and each field is 16-bit in size.

Differences between IPv4 and IPv6

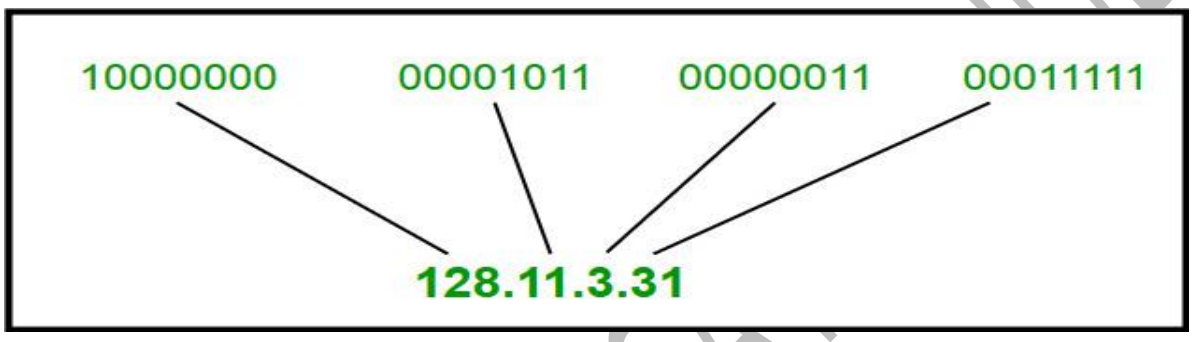
	Ipv4	Ipv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.

Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

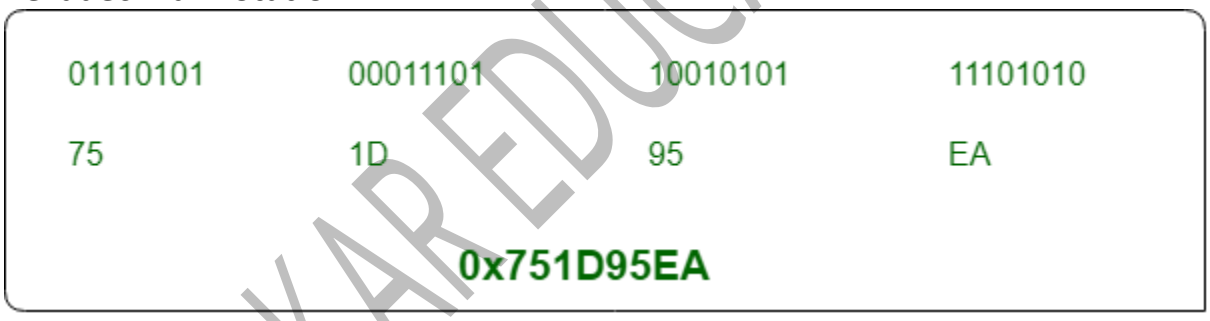
Classful Addressing

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 2^{32}.
Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.

Dotted Decimal Notation:



Hexadecimal Notation:



Some points to be noted about dotted decimal notation:

1. The value of any segment (byte) is between 0 and 255 (both included).
2. There are no zeroes preceding the value in any segment (054 is wrong, 54 is correct).

Classful Addressing
The 32 bit IP address is divided into five sub-classes. These are:

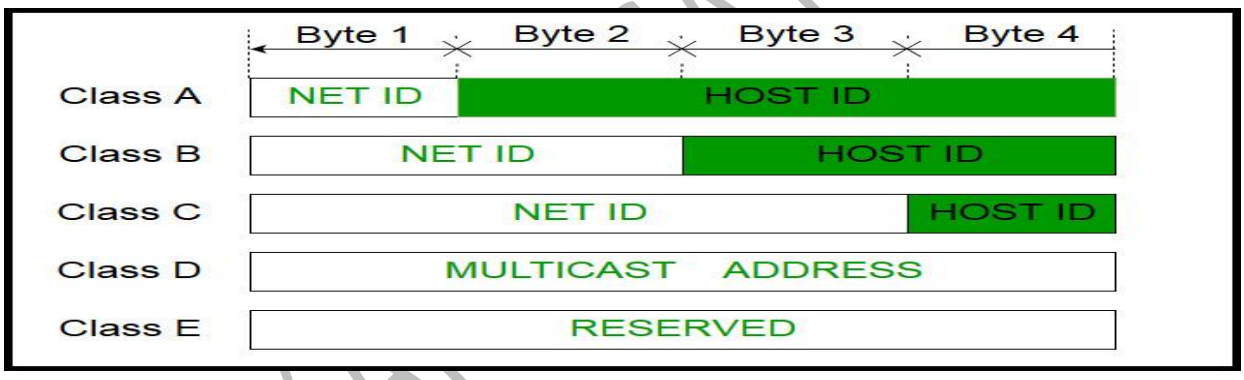
- Class A
- Class B
- Class C

- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.
IPv4 address is divided into two parts:

- **Network ID**
- **Host ID**

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.



Note: IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).

Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

Class A:

IP address belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

- 2^7-2= 126 network ID(Here 2 address is subracted because 0.0.0.0 and 127.x.y.z are special address.)
- 2^24 – 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x



Class A

Class B:

IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.



Class C:

IP address belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address

IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.

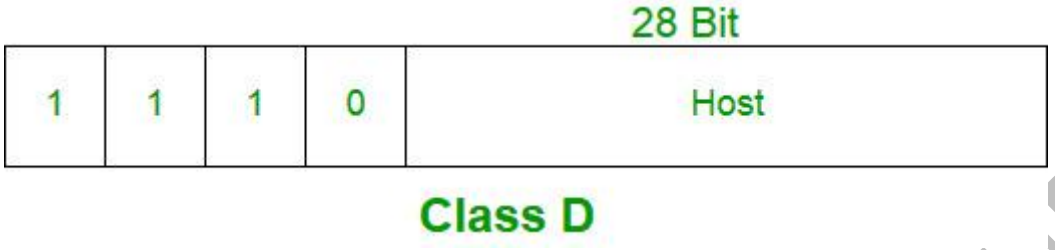


Class D:

IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.

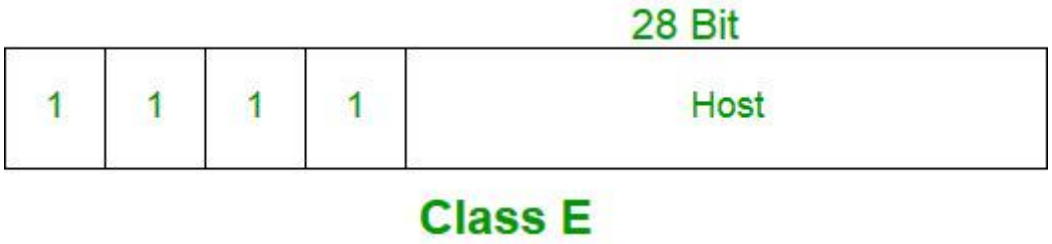
DIVYA EDUCATION HUB

Class D does not posses any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.



Class E:

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



Range of special IP addresses:

169.254.0.0 – 169.254.0.16 : Link local addresses
127.0.0.0 – 127.0.0.8 : Loop-back addresses
0.0.0.0 – 0.0.0.8 : used to communicate within the current network.

Rules for assigning Host ID:

Host ID's are used to identify a host within a network. The host ID are assigned based on the following rules:

- Within any network, the host ID must be unique to that network.
- Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.

DIWAKAR EDUCATION HUB

- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for assigning Network ID:

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Problems with Classful Addressing:

The problem with this classful addressing method is that millions of class A address are wasted, many of the class B address are wasted, whereas, number of addresses available in class C is so small that it cannot cater the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved.

Classless Addressing

Network Address and Mask

Network address – It identifies a network on internet. Using this, we can find range of addresses in the network and total possible number of hosts in the network.

Mask – It is a 32-bit binary number that gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.

The default mask in different classes are :

DIWAKAR EDUCATION HUB

Class A – 255.0.0.0

Class B – 255.255.0.0

Class C – 255.255.255.0

Example : Given IP address 132.6.17.85 and default class B mask, find the beginning address (network address).

Solution : The default mask is 255.255.0.0, which means that the only the first 2 bytes are preserved and the other 2 bytes are set to 0. Therefore, the network address is 132.6.0.0.

Subnetting: Dividing a large block of addresses into several contiguous sub-blocks and assigning these sub-blocks to different smaller networks is called subnetting. It is a practice that is widely used when classless addressing is done.

Classless Addressing

To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address. We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28. Here, subnet mask is found by putting the given number of bits out of 32 as 1, like, in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240.

Some values calculated in subnetting :

1. Number of subnets : Given bits for mask – No. of bits in default mask

2. Subnet address : AND result of subnet mask and the given IP address

3. Broadcast address : By putting the host bits as 1 and retaining the network bits as in the IP address

4. Number of hosts per subnet : $2^{(32 - \text{Given bits for mask})} - 2$

DIWAKAR EDUCATION HUB

5. First Host ID : Subnet address + 1 (adding one to the binary representation of the subnet address)

6. Last Host ID : Subnet address + Number of Hosts

Example : Given IP Address – 172.16.0.0/25, find the number of subnets and the number of hosts per subnet. Also, for the first subnet block, find the subnet address, first host ID, last host ID and broadcast address.

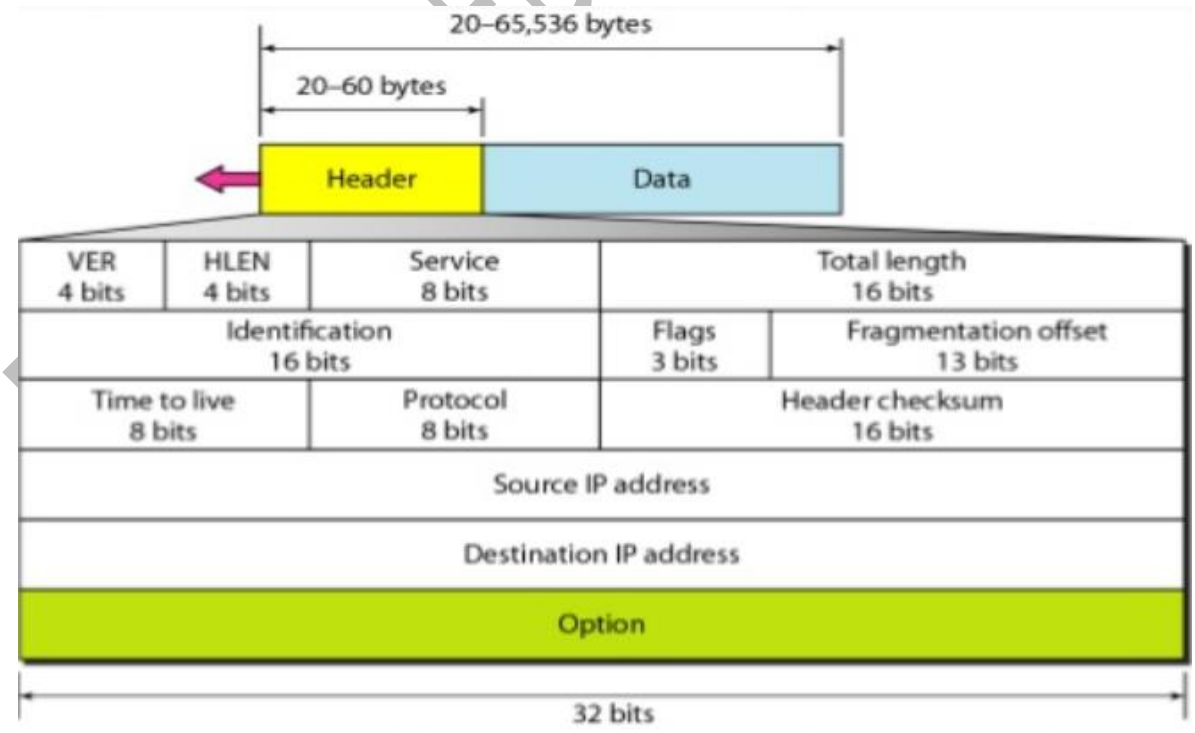
Solution : This is a class B address. So, no. of subnets = $2^{(25-16)} = 2^9 = 512$.

No. of hosts per subnet = $2^{(32-25)} - 2 = 2^7 - 2 = 128 - 2 = 126$

For the first subnet block, we have subnet address = 0.0, first host id = 0.1, last host id = 0.126 and broadcast address = 0.127

IPv4 Datagram Header

IPv4 is a connectionless protocol for a packet- switching network that uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination.



EDUCATION HUB

Packets in the IPv4 layer are called datagrams. A datagram is a variable-length packet consisting of two parts: header and data. The header is 20 to 60 bytes in length and contains information essential to routing.

- **Version (VER):** This 4-bit field defines the version of the IPv4 protocol. Currently, the version is 4. However, version 6 (or IPng) may totally replace version 4 in the future.
- **Header length (HLEN):** This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).
- **Services:** IETF has changed the interpretation and name of this 8-bit field. This field, previously called service type, is now called differentiated services.
- **Type of service:** Low Delay, High Throughput, Reliability (8 bits)
- **Total Length:** Length of header + Data (16 bits), which has a minimum value 20 Bytes and the maximum is 65,535 bytes
- **Identification:** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)
- **Flags:** 3 flags of 1 bit each: reserved bit (must be zero), do not fragment flag, more fragments flag (same order)
- **Fragment Offset:** Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes
- **Time to live:** Datagram's lifetime (8 bits), It prevents the datagram to loop in the network
- **Protocol:** Name of the protocol to which the data is to be passed (8 bits)
- **Header Checksum:** 16 bits header checksum for checking errors in the datagram header
- **Source IP address:** 32 bits IP address of the sender

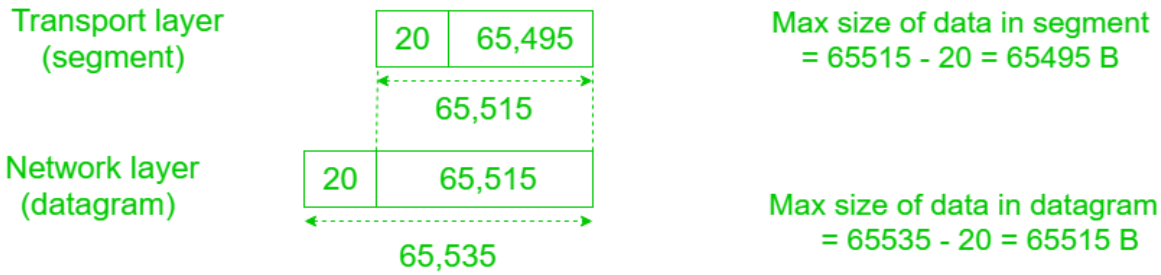
DIWAKAR EDUCATION HUB

- **Destination IP address:** 32 bits IP address of the receiver
- **Option:** Optional information such as source route. Due to the presence of options, the size of the datagram header can be of variable length (20 bytes to 60 bytes).

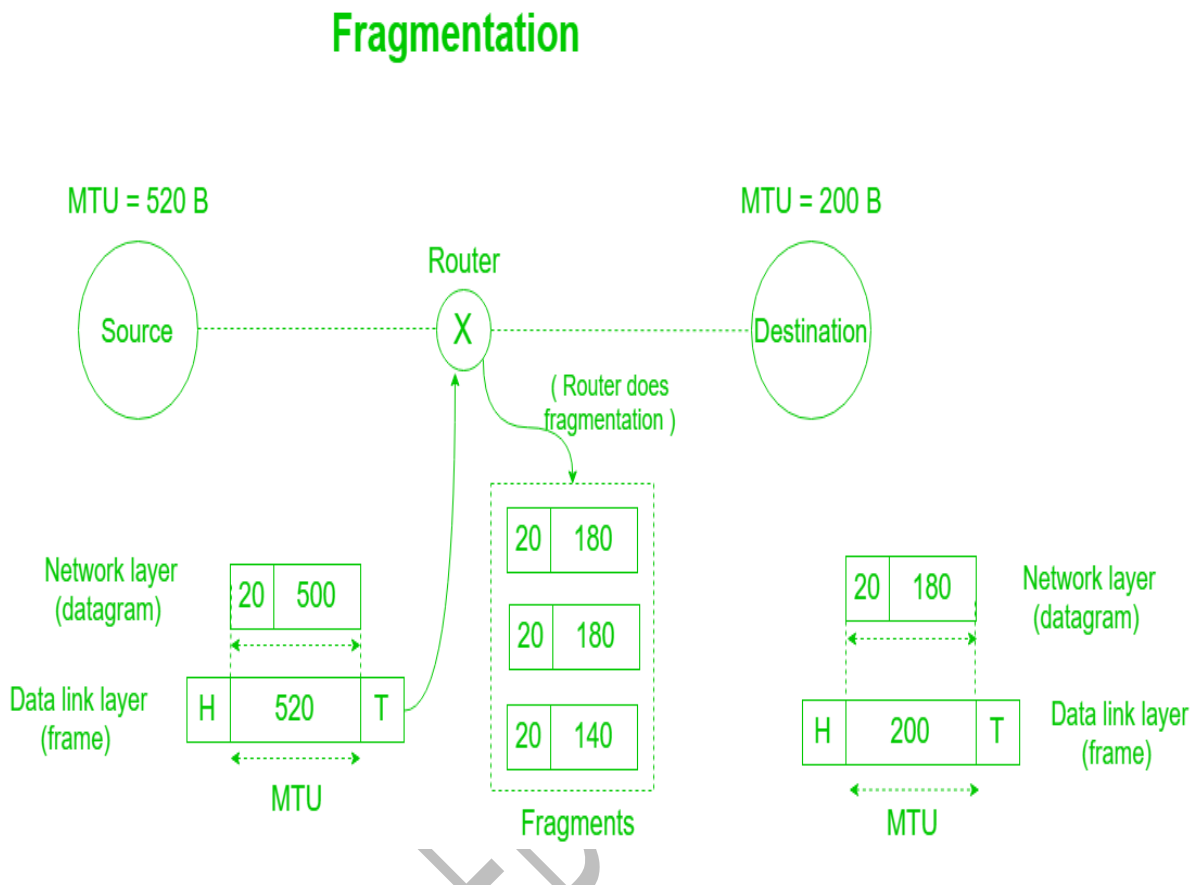
Fragmentation

Fragmentation is done by the network layer when the maximum size of datagram is greater than maximum size of data that can be held a frame i.e., its Maximum Transmission Unit (MTU). The network layer divides the datagram received from transport layer into fragments so that data flow is not disrupted.

- Since there are 16 bits for total length in IP header so, maximum size of IP datagram = $2^{16} - 1 = 65,535$ bytes.



- It is done by network layer at the destination side and is usually done at routers.
- Source side does not require fragmentation due to wise (good) segmentation by transport layer i.e. instead of doing segmentation at transport layer and fragmentation at network layer, the transport layer looks at datagram data limit and frame data limit and does segmentation in such a way that resulting data can easily fit in a frame without the need of fragmentation.



- Receiver identifies the frame with the **identification (16 bits)** field in IP header. Each fragment of a frame has same identification number.
- Receiver identifies sequence of frames using the **fragment offset(13 bits)** field in IP header
- An overhead at network layer is present due to extra header introduced due to fragmentation.

Fields in IP header for fragmentation –

- **Identification (16 bits) –** use to identify fragments of same frame.
- **Fragment offset (13 bits) –** use to identify sequence of fragments in the frame. It generally indicates number of data bytes preceeding or ahead of the fragment.
  Maximum fragment offset possible = (65535 – 20) – 1 = 65514
  {where 65535 is maximum size of datagram and 20 is minimum size of IP header}

So, we need ceil($\log_2 65514$) = 16 bits for fragment offset but fragment offset field has only 13 bits. So, to represent efficiently we need to scale down fragment offset field by $2^{16}/2^{13} = 8$ which acts as a scaling factor. Hence, all fragments except the last fragment should have data in multiples of 8 so that fragment offset $\in$ N.

- **More fragments (MF = 1 bit) –** tells if more fragments ahead of this fragment i.e. if MF = 1, more fragments are ahead of this fragment and if MF = 0, it is the last fragment.
- **Don't fragment (DF = 1 bit) –** if we don't want the packet to be fragmented then DF is set i.e. DF = 1.

Reassembly of Fragments –

It takes place only at destination and not at routers since packets take independent path(datagram packet switching), so all may not meet at a router and hence a need of fragmentation may arise again. The fragments may arrive out of order also.

MF	Fragment Offset	
1	0	→ 1st packet
1	!=0	→ Intermediate packet
0	!=0	→ Last packet
0	0	→ Invalid

Algorithm –

1. Destination should identify that datagram is fragmented from MF, Fragment offset field.

2. Destination should identify all fragments belonging to same datagram from Identification field.
3. Identify the 1st fragment(offset = 0).
4. Identify subsequent fragment using header length, fragment offset.
5. Repeat until MF = 0.

Efficiency –

Efficiency (e) = useful/total = (Data without header)/(Data with header)
Throughput = e * B { where B is bottleneck bandwidth }

Example – An IP router with a Maximum Transmission Unit (MTU) of 200 bytes has received an IP packet of size 520 bytes with an IP header of length 20 bytes. The values of the relevant fields in the IP header.

Explanation – Since MTU is 200 bytes and 20 bytes is header size so, maximum length of data = 180 bytes but it can be represented in fragment offset since not divisible by 8 so, maximum length of data feasible = 176 bytes.
Number of fragments = (520/200) = 3.
Header length = 5 (since scaling factor is 4 therefore, 20/4 = 5)
Efficiency, e = (Data without header)/(Data with header) = 500/560 = 89.2 %

	20 | 176	20 | 176	20 | 148
Fragment Offset	0	22	44
MF	1	1	0
Header length	5	5	5
Total length	196	196	168

So, as far as the algorithm goes, IP header checksum is : **16 bit one's complement of the one's complement sum of all 16 bit words in the header**

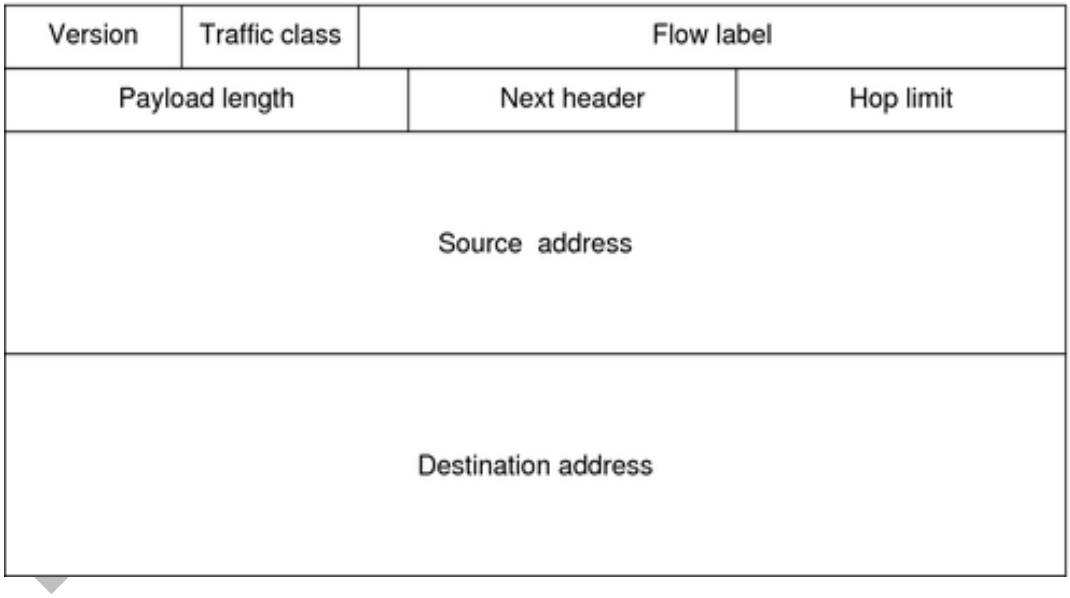
This means that if we divide the IP header is 16 bit words and sum each of them up and then finally do a one's compliment of the sum then the value generated out of this operation would be the checksum.

Now, the above is done at the source side which is sending the data packet. At the destination side which receives the data packet replaces the checksum value in the header with all zeros and then calculates the checksum based on the same algorithm as mentioned above. After a checksum value is obtained then this value is compared with the value that came in the header. This comparison decides whether the IP header is fine or corrupted.

IPv6 Packet Header Format

The IPv6 protocol defines a set of headers, including the basic IPv6 header and the IPv6 extension headers. The following figure shows the fields that appear in the IPv6 header and the order in which the fields appear.

Figure 11-3 IPv6 Basic Header Format



The following list describes the function of each header field.

- **Version** – 4-bit version number of Internet Protocol = 6.
- **Traffic class** – 8-bit traffic class field.
- **Flow label** – 20-bit field.

- **Payload length** – 16-bit unsigned integer, which is the rest of the packet that follows the IPv6 header, in octets.
- **Next header** – 8-bit selector. Identifies the type of header that immediately follows the IPv6 header. Uses the same values as the IPv4 protocol field.
- **Hop limit** – 8-bit unsigned integer. Decremented by one by each node that forwards the packet. The packet is discarded if the hop limit is decremented to zero.
- **Source address** – 128 bits. The address of the initial sender of the packet.
- **Destination address** – 128 bits. The address of the intended recipient of the packet. The intended recipient is not necessarily the recipient if an optional routing header is present.

IPv6 Extension Headers

IPv6 options are placed in separate extension headers that are located between the IPv6 header and the transport-layer header in a packet. Most IPv6 extension headers are not examined or processed by any router along a packet's delivery path until the packet arrives at its final destination. This feature provides a major improvement in router performance for packets that contain options. In IPv4, the presence of any options requires the router to examine all options.

Unlike IPv4 options, IPv6 extension headers can be of arbitrary length. Also, the number of options that a packet carries is not limited to 40 bytes. This feature, in addition to the manner in which IPv6 options are processed, permits IPv6 options to be used for functions that are not practical in IPv4.

To improve performance when handling subsequent option headers, and the transport protocol that follows, IPv6 options are always an integer multiple of 8 octets long. The integer multiple of 8 octets retains the alignment of subsequent headers.

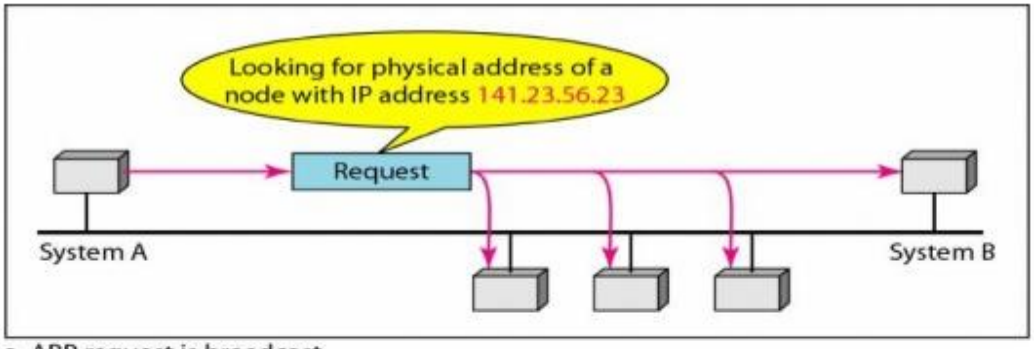
The following IPv6 extension headers are currently defined:

- **Routing** – Extended routing, such as IPv4 loose source route
- **Fragmentation** – Fragmentation and reassembly
- **Authentication** – Integrity and authentication, and security
- **Encapsulating Security Payload** – Confidentiality
- **Hop-by-Hop options** – Special options that require hop-by-hop processing

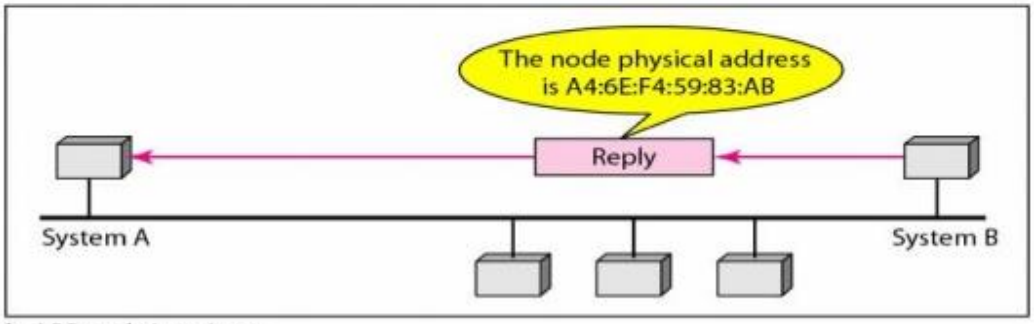
DIWAKAR EDUCATION HUB

- **Destination options** – Optional information to be examined by the destination node

Mapping Logical to Physical Address: ARP



a. ARP request is broadcast



b. ARP reply is unicast

Figure 3.27 ARP operation

Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver. The logical (IP) address is obtained from the DNS if the sender is the host or it is found in a routing table if the sender is a router. But the IP datagram must be encapsulated in a frame to be able to pass through the physical network. This means that the sender needs the physical address of the receiver. The host or the router sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network.

1. Cache Memory

Using ARP is inefficient if system A needs to broadcast an ARP request for each IP packet it needs to send to system B. It could have broadcast the IP packet itself. ARP can be useful if the ARP reply is cached because a system normally sends several packets to the same destination. A system that receives an ARP reply stores the mapping in the cache memory and

keeps it for 20 to 30 minutes unless the space in the cache is exhausted. Before sending an ARP request, the system first checks its cache to see if it can find the mapping.

2. Packet Format

The fields are as follows:

Hardware type: This is a 16-bit field defining the type of the network on which ARP isrunning. Each LAN has been assigned an integer based on its type. For example, Ethernet is given type 1. ARP can be used on any physical network

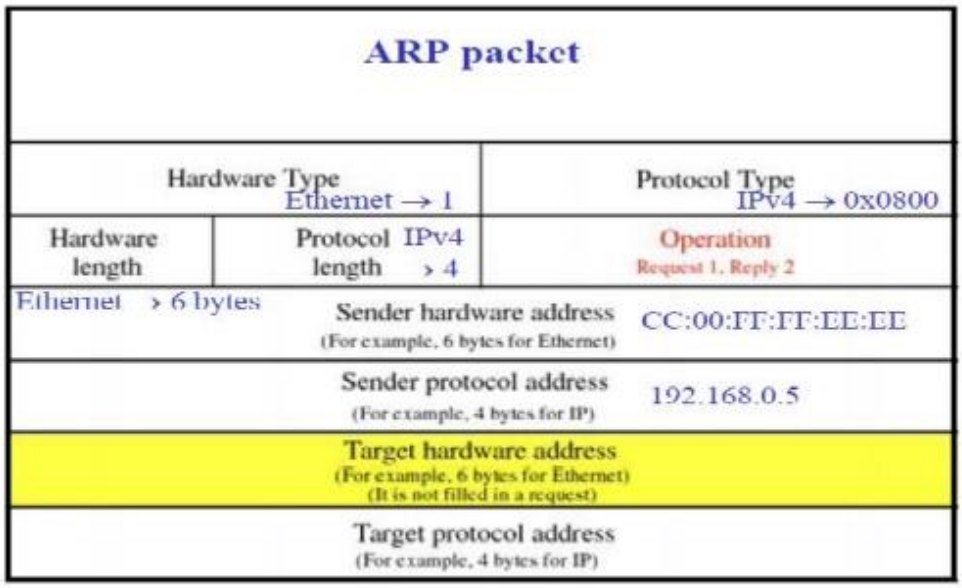


Figure 3.28 ARP Packet

Protocol type: This is a 16-bit field defining the protocol. For example, the value of thisfield for the IPv4 protocol is 080016, ARP can be used with any higher-level protocol.

Hardware length: This is an 8-bit field defining the length of the physical address inbytes. For example, for Ethernet the value is 6.

Protocol length: This is an 8-bit field defining the length of the logical address in bytes.For example, for the IPv4 protocol the value is 4.

Operation: This is a 16-bit field defining the type of packet. Two packet types aredefined: ARP request (1) and ARP reply (2).

Sender hardware address: This is a variable-length field defining the physical addressof the sender. For example, for Ethernet this field is 6 bytes long.

Sender protocol address: This is a variable-length field defining the logical (forexample, IP) address of the sender. For the IP protocol, this field is 4 bytes long.

Target hardware address: This is a variable-length field defining the physical addressof the target. For example, for Ethernet this field is 6 bytes long. For an ARP request message, this field is allOs because the sender does not know the physical address of the target.

Target protocol address: This is a variable-length field defining the logical (forexample, IP) address of the target. For the IPv4 protocol, this field is 4 bytes long.

3. Encapsulation

An ARP packet is encapsulated directly into a data link frame. For example, an ARP packet is encapsulated in an Ethernet frame. Note that the type field indicates that the data carried by the frame are an ARP packet

DIWAKAR EDUCATION HUB

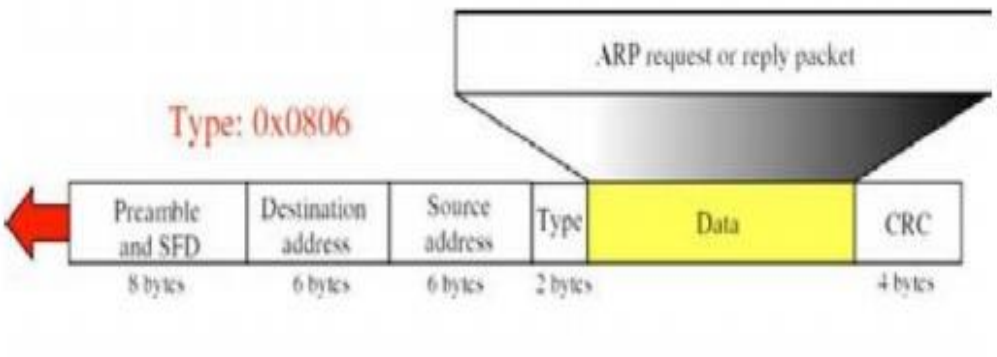


Figure 3.29 Encapsulation

Operation

The steps involved in an ARP process:

1. The sender knows the IP address of the target.

2. IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address, and the target IP address. The target physical address field is filled with 0s.

3. The message is passed to the data link layer where it is encapsulated in a frame by using the physical address of the sender as the source address and the physical broadcast address as the destination address.

4. Every host or router receives the frame. Because the frame contains a broadcast destination address, all stations remove the message and pass it to ARP. All machines except the one targeted drop the packet. The target machine recognizes its IP address.

5. The target machine replies with an ARP reply message that contains its physical address. The message is unicast.

6. The sender receives the reply message. It now knows the physical address of the target machine.

7. The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.

DWAKAR EDUCATION

4. Four Different Cases:

The following are four different cases in which the services of ARP can be used

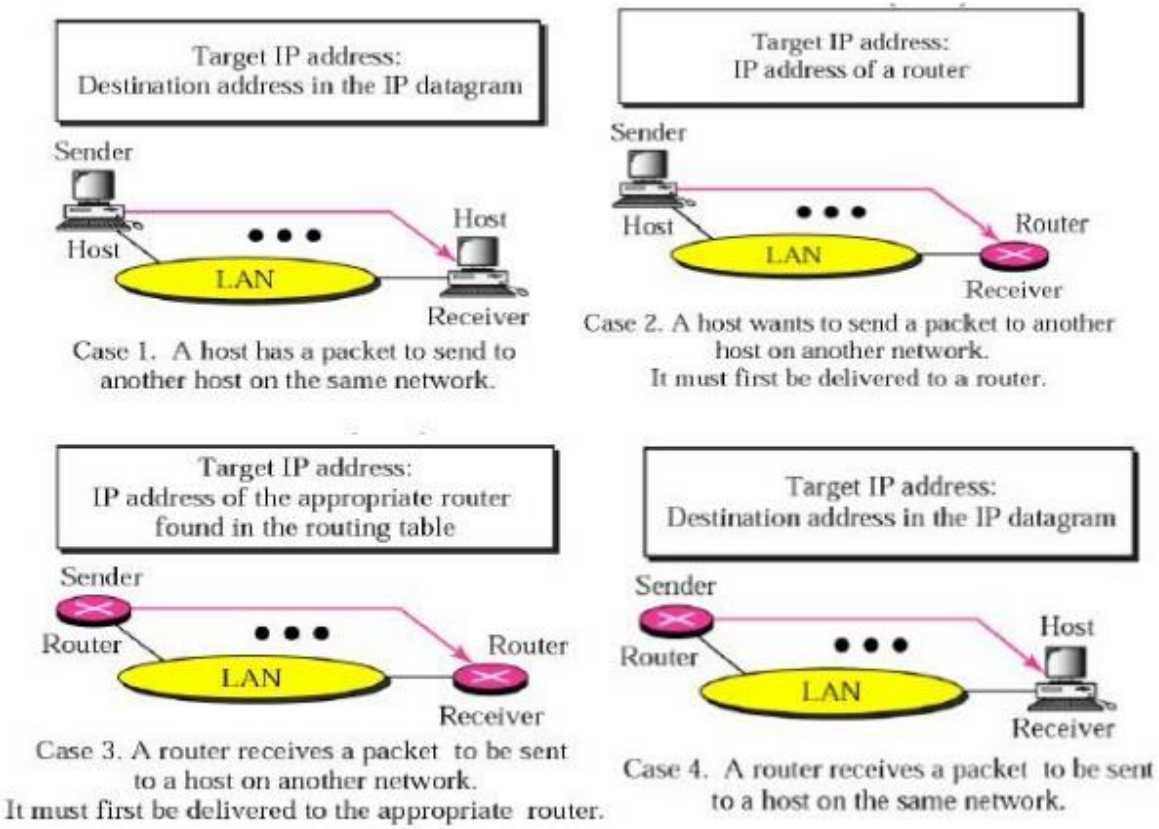


Figure 3.30 Four cases using ARP

1. The sender is a host and wants to send a packet to another host on the same network. In this case, the logical address that must be mapped to a physical address is the destination IP address in the datagram header.

2. The sender is a host and wants to send a packet to another host on another network. In this case, the host looks at its routing table and finds the IP address of the next hop (router) for this destination. If it does not have a routing table, it looks for the IP address of the default router. The IP address of the router becomes the logical address that must be mapped to a physical address.

3. The sender is a router that has received a datagram destined for a host on another network. It checks its routing table and finds the IP address of the next

router. The IP address of the next router becomes the logical address that must be mapped to a physical address.

4. The sender is a router that has received a datagram destined for a host on the same network. The destination IP address of the datagram becomes the logical address that must be mapped to a physical address.

Example 3.17

A host with IP addresses 130.23.43.20 and physical address B2:34:55: 10:22: 10 has a packet to send to another host with IP address 130.23.43.25 and physical address A4:6E:F4:59:83:AB. The two hosts are on the same Ethernet network. Show the ARP request and reply packets encapsulated in Ethernet frames.

Solution

The ARP request and reply packets. Note that the ARP data field in this case is 28 bytes, and that the individual addresses do not fit in the 4-byte boundary. That is why we do not show the regular 4-byte boundaries for these addresses.

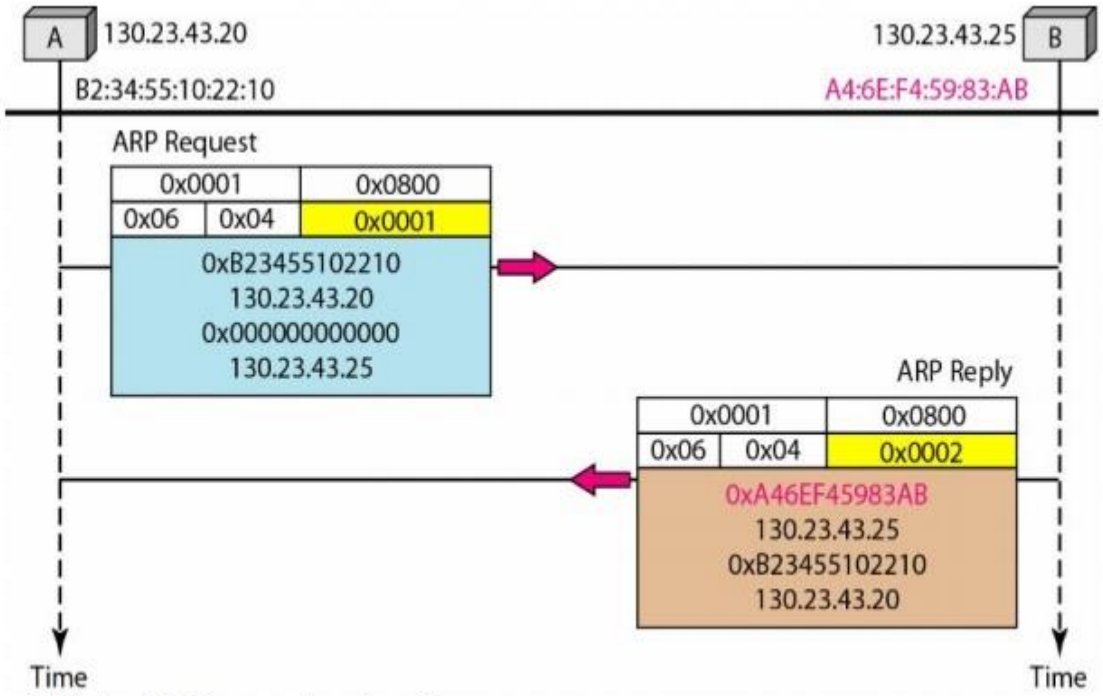


Figure 3.31 An ARP request and reply

5. Proxy ARP

A technique called proxy ARP is used to create a subnetting effect. A proxy ARP is an ARP that acts on behalf of a set of hosts. Whenever a router running a proxy ARP receives an ARP request looking for the IP address of one of these hosts, the router sends an ARP reply announcing its own hardware (physical) address. After the router receives the actual IP packet, it sends the packet to the appropriate host or router. Let us give an example.

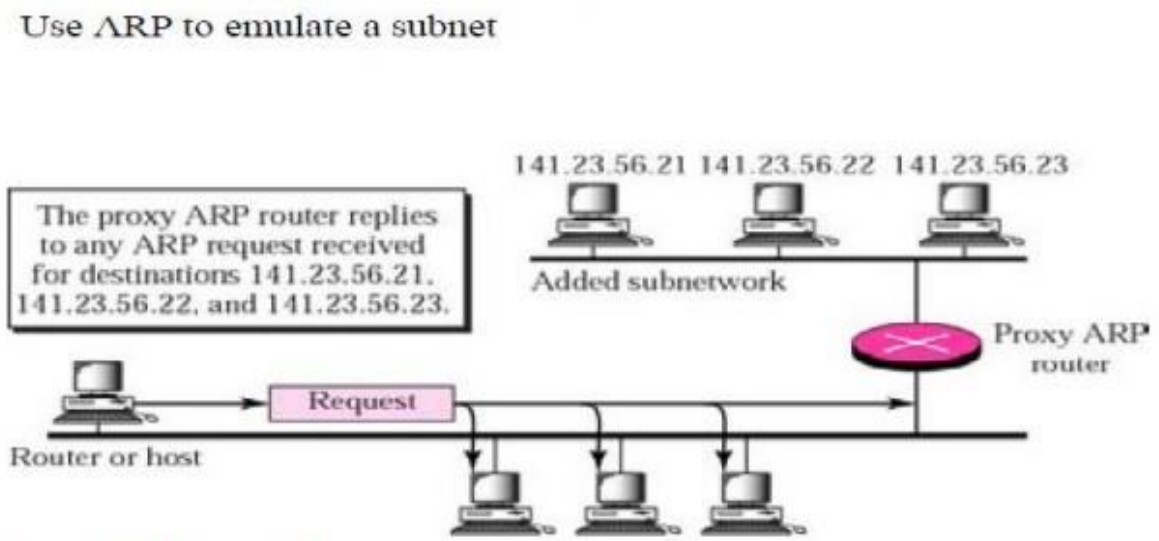


Figure 3.32 Proxy ARP

However, the administrator may need to create a subnet without changing the whole system to recognize subnetted addresses. One solution is to add a router running a proxy ARP. In this case, the router acts on behalf of all the hosts installed on the subnet. When it receives an ARP request with a target IP address that matches the address of one of its proteges (141.23.56.21, 141.23.56.22, or 141.23.56.23), it sends an ARP reply and announces its hardware address as the target hardware address. When the router receives the IP packet, it sends the packet to the appropriate host. This may happen in two cases:

1. A diskless station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.

2. An organization does not have enough IP addresses to assign to each station; it needs to assign IP addresses on demand. The station can send its physical address and ask for a short time lease.

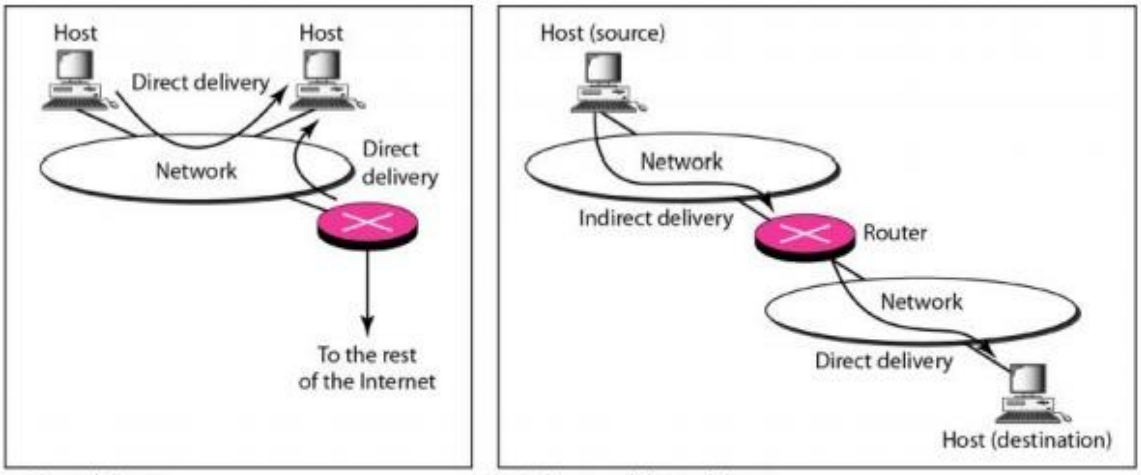
Direct Versus Indirect Delivery

Delivery

The network layer supervises the handling of the packets by the underlying physical networks. We define this handling as the delivery of a packet.

Direct Versus Indirect Delivery

The delivery of a packet to its final destination is accomplished by using two different methods of delivery, direct and indirect



a. Direct delivery b. Indirect and direct delivery

Figure 3.39 Direct and indirect delivery

Direct Delivery

In a direct delivery, the final destination of the packet is a host connected to the same physical network as the deliverer. Direct delivery occurs when the source and destination of the packet are located on the same physical network or when the delivery is between the last router and the destination host. The sender can easily determine if the delivery is direct. It can extract the network address of the

destination (using the mask) and compare this address with the addresses of the networks to which it is connected. If a match is found, the delivery is direct.

Indirect Delivery

If the destination host is not on the same network as the deliverer, the packet is delivered indirectly. In an indirect delivery, the packet goes from router to router until it reaches the one connected to the same physical network as its final destination.

Routing

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

Routing Metrics and Costs

Routing metrics and costs are used for determining the best route to the destination. The factors used by the protocols to determine the shortest path, these factors are known as a metric.

Metrics are the network variables used to determine the best route to the destination. For some protocols use the static metrics means that their value

DIWAKAR EDUCATION HUB

cannot be changed and for some other routing protocols use the dynamic metrics means that their value can be assigned by the system administrator.

The most common metric values are given below:

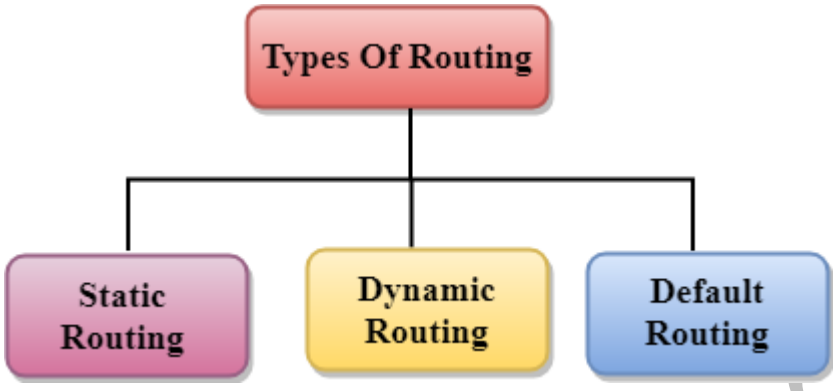
- **Hop count:** Hop count is defined as a metric that specifies the number of passes through internetworking devices such as a router, a packet must travel in a route to move from source to the destination. If the routing protocol considers the hop as a primary metric value, then the path with the least hop count will be considered as the best path to move from source to the destination.
- **Delay:** It is a time taken by the router to process, queue and transmit a datagram to an interface. The protocols use this metric to determine the delay values for all the links along the path end-to-end. The path having the lowest delay value will be considered as the best path.
- **Bandwidth:** The capacity of the link is known as a bandwidth of the link. The bandwidth is measured in terms of bits per second. The link that has a higher transfer rate like gigabit is preferred over the link that has the lower capacity like 56 kb. The protocol will determine the bandwidth capacity for all the links along the path, and the overall higher bandwidth will be considered as the best route.
- **Load:** Load refers to the degree to which the network resource such as a router or network link is busy. A Load can be calculated in a variety of ways such as CPU utilization, packets processed per second. If the traffic increases, then the load value will also be increased. The load value changes with respect to the change in the traffic.
- **Reliability:** Reliability is a metric factor may be composed of a fixed value. It depends on the network links, and its value is measured dynamically. Some networks go down more often than others. After network failure, some network links repaired more easily than other network links. Any reliability factor can be considered for the assignment of reliability ratings, which are generally numeric values assigned by the system administrator.

Types of Routing

Routing can be classified into three categories:

DIWAKAR EDUCATION HUB

- Static Routing
- Default Routing
- Dynamic Routing



Static Routing

- Static Routing is also known as Nonadaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the condition or topology of the networks

Advantages Of Static Routing

Following are the advantages of Static Routing:

- **No Overhead:** It has ho overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing.
- **Bandwidth:** It has not bandwidth usage between the routers.
- **Security:** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

Disadvantages of Static Routing:

Following are the disadvantages of Static Routing:

DIWAKAR EDUCATION

- For a large network, it becomes a very difficult task to add each route manually to the routing table.
- The system administrator should have a good knowledge of a topology as he has to add each route manually.

Default Routing

- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.
- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.
- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table.

Dynamic Routing

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

The Dynamic protocol should have the following features:

- All the routers must have the same dynamic routing protocol in order to exchange the routes.
- If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.

DIWAKAR EDUCATION HUB

Advantages of Dynamic Routing:

- It is easier to configure.
- It is more effective in selecting the best route in response to the changes in the condition or topology.

Disadvantages of Dynamic Routing:

- It is more expensive in terms of CPU and bandwidth usage.
- It is less secure as compared to default and static routing.

Routing algorithm

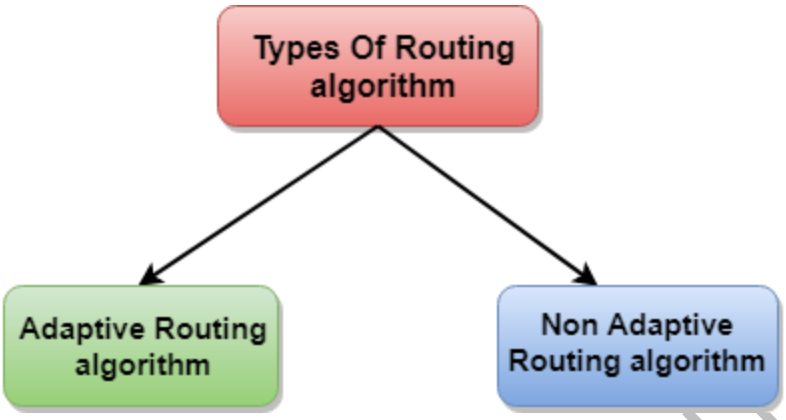
- In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- Whether the network layer provides datagram service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

Classification of a Routing algorithm

The Routing algorithm is divided into two categories:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm

DIWAKAR EDUCATION HUB



Adaptive Routing algorithm

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.
- The main parameters related to this algorithm are hop count, distance and estimated transit time.

An adaptive routing algorithm can be classified into three parts:

- **Centralized algorithm:** It is also known as global routing algorithm as it computes the least-cost path between source and destination by using complete and global knowledge about the network. This algorithm takes the connectivity between the nodes and link cost as input, and this information is obtained before actually performing any calculation. **Link state algorithm** is referred to as a centralized algorithm since it is aware of the cost of each link in the network.
- **Isolation algorithm:** It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.
- **Distributed algorithm:** It is also known as decentralized algorithm as it computes the least-cost path between source and destination in an iterative and distributed manner. In the decentralized algorithm, no node has the knowledge about the cost of all the network links. In the beginning, a node contains the information only about its own directly attached links and through an iterative process of calculation computes the least-cost path to the destination. A Distance vector algorithm is a decentralized

DIWAKAR EDUCATION HU

algorithm as it never knows the complete path from source to the destination, instead it knows the direction through which the packet is to be forwarded along with the least cost path.

Non-Adaptive Routing algorithm

- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

The Non-Adaptive Routing algorithm is of two types:

Flooding: In case of flooding, every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.

Random walks: In case of random walks, a packet sent by the node to one of its neighbors randomly. An advantage of using random walks is that it uses the alternative routes very efficiently.

Differences b/w Adaptive and Non-Adaptive Routing Algorithm

Basis Of Comparison	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.

R EDUCATION HUB

Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.
Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.

TCP

TCP stands for **Transmission Control Protocol**. It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP.

The main functionality of the TCP is to take the data from the application layer. Then it divides the data into a several packets, provides numbering to these packets, and finally transmits these packets to the destination. The TCP, on the other side, will reassemble the packets and transmits them to the application layer. As we know that TCP is a connection-oriented protocol, so the connection will remain established until the communication is not completed between the sender and the receiver.

Features of TCP protocol

The following are the features of a TCP protocol:

- **Transport Layer Protocol**

TCP is a transport layer protocol as it is used in transmitting the data from the sender to the receiver.

DIWAKAR EDUCATION

- **Reliable**

TCP is a reliable protocol as it follows the flow and error control mechanism. It also supports the acknowledgment mechanism, which checks the state and sound arrival of the data. In the acknowledgment mechanism, the receiver sends either positive or negative acknowledgment to the sender so that the sender can get to know whether the data packet has been received or needs to resend.

- **Order of the data is maintained**

This protocol ensures that the data reaches the intended receiver in the same order in which it is sent. It orders and numbers each segment so that the TCP layer on the destination side can reassemble them based on their ordering.

- **Connection-oriented**

It is a connection-oriented service that means the data exchange occurs only after the connection establishment. When the data transfer is completed, then the connection will get terminated.

- **Full duplex**

It is a full-duplex means that the data can transfer in both directions at the same time.

- **Stream-oriented**

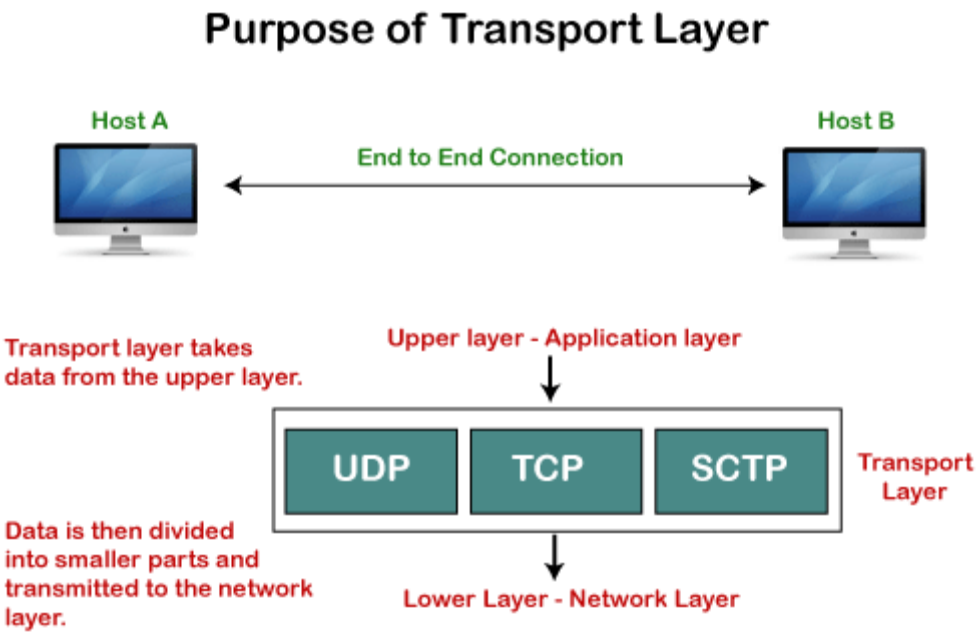
TCP is a stream-oriented protocol as it allows the sender to send the data in the form of a stream of bytes and also allows the receiver to accept the data in the form of a stream of bytes. TCP creates an environment in which both the sender and receiver are connected by an imaginary tube known as a virtual circuit. This virtual circuit carries the stream of bytes across the internet.

Need of Transport Control Protocol

In the layered architecture of a network model, the whole task is divided into smaller tasks. Each task is assigned to a particular layer that processes the task. In the TCP/IP model, five layers are application layer, transport layer, network

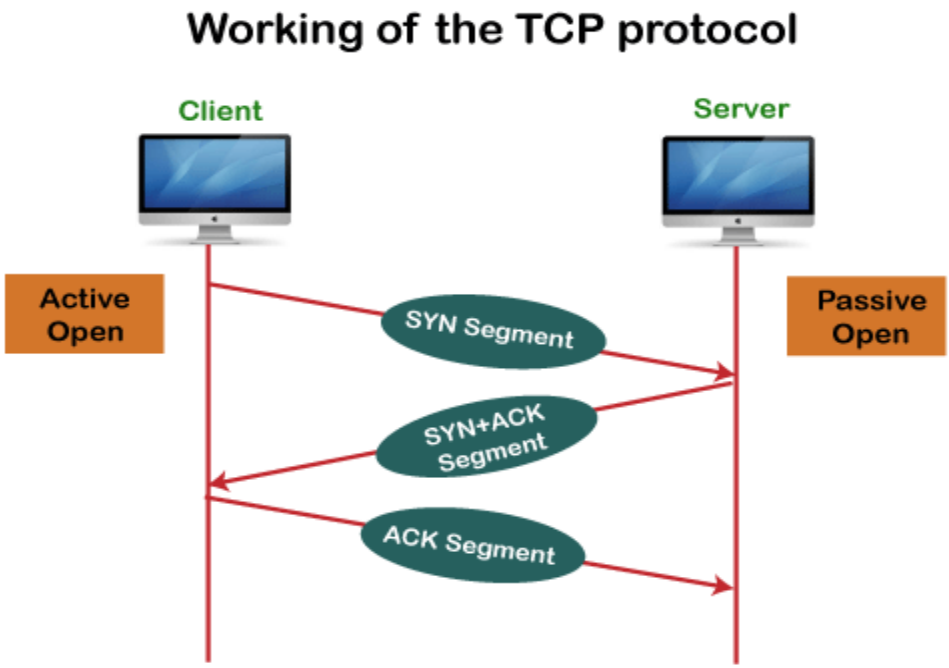
DIWAKAR EDUCATION HUB

layer, data link layer, and physical layer. The transport layer has a critical role in providing end-to-end communication to the directly application processes. It creates 65,000 ports so that the multiple applications can be accessed at the same time. It takes the data from the upper layer, and it divides the data into smaller packets and then transmits them to the network layer.



Working of TCP

In TCP, the connection is established by using three-way handshaking. The client sends the segment with its sequence number. The server, in return, sends its segment with its own sequence number as well as the acknowledgement sequence, which is one more than the client sequence number. When the client receives the acknowledgment of its segment, then it sends the acknowledgment to the server. In this way, the connection is established between the client and the server.



Advantages of TCP

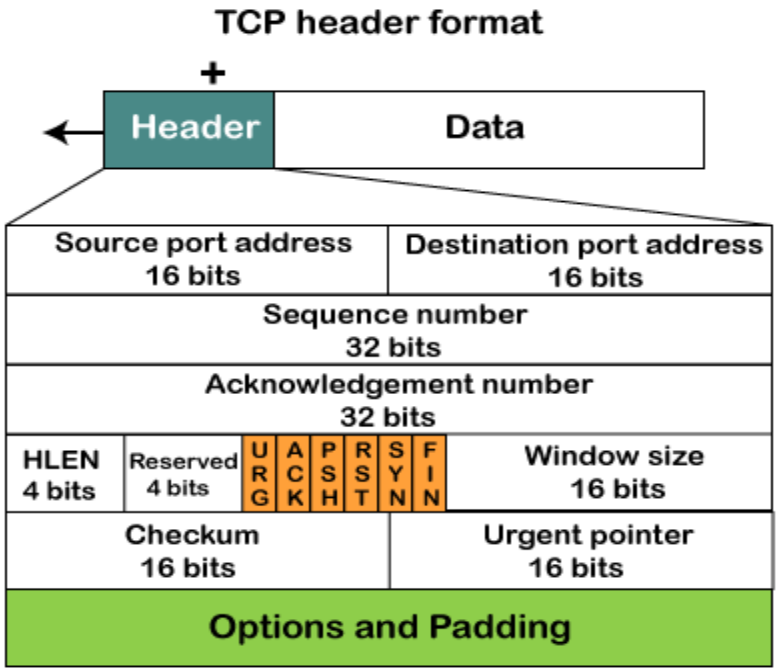
- It provides a connection-oriented reliable service, which means that it guarantees the delivery of data packets. If the data packet is lost across the network, then the TCP will resend the lost packets.
- It provides a flow control mechanism using a sliding window protocol.
- It provides error detection by using checksum and error control by using Go Back or ARP protocol.
- It eliminates the congestion by using a network congestion avoidance algorithm that includes various schemes such as additive increase/multiplicative decrease (AIMD), slow start, and congestion window.

Disadvantage of TCP

It increases a large amount of overhead as each segment gets its own TCP header, so fragmentation by the router increases the overhead.

TCP Header format

DIWAKAR EDUCA



- **Source port:** It defines the port of the application, which is sending the data. So, this field contains the source port address, which is 16 bits.
- **Destination port:** It defines the port of the application on the receiving side. So, this field contains the destination port address, which is 16 bits.
- **Sequence number:** This field contains the sequence number of data bytes in a particular session.
- **Acknowledgment number:** When the ACK flag is set, then this contains the next sequence number of the data byte and works as an acknowledgment for the previous data received. For example, if the receiver receives the segment number 'x', then it responds 'x+1' as an acknowledgment number.
- **HLEN:** It specifies the length of the header indicated by the 4-byte words in the header. The size of the header lies between 20 and 60 bytes. Therefore, the value of this field would lie between 5 and 15.
- **Reserved:** It is a 4-bit field reserved for future use, and by default, all are set to zero.
- **Flags**

  There are six control bits or flags:

  1. **URG:** It represents an urgent pointer. If it is set, then the data is processed urgently.

DIWAKAR EDUCATION

2. **ACK:** If the ACK is set to 0, then it means that the data packet does not contain an acknowledgment.
3. **PSH:** If this field is set, then it requests the receiving device to push the data to the receiving application without buffering it.
4. **RST:** If it is set, then it requests to restart a connection.
5. **SYN:** It is used to establish a connection between the hosts.
6. **FIN:** It is used to release a connection, and no further data exchange will happen.

- **Window size**
  It is a 16-bit field. It contains the size of data that the receiver can accept. This field is used for the flow control between the sender and receiver and also determines the amount of buffer allocated by the receiver for a segment. The value of this field is determined by the receiver.
- **Checksum**
  It is a 16-bit field. This field is optional in UDP, but in the case of TCP/IP, this field is mandatory.
- **Urgent pointer**
  It is a pointer that points to the urgent data byte if the URG flag is set to 1. It defines a value that will be added to the sequence number to get the sequence number of the last urgent byte.
- **Options**
  It provides additional options. The optional field is represented in 32-bits. If this field contains the data less than 32-bit, then padding is required to obtain the remaining bits.

UDP Protocol

In computer networking, the UDP stands for User Datagram Protocol. The David P. Reed developed the UDP protocol in 1980. It is defined in RFC 768, and it is a part of the TCP/IP protocol, so it is a standard protocol over the internet. The UDP protocol allows the computer applications to send the messages in the form of datagrams from one machine to another machine over the Internet Protocol (IP) network. The UDP is an alternative communication protocol to the TCP protocol (transmission control protocol). Like TCP, UDP provides a set of rules that governs how the data should be exchanged over the internet. The UDP works by encapsulating the data into the packet and providing its own header information

DIWAKAR EDUCATION HUB

to the packet. Then, this UDP packet is encapsulated to the IP packet and sent off to its destination. Both the TCP and UDP protocols send the data over the internet protocol network, so it is also known as TCP/IP and UDP/IP. There are many differences between these two protocols. UDP enables the process to process communication, whereas the TCP provides host to host communication. Since UDP sends the messages in the form of datagrams, it is considered the best-effort mode of communication. TCP sends the individual packets, so it is a reliable transport medium. Another difference is that the TCP is a connection-oriented protocol whereas, the UDP is a connectionless protocol as it does not require any virtual circuit to transfer the data.

UDP also provides a different port number to distinguish different user requests and also provides the checksum capability to verify whether the complete data has arrived or not; the IP layer does not provide these two services.

Features of UDP protocol

The following are the features of the UDP protocol:

- **Transport layer protocol**

UDP is the simplest transport layer communication protocol. It contains a minimum amount of communication mechanisms. It is considered an unreliable protocol, and it is based on best-effort delivery services. UDP provides no acknowledgment mechanism, which means that the receiver does not send the acknowledgment for the received packet, and the sender also does not wait for the acknowledgment for the packet that it has sent.

- **Connectionless**

The UDP is a connectionless protocol as it does not create a virtual path to transfer the data. It does not use the virtual path, so packets are sent in different paths between the sender and the receiver, which leads to the loss of packets or received out of order.

Ordered delivery of data is not guaranteed.

DIWAKAR EDUCATION HUB

In the case of UDP, the datagrams are sent in some order will be received in the same order is not guaranteed as the datagrams are not numbered.

- **Ports**

The UDP protocol uses different port numbers so that the data can be sent to the correct destination. The port numbers are defined between 0 and 1023.

- **Faster transmission**

UDP enables faster transmission as it is a connectionless protocol, i.e., no virtual path is required to transfer the data. But there is a chance that the individual packet is lost, which affects the transmission quality. On the other hand, if the packet is lost in TCP connection, that packet will be resent, so it guarantees the delivery of the data packets.

- **Acknowledgment mechanism**

The UDP does have any acknowledgment mechanism, i.e., there is no handshaking between the UDP sender and UDP receiver. If the message is sent in TCP, then the receiver acknowledges that I am ready, then the sender sends the data. In the case of TCP, the handshaking occurs between the sender and the receiver, whereas in UDP, there is no handshaking between the sender and the receiver.

- **Segments are handled independently.**

Each UDP segment is handled individually of others as each segment takes different path to reach the destination. The UDP segments can be lost or delivered out of order to reach the destination as there is no connection setup between the sender and the receiver.

- **Stateless**

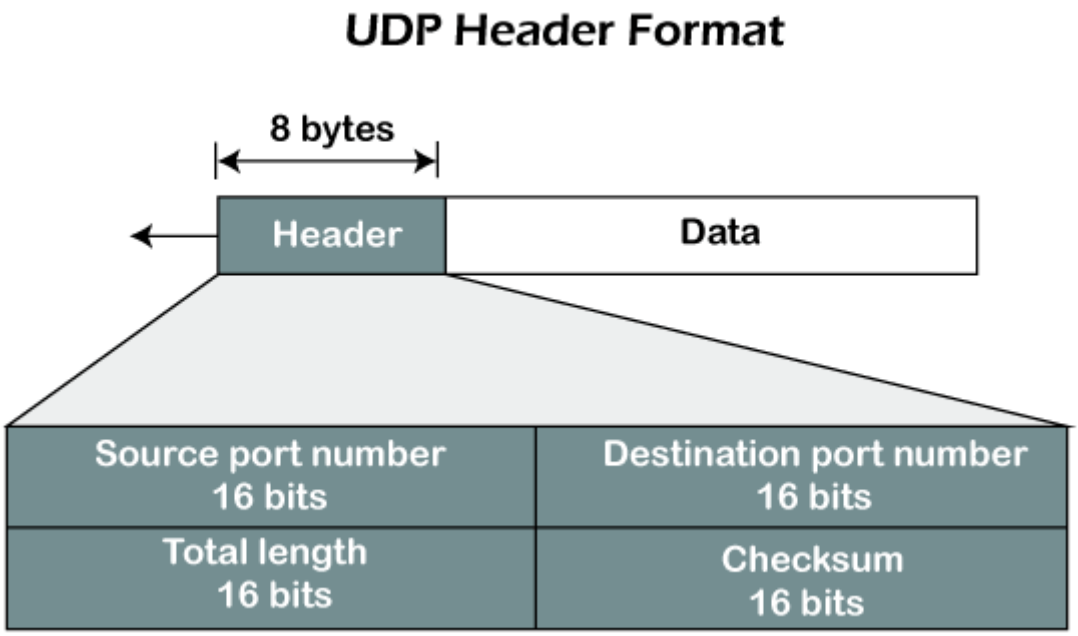
It is a stateless protocol that means that the sender does not get the acknowledgement for the packet which has been sent.

Why do we require the UDP protocol?

DIWAKAR EDUCATION HUB

As we know that the UDP is an unreliable protocol, but we still require a UDP protocol in some cases. The UDP is deployed where the packets require a large amount of bandwidth along with the actual data. For example, in video streaming, acknowledging thousands of packets is troublesome and wastes a lot of bandwidth. In the case of video streaming, the loss of some packets couldn't create a problem, and it can also be ignored.

UDP Header Format



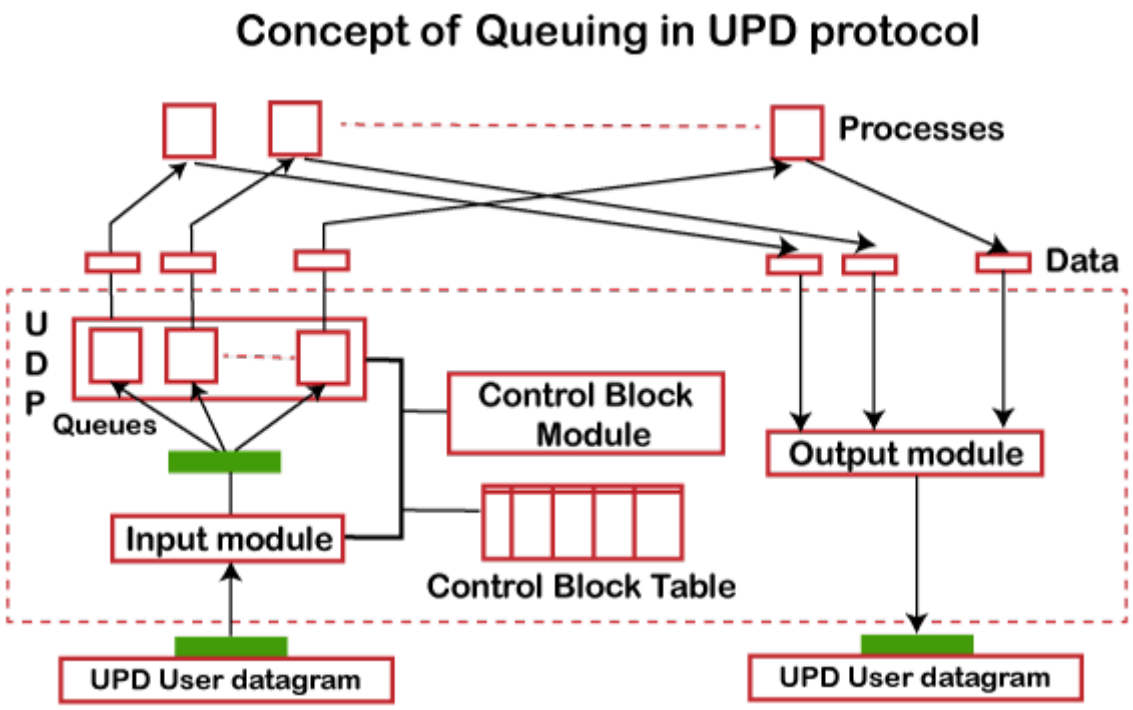
In UDP, the header size is 8 bytes, and the packet size is upto 65,535 bytes. But this packet size is not possible as the data needs to be encapsulated in the IP datagram, and an IP packet, the header size can be 20 bytes; therefore, the maximum of UDP would be 65,535 minus 20. The size of the data that the UDP packet can carry would be 65,535 minus 28 as 8 bytes for the header of the UDP packet and 20 bytes for IP header.

The UDP header contains four fields:

- **Source port number:** It is 16-bit information that identifies which port is going t send the packet.

- **Destination port number:** It identifies which port is going to accept the information. It is 16-bit information which is used to identify application-level service on the destination machine.
- **Length:** It is 16-bit field that specifies the entire length of the UDP packet that includes the header also. The minimum value would be 8-byte as the size of the header is 8 bytes.
- **Checksum:** It is a 16-bits field, and it is an optional field. This checksum field checks whether the information is accurate or not as there is the possibility that the information can be corrupted while transmission. It is an optional field, which means that it depends upon the application, whether it wants to write the checksum or not. If it does not want to write the checksum, then all the 16 bits are zero; otherwise, it writes the checksum. In UDP, the checksum field is applied to the entire packet, i.e., header as well as data part whereas, in IP, the checksum field is applied to only the header field.

Concept of Queuing in UDP protocol



In UDP protocol, numbers are used to distinguish the different processes on a server and client. We know that UDP provides a process to process communication. The client generates the processes that need services while the

server generates the processes that provide services. The queues are available for both the processes, i.e., two queues for each process. The first queue is the incoming queue that receives the messages, and the second one is the outgoing queue that sends the messages. The queue functions when the process is running. If the process is terminated then the queue will also get destroyed.

UDP handles the sending and receiving of the UDP packets with the help of the following components:

- **Input queue:** The UDP packets uses a set of queues for each process.
- **Input module:** This module takes the user datagram from the IP, and then it finds the information from the control block table of the same port. If it finds the entry in the control block table with the same port as the user datagram, it enqueues the data.
- **Control Block Module:** It manages the control block table.
- **Control Block Table:** The control block table contains the entry of open ports.
- **Output module:** The output module creates and sends the user datagram.

Several processes want to use the services of UDP. The UDP multiplexes and demultiplexes the processes so that the multiple processes can run on a single host.

Limitations

- It provides an unreliable connection delivery service. It does not provide any services of IP except that it provides process-to-process communication.
- The UDP message can be lost, delayed, duplicated, or can be out of order.
- It does not provide a reliable transport delivery service. It does not provide any acknowledgment or flow control mechanism. However, it does provide error control to some extent.

Advantages

- It produces a minimal number of overheads.

DIWAKAR EDUCATION HUB

Stream Control Transmission Protocol (SCTP)

- Stream Control Transmission Protocol (SCTP) is a reliable, message-oriented transport layer protocol.
- SCTP has mixed features of TCP and UDP.
- SCTP maintains the message boundaries and detects the lost data, duplicate data as well as out-of-order data.
- SCTP provides the Congestion control as well as Flow control.
- SCTP is especially designed for internet applications.

SCTP Services

Some important services provided by SCTP are as stated below:

1. Process-to- Process communication
SCTP uses all important ports of TCP.

2. Multi- Stream Facility
SCTP provides multi-stream service to each connection, called as association. If one stream gets blocked, then the other stream can deliver the data.

3.Full- Duplex Communication
SCTP provides full-duplex service (the data can flow in both directions at the same time).

4. Connection- Oriented Service
The **SCTP** is a connection oriented protocol, just like TCP with the only difference that, it is called **association in SCTP**. If User1 wants to send and receive message from user2, the steps are :

Step1: The two **SCTPs** establish the connection with each other.
Step2: Once the connection is established, the data gets exchanged in both the directions.
Step3: Finally, the association is terminated.

5. Reliability
SCTP uses an acknowledgement mechanism to check the arrival of data.

Features of SCTP

Some important features of SCTP are as stated below:

1. Transmission Sequence Number (TSN)
The unit of data in SCTP is a **data chunk**. Data transfer in SCTP is controlled by numbering the data chunks. In SCTP, TSN is used to assign the numbers to different data chunks.

2. Stream Identifier (SI)
The **SI** is a **16 bit number** and starts with 0. In SI, there are several streams in each association and it is needed to identify them. Each data chunk needs to carry the SI in the header, so that it is properly placed in its stream on arrival.

3. Packets
In SCTP, the data is carried out in the form of **data chunks** and control information is carried as **control chunks**. Data chunks and control chunks are packed together in the packet.

4. Multihoming
Multihoming allows both ends (sender and receiver) to define **multiple IP addresses** for communication. But, only one of these can be defined as primary address and the remaining can be used as alternative addresses.

Error Control in TCP

TCP protocol has methods for finding out corrupted segments, missing segments, out-of-order segments and duplicated segments.
Error control in TCP is mainly done through use of **three simple techniques** :

1. **Checksum –** Every segment contains a checksum field which is used to find corrupted segment. If the segment is corrupted, then that segment is discarded by the destination TCP and is considered as lost.
2. **Acknowledgement –** TCP has another mechanism called acknowledgement to affirm that the data segments have been delivered. Control segments that contain no data but has sequence number will be acknowledged as well but ACK segments are not acknowledged.

3. **Retransmission –** When a segment is missing, delayed to deliver to receiver, corrupted when it is checked by receiver then that segment is retransmitted again. Segments are retransmitted only during two events: when the sender receives three duplicate acknowledgements (ACK) or when a retransmission timer expires.
    1. **Retransmission after RTO :** TCP always preserve one retransmission time-out (RTO) timer for all sent but not acknowledged segments. When the timer runs out of time, the earliest segment is retransmitted. Here no timer is set for acknowledgement. In TCP, RTO value is dynamic in nature and it is updated using round trip time (RTT) of segments. RTT is the time duration needed for a segment to reach receiver and an acknowledgement to be received to the sender.
    2. **Retransmission after Three duplicate ACK segments :** RTO method works well when the value of RTO is small. If it is large, more time is needed to get confirmation about whether a segment has delivered or not. Sometimes one segment is lost and the receiver receives so many out-of-order segments that they cannot be saved. In order to solve this situation, three duplicate acknowledgement method is used and missing segment is retransmitted immediately instead of retransmitting already delivered segment. This is a fast retransmission because it makes it possible to quickly retransmit lost segments instead of waiting for timer to end.

TCP Congestion Control

TCP uses a congestion window and a congestion policy that avoid congestion.Previously, we assumed that only receiver can dictate the sender's window size. We ignored another entity here, the network. If the network cannot deliver the data as fast as it is created by the sender, it must tell the sender to slow down. In other words, in addition to the receiver, the network is a second entity that determines the size of the sender's window.

Congestion policy in TCP –

1. Slow Start Phase: starts slowly increment is exponential to threshold
2. Congestion Avoidance Phase: After reaching the threshold increment is by 1

DIWAKAR EDUCATION HUB

3. Congestion Detection Phase: Sender goes back to Slow start phase or Congestion avoidance phase.

Slow Start Phase : exponential increment – In this phase after every RTT the congestion window size increments exponentially.

Initially cwnd = 1

After 1 RTT, cwnd = 2^(1) = 2

2 RTT, cwnd = 2^(2) = 4

3 RTT, cwnd = 2^(3) = 8

Congestion Avoidance Phase : additive increment – This phase starts after the threshold value also denoted as ssthresh. The size of cwnd(congestion window) increases additive. After each RTT cwnd = cwnd + 1.

Initially cwnd = i

After 1 RTT, cwnd = i+1

2 RTT, cwnd = i+2

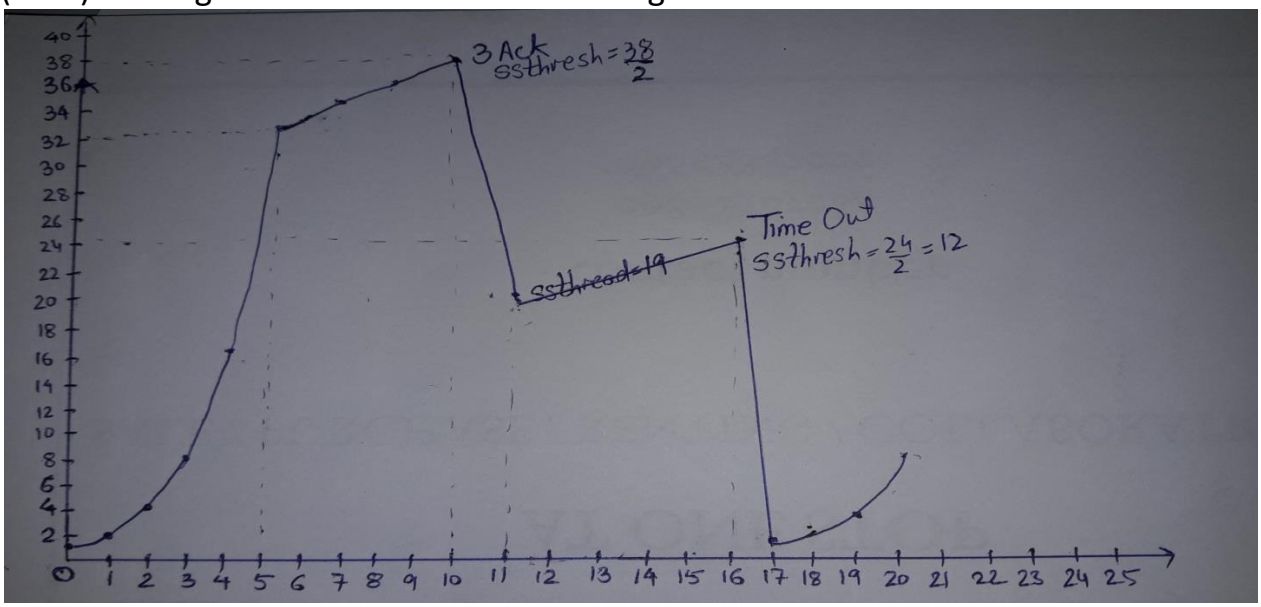
3 RTT, cwnd = i+3

Congestion Detection Phase : multiplicative decrement – If congestion occurs, the congestion window size is decreased. The only way a sender can guess that congestion has occurred is the need to retransmit a segment. Retransmission is needed to recover a missing packet which is assumed to have been dropped by a router due to congestion. Retransmission can occur in one of two cases: when the RTO timer times out or when three duplicate ACKs are received.

- **Case 1 : Retransmission due to Timeout –** In this case congestion possibility is high.
  (a) ssthresh is reduced to half of the current window size.
  (b) set cwnd = 1
  (c) start with slow start phase again.

- **Case 2 : Retransmission due to 3 Acknowledgement Duplicates –** In this case congestion possibility is less.
  (a) ssthresh value reduces to half of the current window size.
  (b) set cwnd= ssthresh
  (c) start with congestion avoidance phase

Example – Assume a TCP protocol experiencing the behavior of slow start. At 5th transmission round with a threshold (ssthresh) value of 32 goes into congestion avoidance phase and continues till 10th transmission. At 10th transmission round, 3 duplicate ACKs are received by the receiver and enter into additive increase mode. Timeout occurs at 16th transmission round. Plot the transmission round (time) vs congestion window size of TCP segments.



TCP Flow Control

TCP is the protocol that guarantees we can have a reliable communication channel over an unreliable network. When we send data from a node to another, packets can be lost, they can arrive out of order, the network can be congested or the receiver node can be overloaded. When we are writing an application, though, we usually don't need to deal with this complexity, we just write some data to a socket and TCP makes sure the packets are delivered correctly to the receiver node. Another important service that TCP provides is what is called Flow Control. Let's talk about what that means and how TCP does its magic.

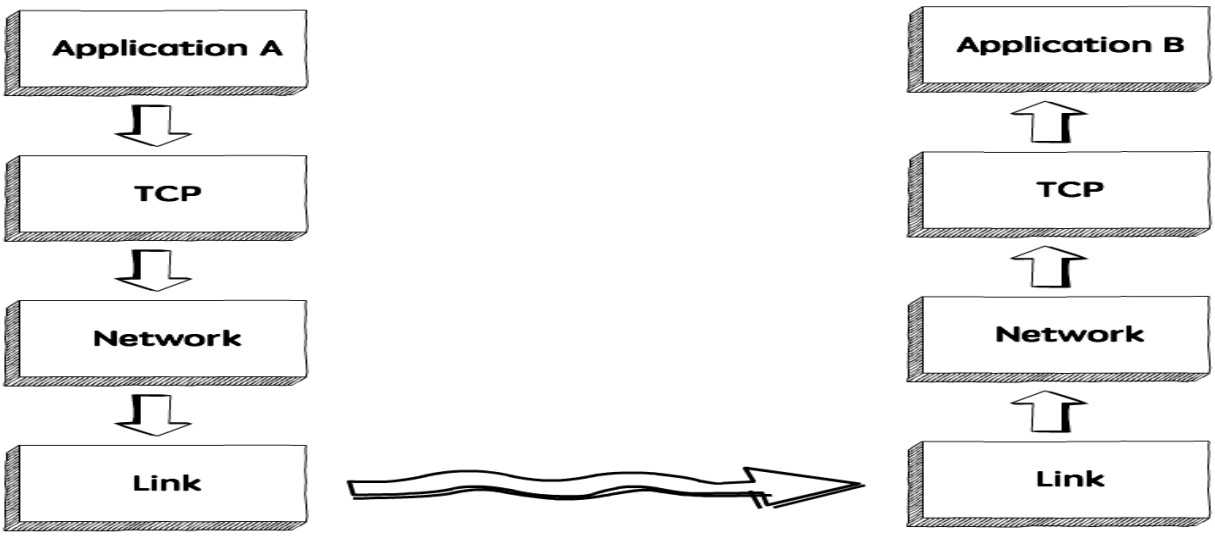
What is Flow Control (and what it's not)

Flow Control basically means that TCP will ensure that a sender is not overwhelming a receiver by sending packets faster than it can consume. It's pretty similar to what's normally called Back pressure in the Distributed Systems literature. The idea is that a node receiving data will send some kind of feedback to the node sending the data to let it know about its current condition.

It's important to understand that this is **not** the same as Congestion Control. Although there's some overlap between the mechanisms TCP uses to provide both services, they are distinct features. Congestion control is about preventing a node from overwhelming the network (i.e. the links between two nodes), while Flow Control is about the end-node.

How it works

When we need to send data over a network, this is normally what happens.



The sender application writes data to a socket, the transport layer (in our case, TCP) will wrap this data in a segment and hand it to the network layer (e.g. IP), that will somehow route this packet to the receiving node.

On the other side of this communication, the network layer will deliver this piece of data to TCP, that will make it available to the receiver application as an exact

copy of the data sent, meaning if will not deliver packets out of order, and will wait for a retransmission in case it notices a gap in the byte stream.

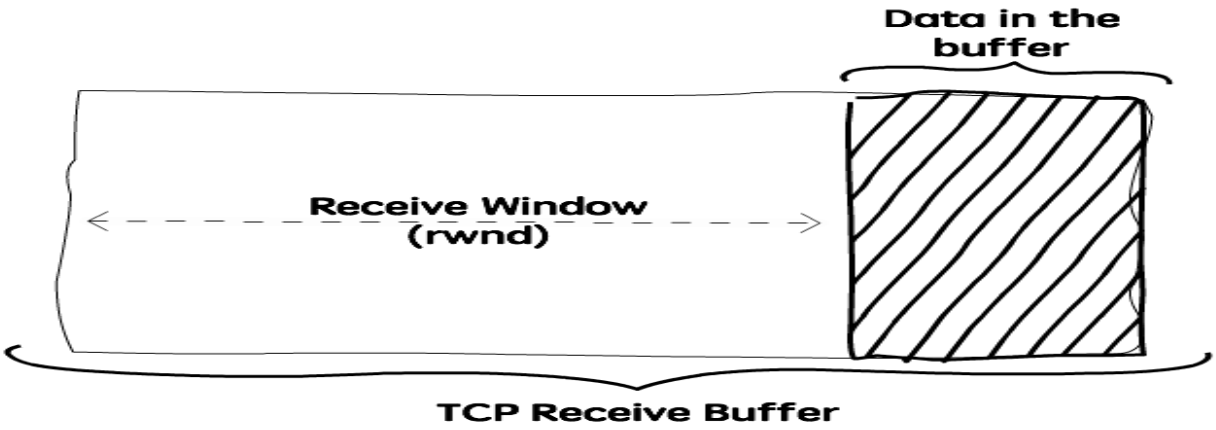
If we zoom in, we will see something like this.



TCP stores the data it needs to send in the send buffer, and the data it receives in the receive buffer. When the application is ready, it will then read data from the receive buffer.

Flow Control is all about making sure we don't send more packets when the receive buffer is already full, as the receiver wouldn't be able to handle them and would need to drop these packets.

To control the amount of data that TCP can send, the receiver will advertise its Receive Window (rwnd), that is, the spare room in the receive buffer.



Every time TCP receives a packet, it needs to send an ack message to the sender, acknowledging it received that packet correctly, and with this ack message it sends the value of the current receive window, so the sender knows if it can keep sending data.

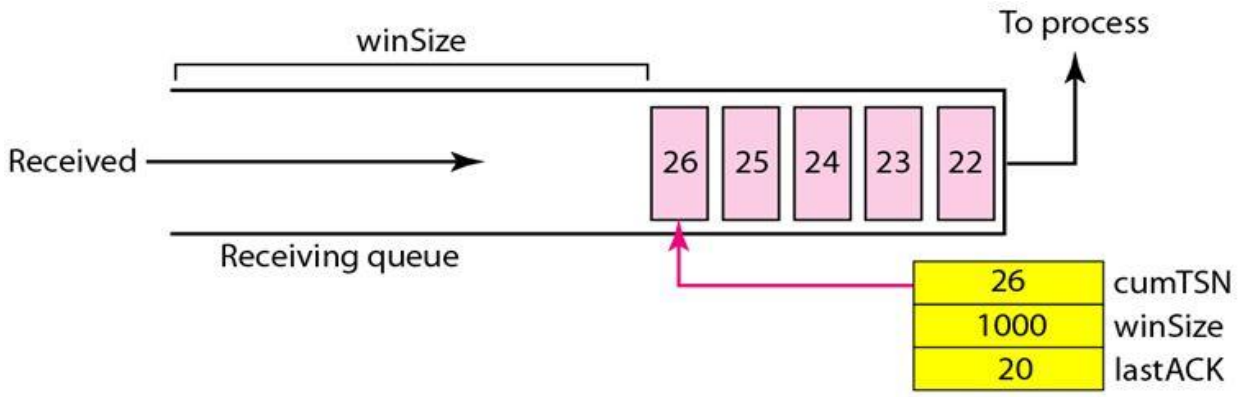
Flow control in SCTP

Flow control in SCTP is similar to that in TCP. In SCTP, we need to handle two units of data, the byte and the chunk. The values of rwnd and cwnd are expressed in bytes; the values of TSN and acknowledgments are expressed in chunks. Current SCTP implementations still use a byte-oriented window for flow control.

Receiver Site:

The receiver has one buffer (queue) and three variables. The queue holds the received data chunks that have not yet been read by the process. The first variable holds the last TSN received, cumTSN. The second variable holds the available buffer size; winsize. The third variable holds the last accumulative acknowledgment, lastACK. The following figure shows the queue and variables at the receiver site.

DIWAKAR EDUCA



1. When the site receives a data chunk, it stores it at the end of the buffer (queue) and subtracts the size of the chunk from winSize. The TSN number of the chunk is stored in the cumTSN variable.

2. When the process reads a chunk, it removes it from the queue and adds the size of the removed chunk to winSize (recycling).

3. When the receiver decides to send a SACK, it checks the value of lastAck; if it is less than cumTSN, it sends a SACK with a cumulative TSN number equal to the cumTSN. It also includes the value of winSize as the advertised window size.

Sender Site:

The sender has one buffer (queue) and three variables: curTSN, rwnd, and inTransit, as shown in the following figure. We assume each chunk is 100 bytes long.

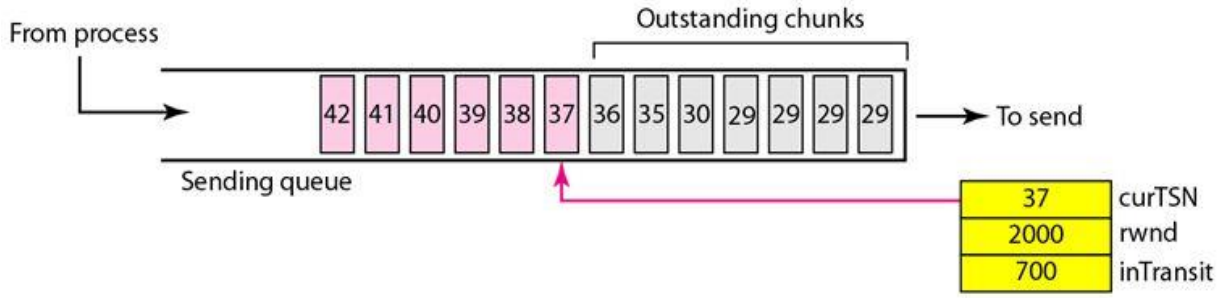
The buffer holds the chunks produced by the process that either have been sent or are ready to be sent. The first variable, curTSN, refers to the next chunk to be sent. All chunks in the queue with a TSN less than this value have been sent, but not acknowledged; they are outstanding. The second variable, rwnd, holds the last value advertised by the receiver (in bytes). The third variable, inTransit, holds the number of bytes in transit, bytes sent but not yet acknowledged. The following is the procedure used by the sender.

1. A chunk pointed to by curTSN can be sent if the size of the data is less than or equal to the quantity rwnd - inTransit. After sending the chunk, the value of

DIWAKAR EDUCATION HUB

curTSN is incremented by 1 and now points to the next chunk to be sent. The value of inTransit is incremented by the size of the data in the transmitted chunk.

2. When a SACK is received, the chunks with a TSN less than or equal to the cumulative TSN in the SACK are removed from the queue and discarded. The sender does not have to worry about them anymore. The value of inTransit is reduced by the total size of the discarded chunks. The value of rwnd is updated with the value of the advertised window in the SACK.

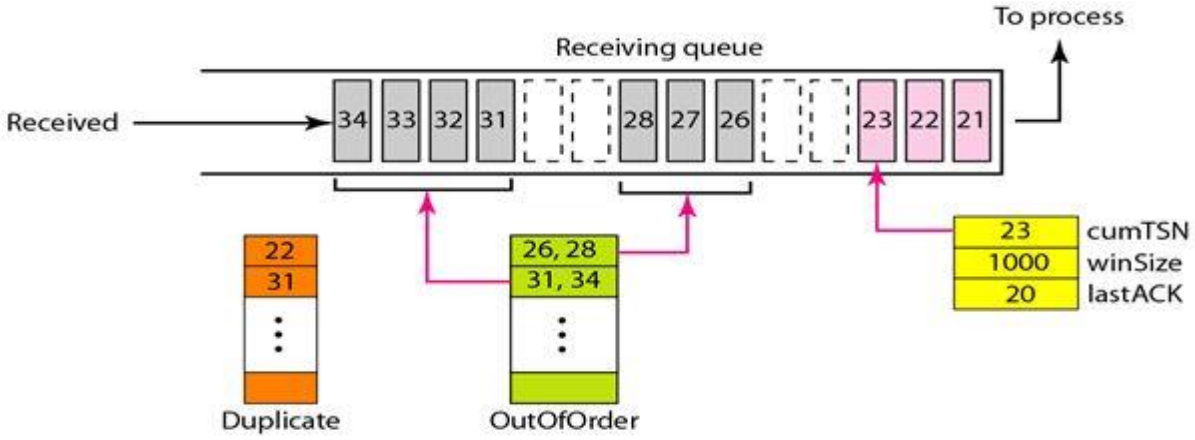


Error Control in SCTP

SCTP, like TCP, is a reliable transport layer protocol. It uses a SACK chunk to report the state of the receiver buffer to the sender. Each implementation uses a different set of entities and timers for the receiver and sender sites.

Receiver Site:

The receiver stores all chunks that have arrived in its queue including the out-of-order ones. However, it leaves spaces for any missing chunks. It discards duplicate messages, but keeps track of them for reports to the sender. The following figure shows a typical design for the receiver site and the state of the receiving queue at a particular point in time.

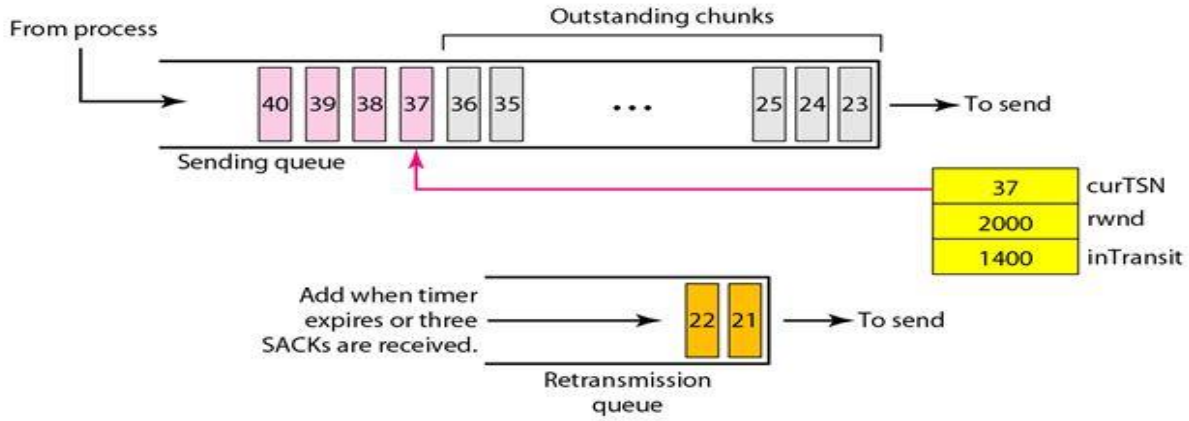


The last acknowledgment sent was for data chunk 20. The available window size is 1000 bytes. Chunks 21 to 23 have been received in order. The first out-of-order block contains chunks 26 to 28. The second out-of-order block contains chunks 31 to 34. A variable holds the value of cumTSN. An array of variables keeps track of the beginning and the end of each block that is out of order. An array of variables holds the duplicate chunks received. Note that there is no need for storing duplicate chunks in the queue and they will be discarded.
The figure also shows the SACK chunk that will be sent to report the state of the receiver to the sender. The TSN numbers for out-of-order chunks are relative (offsets) to the cumulative TSN.

Sender Site

At the sender site, it needs two buffers (queues): a sending queue and a retransmission queue. We also use the three variables rwnd, inTransit, and curTSN as described in the previous section. The following figure shows a typical design.

DIWAKAR EDUCATION



The sending queue holds chunks 23 to 40. The chunks 23 to 36 have already been sent, but not acknowledged; they are outstanding chunks. The curTSN points to the next chunk to be sent (37). We assume that each chunk is 100 bytes, which means that 1400 bytes of data (chunks 23 to 36) is in transit.

The sender at this moment has a retransmission queue. When a packet is sent, a retransmission timer starts for that packet (all data chunks in that packet). Some implementations use one single timer for the entire association, but we continue with our tradition of one timer for each packet for simplification.

When the retransmission timer for a packet expires, or four duplicate SACKs arrive that declare a packet as missing the chunks in that packet are moved to the retransmission queue to be resent. These chunks are considered lost, rather than outstanding. The chunks in the retransmission queue have priority.

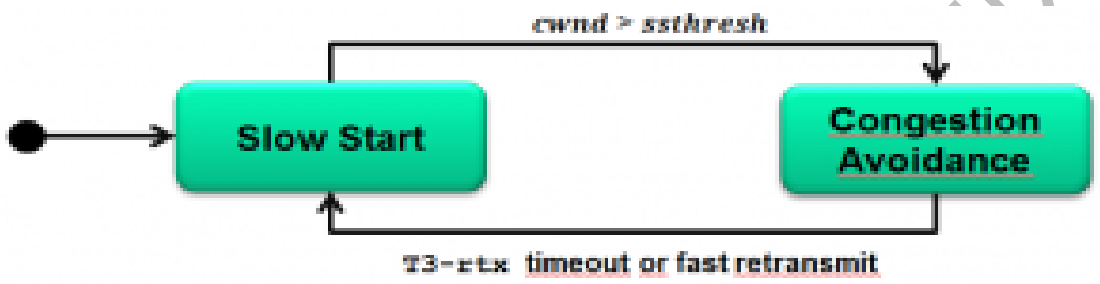
SCTP Congestion Control

Congestion control tries avoiding overload situations in network components like routers.
Congestion in network components can lead to packet loss which is handled by the error control function of SCTP (see below). The goal of congestion control is to avoid packet loss in the first place.

SCTP congestion control key facts

•SCTP congestion control is based on RFC2581 with some minor modifications.
•Congestion control is applied to the entire association, not individual streams.

•SCTP maintains a separate cwnd parameter for each peer destination address in multihomed scenarios.
•As defined in RFC2581, the transmission rate starts slowly at the beginning (slow start phase), based on feedback provided by received SACK chunks. After the slow start phase, SCTP enters the congestion avoidance phase. In case of congestion in the network, SCTP immediately reverts back to the slow start phase.

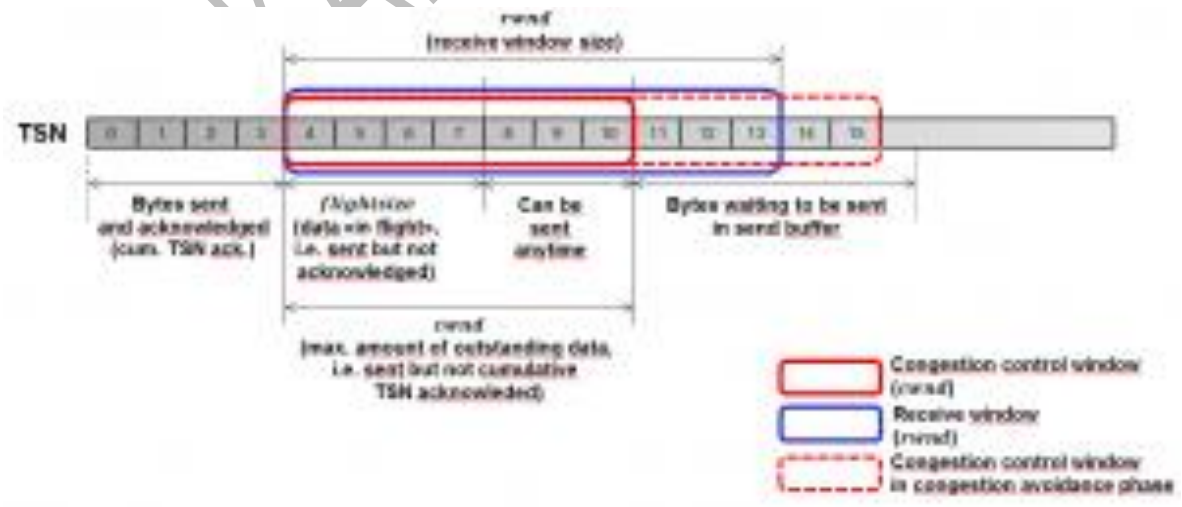


SCTP Slow Start and Congestion Avoidance Phases

SCTP congestion control window cwnd

cwnd and rwnd (or a_rwnd = advertised receiver window size) define 2 windows where the smaller of the 2 determines the maximum amount of data that can be sent.

After the slow start phase, cwnd is large so that rwnd becomes the dominant window size.



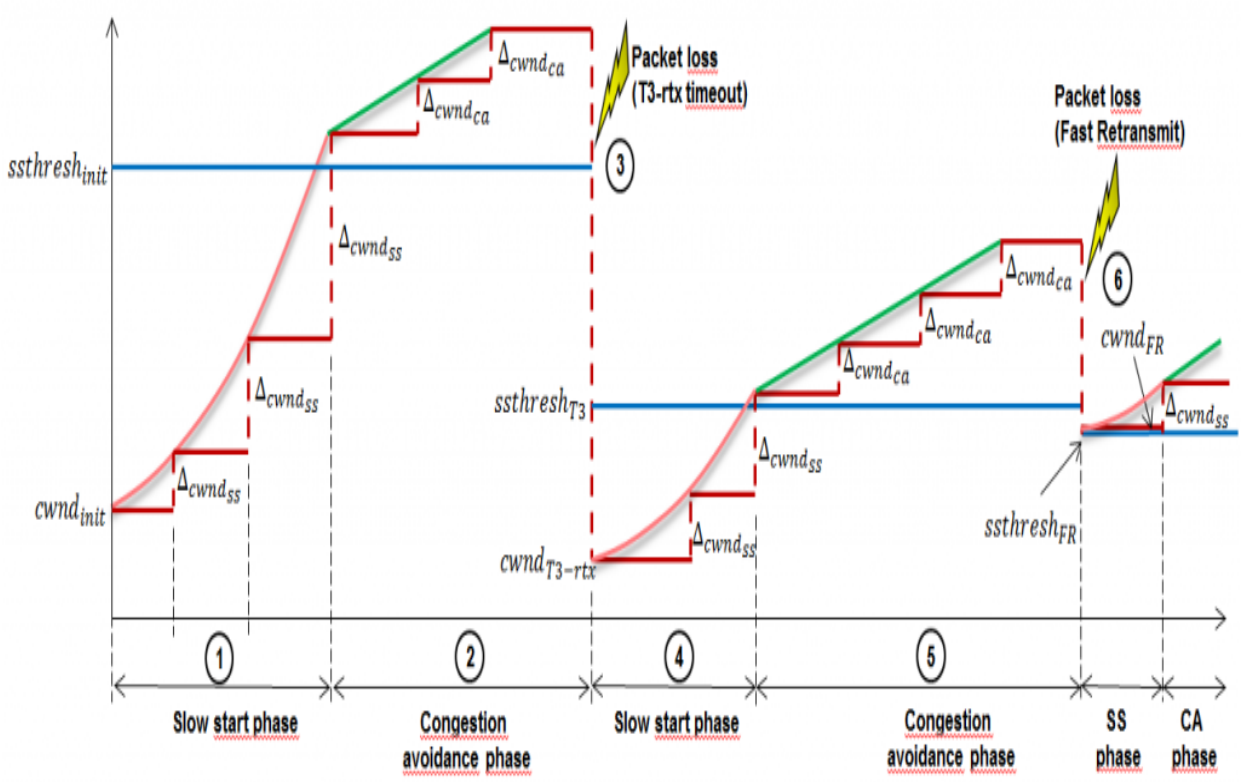
Congestion Control Window

Slow start and congestion avoidance phases

The general mechanism applied in SCTP congestion control (as per RFC2581) is to slowly increase the congestion window size cwnd, but to rapidly collapse the window when there are signs of congestion.

Packet loss is deemed a sign of congestion. Note, however, that this is not always true (e.g. on wireless links there may be packet loss due to radio signal interferences).

Congestion control is applied to the entire association, not individual streams. Nevertheless, cwnd is maintained per destination transport address (multihomed scenarios).



Slow Start and Congestion Avoidance Phases

WWW

The full form of WWW is the **World Wide Web.** WWW is also called a Web and it is a catalogue of an order of all websites connected to the worldwide Internet. It is an information system in which linked hypertext data and resources are accessed over the Internet. Using a web browser, a user can access a web page and a user can navigate between the web pages using hyperlinks where images, texts, and other multimedia data and content can be carried on a website page.

Protocols used by the World Wide Web

WWW uses three protocols, namely

1. Hypertext Transfer Protocol (HTTP)
2. Hypertext markup language (HTML)
3. Uniform resource locator (URLs)

History of WWW

- Tim Berners-Lee and his colleagues at CERN, an international scientific organization based in Geneva, Switzerland, began developing the World Wide Web in 1989. They created the HTTP protocol which standardized server-client communication. In January 1992, their text-based Web browser was made available for publication.
- The World Wide Web quickly gained recognition with the development of a web browser called Mosaic, set up by Marc Andreessen and others at the National Center for Supercomputing Applications at the University of Illinois in the United States, and launched in September 1993.
- In April 1994 Andreessen co-founded Netscape Communications Corporation, soon after its launch, Netscape Navigator became the powerful Web browser.
- In 1995 the giant software company Microsoft Corporation established its own Internet Explorer (IE) browser. In 1996 IE was incorporated into the Windows operating system and IE shortly became a popular Web browser.
- The first real competitor to IE was Mozilla's Firefox, launched in 2004.
- In 2008 google launched chrome. By 2013, compared to IE and Firefox, Chrome had become a powerful browser. In 2015, Microsoft discontinued IE replacing it with Edge.

DIWAKAR EDUCATION HUB

Advantages

- Can assist you with studies
- You can do grocery and other shopping online.
- You can contact relatives and friends.

Disadvantages

- Many pages could be misleading, and may steal our data, cash
- Abuse, harassment, racism etc are common nowadays.

URL (Uniform Resource Locator)

A URL (Uniform Resource Locator) is a unique identifier used to locate a resource on the internet. It is also referred to as a web address. URLs consist of multiple parts -- including a protocol and domain name -- that tell a web browser how and where to retrieve a resource.

End users use URLs by typing them directly into the address bar of a browser or by clicking a hyperlink found on a webpage, bookmark list, in an email or from another application.

How is a URL structured?

The URL contains the name of the protocol needed to access a resource, as well as a resource name. The first part of a URL identifies what protocol to use as the primary access medium. The second part identifies the IP address or domain name -- and possibly subdomain -- where the resource is located.

URL protocols include HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP Secure) for web resources, mail to for email addresses, FTP for files on a File Transfer Protocol (FTP) server, and telnet for a session to access remote computers. Most URL protocols are followed by a colon and two forward slashes; “mail to” is followed only by a colon.

Optionally, after the domain, a URL can also specify:

- a path to a specific page or file within a domain;

DIWAKAR EDUCATION HUB

- a network port to use to make the connection;
- a specific reference point within a file, such as a named anchor in an HTML file; and
- a query or search parameters used -- commonly found in URLs for search results.

A URL (Uniform Resource Locator) contains the information, which is as follows:

- The port number on the server, which is optional.
- It contains a protocol that is used to access the resource.
- The location of the server
- A fragment identifier
- In the directory structure of the server, it contains the location of the resource.

The additional information about the URL is described below with the help of an example:

http:// or https://

The http is a protocol that stands for Hypertext Transfer Protocol. It tells the browser to which protocol will be preferred to use for accessing the information that is specified in the domain.

The https (Hypertext Transfer Protocol Secure) is an enhanced protocol as compared to http as it concerned with security. It provides the surety that the information, which is transmitted over HTTP is secure and encrypted. The colon (:) and two forward slashes (//) are used to separate the protocol from the rest of the part of the URL.

www.

- The www is used to distinguish the content, which stands for World Wide Web. This portion of the URL can be left out many times, as it is not required..

deh.htm

The jtp.htm is the name of the web page, and the .htm is the file extension of the web page, which describes the file is an HTML file. There are many other file extensions available on the internet such as .php, .html, .xml, .jpg, .gif, .asp, .cgi, etc.

Where is the URL located?

A URL is located in the address bar or search bar at the top of the browser window. The URL is always visible in the desktop computers and laptop unless our browser is being displayed in full screen. In most of the smartphones and tablets, when you scroll down the page, the URL will disappear and only show the domain when visible. To visible the address bar, you need to scroll up the page. And, if only the domain is shown and you want to see full address, tapping on the address bar to show the full address.

What characters cannot be used in the URL?

It is realized by many people that space is not allowed in a URL. The URL string can contain only symbols **! $-_+*'()**, including **alphanumeric characters** as it is documented in RFC 1738. Any other characters must be encoded in the URL if needed.

Is an IP address the same as a web address or a URL?

- An IP address is not the same as a web address or a URL, as it is a unique number that is assigned to each device on a network. A domain name is assigned a unique IP address on the World Wide Web, and when entered an URL like https://www.diwakarhub.com, it is translated by DNS into an IP

address that used by routers to find web servers. Instead of using an IP address, a domain name is used as it is easy to remember by humans.

Understanding more complex URLs and parameters

A URL performs additional functions and added the parameters (additional information) to the end of the URL when it points to a script. For example, when you search any query on any search engine, it points to a search results page, including the additional information with the search query words.

Why URL?

- The URL is beneficial, as the written information in the URL provides users the option to switch from one web page to another by clicking only one mouse click.
- Every URL is unique and tells users how to access a specific resource.
- When a user types a URL into the web browser and opens any hyperlink from search results, the browser forwards a request to a webserver to fetch files related to thesearch query.
- A website domain or URL identifies one particular file, and it is the most important part of your website. Usually, by using words that end with .net, .com, or .org, you can get traffic on your website.

DNS

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

The full form of DNS is the **Domain Name System** . DNS is linked to the internet and focused on a system using Internet Protocol (IP). DNS servers are required for the working of DNS. The IP address is calculated with the aid of a lookup table.

Each computer system or website has its own unique IP address. It's a lengthy digital code. DNS is an IP service that translates the name of a domain into an individual IP address. DNS is alphabetic, and thus convenient and straightforward.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

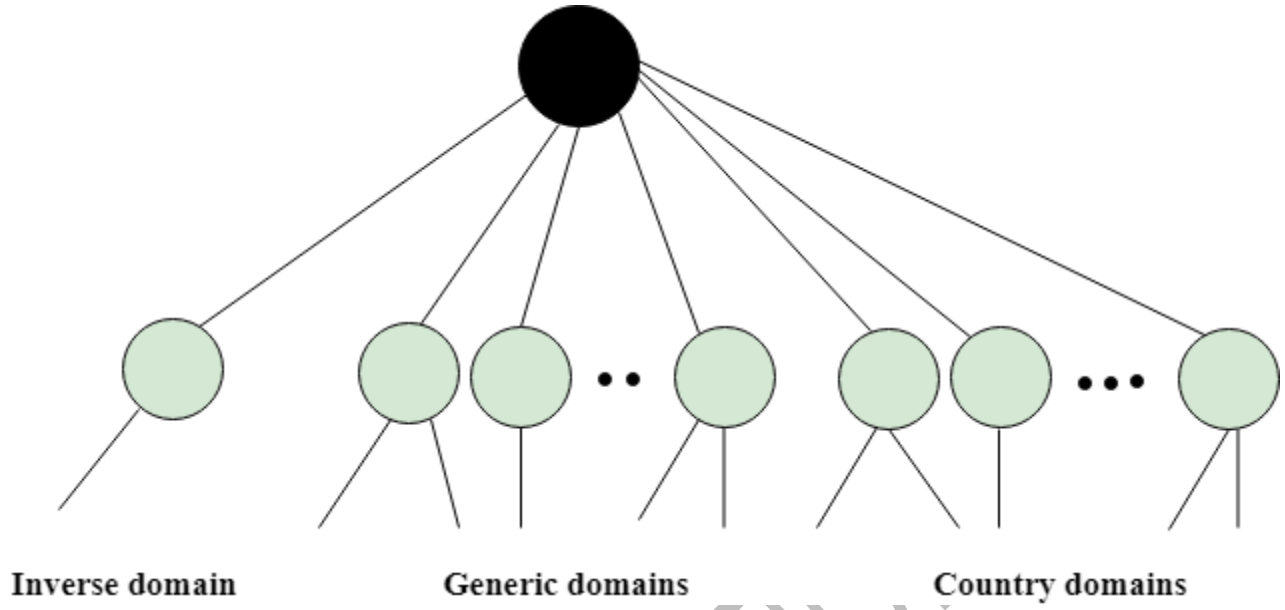
DNS

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.

DWARKA EDUCATION HUB

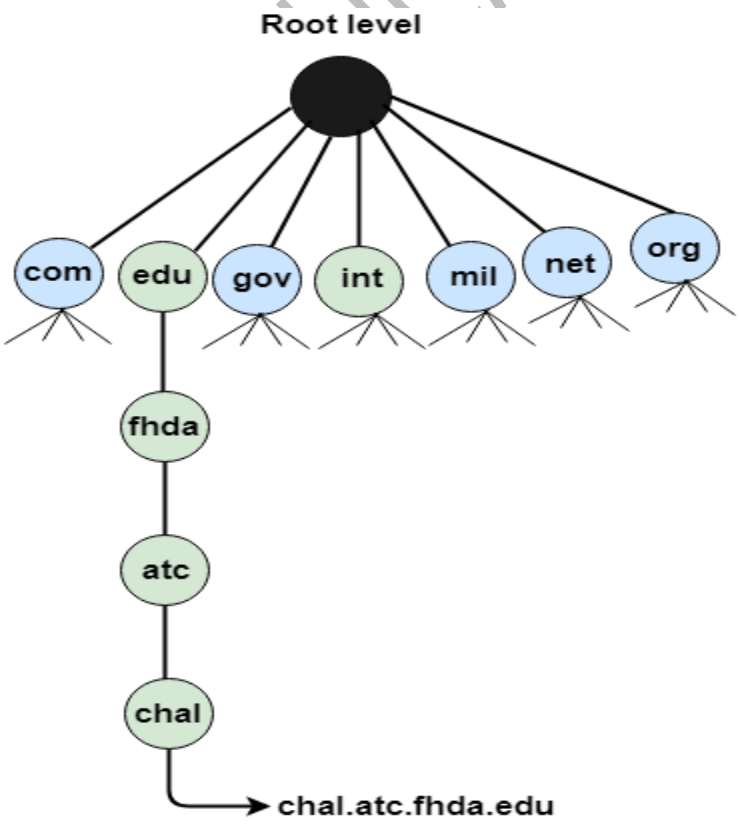


Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions

info	Information service providers
int	International Organizations
mil	Military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations



Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

There are 4 DNS servers involved in loading a webpage:

- DNS recursor - The recursor can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursor is then responsible for making additional requests in order to satisfy the client's DNS query.

DIWAKAR EDUCATION HUB

- **Root nameserver** - The root server is the first step in translating (resolving) human readable host names into IP addresses. It can be thought of like an index in a library that points to different racks of books - typically it serves as a reference to other more specific locations.
- TLD nameserver - The top level domain server (TLD) can be thought of as a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is “com”).
- Authoritative nameserver - This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition. The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (the librarian) that made the initial request.

Working principles of DNS

DNS is essential because, while domain names are easy to remember for people, computers or devices, sites are accessed based on IP addresses. Working in DNS is processed, with the help of DNS servers. Into a web browser, when a domain name entered by the user, the supplication goes to the DNS server. The DNS server decides the IP address by using a lookup table. Then, it transmits the supplied information to the user’s web browser through genuine servers.

Information from all website domain servers on the internet is collected and kept at the Central Registry. Host companies and service providers regularly interact with the Central Registry to obtain updated DNS data. Your Internet Service Provider will view the DNS associated with the domain name when you type in a web address, translate it into a machine-friendly IP address and direct your Internet connection to the correct website. Usually, it takes around 12-36 hours for the domain name servers world-wide to be updated and able to obtain the data after you register a new domain name or when updating the DNS servers on your domain name. These 36 hours is called propagation.

Important features of DNS

DNYANADEEP EDUCATION

- The number of features is responsible for the success of DNS, some of them are
- A DNS consists of a distributed database.
- Additional lists of data are also reserved within the DNS database.
- DNS server offers user interface and excellent features. A considerable amount of DNS has to be managed through the user interface.

Advantages

- The users receive important messages with zero downtime.
- Through Anycast technology, in an instance of maintenance or downtime, the supplications are answered by the nearest node.
- DNS immediately rectifies the errors.

Disadvantages

- ICANN can control the DNS root registry that is a private non – profit organization that connects to a particular country and difficulties the abstract idea of network neutrality.
- The collapse of DNS would destroy the World Wide Web(WWW), even if there are more than one root server and backup servers, which will cause immense harm at different locations, DNS servers have decided.

EDUCATION HUB

Name-to-Address Resolution

Though it supports the complex, worldwide hierarchy of computers on the Internet, the basic function of DNS is actually very simple: providing **name-to-address resolution** for TCP/IP-based networks. Name-to-address resolution, also referred to as mapping, is the process of finding the IP address of a computer in a database by using its host name as an index.

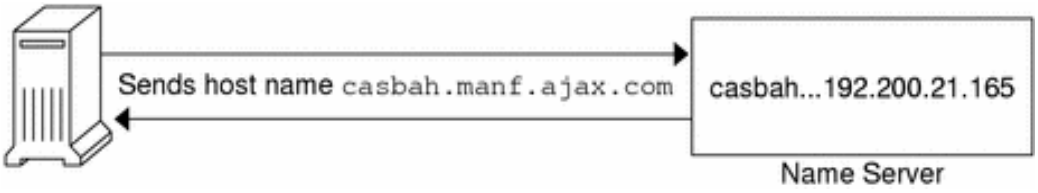
Name-to-address mapping occurs when a program running on your local machine needs to contact a remote computer. The program most likely will know the host name of the remote computer but might not know how to locate it, particularly if the remote machine is in another company, miles from your site. To get the

remote machine's address, the program requests assistance from the DNS software running on your local machine, which is considered a **DNS client**.

Your machine sends a request to a **DNS name server**, which maintains the distributed DNS database. The files in the DNS database bear little resemblance to the NIS+ host or ipnodes Table or even the
local /etc/hosts or /etc/inet/ipnodes file, though they maintain similar information: the host names, the ipnode names, IPv4 and IPv6 addresses, and other information about a particular group of computers. The name server uses the host name our machine sent as part of its request to find or "resolve" the IP address of the remote machine. It then returns this IP address to our local machine **if** the host name is in its DNS database.

The following figure shows name-to-address mapping as it occurs between a DNS client and a name server, probably on the client's local network.

Figure 3–1 Name to Address Resolution



If the host name is not in that name server's DNS database, this indicates that the machine is outside of its authority, or, to use DNS terminology, outside the **local administrative domain**. Thus, each name server is spoken of as being "authoritative" for its local administrative domain.

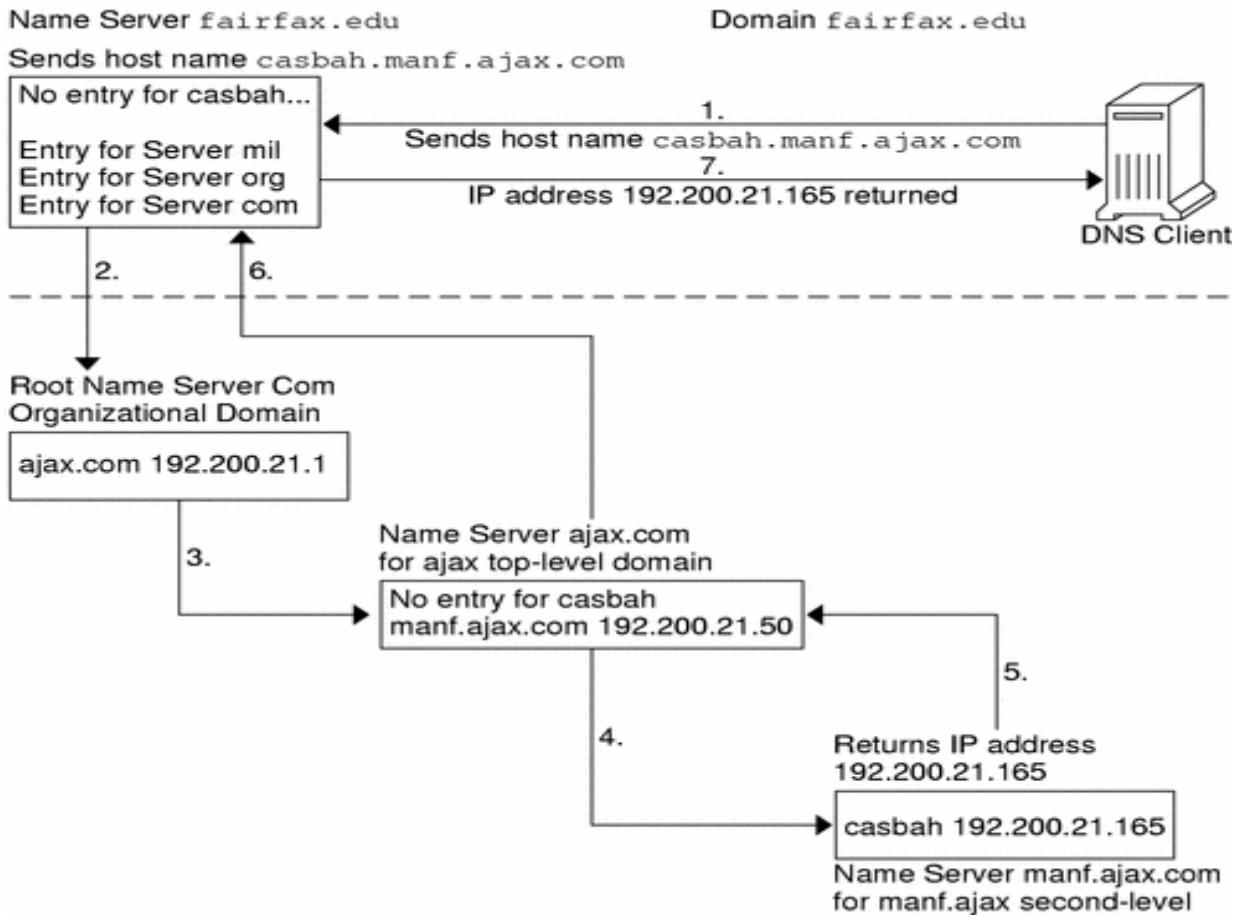
Fortunately, the local name server maintains a list of host names and IP addresses of **root domain name servers**, to which it will forward the request from our machine. These root name servers are authoritative for huge organizational domains, as explained fully in DNS Hierarchy and the Internet. These hierarchies resemble UNIX file systems, in that they are organized into an upside down tree structure.

Each root name server maintains the host names and IP addresses of top level domain name servers for a company, a university, or other large organizations.

The root name server sends our request to the top-level name servers that it knows about. If one of these servers has the IP address for the host you requested, it will return the information to our machine. If the top-level servers do not know about the host you requested, they pass the request to second-level name servers for which they maintain information. Our request is then passed on down through the vast organizational tree. Eventually, a name server that has information about our requested host in its database will return the IP address back to our machine.

The following figure shows name-to-address resolution outside the local domain.

Figure 3–2 Name to Address Resolution for a Remote Host



Electronic Mail Architecture

E-mail is defined as the transmission of messages on the Internet. It is one of the most commonly used features over communications networks that may contain text, files, images, or other attachments. Generally, it is information that is stored on a computer sent through a network to a specified individual or group of individuals.

Email messages are conveyed through email servers; it uses multiple protocols within the TCP/IP suite. For example, SMTP is a protocol, stands for simple mail transfer protocol and used to send messages whereas other protocols IMAP or POP are used to retrieve messages from a mail server. If we want to login to our mail account, we just need to enter a valid email address, password, and the mail servers used to send and receive messages.

Although most of the webmail servers automatically configure your mail account, therefore, we only required to enter your email address and password. However, we may need to manually configure each account if we use an email client like Microsoft Outlook or Apple Mail. In addition, to enter the email address and password, we may also need to enter incoming and outgoing mail servers and the correct port numbers for each one.

Email messages include three components, which are as follows:

- **Message envelope:** It depicts the email's electronic format.
- **Message header:** It contains email subject line and sender/recipient information.
- **Message body:** It comprises images, text, and other file attachments.

The email was developed to support rich text with custom formatting, and the original email standard is only capable of supporting plain text messages. In modern times, email supports HTML (Hypertext markup language), which makes it capable of emails to support the same formatting as websites. The email that supports HTML can contain links, images, CSS layouts, and also can send files or "email attachments" along with messages. Most of the mail servers enable users to send several attachments with each message. The attachments were typically limited to one megabyte in the early days of email. Still, nowadays, many mail servers are able to support email attachments of 20 megabytes or more in size.

DIWAKAR EDUCATION HUB

In **1971**, as a test e-mail message, Ray Tomlinson sent the first e-mail to himself. This email was contained the text "something like QWERTYUIOP." However, the e-mail message was still transmitted through ARPANET, despite sending the e-mail to himself. Most of the electronic mail was being sent as compared to postal mail till **1996**.

Differences between email and webmail

The term email is commonly used to describe both browser-based electronic mail and non-browser-based electronic mail today. The AOL and Gmail are browser-based electronic mails, whereas Outlook for Office 365 is non-browser-based electronic mail. However, to define email, a difference was earlier made as a non-browser program that needed a dedicated client and email server. The non-browser emails offered some advantages, which are enhanced security, integration with corporate software platforms, and lack of advertisements.

Uses of email

Email can be used in different ways: it can be used to communicate either within an organization or personally, including between two people or a large group of people. Most people get benefit from communicating by email with colleagues or friends or individuals or small groups. It allows you to communicate with others around the world and send and receive images, documents, links, and other attachments. Additionally, it offers benefit users to communicate with the flexibility on their own schedule.

There is another benefit of using email; if you use it to communicate between two people or small groups that will beneficial to remind participants of approaching due dates and time-sensitive activities and send professional follow-up emails after appointments. Users can also use the email to quickly remind all upcoming events or inform the group of a time change. Furthermore, it can be used by companies or organizations to convey information to large numbers of employees or customers. Mainly, email is used for newsletters, where mailing list subscribers are sent email marketing campaigns directly and promoted content from a company.

Email can also be used to move a latent sale into a completed purchase or turn leads into paying customers. For example, a company may create an email that is

DWAKAR EDUCATION HUB

used to send emails automatically to online customers who contain products in their shopping cart. This email can help to remind consumers that they have items in their cart and stimulate them to purchase those items before the items run out of stock. Also, emails are used to get reviews by customers after making a purchase. They can survey by including a question to review the quality of service.

History of E-mail

As compared to ARPANet or the Internet, email is much older. The early email was just a small advance, which is known as a file directory in nowadays. It was used to just put a message in other user's directory in the place where they were able to see the message by logging in. For example, the same as leaving a note on someone's desk. Possibly MAILBOX was used at Massachusetts Institute of Technology, which was the first email system of this type from 1965. For sending messages on the same computer, another early program was *SNDMSG*.

Users were only able to send messages to several users of the same computer through email when the internetworking was not beginning. And, the problem became a little more complex when computers began to talk to each other over networks, we required to put a message in an envelope and address it for the destination.

Later in ***1972, Ray Tomlinson*** invented email to remove some difficulties. Tomlinson worked (Like many of the Internet inventors) for Newman and Bolt Beranek as an ARPANET contractor. To denote sending messages from one computer to another, he picked up the @ symbol from the keyboard. Then, it became easy to send a message to another with the help of Internet standards; they were only required to propose name-of-the-user@name-of-the-computer. One of the first users of the new system was Internet pioneer Jon Postel. Also, describing as a "nice hack," credited goes to Jon Postel.

Although the World Wide Web offers many services, email is the most widely used facility and remains the most important application of the Internet. On the international level, over 600 million people use email. There were hundreds of email users by 1974, as ARPANET ultimately encouraged it. Furthermore, email caused a radical shift in Arpa's purpose, as it became the savior of Arpanet.

DIWAKAR EDUCATION HUB

From there were rapid developments in the field of the email system. A big enhancement was to sort emails; some email folders for his boss were invented by Larry Roberts. To organize an email, John Vittal developed some software in 1976. By 1976 commercial packages began to appear, and email had really taken off. The email had changed people and took them from Arpanet to the Internet. Here was appeared some interesting features that ordinary people all over the world wanted to use.

Some years later, Ray Tomlinson observed about email. As compared to the previous one, any single development is stepping rapidly and nearly followed by the next. I think that all the developments would take a big revolution.

When personal computers came on the scene, the offline reader was one of the first new developments. Then, email users became able to store their email on their own personal computers with the help of offline reader and read it. Also, without actually being connected to the network, they were able to prepare replies like Microsoft Outlook can do today. In parts of the world, this was specifically useful for people where the telephone was expensive as compared to the email system.

Without being connected to a telephone, it was able to prepare a reply with connection charges of many dollars a minute and then get on the network to send it. Also, it was useful as the offline mode allowed for more simple user interfaces. In this modern time of very few standards being connected directly to the host email system often resulted in no capacity for text to wrap around on the screen of the user's computer, and backspace keys and delete keys may not work and other such annoyances. Offline readers helped out more to overcome these kinds of difficulties.

The SMTP (simple mail transfer protocol) was the first important email standard. It was a fairly naïve protocol that is still in use. And, it was made in terms of no attempt to find the person who sent a message that was the right or not what they claimed to be. In the email addresses, fraudulent was very easy and is still available. Later, these basic flaws were used in the protocol by security frauds, worms and viruses, and spammers forging identities. From 2004, some of these problems are still being processed for a solution.

DIWAKAR EDUCATION HUB

But as developed email system offered some important features that helped out people to understand easily about email. In 1988, Steve Dorner developed Eudora that was one of the first good commercial systems. But it did not appear for a long time after Pegasus mail come. Servers began to appear as a standard when Internet standards POP (Post office protocol) for email began to mature. Each server was a little different before standard post office protocol (POP). POP was an important standard that allowed users to work together.

Individual dialup users were required to charges for an email per-minute in those days. Also, on the Internet, email and email discussion groups were the main uses for most people. There were several issues on a wide variety of subjects; they became USENET as a body of newsgroups.

With the World Wide Web (WWW), email became available with a simple user interface that was offered by providers like Hotmail and Yahoo. And, users did not require to pay any charges on these platforms. Now everyone wanted at least one email address as it is much simple and affordable, and the medium was adopted by millions of people.

Internet Service Providers (ISPs) started to connect people with each other all over the world by the **1980s**. Also, by **1993** the use of the Internet was becoming widespread, and the word electronic mail was replaced by email.

Today, email has become a primary platform to communicate with people all over the world. There are continuing updates to the system with so many people using email for communication. Although email has some security issues, there have been laws passed to prevent the spread of junk email over the years.

Advantages of Email

There are many advantages of email, which are as follows:

- **Cost-effective:** Email is a very cost-effective service to communicate with others as there are several email services available to individuals and organizations for free of cost. Once a user is online, it does not include any additional charge for the services.
- Email offers users the benefit of accessing email from anywhere at any time if they have an Internet connection.

DIWAKAR EDUCATION HUB

- Email offers you an incurable communication process, which enables you to send a response at a convenient time. Also, it offers users a better option to communicate easily regardless of different schedules users.
- **Speed and simplicity:** Email can be composed very easily with the correct information and contacts. Also, minimum lag time, it can be exchanged quickly.
- **Mass sending:** You can send a message easily to large numbers of people through email.
- Email exchanges can be saved for future retrieval, which allows users to keep important conversations or confirmations in their records and can be searched and retrieved when they needed quickly.
- Email provides a simple user interface and enables users to categorize and filter their messages. This can help you recognize unwanted emails like junk and spam mail. Also, users can find specific messages easily when they are needed.
- As compared to traditional posts, emails are delivered extremely fast.
- Email is beneficial for the planet, as it is paperless. It reduces the cost of paper and helps to save the environment by reducing paper usage.
- It also offers a benefit to attaching the original message at the time you reply to an email. This is beneficial when you get hundreds of emails a day, and the recipient knows what you are talking about.
- Furthermore, emails are beneficial for advertising products. As email is a form of communication, organizations or companies can interact with a lot of people and inform them in a short time.

Disadvantages of Email

- **Impersonal:** As compared to other forms of communication, emails are less personal. For example, when you talk to anyone over the phone or meeting face to face is more appropriate for communicating than email.
- **Misunderstandings:** As email includes only text, and there is no tone of voice or body language to provide context. Therefore, misunderstandings can occur easily with email. If someone sends a joke on email, it can be taken seriously. Also, well-meaning information can be quickly typed as rude or aggressive that can impact wrong. Additionally, if someone types with short abbreviations and descriptions to send content on the email, it can easily be misinterpreted.

DIWAKAR EDUCATION HUB

- **Malicious Use:** As email can be sent by anyone if they have an only email address. Sometimes, an unauthorized person can send you mail, which can be harmful in terms of stealing your personal information. Thus, they can also use email to spread gossip or false information.
- **Accidents Will Happen:** With email, you can make fatal mistakes by clicking the wrong button in a hurry. For instance, instead of sending it to a single person, you can accidentally send sensitive information to a large group of people. Thus, the information can be disclosed, when you have clicked the wrong name in an address list. Therefore, it can be harmful and generate big trouble in the workplace.
- **Spam:** Although in recent days, the features of email have been improved, there are still big issues with unsolicited advertising arriving and spam through email. It can easily become overwhelming and takes time and energy to control.
- **Information Overload:** As it is very easy to send email to many people at a time, which can create information overload. In many modern workplaces, it is a major problem where it is required to move a lot of information and impossible to tell if an email is important. And, email needs organization and upkeep. The bad feeling is one of the other problems with email when you returned from vacation and found hundreds of unopened emails in your inbox.
- **Viruses:** Although there are many ways to travel viruses in the devices, email is one of the common ways to enter viruses and infect devices. Sometimes when you get a mail, it might be the virus come with an attached document. And, the virus can infect the system when you click on the email and open the attached link. Furthermore, an anonymous person or a trusted friend or contact can send infected emails.
- **Pressure to Respond:** If you get emails and you do not answer them, the sender can get annoyed and think you are ignoring them. Thus, this can be a reason to make pressure on your put to keep opening emails and then respond in some way.
- **Time Consuming:** When you get an email and read, write, and respond to emails that can take up vast amounts of time and energy. Many modern workers spend their most time with emails, which may be caused to take more time to complete work.

DIWAKAR EDUCATION HUB

- **Overlong Messages:** Generally, email is a source of communication with the intention of brief messages. There are some people who write overlong messages that can take much time than required.
- **Insecure:** There are many hackers available that want to gain your important information, so email is a common source to seek sensitive data, such as political, financial, documents, or personal messages. In recent times, there have various high-profile cases occurred that shown how email is insecure about information theft.

Different types of Email

There are many types of email; such are as follows:

Newsletters: It is studying by Clutch, the newsletter is the most common type of email that are routinely sent to all mailing list subscribers, either daily, weekly, or monthly. These emails often contain from the blog or website, links curated from other sources, and selected content that the company has recently published. Typically, Newsletter emails are sent on a consistent schedule, and they offer businesses the option to convey important information to their client through a single source. Newsletters might also incorporate upcoming events or new, webinars from the company, or other updates.

Lead Nurturing: Lead-nurturing emails are a series of related emails that marketers use to take users on a journey that may impact their buying behavior. These emails are typically sent over a period of several days or weeks. Lead-nurturing emails are also known as trigger campaigns, which are used for solutions in an attempt to move any prospective sale into a completed purchase and educate potential buyers on the services. These emails are not only helpful for converting emails but also drive engagement. Furthermore, lead-nurturing emails are initiated by a potential buyer taking initial action, such as clicking links on a promotional email or downloading a free sample.

Promotional emails: It is the most common type of B2B (Business to Business) email, which is used to inform the email list of your new or existing products or services. These types of emails contain creating new or repeat customers, speeding up the buying process, or encouraging contacts to take some type of action. It provides some critical benefits to buyers, such as a free month of

DIWAKAR EDUCATION HUB

service, reduced or omitted fees for managed services, or percentage off the purchase price.

Standalone Emails: These emails are popular like newsletters emails, but they contain a limitation. If you want to send an email with multiple links or blurbs, your main call-to-action can weaken. Your subscriber may skip your email and move on, as they may click on the first link or two in your email but may not come back to the others.

Onboarding emails: An onboarding email is a message that is used to strengthen customer loyalty, also known as post-sale emails. These emails receive users right after subscription. The onboarding emails are sent to buyers to familiarize and educate them about how to use a product effectively. Additionally, when clients faced with large-scale service deployments, these emails help them facilitate user adoption.

Transactional: These emails are related to account activity or a commercial transaction and sent from one sender to one recipient. Some examples of transactional email are purchase confirmations, password reminder emails, and personalized product notifications. These emails are used when you have any kind of e-commerce component to your business. As compared to any other type of email, the transactional email messages have 8x the opens and clicks.

Plain-Text Emails: It is a simple email that does not include images or graphics and no formatting; it only contains the text. These types of emails may worth it if you try to only ever send fancy formatted emails, text-only messages. According to HubSpot, although people prefer fully designed emails with various images, plain text emails with less HTML won out in every A/B test. In fact, HTML emails contain lower open and click-through rates, and plain text emails can be great for blog content, event invitations, and survey or feedback requests. Even if you do not send plainer emails, but you can boost your open and click through rates by simplifying your emails and including fewer images.

Welcome emails: It is a type of B2B email and common parts of onboarding emails that help users get acquainted with the brand. These emails can improve subscriber constancy as they include additional information, which helps to the new subscriber in terms of a business objective. Generally, welcome emails are

DIWAKAR EDUCATION HUB

sent buyers who got a subscription to a business's opt-in activities, such as a blog, mailing list, or webinar. Also, these emails can help businesses to build a better relationship between customers.

Examples of email attacks

Although there are many ways to travel viruses in the devices, email is one of the most common vectors for cyberattacks. The methods include spoofing, spamming, spear-phishing, phishing, ransomware, and business email compromise (BEC).

There are many organizations (around 7710) hit by a BEC attack every month, as one out of every 412 emails contains a malware attack. According to the Symantec Internet Threat Security Report, spear-phishing is the most widely used infection vector. Below is given a complete description of these types of attacks:

- **Phishing:** A form of fraud in which the attacks are the practice of sending fraudulent communications that appear to come from a reputable entity or person in email or other communication channels. Usually, it is done through the email; phishing emails are used by attackers to steal sensitive data like credit card and login information or to install malware on the victim's machine. Additionally, everyone should learn about a phishing attack in order to protect themselves, as it is a common type of cyberattack. The common features of phishing emails are Sense of urgency, Hyperlinks, Too Good to Be True, Unusual sender, Attachments.
- **Spamming:** Spam email is unsolicited bulk messages sent without explicit consent from the recipient, which is also known as junk email. Since the 1990s, spam is a problem faced by most email users and has been increasing in popularity. Obtained by spambots, spam mail recipients have had their email addresses (automated programs), which crawl the Internet to find email addresses. This is the dark side of email marketing in which spammers use spambots to create email distribution lists. Typically, an email is sent by a spammer to millions of email addresses with the expectation that only a few numbers of an email address will respond or interact with the message.
- **Spoofing:** Email spoofing is an email message that could be obtained from someone or somewhere other than the intended source. It is a popular

DIWAKAR EDUCATION HUB

strategy that is used in spam and phishing campaigns as core email protocols do not have a built-in method of authentication. And, when people think the email has been sent by a legitimate or familiar source, they are more likely to open an email. Thus, it is a common tactic used for spam and phishing emails. The email spoofing is used with the purpose of getting mail recipients to open emails and possibly respond to a solicitation.

- **Business email compromise (BEC):** A BEC is an exploit in which an authorized person or attacker hacks to a business email account and spoofs the owner's identity to defraud the company, its customers, partners of money. Often, an attacker simply creates an account with an email address that is almost identical to one on the corporate network, which creates trust between the victim and their email account. Sometimes, a BEC is also known as a man-in-the-email attack. Some samples of BEC email messages that contain the word in subject, such as urgent, transfer, request, payment, and more. There are five types of BEC scams on the basis of the FBI, which are False Invoice Scheme, CEO Fraud, Data Theft, Attorney Impersonation, Account Compromise.
- **Spear-phishing:** Email spoofing is an attack where hackers target an individual or specific organization to gain sensitive information through unauthorized access. Spear phishing is not initiated by random hackers but attempted by perpetrators to gain financial benefits or secrets information. It is an attack in which attackers send emails to specific and well-researched targets while purporting to be a trusted sender. The main objective of spear phishing is to convince victims to hand over information or money and infect devices with malware.
- **Ransomware:** It is a subset of malware that is used to encrypt a victim's files. Typically, it locks data by encryption on the victim's system. Typically, it locks data by encryption on the victim's system, and attackers demand payments before the ransomed data is decrypted. Unlike other types of attacks, the primary goal of ransomware attacks is just about always monetary. Usually, when the exploit occurs, a victim is notified about the attack and is given instructions for how to recover from the attack.

Popular email sites

There are some free email website examples include the following:

DIWAKAR EDUCATION HUB

- AOL
- Zoho
- Gmail
- ProtonMail
- Com
- Microsoft Outlook
- Yahoo Mail

Email is a platform that allows users to communicate with people or groups of people around the world. As email security is more important but consequent, it is not inherently secure.

There are many techniques that can be used by individuals, organizations, and service providers. These techniques provide how to protect sensitive information with email communication and accounts from unauthorized access, loss, or destruction.

Individuals can protect their account with the help of creating strong passwords and changing them frequently. They can use alphabetical, numerical, special symbols to make a strong password that helps to protect your account. Users can also install and run an antivirus and antimalware software on their computer, as well as create spam filters and folders to separate potentially malicious emails and junk mail.

Also, there are some techniques the helps organizations to secure email include implementing an email security gateway, training employees on deploying automated email encryption solutions, and proper email usage. By processing and scanning all received emails, email gateways check emails for threats, and analyze that should be allowed into the system or not. A multilayered gateway is a powerful technique since attacks are increasing rapidly and becoming complicated and sophisticated. Some emails that cannot be caught by the gateway, training employees on how to differentiate malicious messages, and properly use email are the best approach, which helps users avoid threatening mails.

For potentially sensitive information, the automated email encryption solutions are used that scans all outgoing messages; it will encrypt the sensitive information

DIWAKAR EDUCATION HUB

before it is sent to the intended recipient. This process helps to send email securely and prevent hackers from gaining access to the secret information, even if they stop it. The only intended recipient can view the original information with permission.

Email service providers can also help to enhance security with the help of accessing control standards and mechanisms and establishing a strong password. Additionally, providers should also offer digital signatures and encryption solutions to secure emails in transit and in users' inboxes. Finally, to protect users from malicious, unrecognized, and untrustworthy messages, service providers should implement firewalls and spam-filtering software applications.

What can be sent in an e-mail?

An email is a platform that enables users to communicate with each other. It allows users to send text messages, including a file or other data on the e-mail all over the world. It is also possible to attach a picture, word processor document, PDF, program, movie, or any file stored on your computer in an e-mail. However, due to some security issues, it may not be possible to send certain types of files on the email; they need some additional steps. For example, the .exe file can be blocked by many companies from being sent over the email, and you will need to compress the file into a .zip file format. Additionally, you may be unable to send any large files or programs from being sent over e-mail as most e-mail providers have file size restrictions.

What should be write e-mail or email?

You can use any word email or e-mail according to the style guide you are following as both are valid and have the same meaning. However, the e-mail word has a hyphen and is a compound noun that describes "electronic" and "mail."

How to send and receive e-mail

E-mail program

You can use an email program to send and receive an email. An email program is also known as an e-mail client. There are many email programs available to send

DIWAKAR EDUCATION HUB

and receive an email, including Mozilla Thunderbird and Microsoft Outlook. A server is used to store and deliver your messages while you use an email client. Often, your ISP (Internet service provider) host this server but can be another Internet company to host this server. To download the new emails, an email client requires connecting a server, whereas online stored emails are always available on Internet-connected devices.

Online e-mail

An online e-mail service or webmail is an alternative way and the popular solution for most people in sending and receiving e-mail. Examples of online emails are Yahoo Mail, Gmail, and Hotmail (now Outlook.com).

Some of the popular e-mail clients?

Today, there are different software-based e-mail clients available for users, but these are not online. Below is given a list that contains the most popular clients.

- Microsoft Outlookv
- Mail for Windows 10
- DreamMail
- Mozilla Thunderbird
- eM Client
- Mailbird

What makes a valid e-mail address?

Users need to follow the various rule that is given below to make valid email address:

- A username followed by @ (the at sign) is most important for an email address, which is followed by the domain name with a domain suffix. Hence, an e-mail must have a username.
- The domain name cannot be longer than 254 characters, and the username cannot be longer than 64 characters long.
- An email must have only one @ sign.
- An email should not have space and special characters like \ [ ] ( ) , : ; < >. Sometimes, few symbols such as backslash, space, and quotation mark

DIWAKAR EDUCATION HUB

work must be preceded with a forward slash. But these characters are not allowed by some email providers.

- In the email, the email address and username cannot start or end with a period.
- The two or more successive periods are not allowed in the email.

SMTP

Email is emerging as one of the most valuable services on the internet today. Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver's side.

SMTP Fundamentals

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly.

SMTP Protocol

The SMTP model is of two type :

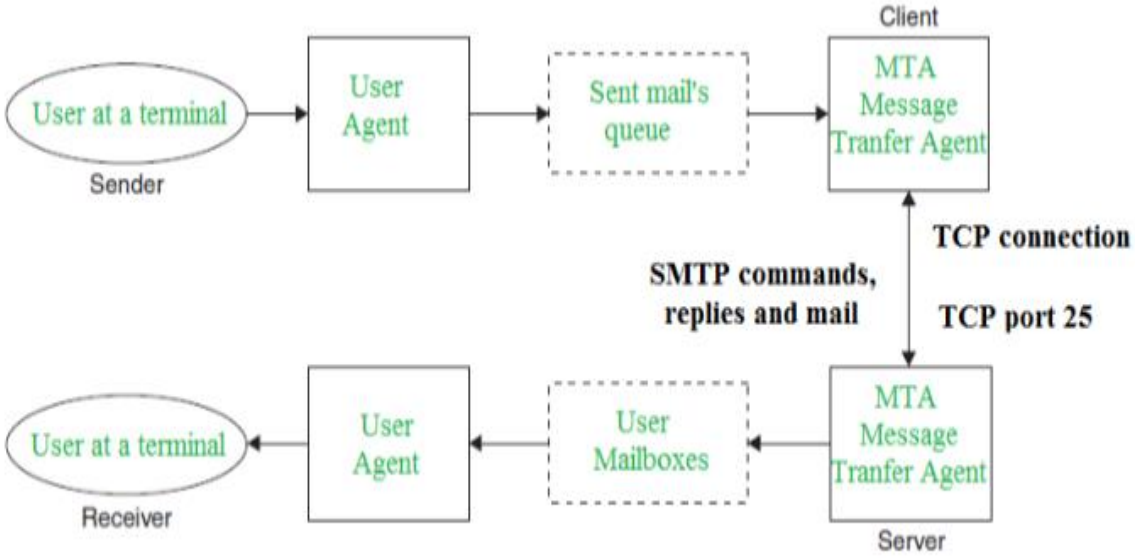
1. End-to- end method
2. Store-and- forward method

The end to end model is used to communicate between different organizations whereas the store and forward method are used within an organization. A SMTP client who wants to send the mail will contact the destination's host SMTP directly in order to send the mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP.
The client SMTP is the one which initiates the session let us call it as the client-SMTP and the server SMTP is the one which responds to the session request and let us call it as receiver-SMTP. The client- SMTP will start the session and the receiver-SMTP will respond to the request.

DIWAKAR EDUCATION HUB

Model of SMTP system

In the SMTP model user deals with the user agent (UA) for example Microsoft Outlook, Netscape, Mozilla, etc. In order to exchange the mail using TCP, MTA is used. The users sending the mail do not have to deal with the MTA it is the responsibility of the system admin to set up the local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.



Both the SMTP-client and MSTP-server should have 2 components:

1. User agent (UA)
2. Local MTA

Communication between sender and the receiver :

The senders, user agent prepare the message and send it to the MTA. The MTA functioning is to transfer the mail across the network to the receivers MTA. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.

SENDING EMAIL:

Mail is sent by a series of request and response messages between the client and a server. The message which is sent across consists of a header and the body. A null line is used to terminate the mail header. Everything which is after the null line is considered as the body of the message which is a sequence of ASCII characters. The message body contains the actual information read by the receipt.

RECEIVING EMAIL:

The user agent at the server side checks the mailboxes at a particular time of intervals. If any information is received it informs the user about the mail. When the user tries to read the mail it displays a list of mails with a short description of each mail in the mailbox. By selecting any of the mail user can view its contents on the terminal.

Some SMTP Commands:

- HELO – Identifies the client to the server, fully qualified domain name, only sent once per session
- MAIL – Initiate a message transfer, fully qualified domain of originator
- RCPT – Follows MAIL, identifies an addressee, typically the fully qualified name of the addressee and for multiple addressees use one RCPT for each addressee
- DATA – send data line by line

POP

POP stands for **Point of Presence (also known as Post Office Protocol)**.

It is a point where many devices share a connection and can communicate with each other. We can say that it is a man-made demarcation point (a point where the public network of a company ends and the private network of the customer begins for eg. the point at which your broadband cable enters the house) between communicating entities. It basically consists of high-speed telecommunications equipment and technologies helps in bringing together people from all over the internet.

DIWAKAR EDUCATION HUB

An example of this would be the local access point that connects customers via their internet service provider (ISP) to the rest of the world. The size of an ISP can be calculated by seeing the number of POPs that the service provider has. The normal houses routers, modems, servers, switches, and other such devices that have to share data over networks all use POPs. Internet Service Providers have multiple POPs.

Characteristics of POP :

- Post Office Protocol is an open protocol, defined by Internet RFCs.
- It allows access to new mail from a spread of client platform types.
- It supports download and delete functions even when offline.
- It requires no mail gateways due to its native nature.
- POP can handle email access only while the emails are sent by SMTP.

RFC 918 got published in 1984 which defined the Post Office Protocol (POP). The explanation of why POP came in the picture was to supply a neater way for a client computer to retrieve e-mail on an SMTP (Simple Mail Transfer Protocol) server so that it can be used locally. POP Version 2 got published in 1985.

It improvised the capabilities of POP by defining a far impressive set of commands further as replies. RFC 1939 was published in 1996 and POP3 has not been improvised since that point.

Examples:

- **Carrier hotels :**
  These buildings are extremely secure with size averaging around 54, 000 square feet. These hotels offer hardware and software installation, updation and several other services.
- **Meet-me rooms :**
  Meet-Me Rooms (MMRs) are small space inside carrier hotels, averaging around 5, 000 square feet. These small rooms house interconnects networking equipment owned by many telecommunication companies.

DIWAKAR EDUCATION HUB

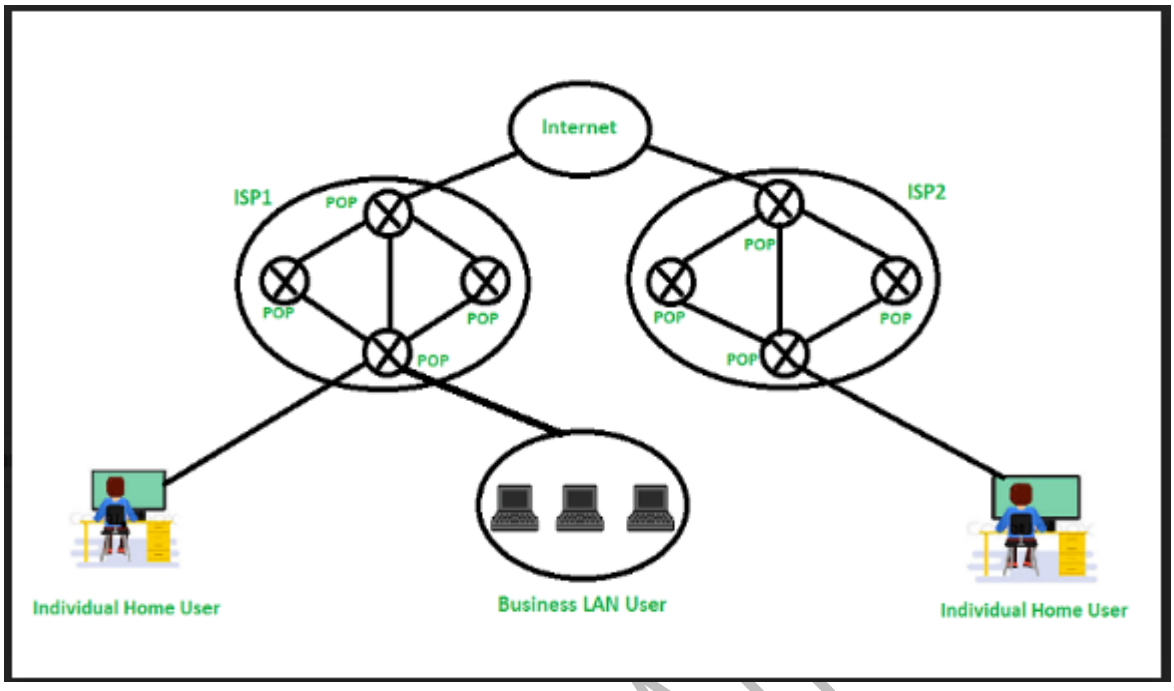


Figure – Post Office Protocol (POP)

Working:
POP's working is based on its five important equipment which are:

1. **Base stations –** A central point of reference to an access point and bandwidth management to ensure evenly distribution of the connection speed of the customer.
2. **Client equipment –** utilized by customers to link with the base stations
3. **Network switches –** Used for proper distribution
4. **Routers –** Provides multiple paths for the data to be shared in the network
5. **Firewall –** Used for securing the network from threats (internal and external)

Advantages:
The latest version of Post Office Protocol (POP3) is that the most widely used protocol and is being supported by most of the email clients.

It provides a convenient and standard way for users to access mailboxes and download messages. An important advantage of this is that the mail messages get delivered to the client PC and they can be read with or without accessing the web.

More advantages are:

- Creation of latest messages impossible without being logged onto the web
- All messages get stored on the disc drive of your computer
- As the attachments are already on your PC, opening them may be a quicker process
- There isn't any maximum size on your mailbox, except as determined by the scale of your disc drive

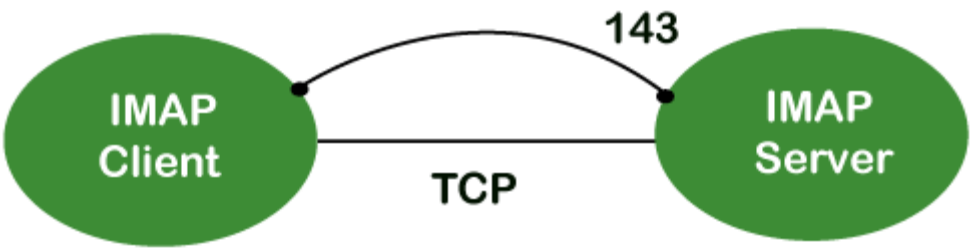
Disadvantages:

- Consumes large memory as all the messages are stored on the disc drive
- Opening attachments may be a fast process unless the attachment contains a virus
- Since all attachments get downloaded on your computer, there's a danger of virus attack if they're not
  scanned by antivirus softwares as these scans are only 60% effective
- Email folders can become corrupted and might even drift.

IMAP Protocol

IMAP stands for **Internet Message Access Protocol**. It is an application layer protocol which is used to receive the emails from the mail server. It is the most commonly used protocols like POP3 for retrieving the emails.

It also follows the client/server model. On one side, we have an IMAP client, which is a process running on a computer. On the other side, we have an IMAP server, which is also a process running on another computer. Both computers are connected through a network.



OMKAR EDUCATION HUB

The IMAP protocol resides on the TCP/IP transport layer which means that it implicitly uses the reliability of the protocol. Once the TCP connection is established between the IMAP client and IMAP server, the IMAP server listens to the port 143 by default, but this port number can also be changed.

By default, there are two ports used by IMAP:

- Port 143: It is a non-encrypted IMAP port.
- Port 993: This port is used when IMAP client wants to connect through IMAP securely.

Why should we use IMAP instead of POP3 protocol?

POP3 is becoming the most popular protocol for accessing the TCP/IP mailboxes. It implements the offline mail access model, which means that the mails are retrieved from the mail server on the local machine, and then deleted from the mail server. Nowadays, millions of users use the POP3 protocol to access the incoming mails. Due to the offline mail access model, it cannot be used as much. The online model we would prefer in the ideal world. In the online model, we need to be connected to the internet always. The biggest problem with the offline access using POP3 is that the mails are permanently removed from the server, so multiple computers cannot access the mails. The solution to this problem is to store the mails at the remote server rather than on the local server. The POP3 also faces another issue, i.e., data security and safety. The solution to this problem is to use the disconnected access model, which provides the benefits of both online and offline access. In the disconnected access model, the user can retrieve the mail for local use as in the POP3 protocol, and the user does not need to be connected to the internet continuously. However, the changes made to the mailboxes are synchronized between the client and the server. The mail remains on the server so different applications in the future can access it. When developers recognized these benefits, they made some attempts to implement the disconnected access model. This is implemented by using the POP3 commands that provide the option to leave the mails on the server. This works, but only to a limited extent, for example, keeping track of which messages are new or old become an issue when both are retrieved and left on the server. So, the POP3 lacks some features which are required for the proper disconnected access model.

DIWAKAR EDUCATION HUB

In the mid-1980s, the development began at Stanford University on a new protocol that would provide a more capable way of accessing the user mailboxes. The result was the development of the interactive mail access protocol, which was later renamed as **Internet Message Access Protocol**.

IMAP History and Standards

The first version of IMAP was formally documented as an internet standard was IMAP version 2, and in RFC 1064, and was published in July 1988. It was updated in RFC 1176, August 1990, retaining the same version. So they created a new document of version 3 known as IMAP3. In RFC 1203, which was published in February 1991. However, IMAP3 was never accepted by the market place, so people kept using IMAP2. The extension to the protocol was later created called IMAPbis, which added support for Multipurpose Internet Mail Extensions (MIME) to IMAP. This was a very important development due to the usefulness of MIME. Despite this, IMAPbis was never published as an RFC. This may be due to the problems associated with the IMAP3. In December 1994, IMAP version 4, i.e., IMAP4 was published in two RFCs, i.e., RFC 1730 describing the main protocol and RFC 1731 describing the authentication mechanism for IMAP 4. IMAP 4 is the current version of IMAP, which is widely used today. It continues to be refined, and its latest version is actually known as IMAP4rev1 and is defined in RFC 2060. It is most recently updated in RFC 3501.

IMAP Features

IMAP was designed for a specific purpose that provides a more flexible way of how the user accesses the mailbox. It can operate in any of the three modes, i.e., online, offline, and disconnected mode. Out of these, offline and disconnected modes are of interest to most users of the protocol.

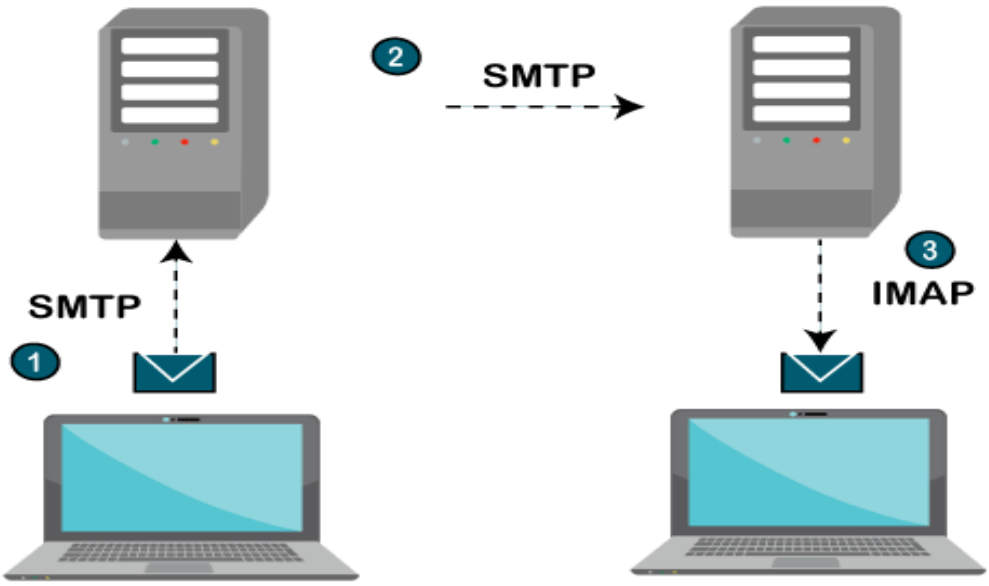
The following are the features of an IMAP protocol:

- Access and retrieve mail from remote server: The user can access the mail from the remote server while retaining the mails in the remote server.
- Set message flags: The message flag is set so that the user can keep track of which message he has already seen.

DIWAKAR EDUCATION HUB

- Manage multiple mailboxes: The user can manage multiple mailboxes and transfer messages from one mailbox to another. The user can organize them into various categories for those who are working on various projects.
- Determine information prior to downloading: It decides whether to retrieve or not before downloading the mail from the mail server.
- Downloads a portion of a message: It allows you to download the portion of a message, such as one body part from the mime-multi part. This can be useful when there are large multimedia files in a short-text element of a message.
- Organize mails on the server: In case of POP3, the user is not allowed to manage the mails on the server. On the other hand, the users can organize the mails on the server according to their requirements like they can create, delete or rename the mailbox on the server.
- Search: Users can search for the contents of the emails.
- Check email-header: Users can also check the email-header prior to downloading.
- Create hierarchy: Users can also create the folders to organize the mails in a hierarchy.

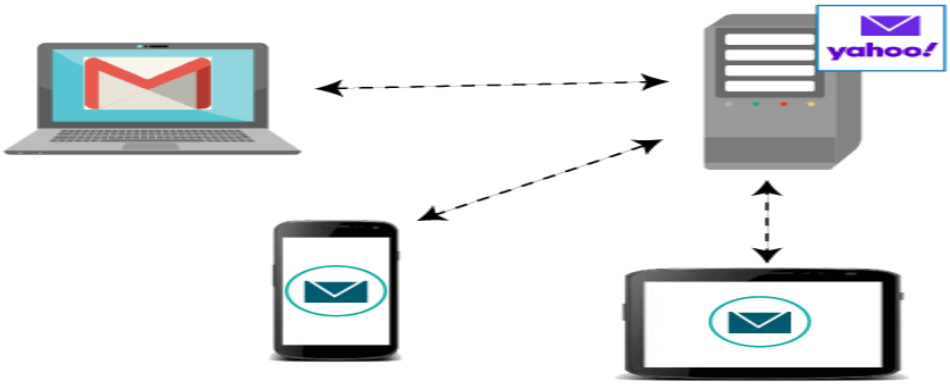
IMAP General Operation



EDUCATION HUB

1. The IMAP is a client-server protocol like POP3 and most other TCP/IP application protocols. The IMAP4 protocol functions only when the IMAP4 must reside on the server where the user mailboxes are located. In c the POP3 does not necessarily require the same physical server that provides the SMTP services. Therefore, in the case of the IMAP protocol, the mailbox must be accessible to both SMTP for incoming mails and IMAP for retrieval and modifications.
2. The IMAP uses the Transmission Control Protocol (TCP) for communication to ensure the delivery of data and also received in the order.
3. The IMAP4 listens on a well-known port, i.e., port number 143, for an incoming connection request from the IMAP4 client.

The IMAP protocol through a simple example.



The IMAP protocol synchronizes all the devices with the main server. Let's suppose we have three devices desktop, mobile, and laptop as shown in the above figure. If all these devices are accessing the same mailbox, then it will be synchronized with all the devices. Here, synchronization means that when mail is opened by one device, then it will be marked as opened in all the other devices, if we delete the mail, then the mail will also be deleted from all the other devices. So, we have synchronization between all the devices. In IMAP, we can see all the folders like spam, inbox, sent, etc. We can also create our own folder known as a custom folder that will be visible in all the other devices.

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.

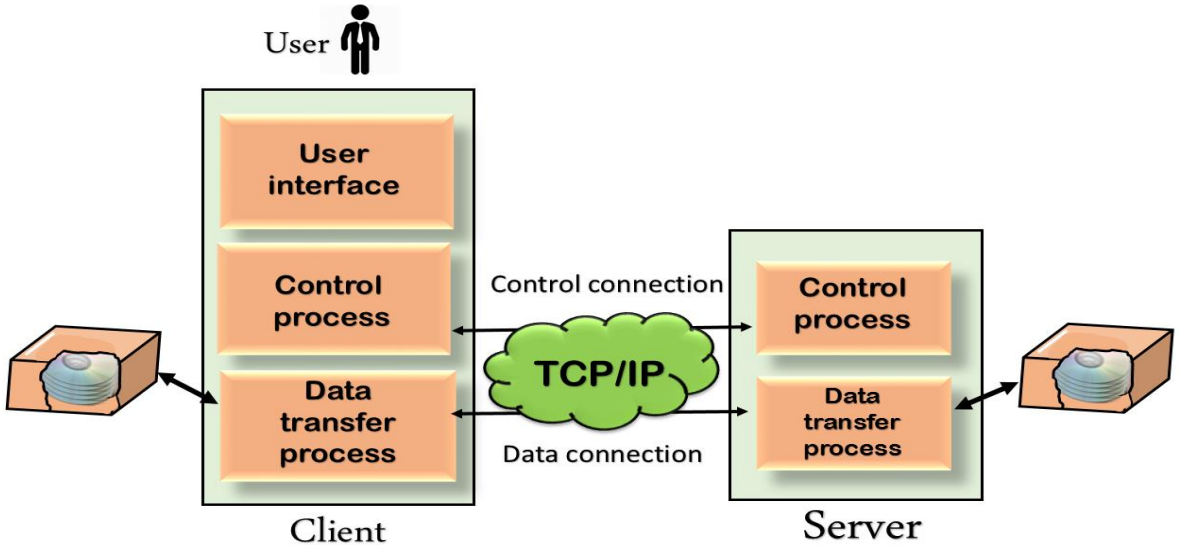
Objectives of FTP

- 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?

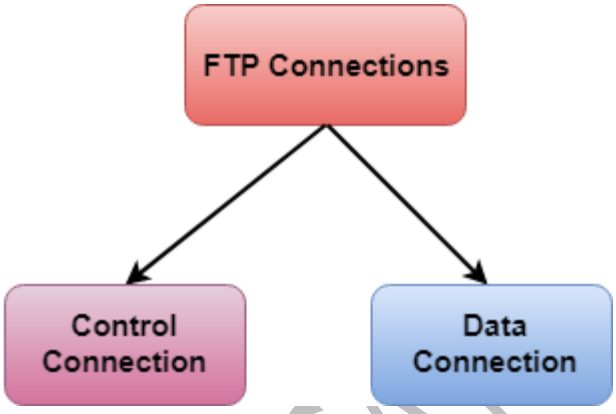
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. 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.

DIWAKAR EDUCA

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.

Telnet

- The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand.
- The better solution is to provide a general client-server program that lets the user access any application program on a remote computer. Therefore, a program that allows a user to log on to a remote computer. A popular

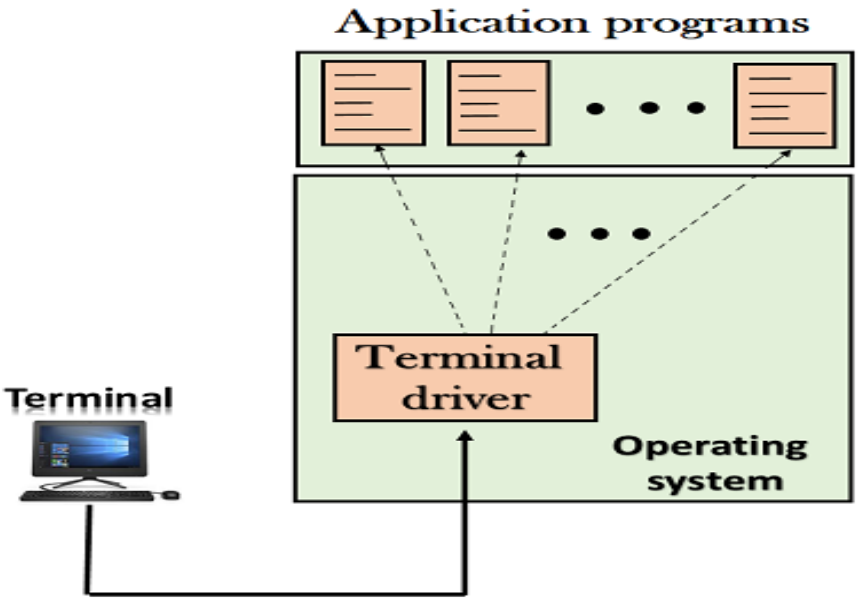
DIWAKAR EDUCATION HUB

client-server program Telnet is used to meet such demands. Telnet is an abbreviation for **Terminal Network**.

- Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.

There are two types of login:

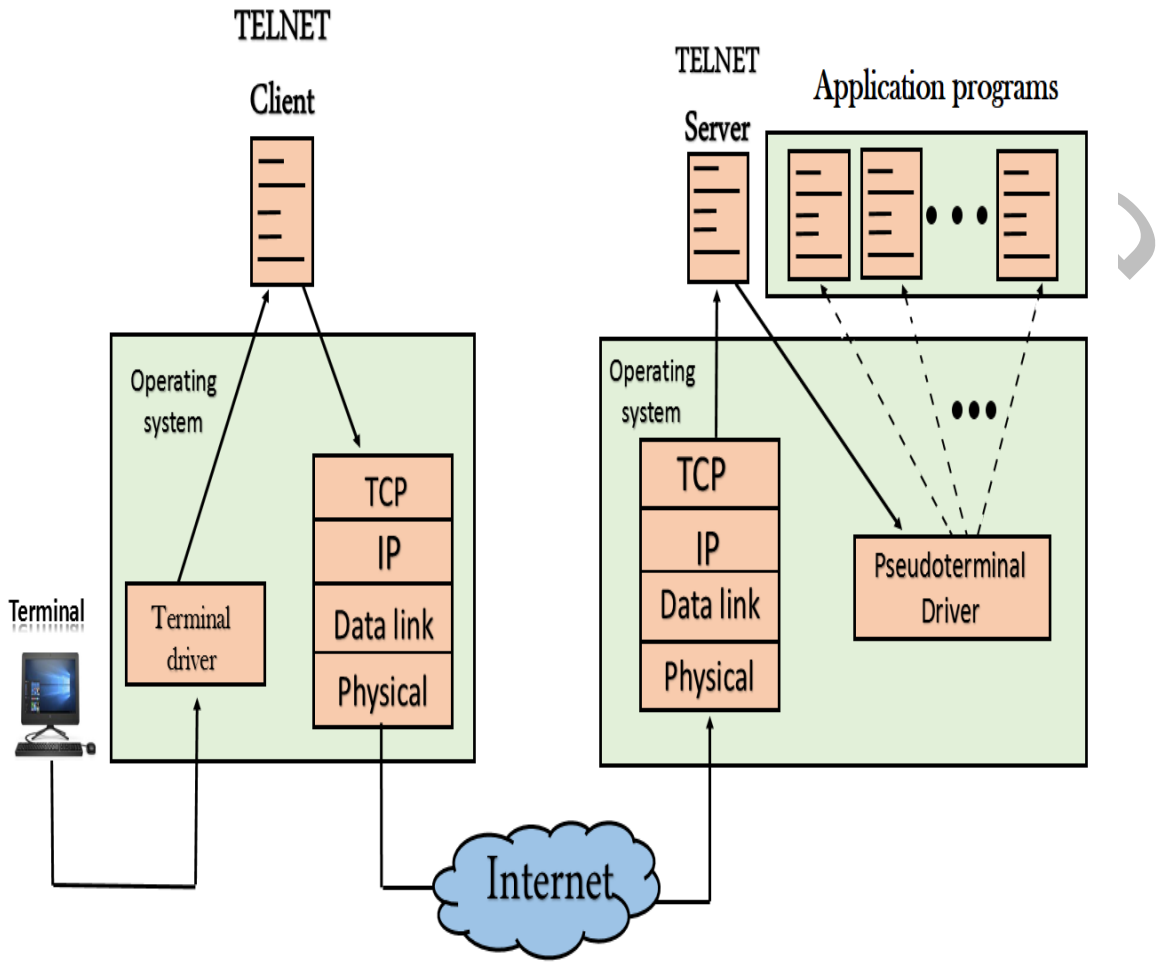
Local Login



- When a user logs into a local computer, then it is known as local login.
- When the workstation running terminal emulator, the keystrokes entered by the user are accepted by the terminal driver. The terminal driver then passes these characters to the operating system which in turn, invokes the desired application program.
- However, the operating system has special meaning to special characters. For example, in UNIX some combination of characters have special meanings such as control character with "z" means suspend. Such situations do not create any problem as the terminal driver knows the meaning of such characters. But, it can cause the problems in remote login.

DIWAKAR "JB

Remote login



- When the user wants to access an application program on a remote computer, then the user must perform remote login.

How remote login occurs

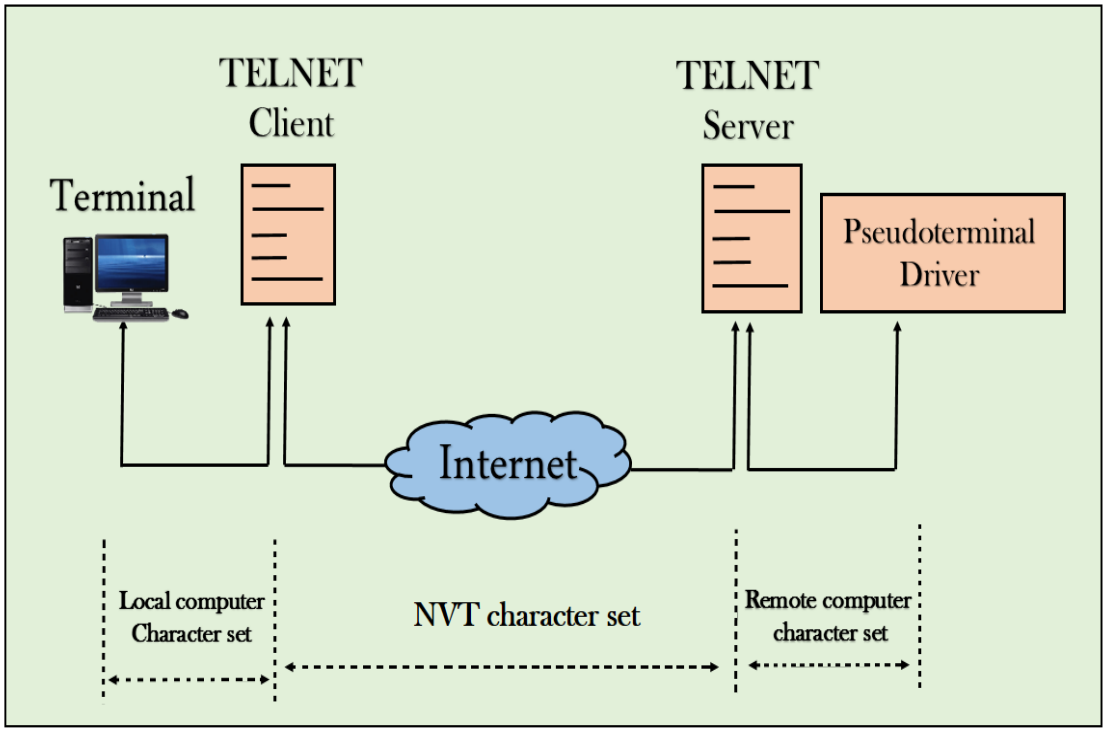
At the local site

The user sends the keystrokes to the terminal driver, the characters are then sent to the TELNET client. The TELNET client which in turn, transforms the characters to a universal character set known as network virtual terminal characters and delivers them to the local TCP/IP stack

At the remote site

The commands in NVT forms are transmitted to the TCP/IP at the remote machine. Here, the characters are delivered to the operating system and then pass to the TELNET server. The TELNET server transforms the characters which can be understandable by a remote computer. However, the characters cannot be directly passed to the operating system as a remote operating system does not receive the characters from the TELNET server. Therefore it requires some piece of software that can accept the characters from the TELNET server. The operating system then passes these characters to the appropriate application program.

Network Virtual Terminal (NVT)



- The network virtual terminal is an interface that defines how data and commands are sent across the network.
- In today's world, systems are heterogeneous. For example, the operating system accepts a special combination of characters such as

end-of-file token running a DOS operating system *ctrl+z* while the token running a UNIX operating system is *ctrl+d*.

- TELNET solves this issue by defining a universal interface known as network virtual interface.
- The TELNET client translates the characters that come from the local terminal into NVT form and then delivers them to the network. The Telnet server then translates the data from NVT form into a form which can be understandable by a remote computer.

Computer Network Security

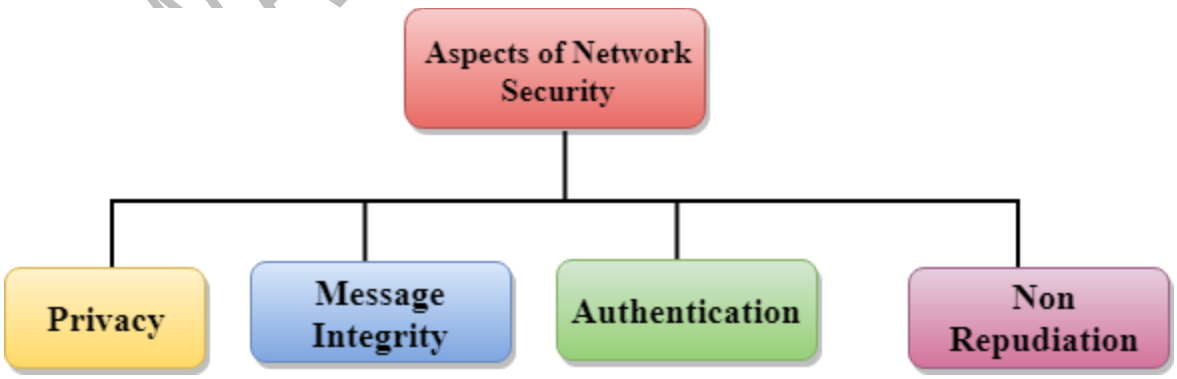
Computer network security consists of measures taken by business or some organizations to monitor and prevent unauthorized access from the outside attackers.

Different approaches to computer network security management have different requirements depending on the size of the computer network. For example, a home office requires basic network security while large businesses require high maintenance to prevent the network from malicious attacks.

Network Administrator controls access to the data and software on the network. A network administrator assigns the user ID and password to the authorized person.

Aspects of Network Security:

Following are the desirable properties to achieve secure communication:



VAKAR EDUCATION HUB

- **Privacy:** Privacy means both the sender and the receiver expects confidentiality. The transmitted message should be sent only to the intended receiver while the message should be opaque for other users. Only the sender and receiver should be able to understand the transmitted message as eavesdroppers can intercept the message. Therefore, there is a requirement to encrypt the message so that the message cannot be intercepted. This aspect of confidentiality is commonly used to achieve secure communication.
- **Message Integrity:** Data integrity means that the data must arrive at the receiver exactly as it was sent. There must be no changes in the data content during transmission, either maliciously or accident, in a transit. As there are more and more monetary exchanges over the internet, data integrity is more crucial. The data integrity must be preserved for secure communication.
- **End-point authentication:** Authentication means that the receiver is sure of the sender?s identity, i.e., no imposter has sent the message.
- **Non-Repudiation:** Non-Repudiation means that the receiver must be able to prove that the received message has come from a specific sender. The sender must not deny sending a message that he or she send. The burden of proving the identity comes on the receiver. For example, if a customer sends a request to transfer the money from one account to another account, then the bank must have a proof that the customer has requested for the transaction.

Malware

Malware is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user's permission. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware and other malicious programs.

Types of Malware:

- **Viruses –**
  A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file

DIWAKAR EDUCATION HUB

can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

- **Worms –**
  Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.
- **Spyware –**
  Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

- **Trojan horse –**
  A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, audio files.
- **Logic Bombs –**
  A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cybersecurity specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.
- **Ransomware –**
  Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key which is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system.
- **Backdoors –**
  A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant the cyber criminals future access to the

DWAKAR EDUCATION HUB

system even if the organization fixes the original vulnerability used to attack the system.

- **Rootkits –**
  A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.
- **Keyloggers –**
  Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

Steganography

Steganography, or cover writing, is a method where a secret method is converted into fake looking message. This technique helps to keep a message secret. It is pretty difficult to use and understand. Structure of data remains unaltered in Steganography. It is used in text, audio, video or images.

Steganography is a method in which secret message is hidden in a cover media. Steganography means covered writing. Steganography is the idea to prevent secret information by creating the suspicion. Steganography is less popular than Cryptography. In steganography, structure of data is not usually altered.
The forms of steganography are:

1. Text
2. Audio
3. Video
4. Images
5. Network or Protocol

Cryptography

Cryptography or secret writing, is a method where a secret method is converted in cipher text and sent to other person who then decrypt the cipher text into plain text. Cryptography can be classified as Symmetric key cryptography or Asymmetric key cryptography.

Cryptography means secret writing. In cryptography, sender does not send message directly to the receiver, before sending information to the receiver information or plain text is converted into cipher text by using some encryption algorithm then send to the receiver and receiver decrypt the cipher text into plain text to read the original information.
It is of two types:

1. Symmetric key cryptography
2. Asymmetric key cryptography

Following are some of the important differences between Steganography and Cryptography.

Sr. No.	Key	Steganography	Cryptography
1	Type	Steganography refers to Cover Writing.	Cryptography refers to Secret Writing.
2	Popularity	Steganography is less popular than Cryptography.	Cryptography is more popular than Steganography.
3	Integrity	Structure of data remains same.	Structure of data can be altered.
4	Attack	Attack in Steganography is termed as Steganalysis.	Attack in Cryptography is termed as Cryptanalysis.
5	Security Principles	Steganography supports Confidentiality and Authentication.	Cryptography supports Confidentiality, Authentication, Data integrity and Non-repudiation.

Sr. No.	Key	Steganography	Cryptography
6	Parameter	Steganography requires a parameter like key.	Cryptography may not need any key.

Secret-Key Algorithms and Public-Key Algorithms

Privacy

The concept of how to achieve privacy has not been changed for thousands of years: the message cannot be encrypted. The message must be rendered as opaque to all the unauthorized parties. A good encryption/decryption technique is used to achieve privacy to some extent. This technique ensures that the eavesdropper cannot understand the contents of the message.

Encryption/Decryption

Encryption: Encryption means that the sender converts the original information into another form and sends the unintelligible message over the network.

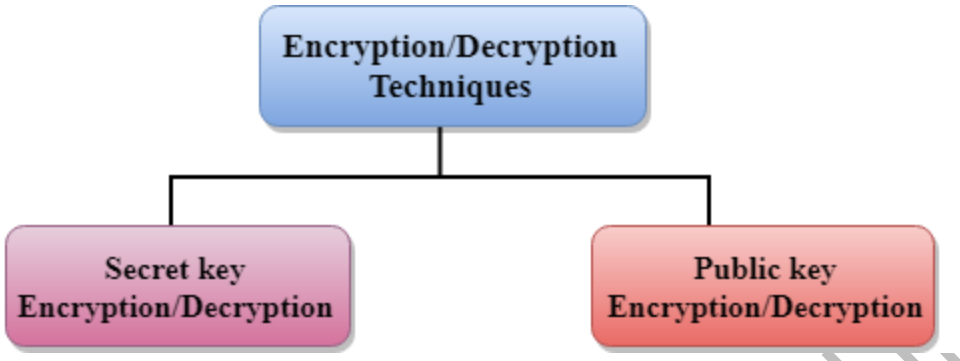
Decryption: Decryption reverses the Encryption process in order to transform the message back to the original form.

The data which is to be encrypted at the sender site is known as plaintext, and the encrypted data is known as ciphertext. The data is decrypted at the receiver site.

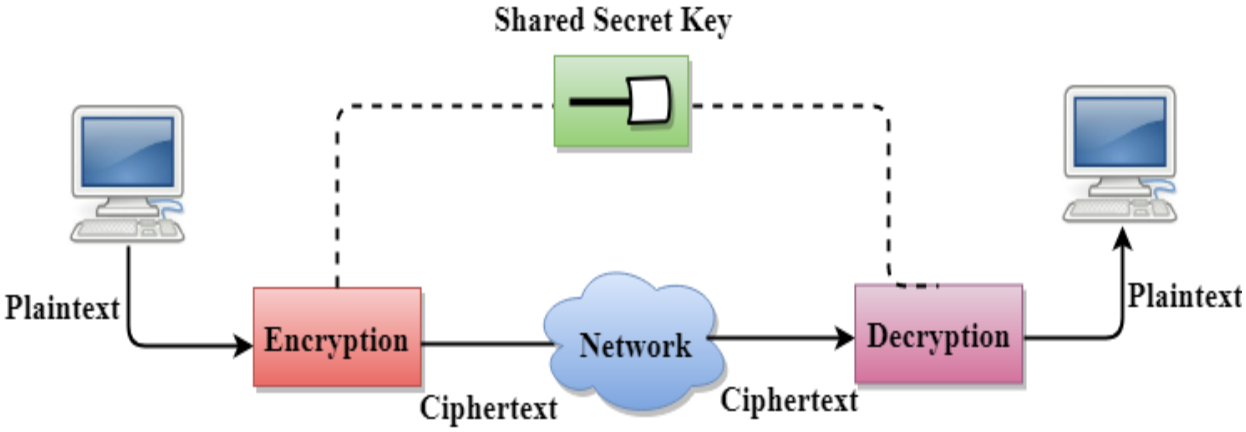
There are two types of Encryption/Decryption techniques:

- Privacy with secret key Encryption/Decryption
- Privacy with public key Encryption/Decryption

DIWAKAR EDUCATION HUB



Secret Key Encryption/Decryption technique



- In Secret Key Encryption/Decryption technique, the same key is used by both the parties, i.e., the sender and receiver.
- The sender uses the secret key and encryption algorithm to encrypt the data; the receiver uses this key and decryption algorithm to decrypt the data.
- In Secret Key Encryption/Decryption technique, the algorithm used for encryption is the inverse of the algorithm used for decryption. It means that if the encryption algorithm uses a combination of addition and multiplication, then the decryption algorithm uses a combination of subtraction and division.
- The secret key encryption algorithm is also known as symmetric encryption algorithm because the same secret key is used in bidirectional communication.
- In secret key encryption/decryption algorithm, the secret code is used by the computer to encrypt the information before it is sent over the network to another computer.

- The secret key requires that we should know which computers are talking to each other so that we can install the key on each computer.

Data Encryption Standard (DES)

- The Data Encryption Standard (DES) was designed by IBM and adopted by the U.S. government as the standard encryption method for nonmilitary and nonclassified use.
- The Data Encryption Standard is a standard used for encryption, and it is a form of Secret **Key Cryptography**.

Advantage

Efficient: The secret key algorithms are more efficient as it takes less time to encrypt the message than to encrypt the message by using a public key encryption algorithm. The reason for this is that the size of the key is small. Due to this reason, Secret Key Algorithms are mainly used for encryption and decryption.

Disadvantages of Secret Key Encryption

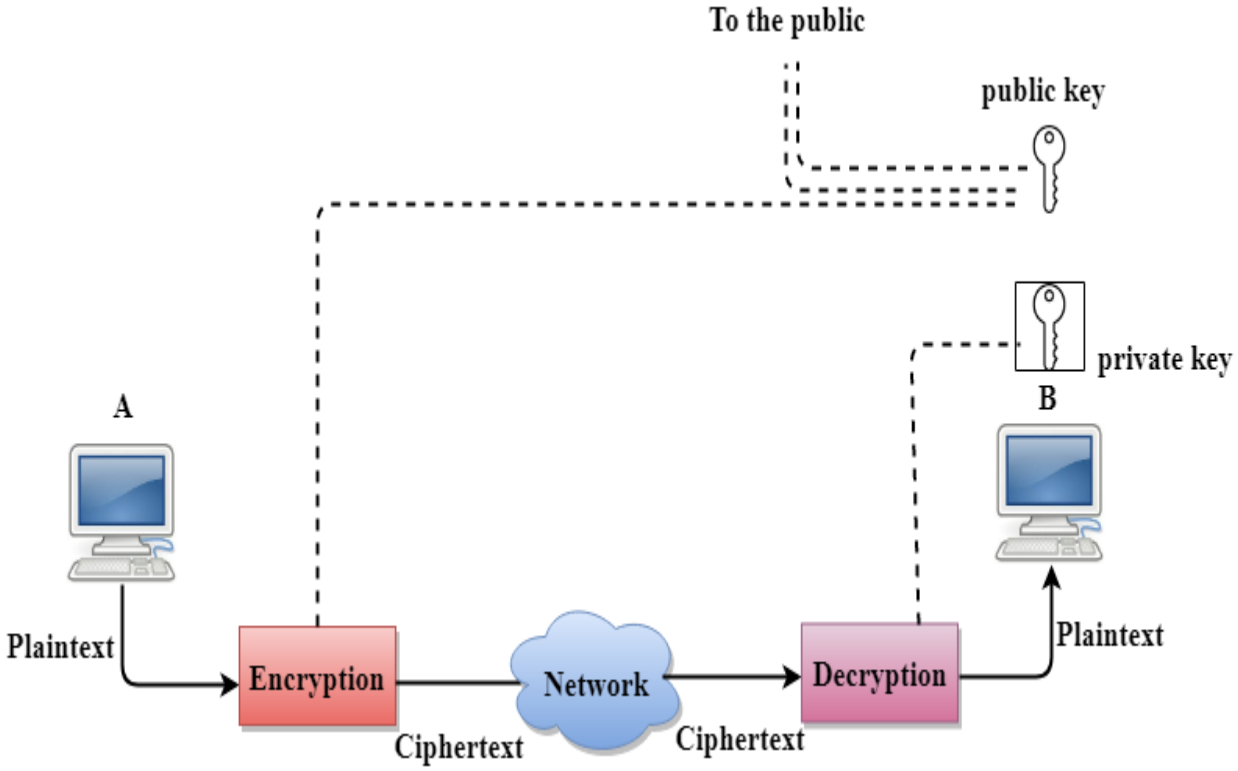
The Secret Key Encryption/Decryption has the following disadvantages:

- Each pair of users must have a secret key. If the number of people wants to use this method in the world is N, then there are N(N-1)/2 secret keys. For example, for one million people, then there are half billion secret keys.
- The distribution of keys among different parties can be very difficult. This problem can be resolved by combining the Secret Key Encryption/Decryption with the Public Key Encryption/Decryption algorithm.

Public Key Encryption/Decryption technique

- There are two keys in public key encryption: a private key and a public key.
- The private key is given to the receiver while the public key is provided to the public.

DIWAKAR EDUCATION HUB



In the above figure, we see that A is sending the message to user B. 'A' uses the public key to encrypt the data while 'B' uses the private key to decrypt the data.

- In public key Encryption/Decryption, the public key used by the sender is different from the private key used by the receiver.
- The public key is available to the public while the private key is kept by each individual.
- The most commonly used public key algorithm is known as RSA.

Advantages of Public Key Encryption

- The main restriction of private key encryption is the sharing of a secret key. A third party cannot use this key. In public key encryption, each entity creates a pair of keys, and they keep the private one and distribute the public key.
- The number of keys in public key encryption is reduced tremendously. For example, for one million users to communicate, only two million keys are required, not a half-billion keys as in the case of secret key encryption.

Disadvantages of Public Key Encryption

- **Speed:** One of the major disadvantage of the public-key encryption is that it is slower than secret-key encryption. In secret key encryption, a single shared key is used to encrypt and decrypt the message which speeds up the process while in public key encryption, different two keys are used, both related to each other by a complex mathematical process. Therefore, we can say that encryption and decryption take more time in public key encryption.
- **Authentication:** A public key encryption does not have a built-in authentication. Without authentication, the message can be interpreted or intercepted without the user's knowledge.
- **Inefficient:** The main disadvantage of the public key is its complexity. If we want the method to be effective, large numbers are needed. But in public key encryption, converting the plaintext into ciphertext using long keys takes a lot of time. Therefore, the public key encryption algorithms are efficient for short messages not for long messages.

Differences b/w Secret Key Encryption & Public Key Encryption

Basis for Comparison	Secret Key Encryption	Public Key Encryption
Define	Secret Key Encryption is defined as the technique that uses a single shared key to encrypt and decrypt the message.	Public Key Encryption is defined as the technique that uses two different keys for encryption and decryption.
Efficieny	It is efficient as this technique is recommended for large amounts of text.	It is inefficient as this technique is used only for short messages.
Other name	It is also known as Symmetric Key encryption.	It is also known as Asymmetric Key Encryption.

Speed	Its speed is high as it uses a single key for encryption and decryption.	Its speed is slow as it uses two different keys, both keys are related to each other through the complicated mathematical process.
Algorithms	The Secret key algorithms are DES, 3DES, AES & RCA.	The Public key algorithms are Diffie-Hellman, RSA.
Purpose	The main purpose of the secret key algorithm is to transmit the bulk data.	The main purpose of the public key algorithm is to share the keys securely.

Digital Signature

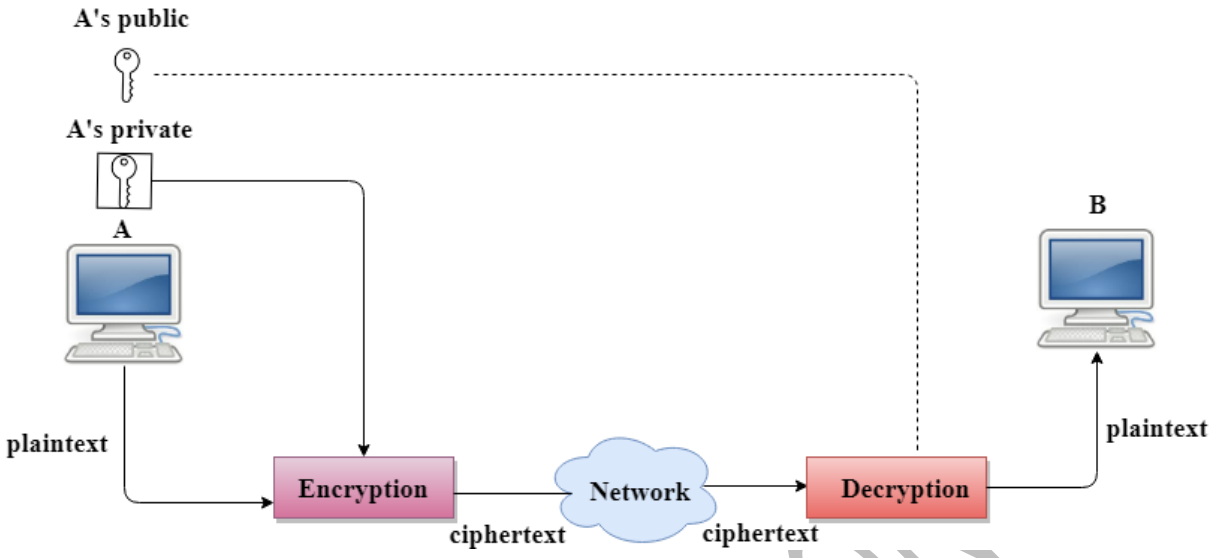
The Digital Signature is a technique which is used to validate the authenticity and integrity of the message. We know that there are four aspects of security: privacy, authentication, integrity, and non-repudiation. We have already discussed the first aspect of security and other three aspects can be achieved by using a digital signature.

The basic idea behind the Digital Signature is to sign a document. When we send a document electronically, we can also sign it. We can sign a document in two ways: to sign a whole document and to sign a digest.

Signing the Whole Document

- In Digital Signature, a public key encryption technique is used to sign a document. However, the roles of a public key and private key are different here. The sender uses a private key to encrypt the message while the receiver uses the public key of the sender to decrypt the message.
- In Digital Signature, the private key is used for encryption while the public key is used for decryption.
- Digital Signature cannot be achieved by using secret key encryption.

DIWAKAR EDUCATION



Digital Signature is used to achieve the following three aspects:

- **Integrity:** The Digital Signature preserves the integrity of a message because, if any malicious attack intercepts a message and partially or totally changes it, then the decrypted message would be impossible.
- **Authentication:** We can use the following reasoning to show how the message is authenticated. If an intruder (user X) sends a message pretending that it is coming from someone else (user A), user X uses her own private key to encrypt the message. The message is decrypted by using the public key of user A. Therefore this makes the message unreadable. Encryption with X's private key and decryption with A's public key results in garbage value.
- **Non-Repudiation:** Digital Signature also provides non-repudiation. If the sender denies sending the message, then her private key corresponding to her public key is tested on the plaintext. If the decrypted message is the same as the original message, then we know that the sender has sent the message.

Note: Digital Signature does not provide privacy. If there is a need for privacy, then another layer of encryption/decryption is applied.

Signing the Digest

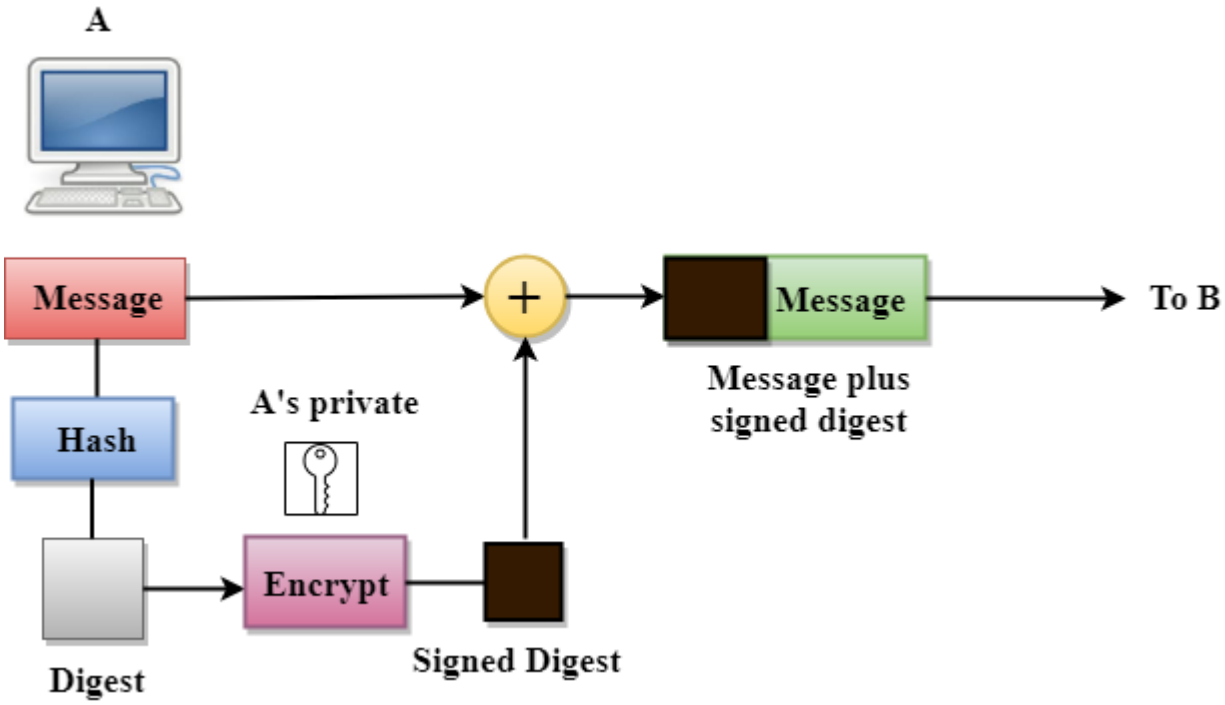
- Public key encryption is efficient if the message is short. If the message is long, a public key encryption is inefficient to use. The solution to this problem is to let the sender sign a digest of the document instead of the whole document.
- The sender creates a miniature version (digest) of the document and then signs it, the receiver checks the signature of the miniature version.
- The hash function is used to create a digest of the message. The hash function creates a fixed-size digest from the variable-length message.
- The two most common hash functions used: MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1). The first one produces 120-bit digest while the second one produces a 160-bit digest.
- A hash function must have two properties to ensure the success:
    - First, the digest must be one way, i.e., the digest can only be created from the message but not vice versa.
    - Second, hashing is a one-to-one function, i.e., two messages should not create the same digest.

Following are the steps taken to ensure security:

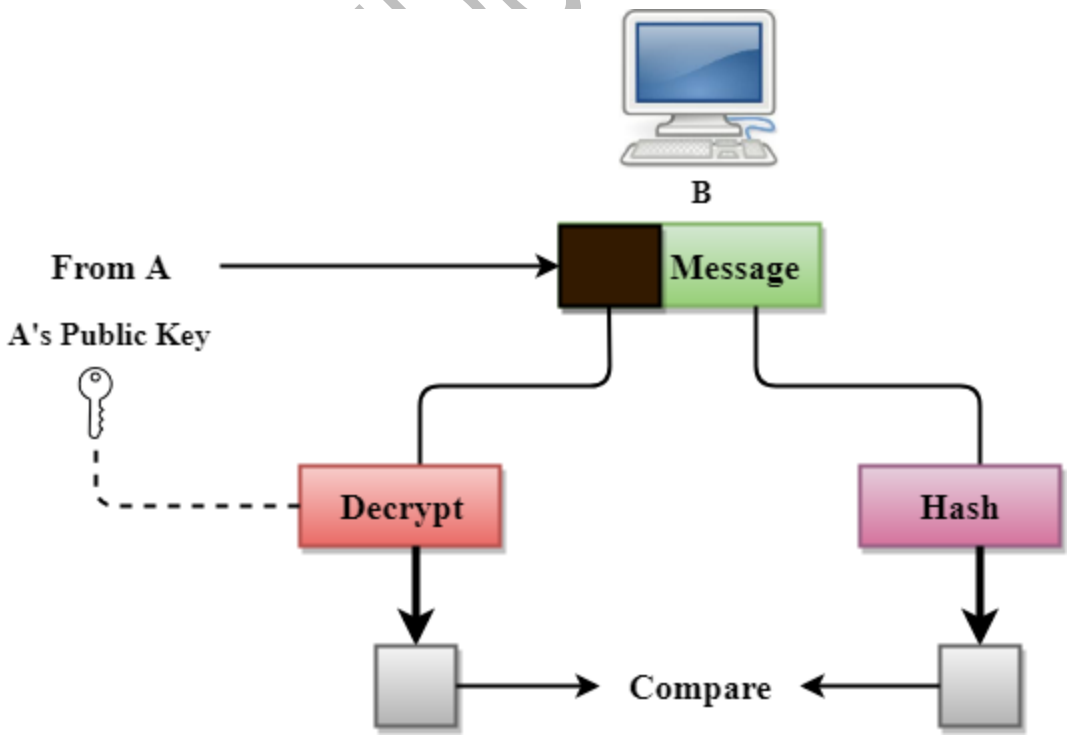
- The miniature version (digest) of the message is created by using a hash function.
- The digest is encrypted by using the sender's private key.
- After the digest is encrypted, then the encrypted digest is attached to the original message and sent to the receiver.
- The receiver receives the original message and encrypted digest and separates the two. The receiver implements the hash function on the original message to create the second digest, and it also decrypts the received digest by using the public key of the sender. If both the digests are same, then all the aspects of security are preserved.

At the Sender site

DIWAKAR EDUCATION HUB



At the Receiver site



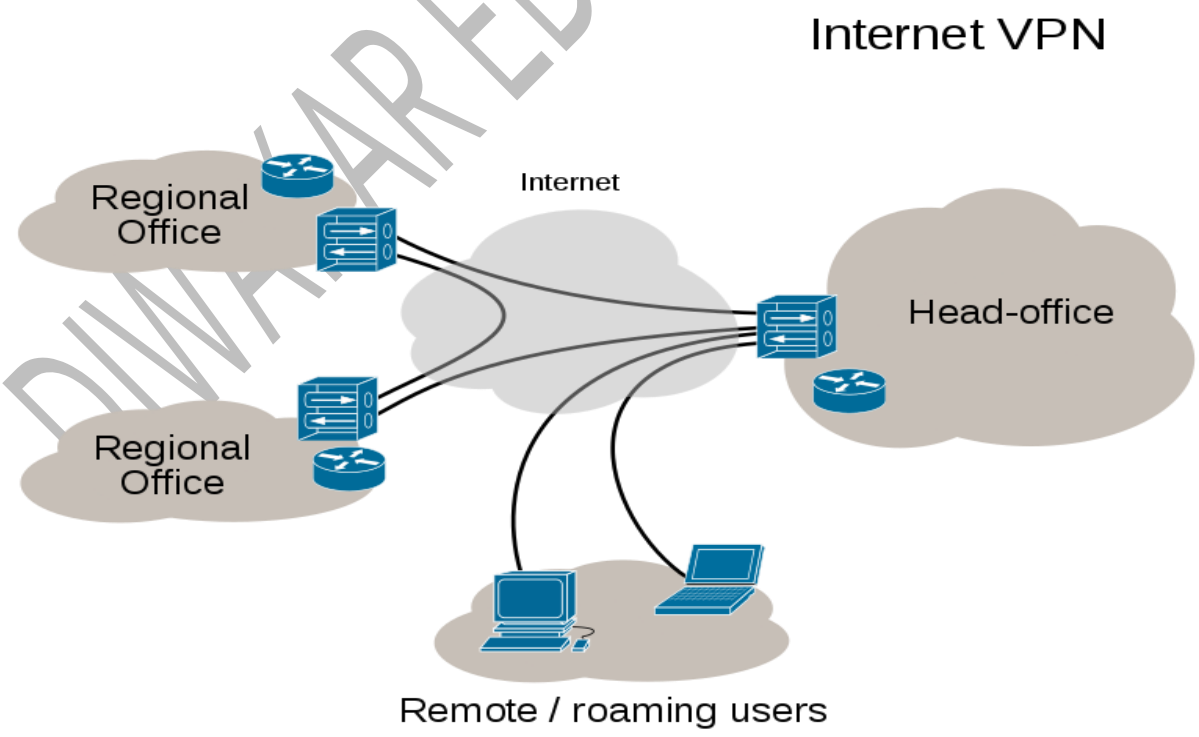
Virtual Private Networks VPN

A virtual private network (VPN) is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible. A VPN provides varying levels of security so that traffic sent through the VPN connection stays isolated from other computers on the intermediate network, either through the use of a dedicated connection from one “end” of the VPN to the other, or through encryption. VPNs can connect individual users to a remote network or connect multiple networks together.

For example, users may use a VPN to connect to their work computer terminal from home and access their email, files, images, etc.

Through VPNs, users are able to access resources on remote networks, such as files, printers, databases, or internal websites. VPN remote users get the impression of being directly connected to the central network via a point-to-point link.

An image of VPN



DIWAKAR EDUCATION HUB

VPN systems can be classified by:

- the protocols used to tunnel the traffic
- the tunnel's termination point, i.e., customer edge or network-provider edge
- whether they offer site-to-site or remote-access connectivity
- the levels of security provided
- the OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity

Security mechanisms

VPNs typically require remote access to be authenticated and make use of encryption techniques to prevent disclosure of private information.

VPNs provide security through tunneling protocols and security procedures such as encryption. Their security model provides:

- Confidentiality such that even if traffic is sniffed, an attacker would only see encrypted data which he/she cannot understand
- Allowing sender authentication to prevent unauthorized users from accessing the VPN
- Message integrity to detect any instances of transmitted messages having been tampered with

Secure VPN protocols include the following:

- IPSec (Internet Protocol Security) was developed by the Internet Engineering Task Force (IETF), and was initially developed for IPv6, which requires it. This standards-based security protocol is also widely used with IPv4. Layer 2 Tunneling Protocol frequently runs over IPSec. Its design meets most security goals: authentication, integrity, and confidentiality. IPSec functions through encrypting and encapsulating an IP packet inside an IPSec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic, as it does in the OpenVPN project, or secure an individual connection. A number of vendors provide remote access VPN capabilities through SSL. An

DIWAKAR EDUCATION HUB

SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.

- Datagram Transport Layer Security (DTLS), is used in Cisco AnyConnect VPN, to solve the issues SSL/TLS has with tunneling over UDP.
- Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
- Microsoft's Secure Socket Tunneling Protocol (SSTP), introduced in Windows Server 2008 and in Windows Vista Service Pack 1. SSTP tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL 3.0 channel.
- MPVPN (Multi Path Virtual Private Network). Ragula Systems Development Company owns the registered trademark "MPVPN".
- Secure Shell (SSH) VPN – OpenSSH offers VPN tunneling (distinct from port forwarding) to secure remote connections to a network or inter-network links. OpenSSH server provides a limited number of concurrent tunnels and the VPN feature itself does not support personal authentication.

Authentication

Tunnel endpoints must authenticate before secure VPN tunnels can be established.

User-created remote access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods.

Network-to-network tunnels often use passwords or digital certificates, as they permanently store the key to allow the tunnel to establish automatically and without intervention from the user.

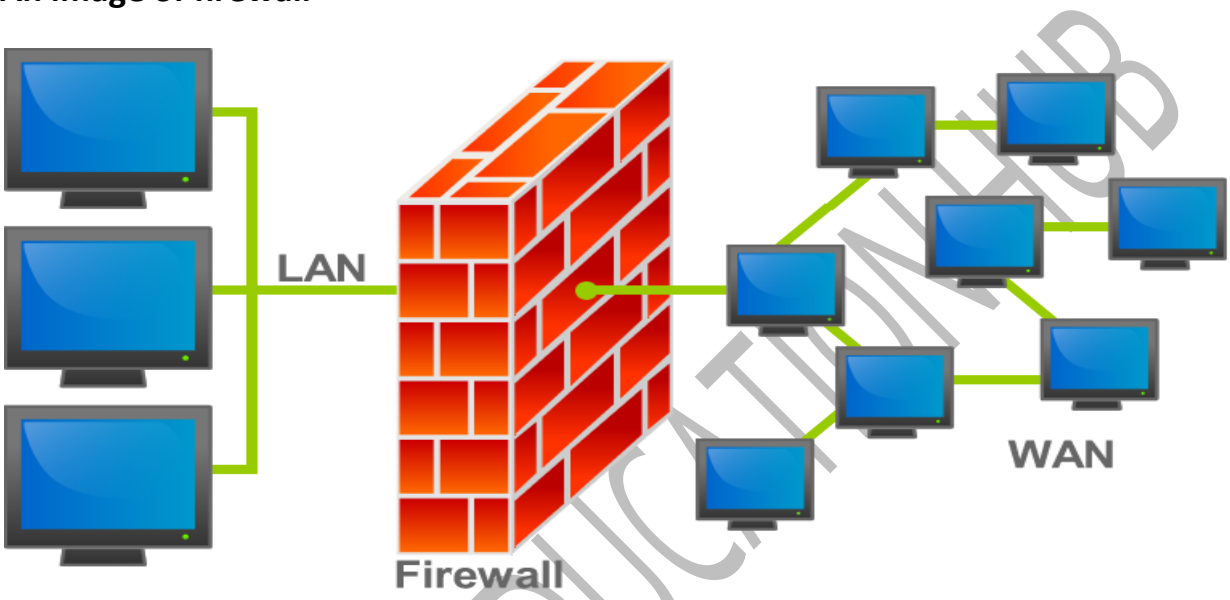
Firewalls

A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted.

DIWAKAR EDUCATION HUB

Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

An image of firewall



An example of a user interface for a firewall on Ubuntu



Evolution

First generation: packet filters

The first paper published on firewall technology was in 1988, when engineers from Digital Equipment Corporation (DEC) developed filter systems known as packet filter firewalls. This fairly basic system was the first generation of what became a highly involved and technical internet security feature. At AT&T Bell Labs, Bill Cheswick and Steve Bellovin were continuing their research in packet filtering and developed a working model for their own company based on their original first generation architecture.

Packet filters act by inspecting the "packets" which transfer between computers on the Internet. If a packet matches the packet filter's set of rules, the packet filter will drop (silently discard) the packet, or reject it (discard it, and send "error responses" to the source).

This type of packet filtering pays no attention to whether a packet is part of an existing stream of traffic (i.e. it stores no information on connection "state"). Instead, it filters each packet based only on information contained in the packet itself (most commonly using a combination of the packet's source and destination address, its protocol, and, for TCP and UDP traffic, the port number).

TCP and UDP protocols constitute most communication over the Internet, and because TCP and UDP traffic by convention uses well known ports for particular types of traffic, a "stateless" packet filter can distinguish between, and thus control, those types of traffic (such as web browsing, remote printing, email transmission, file transfer), unless the machines on each side of the packet filter are both using the same non-standard ports.

Packet filtering firewalls work mainly on the first three layers of the OSI reference model, which means most of the work is done between the network and physical layers, with a little bit of peeking into the transport layer to figure out source and destination port numbers. When a packet originates from the sender and filters through a firewall, the device checks for matches to any of the packet filtering rules that are configured in the firewall and drops or rejects the packet accordingly. When the packet passes through the firewall, it filters the packet on a protocol/port number basis (GSS). For example, if a rule in the firewall exists to block telnet access, then the firewall will block the TCP protocol for port number 23.

DIWAKAR EDUCATION HUB

Second generation: "stateful" filters

From 1989-1990 three colleagues from AT&T Bell Laboratories, Dave Presetto, Janardan Sharma, and Kshitij Nigam, developed the second generation of firewalls, calling them circuit level firewalls.

Second-generation firewalls perform the work of their first-generation predecessors but operate up to layer 4 (transport layer) of the OSI model. This is achieved by retaining packets until enough are available to make a judgement about its state. Known as stateful packet inspection, it records all connections passing through it and determines whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection. Though static rules are still used, these rules can now contain connection state as one of their test criteria.

Certain denial-of-service attacks bombard the firewall with thousands of fake connection packets in an attempt to overwhelm it by filling its connection state memory.

Third generation: application layer

The key benefit of application layer filtering is that it can "understand" certain applications and protocols (such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP)). This is useful as it is able to detect if an unwanted protocol is attempting to bypass the firewall on an allowed port, or detect if a protocol is being abused in any harmful way.

The existing deep packet inspection functionality of modern firewalls can be shared by Intrusion prevention systems (IPS).

Another axis of development is about integrating identity of users into Firewall rules. Many firewalls provide such features by binding user identities to IP or MAC addresses, which is very approximate and can be easily turned around.

Types

There are different types of firewalls depending on where the communication is taking place, where the communication is intercepted and the state that is being traced.

DIWAKAR EDUCATION HUB

Network layer or packet filters

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. The term "packet filter" originated in the context of BSD operating systems.

Network layer firewalls generally fall into two sub-categories, stateful and stateless. Stateful firewalls maintain context about active sessions, and use that "state information" to speed packet processing. Any existing network connection can be described by several properties, including source and destination IP address, UDP or TCP ports, and the current stage of the connection's lifetime (including session initiation, handshaking, data transfer, or completion connection). If a packet does not match an existing connection, it will be evaluated according to the ruleset for new connections. If a packet matches an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing.

Stateless firewalls require less memory, and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However, they cannot make more complex decisions based on what stage communications between hosts have reached.

Modern firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, of the source, and many other attributes.

Commonly used packet filters on various versions of Unix are ipf (various), ipfw (FreeBSD/Mac OS X), pf (OpenBSD, and all other BSDs), iptables/ipchains (Linux).

Application-layer

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender).

DIWAKAR EDUCATION HUB

On inspecting all packets for improper content, firewalls can restrict or prevent outright the spread of networked computer worms and trojans. The additional inspection criteria can add extra latency to the forwarding of packets to their destination.

Application firewalls function by determining whether a process should accept any given connection. Application firewalls accomplish their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. Application firewalls that hook into socket calls are also referred to as socket filters. Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis. Generally, prompts are used to define rules for processes that have not yet received a connection. It is rare to find application firewalls not combined or used in conjunction with a packet filter.

Also, application firewalls further filter connections by examining the process ID of data packets against a ruleset for the local process involved in the data transmission. The extent of the filtering that occurs is defined by the provided ruleset. Given the variety of software that exists, application firewalls only have more complex rulesets for the standard services, such as sharing services. These per process rulesets have limited efficacy in filtering every possible association that may occur with other processes. Also, these per process ruleset cannot defend against modification of the process via exploitation, such as memory corruption exploits. Because of these limitations, application firewalls are beginning to be supplanted by a new generation of application firewalls that rely on mandatory access control (MAC), also referred to as sandboxing, to protect vulnerable services.

Proxies

A proxy server (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user.

DIWAKAR EDUCATION HUB

Proxies make tampering with an internal system from the external network more difficult and misuse of one internal system would not necessarily cause a security breach exploitable from outside the firewall (as long as the application proxy remains intact and properly configured). Conversely, intruders may hijack a publicly reachable system and use it as a proxy for their own purposes; the proxy then masquerades as that system to other internal machines. While use of internal address spaces enhances security, crackers may still employ methods such as IP spoofing to attempt to pass packets to a target network.

Network address translation

Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918. Firewalls often have such functionality to hide the true address of protected hosts. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defense against network reconnaissance.

There are several types of firewall techniques:

- Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
- Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

DIWAKAR EDUCATION HUB

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

Mobile Technology & Reach

Mobile technology has grown leaps and bounds over the last few decades. The journey from the clunky wireless phone to sleek smartphone has been peppered by a number of amazing innovations and discoveries.

With the 3G mobiles available today, users can do a lot more with their smartphones than just sending a voicemail or SMS. They can browse the web, check the weather, read a book, prepare a to-do-list, carry their favorite music around, find their way around a new city with GPRS, and do much more.



Mobile Marketing Technology & Reach

In such a scenario, every business person willing to practice the mobile marketing technique has to be aware about the following top 5 ways in which mobile technologies have changed the way users interact with mobile devices −

Anywhere anytime access

Unlike laptops and desktops, tablet and mobile devices are easy to carry around. Users can access the internet in their mobile devices at anytime and anywhere and it has decreased use of the laptops.

Mobile Apps are easier than websites

Companies that have an online customer base for instance e-commerce portals have noticed that the sales and subscriptions they get from their apps are higher in comparison to that of their websites. This means, online purchasing from the mobile phones are easier.

Advertisements should be personalized

Most of the users feel that the mobile are more personal device than say a laptop or a desktop. Therefore, they expect that the content they receive on their mobile phones must be personalized as well.

Social media is a prime channel

Whether your customers are business professionals, students, home-makers, teenagers etc., commonly, they spend more than 3 hours a week on social media channels, such as Twitter, Facebook etc. Surprisingly, most of these customers access these channels on their smartphones.

Mobiles are turning into mini-computers

Slowly but surely technicians and developers are packing the mobile phones with computer-like features. With bigger screens, faster performance, optimum storage capacity, longer battery life, and a ton of productivity booster

applications. The evolution of phones from a simple calling device to multi-tasking-pocket-size computers has revolutionized the world.



Global System for Mobile communication (GSM)

GSM

GSM stands for Global System for Mobile communications. GSM is one of the most widely used digital wireless telephony system. It was developed in Europe in 1980s and is now international standard in Europe, Australia, Asia and Africa. Any GSM handset with a SIM (Subscriber Identity Module) card can be used in any country that uses this standard. Every SIM card has a unique identification number. It has memory to store applications and data like phone numbers, processor to carry out its functions and software to send and receive messages

GSM technology uses TDMA (Time Division Multiple Access) to support up to eight calls simultaneously. It also uses encryption to make the data more secure.

The frequencies used by the international standard is 900 MHz to 1800 MHz However, GSM phones used in the US use 1900 MHz frequency and hence are not compatible with the international system.

- GSM stands for **G**lobal **S**ystem for **M**obile Communication. It is a digital cellular technology used for transmitting mobile voice and data services.

- The concept of GSM emerged from a cell-based mobile radio system at Bell Laboratories in the early 1970s.
- GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard.
- GSM is the most widely accepted standard in telecommunications and it is implemented globally.
- GSM is a circuit-switched system that divides each 200 kHz channel into eight 25 kHz time-slots. GSM operates on the mobile communication bands 900 MHz and 1800 MHz in most parts of the world. In the US, GSM operates in the bands 850 MHz and 1900 MHz.
- GSM owns a market share of more than 70 percent of the world's digital cellular subscribers.
- GSM makes use of narrowband Time Division Multiple Access (TDMA) technique for transmitting signals.
- GSM was developed using digital technology. It has an ability to carry 64 kbps to 120 Mbps of data rates.
- Presently GSM supports more than one billion mobile subscribers in more than 210 countries throughout the world.
- GSM provides basic to advanced voice and data services including roaming service. Roaming is the ability to use your GSM phone number in another GSM network.

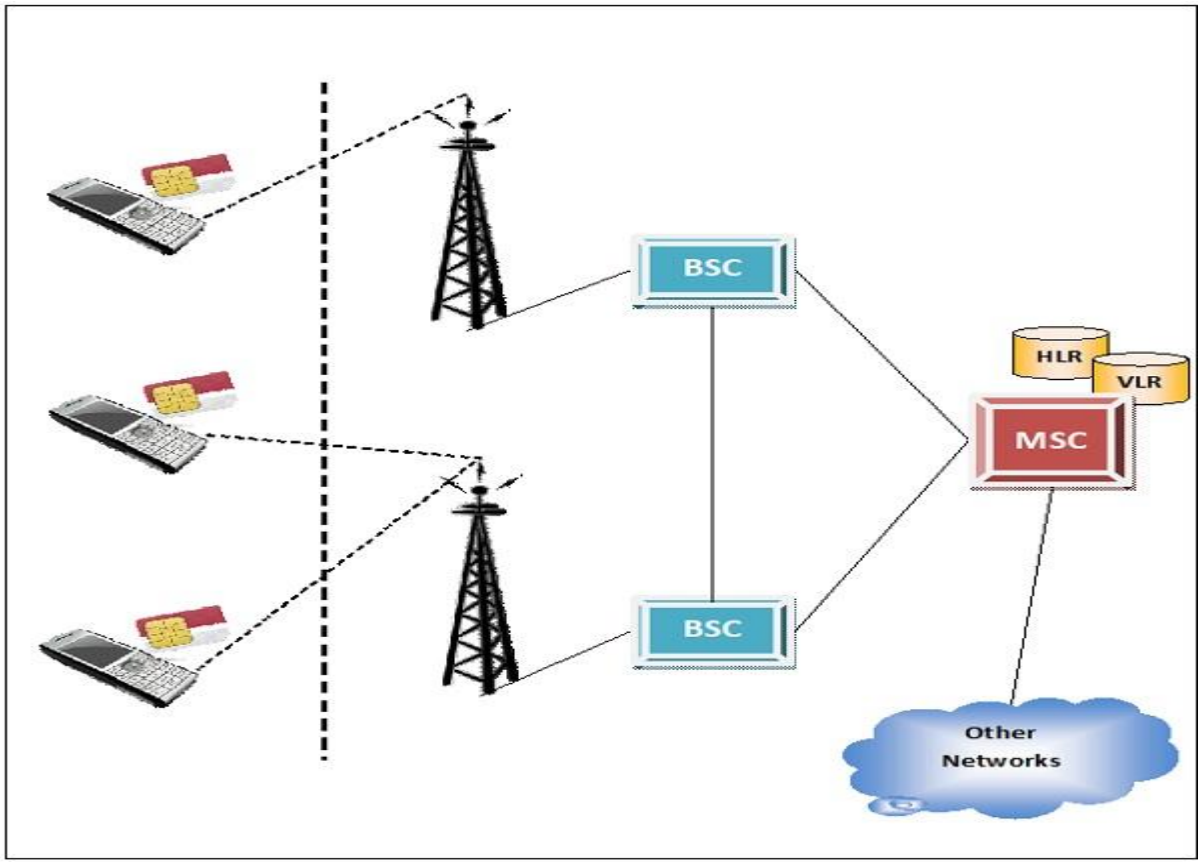
Global System for Mobile communication (GSM) architecture comprises of the following components −

- **Mobile Station** : The mobile station is the mobile phone, which comprises of the mobile handset and SIM card. The mobile handset comprises of the transceiver, the display and its processor. SIM stands for SubscriberIdentity Module. It is a removable chip that contains account information of the subscriber and connects the handset to the mobile network system.
- **Air Interface** : The air interface is the interface between the mobile station and the Base Transceiver Station. It is also called the UM interface as it is analogous to U interface of ISDN. GSM runs on a range of frequencies including 900, 1800 and 1900 MHz. It uses frequency division duplex (FDD) that divides the channel into several sub-bands. Each of the sub-bands are shared by multiple mobiles through time division multiplexing (TDM).

- **Base Station Subsystem** : It is a connection between the mobile station and the mobile switching center. It comprises of two parts −
    - **Base Transceiver Station (BTU) –** It handles the protocols for communication with the mobile stations using radio transceivers.
    - **Base Station Controller (BSC) –** It controls the radio resources of the cell, interfaces with the mobile switching center and also handles handoff.
- **Mobile Switching Center (MSC)** : It provides the basic network connection to the mobile network and gives access to other networks like PSTN, ISDN and the Internet. It maintains databases to locate mobiles. The databases are −
    - **Visitor Location Register (VLR) –** It is a database of nearby mobiles that are managed by a cell.
    - **Home Location Register (HLR) –** It is a database of last known location of each mobile.
    - **International Mobile Equipment Identity (IMEI) –** It is an account of all the mobiles wherein each mobile is identified by its own IMEI number.

Diagrammatic Representation of GSM Architecture

DIWAKAR EDU



Why GSM?

Listed below are the features of GSM that account for its popularity and wide acceptance.

- Improved spectrum efficiency
- International roaming
- Low-cost mobile sets and base stations (BSs)
- High-quality speech
- Compatibility with Integrated Services Digital Network (ISDN) and other telephone company services
- Support for new services

User Services

GSM offers much more than just voice telephony. Contact your local GSM network operator to the specific services that you can avail.

GSM offers three basic types of services:

- Telephony services or teleservices
- Data services or bearer services
- Supplementary services

Teleservices

The abilities of a Bearer Service are used by a Teleservice to transport data. These services are further transited in the following ways:

Voice Calls

The most basic Teleservice supported by GSM is telephony. This includes full-rate speech at 13 kbps and emergency calls, where the nearest emergency-service provider is notified by dialing three digits.

Videotext and Facsmile

Another group of teleservices includes Videotext access, Teletex transmission, Facsmile alternate speech and Facsmile Group 3, Automatic Facsmile Group, 3 etc.

Short Text Messages

Short Messaging Service (SMS) service is a text messaging service that allows sending and receiving text messages on your GSM mobile phone. In addition to simple text messages, other text data including news, sports, financial, language, and location-based data can also be transmitted.

Bearer Services

Data services or Bearer Services are used through a GSM phone. to receive and send data is the essential building block leading to widespread mobile Internet access and mobile data transfer. GSM currently has a data transfer rate of 9.6k. New developments that will push up data transfer rates for GSM users are HSCSD (high speed circuit switched data) and GPRS (general packet radio service) are now available.

Supplementary Services

Supplementary services are additional services that are provided in addition to teleservices and bearer services. These services include caller identification, call forwarding, call waiting, multi-party conversations, and barring of outgoing (international) calls, among others. A brief description of supplementary services is given here:

- **Conferencing** : It allows a mobile subscriber to establish a multiparty conversation, i.e., a simultaneous conversation between three or more subscribers to setup a conference call. This service is only applicable to normal telephony.
- **Call Waiting** : This service notifies a mobile subscriber of an incoming call during a conversation. The subscriber can answer, reject, or ignore the incoming call.
- **Call Hold** : This service allows a subscriber to put an incoming call on hold and resume after a while. The call hold service is applicable to normal telephony.
- **Call Forwarding** : Call Forwarding is used to divert calls from the original recipient to another number. It is normally set up by the subscriber himself. It can be used by the subscriber to divert calls from the Mobile Station when the subscriber is not available, and so to ensure that calls are not lost.
- **Call Barring** : Call Barring is useful to restrict certain types of outgoing calls such as ISD or stop incoming calls from undesired numbers. Call barring is a flexible service that enables the subscriber to conditionally bar calls.
- **Number Identification** : There are following supplementary services related to number identification:
    - **Calling Line Identification Presentation** : This service displays the telephone number of the calling party on your screen.
    - **Calling Line Identification Restriction** : A person not wishing their number to be presented to others subscribes to this service.
    - **Connected Line Identification Presentation** : This service is provided to give the calling party the telephone number of the person to whom they are connected. This service is useful in situations such as forwarding's where the number connected is not the number dialled.
    - **Connected Line Identification Restriction** : There are times when the person called does not wish to have their number presented and so

they would subscribe to this person. Normally, this overrides the presentation service.

- **Malicious Call Identification** : The malicious call identification service was provided to combat the spread of obscene or annoying calls. The victim should subscribe to this service, and then they could cause known malicious calls to be identified in the GSM network, using a simple command.

- **Advice of Charge (AoC)** : This service was designed to give the subscriber an indication of the cost of the services as they are used. Furthermore, those service providers who wish to offer rental services to subscribers without their own SIM can also utilize this service in a slightly different form. AoC for data calls is provided on the basis of time measurements.
- **Closed User Groups (CUGs)** : This service is meant for groups of subscribers who wish to call only each other and no one else.
- **Unstructured supplementary services data (USSD)** : This allows operator-defined individual services.

CDMA

Code Division Multiple Access (CDMA) is a sort of multiplexing that facilitates various signals to occupy a single transmission channel. It optimizes the use of available bandwidth. The technology is commonly used in ultra-high-frequency (UHF) cellular telephone systems, bands ranging between the 800-MHz and 1.9-GHz.

CDMA Overview

Code Division Multiple Access system is very different from time and frequency multiplexing. In this system, a user has access to the whole bandwidth for the entire duration. The basic principle is that different CDMA codes are used to distinguish among the different users.

Techniques generally used are direct sequence spread spectrum modulation (DS-CDMA), frequency hopping or mixed CDMA detection (JDCDMA). Here, a signal is generated which extends over a wide bandwidth. A code called **spreading code** is used to perform this action. Using a group of codes, which are orthogonal to each

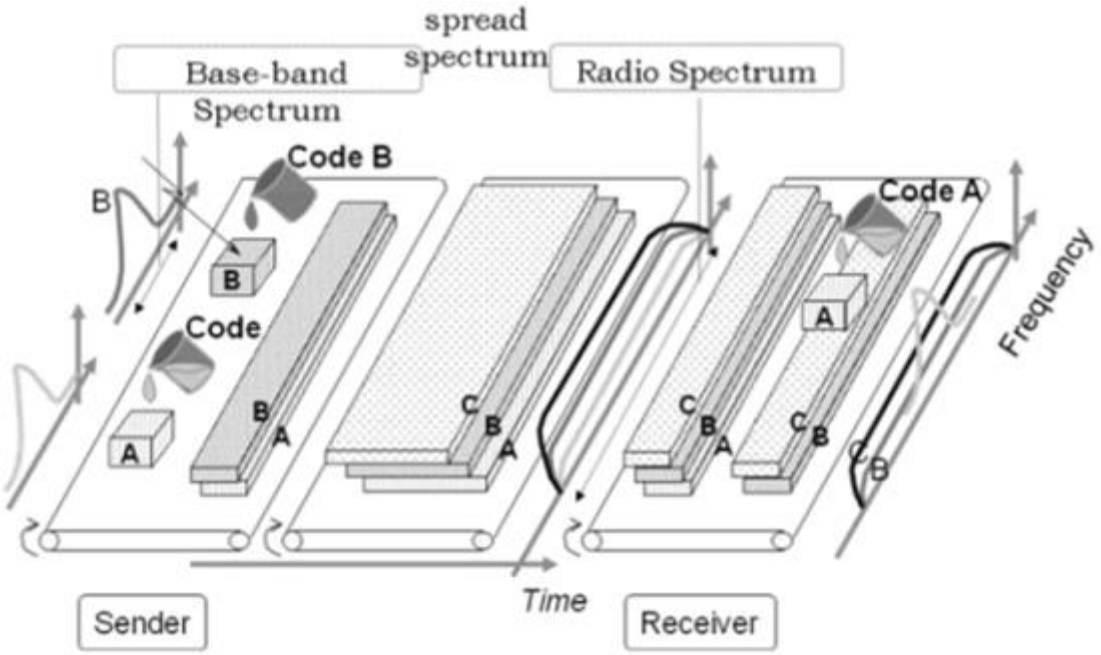
other, it is possible to select a signal with a given code in the presence of many other signals with different orthogonal codes.

How Does CDMA Work?

CDMA allows up to 61 concurrent users in a 1.2288 MHz channel by processing each voice packet with two PN codes. There are 64 Walsh codes available to differentiate between calls and theoretical limits. Operational limits and quality issues will reduce the maximum number of calls somewhat lower than this value.

In fact, many different "signals" baseband with different spreading codes can be modulated on the same carrier to allow many different users to be supported. Using different orthogonal codes, interference between the signals is minimal. Conversely, when signals are received from several mobile stations, the base station is capable of isolating each as they have different orthogonal spreading codes.

The following figure shows the technicality of the CDMA system. During the propagation, we mixed the signals of all users, but by that you use the same code as the code that was used at the time of sending the receiving side. You can take out only the signal of each user.



CDMA Capacity

The factors deciding the CDMA capacity are −

- Processing Gain
- Signal to Noise Ratio
- Voice Activity Factor
- Frequency Reuse Efficiency

Capacity in CDMA is soft, CDMA has all users on each frequency and users are separated by code. This means, CDMA operates in the presence of noise and interference.

In addition, neighboring cells use the same frequencies, which means no re-use. So, CDMA capacity calculations should be very simple. No code channel in a cell, multiplied by no cell. But it is not that simple. Although not available code channels are 64, it may not be possible to use a single time, since the CDMA frequency is the same.

Centralized Methods

- The band used in CDMA is 824 MHz to 894 MHz (50 MHz + 20 MHz separation).
- Frequency channel is divided into code channels.
- 1.25 MHz of FDMA channel is divided into 64 code channels.

Processing Gain

CDMA is a spread spectrum technique. Each data bit is spread by a code sequence. This means, energy per bit is also increased. This means that we get a gain of this.

P (gain) = 10log (W/R)

W is Spread Rate

R is Data Rate

For CDMA P (gain) = 10 log (1228800/9600) = 21dB

This is a gain factor and the actual data propagation rate. On an average, a typical transmission condition requires a signal to the noise ratio of 7 dB for the adequate quality of voice.

Translated into a ratio, signal must be five times stronger than noise.

Actual processing gain = P (gain) - SNR

= 21 – 7 = 14dB

CDMA uses variable rate coder

The Voice Activity Factor of 0.4 is considered = -4dB.

Hence, CDMA has 100% frequency reuse. Use of same frequency in surrounding cells causes some additional interference.

In CDMA frequency, reuse efficiency is 0.67 (70% eff.) = -1.73dB

Advantages of CDMA

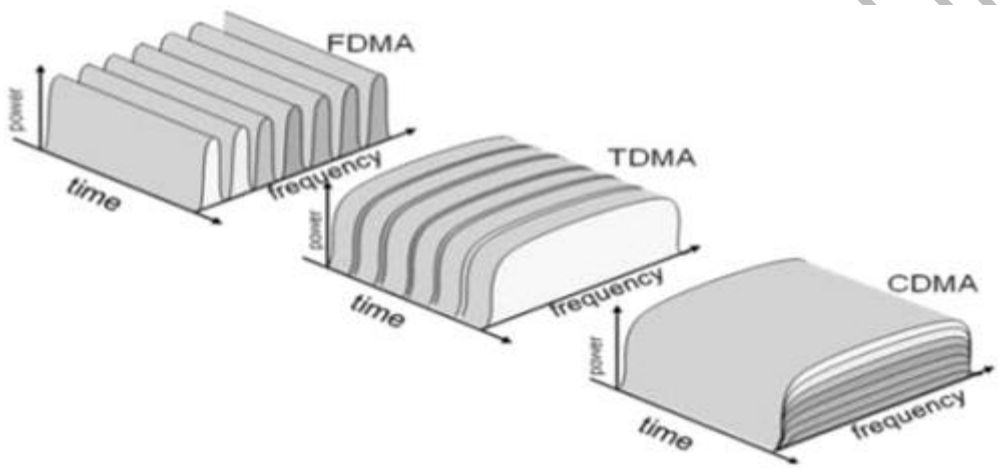
CDMA has a soft capacity. The greater the number of codes, the more the number of users. It has the following advantages −

- CDMA requires a tight power control, as it suffers from near-far effect. In other words, a user near the base station transmitting with the same power will drown the signal latter. All signals must have more or less equal power at the receiver
- Rake receivers can be used to improve signal reception. Delayed versions of time (a chip or later) of the signal (multipath signals) can be collected and used to make decisions at the bit level.
- Flexible transfer may be used. Mobile base stations can switch without changing operator. Two base stations receive mobile signal and the mobile receives signals from the two base stations.
- Transmission Burst − reduces interference.

Disadvantages of CDMA

The disadvantages of using CDMA are as follows −

- The code length must be carefully selected. A large code length can induce delay or may cause interference.
- Time synchronization is required.
- Gradual transfer increases the use of radio resources and may reduce capacity.
- As the sum of the power received and transmitted from a base station needs constant tight power control. This can result in several handovers.



Usage

- It is used in the Global Positioning System (GPS).
- It is used by several mobile phone companies (e.g. Qualcomm standard IS-2000 also known as CDMA2000)
- W-CDMA is used in UTMS 3G mobile phone standard.
- CDMA has been used in OmniTRACS satellite system for transportation.

Categories of CDMA

- Synchronous CDMA (orthogonal codes)
- Asynchronous CDMA (pseudorandom codes)

Difference between CDMA and GSM

The major difference between CDMA and GSM are given below.

Criteria	CDMA	GSM
Technology	CDMA is based on spread-spectrum technology which makes the optimum use of available bandwidth.	GSM operates on the wedge spectrum. it uses both time division multiple access (TDMA) and frequency division multiple access (fdma). TDMA provide multi-user access by cutting up the channel into different time slice and fdma provides the multi-user access by separating the used frequency.
Security	CDMA is more secure than GSM.	GSM is less secure than CDMA.
Global reach	CDMA is used in usa and some part of canada and japan. CDMA is used only by 24% of the users worldwide.	GSM is used over 80% of the world network in over 210 countries. GSM is used 76% of the users worldwide.
Data Transfer Rate	CDMA has faster data transfer as compared to GSM.	GSM has slower data transfer as compared to CDMA.
Radiation exposure	CDMA phones emits less radiation than GSM phones.	GSM phones emits continuous wave pulses and emits almost 28 times more radiation than CDMA phones.

Technical Challenges of Mobile Computing

Mobile Computing is defined as a computing environment which is mobile and moves along with the user. There are various number of challenges that affected mobile computing and it has to overcome them. Some of the major technical challenges faced by mobile computing are:

1. Mobility

2. Wireless Medium

3. Portability

These are explained as following below:

1. Mobility:
It is the most important aspect of mobile computing, but it has to face the certain challenges which are :

- Auto configuration of the system, as the environment of the system is developing continuously. Hence for every change, it has to configure itself to the new situation.
- Location management is also a big objection in mobility. To manage the location, following tasks are to be performed regularly over a fixed period of time.
    - Track user's call.
    - Update user's position and data.
- To maintain the heterogenity is also a big task as the system is keep moving in a large variation of situations
- Range of spectrum.
- Verification of security.

2. Wireless Medium:
The transmission medium in mobile computing is wireless, therefore the following points are considered:

- Various interferences occurs in the mobile computing by the different elements in the environment.
- Accuracy and quantity of bandwidth should be sufficient.
- Network cost is feasible.

3. Portability:
This means that the communication device moves, for eg. mobile phones. The following mobile constraints are to be considered as the devices are also mobile:

DIWAKAR EDUCATION HUB

- Minimum number of resources are used.
- Security is very less, as security risks include the processing of fake transactions, unauthorized access of data and program files, and the physical theft or damage of the device.
- Restrictions of the battery.

Mobile IP

This is an **IETF (Internet Engineering Task Force)** standard communications protocol designed to allow mobile devices' (such as laptop, PDA, mobile phone, etc.) users to move from one network to another while maintaining their permanent IP (Internet Protocol) address.

Defined in RFC (Request for Comments) 2002, mobile IP is an enhancement of the internet protocol (IP) that adds mechanisms for forwarding internet traffic to mobile devices (known as mobile nodes) when they are connecting through other than their home network.

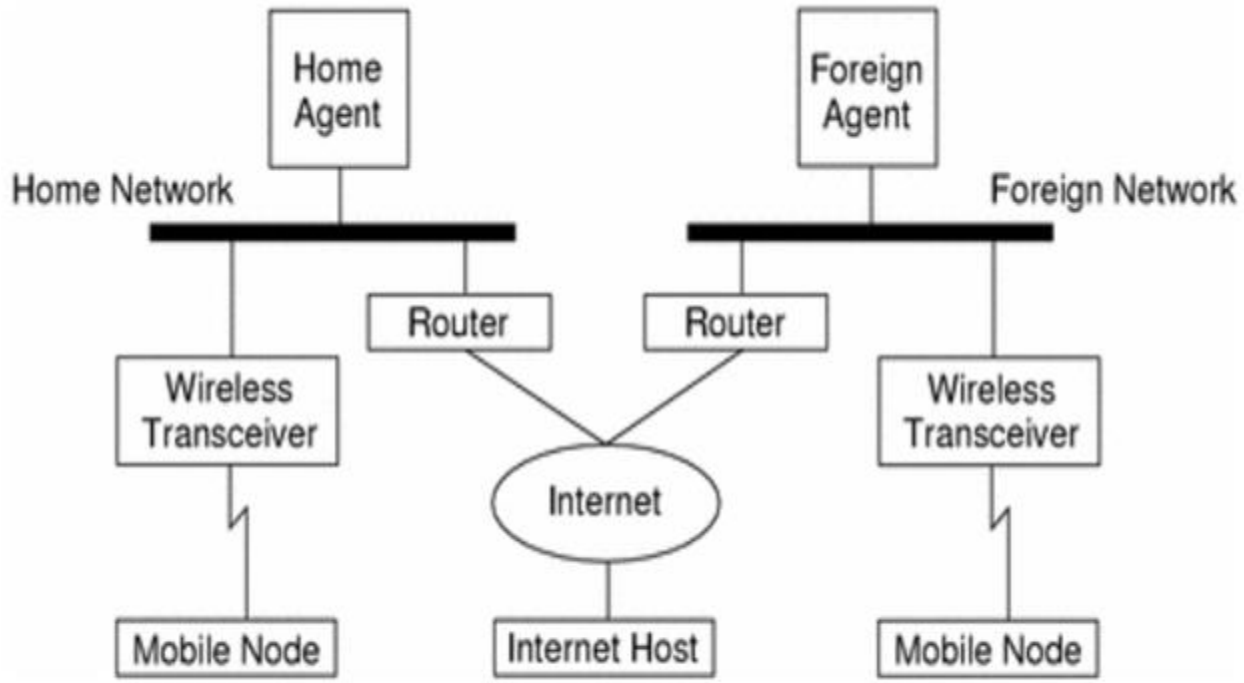


Fig: Mobile IP topology

The following case shows how a datagram moves from one point to another within the Mobile IP framework.

- First of all, the internet host sends a datagram to the mobile node using the mobile node's home address (normal IP routing process).
- If the mobile node (MN) is on its home network, the datagram is delivered through the normal IP (Internet Protocol) process to the mobile node. Otherwise the home agent picks up the datagram.
- If the mobile node (MN) is on foreign network, the home agent (HA) forwards the datagram to the foreign agent.
- The foreign agent (FA) delivers the datagram to the mobile node.
- Datagrams from the MN to the Internet host are sent using normal IP routing procedures. If the mobile node is on a foreign network, the packets are delivered to the foreign agent. The FA forwards the datagram to the Internet host.

In the case of wireless communications, the above illustrations depict the use of wireless transceivers to transmit the datagrams to the mobile node. Also, all datagrams between the Internet host and the MN use the mobile node's home address regardless of whether the mobile node is on a home or foreign network. The care-of address (COA) is used only for communication with mobility agents and is never seen by the Internet host.

Components of Mobile IP

The mobile IP has following three components as follows:

1. Mobile Node (MN)

The mobile node is an end system or device such as a cell phone, PDA (Personal Digital assistant), or laptop whose software enables network roaming capabilities.

2. Home Agent (HA)

The home agent provides several services for the mobile node and is located in the home network. The tunnel for packets towards the mobile node starts at home agent. The home agent maintains a location registry, i.e. it is informed of

DIWAKAR EDUCATION HUB

the mobile node's location by the current COA (care of address). Following alternatives for the implementation of an HA exist.

- Home agent can be implemented on a **router** that is responsible for the home network. This is obviously the best position, because without optimization to mobile IP, all packets for the MN have to go through the router anyway.
- If changing the router's software is not possible, the home agent could also be implemented on an **arbitrary node** in the subset. One biggest disadvantage of this solution is the double crossing of the router by the packet if the MN is in a foreign network. A packet for the mobile node comes in via the router; the HA sends it through the tunnel which again crosses the router.

3. Foreign Agent (FA)

The foreign agent can provide several services to the mobile node during its visit to the foreign network. The FA can have the COA (care or address) acting as a tunnel endpoint and forwarding packets to the MN. The foreign agent can be the default router for the MN.

Foreign agent can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.

In short, FA is a router that may function as the point of attachment for the mobile node when it roams to a foreign network delivers packets from the home agent to the mobile node.

4. Care of Address (COA)

The Care- of- address defines the current location of the mobile node from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the mobile node is done using a tunnel. To be more precise, the COA marks the endpoint of the tunnel, i.e. the address where packets exit the tunnel.

There are two different possibilities for the location of the care of address:

DIWAKAR EDUCATION HUB

1. **Foreign Agent COA:** The COA could be located at the foreign agent, i.e. the COA is an IP address of the foreign agent. The foreign agent is the tunnel endpoint and forwards packets to the MN. Many MN using the FA can share this COA as common COA.
2. **Co-located COA:** The COA is co-located if the MN temporarily acquired an additional IP address which acts as a COA. This address is now topologically correct, and the tunnel endpoint is at the mobile node. Co-located address can be acquired using services such as DHCP. One problem associated with this approach is need for additional addresses if MNs request a COA. This is not always a good idea considering the scarcity of IPv4 addresses.

5. Correspondent Node (CN)

At least one partner is needed for communication. The correspondent node represents this partner for the MN. The correspondent node can be a fixed or mobile node.

6. Home Network

The home network is the subset the MN belongs to with respect to its IP address. No mobile IP support is needed within this network.

7. Foreign network

The foreign network is the current subset the MN visits and which is not the home network.

Process of Mobile IP

The mobile IP process has following three main phases, which are:

1. Agent Discovery

During the agent discovery phase the HA and FA advertise their services on the network by using the ICMP router discovery protocol (IROP).

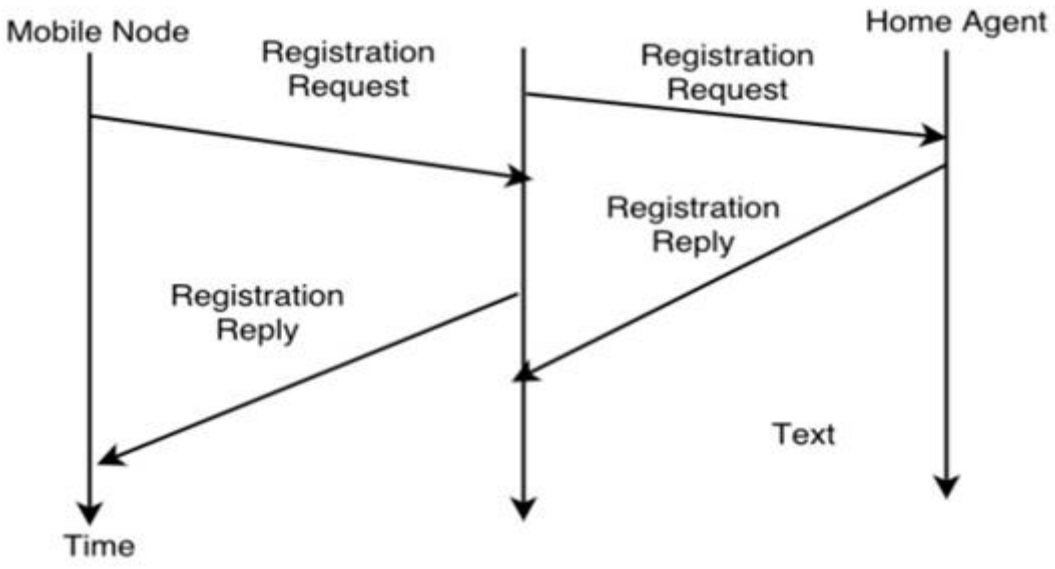
Mobile IP defines two methods: agent advertisement and agent solicitation which are in fact router discovery methods plus extensions.

DIWAKAR EDUCATION HUB

- **Agent advertisement:** For the first method, FA and HA advertise their presence periodically using special agent advertisement messages. These messages advertisement can be seen as a beacon broadcast into the subnet. For this advertisement internet control message protocol (ICMP) messages according to RFC 1256, are used with some mobility extensions.
- **Agent solicitation:** If no agent advertisements are present or the inter arrival time is too high, and an MN has not received a COA, the mobile node must send agent solicitations. These solicitations are again bases on RFC 1256 for router solicitations.

2. Registration

The main purpose of the registration is to inform the home agent of the current location for correct forwarding of packets.



Registration can be done in two ways depending on the location of the COA.

- **If the COA is at the FA**, the MN sends its registration request containing the COA to the FA which is forwarding the request to the HA. The HA now set up a **mobility binding** containing the mobile node's home IP address and the current COA.

Additionally, the mobility biding contains the lifetime of the registration which is negotiated during the registration process. Registration expires automatically after the lifetime and is deleted; so a mobile node should register before expiration. After setting up the mobility binding, the HA send a reply message back to the FA which forwards it to the MN.

- **If the COA is co-located**, registration can be very simpler. The mobile node may send the request directly to the HA and vice versa. This by the way is also the registration procedure for MNs returning to their home network.

3. Tunneling

A tunnel is used to establish a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets which are entering in a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel is achieved with the help of encapsulation.

Tunneling is also known as "**port forwarding**" is the transmission and data intended for use only within a private, usually corporate network through a public network.

Mobile Communication Protocols

Any device that does not need to remain at one place to carry out its functions is a mobile device. So laptops, smartphones and personal digital assistants are some examples of mobile devices. Due to their portable nature, mobile devices connect to networks wirelessly. Mobile devices typically use radio waves to communicate with other devices and networks. Here we will discuss the protocols used to carry out mobile communication.

Mobile communication protocols use multiplexing to send information. Multiplexing is a method to combine multiple digital or analog signals into one signal over the data channel. This ensures optimum utilization of expensive resource and time. At the destination these signals are de-multiplexed to recover individual signals.



These are the types of multiplexing options available to communication channels –

- **FDM (Frequency Division Multiplexing)** − Here each user is assigned a different frequency from the complete spectrum. All the frequencies can then simultaneously travel on the data channel.
- **TDM (Time Division Multiplexing)** − A single radio frequency is divided into multiple slots and each slot is assigned to a different user. So multiple users can be supported simultaneously.
- **CDMA (Code Division Multiplexing)** − Here several users share the same frequency spectrum simultaneously. They are differentiated by assigning unique codes to them. The receiver has the unique key to identify the individual calls.

GSM

GSM stands for Global System for Mobile communications. GSM is one of the most widely used digital wireless telephony system. It was developed in Europe in 1980s and is now international standard in Europe, Australia, Asia and Africa. Any

GSM handset with a SIM (Subscriber Identity Module) card can be used in any country that uses this standard. Every SIM card has a unique identification number. It has memory to store applications and data like phone numbers, processor to carry out its functions and software to send and receive messages

GSM technology uses TDMA (Time Division Multiple Access) to support up to eight calls simultaneously. It also uses encryption to make the data more secure.

The frequencies used by the international standard is 900 MHz to 1800 MHz However, GSM phones used in the US use 1900 MHz frequency and hence are not compatible with the international system.

CDMA

CDMA stands for Code Division Multiple Access. It was first used by the British military during World War II. After the war its use spread to civilian areas due to high service quality. As each user gets the entire spectrum all the time, voice quality is very high. Also, it is automatically encrypted and hence provides high security against signal interception and eavesdropping.

WLL

WLL stands for Wireless in Local Loop. It is a wireless local telephone service that can be provided in homes or offices. The subscribers connect to their local exchange instead of the central exchange wirelessly. Using wireless link eliminates last mile or first mile construction of network connection, thereby reducing cost and set up time. As data is transferred over very short range, it is more secure than wired networks.

WLL system consists of user handsets and a base station. The base station is connected to the central exchange as well as an antenna. The antenna transmits to and receives calls from users through terrestrial microwave links. Each base station can support multiple handsets depending on its capacity.

GPRS

GPRS stands for General Packet Radio Services. It is a packet based wireless communication technology that charges users based on the volume of data they

send rather than the time duration for which they are using the service. This is possible because GPRS sends data over the network in packets and its throughput depends on network traffic. As traffic increases, service quality may go down due to congestion, hence it is logical to charge the users as per data volume transmitted.

GPRS is the mobile communication protocol used by second (2G) and third generation (3G) of mobile telephony. It pledges a speed of 56 kbps to 114 kbps, however the actual speed may vary depending on network load.

Communication Satellites

A communication satellite is an artificial satellite that acts as a large repeater in the sky. It receives signals from the source transmitter, amplifies using transponders, and relays them to the receiver. Thus, it creates a communication channel between locations of the earth that would not have been able to communicate due to long distance or obstruction by earth's curvature.

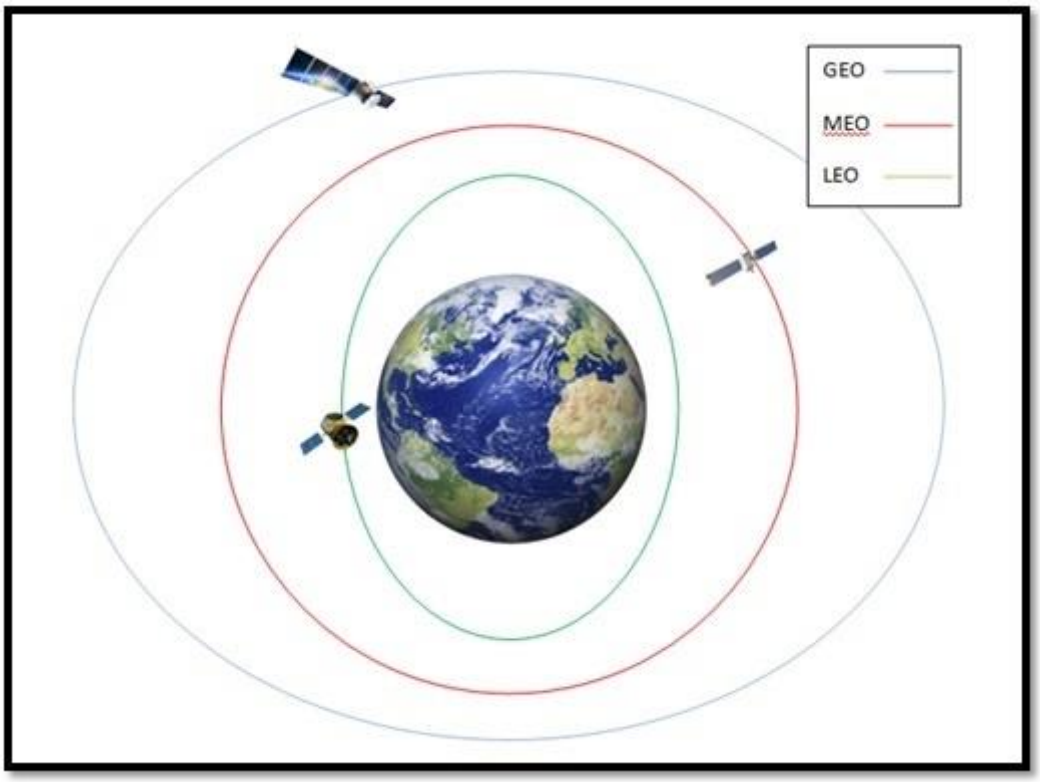
Communication satellites may be owned by government or private organizations. Presently, there are more than 2000 communication satellites in the sky. Some of its uses are −

- Internet
- Military operations
- Television
- Telephone
- Radio

Communication satellites are broadly categorized into three types depending upon the orbit in which they are placed.

- **Geostationary Satellite (GEO)** − They are at 36,000 km from the earth's surface. They have same orbital period as earth's rotation. So they appear to be still in the sky. At least 3 GEOs are needed for global coverage.
- **Medium Earth Orbit Satellite (MEO)** − They are placed between the two Van Allen belts, at a distance between 2,000 km to 36,000 km from the earth's surface. At least 10 MEOs are needed for global coverage.

- **Low Earth Orbit Satellite (LEO)** − They are situated below the Lower Van Allen belt. Their orbital altitude is 160 km to 2000 km. For global coverage, as high as 50 LEOs are required.



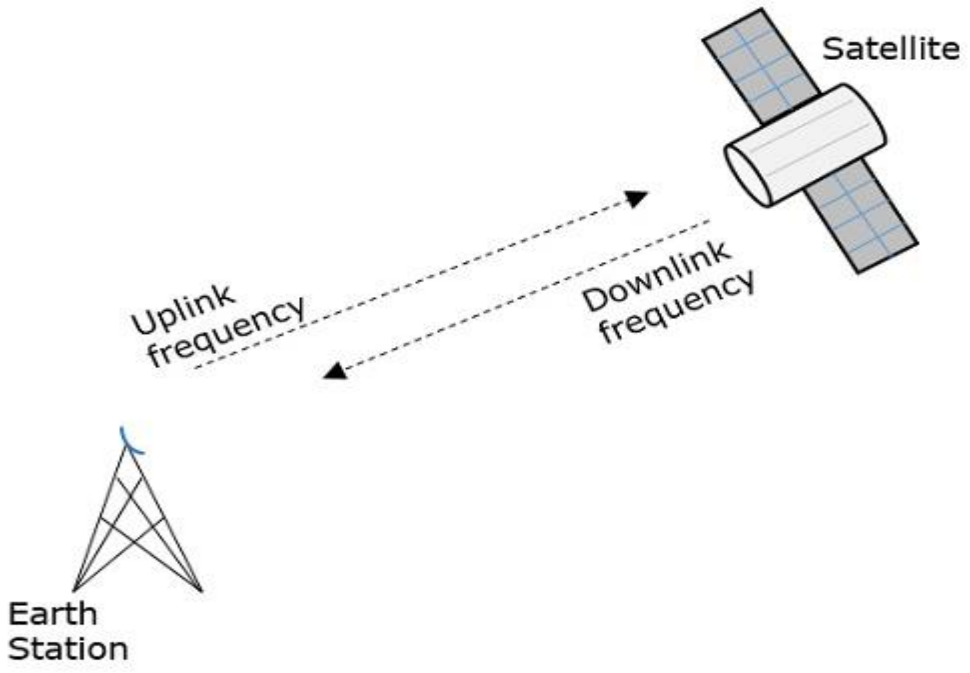
Principles of Satellite Communications

A **satellite** is a body that moves around another body in a mathematically predictable path called an **Orbit**. A communication satellite is nothing but a microwave repeater station in space that is helpful in telecommunications, radio, and television along with internet applications.

A **repeater** is a circuit which increases the strength of the signal it receives and retransmits it. But here this repeater works as a **transponder**, which changes the frequency band of the transmitted signal, from the received one.

The frequency with which the signal is sent into the space is called **Uplink frequency**, while the frequency with which it is sent by the transponder is **Downlink frequency**.

The following figure illustrates this concept clearly.



Now, a look at the advantages, disadvantages and applications of satellite communications.

Satellite Communication – Advantages

There are many Advantages of satellite communications such as −

- Flexibility
- Ease in installing new circuits
- Distances are easily covered and cost doesn't matter
- Broadcasting possibilities
- Each and every corner of earth is covered
- User can control the network

Satellite Communication – Disadvantages

Satellite communication has the following drawbacks −

- The initial costs such as segment and launch costs are too high.
- Congestion of frequencies

- Interference and propagation

Satellite Communication – Applications

Satellite communication finds its applications in the following areas −

- In Radio broadcasting.
- In TV broadcasting such as DTH.
- In Internet applications such as providing Internet connection for data transfer, GPS applications, Internet surfing, etc.
- For voice communications.
- For research and development sector, in many areas.
- In military applications and navigations.

The orientation of the satellite in its orbit depends upon the three laws called as Kepler's laws.

Kepler's Laws

Johannes Kepler (1571-1630) the astronomical scientist, gave 3 revolutionary laws, regarding the motion of satellites. The path followed by a satellite around its primary (the earth) is an **ellipse**. Ellipse has two foci - **F1** and **F2**, the earth being one of them.

If the distance from the center of the object to a point on its elliptical path is considered, then the farthest point of an ellipse from the center is called as **apogee** and the shortest point of an ellipse from the center is called as **perigee**.

Kepler's 1st Law

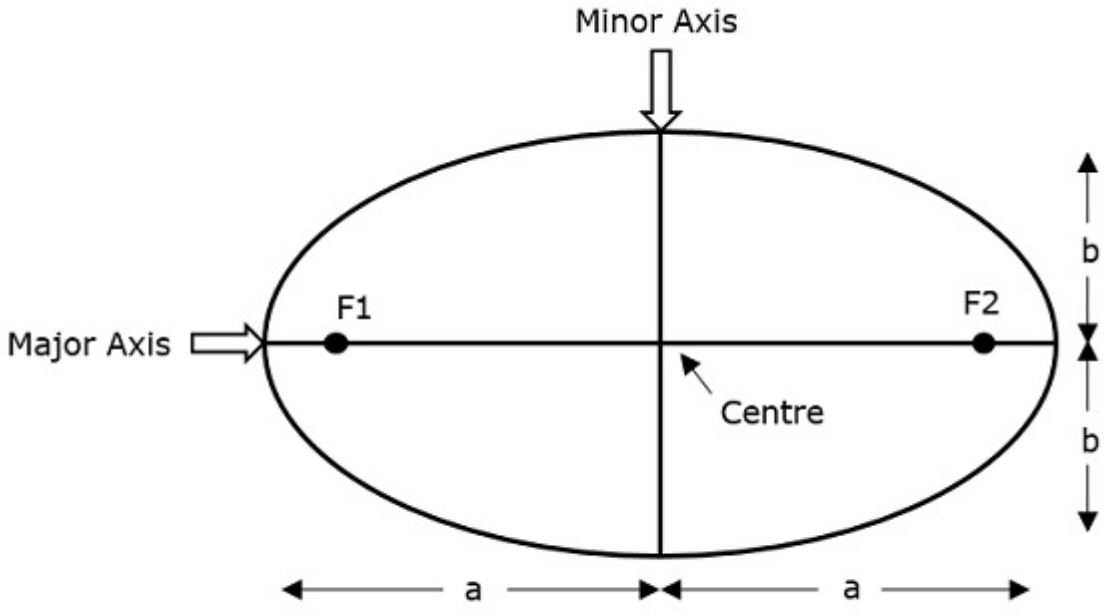
Kepler's 1st law states that, "every planet revolves around the sun in an elliptical orbit, with sun as one of its foci." As such, a satellite moves in an elliptical path with earth as one of its foci.

The semi major axis of the ellipse is denoted as '**a**' and semi minor axis is denoted as **b**. Therefore, the eccentricity e of this system can be written as −

$$e = \frac{\sqrt{a^{2}-b^{2}}}{a}$$

- **Eccentricity (e)** − It is the parameter which defines the difference in the shape of the ellipse rather than that of a circle.
- **Semi-major axis (a)** − It is the longest diameter drawn joining the two foci along the center, which touches both the apogees (farthest points of an ellipse from the center).
- **Semi-minor axis (b)** − It is the shortest diameter drawn through the center which touches both the perigees (shortest points of an ellipse from the center).

These are well described in the following figure.



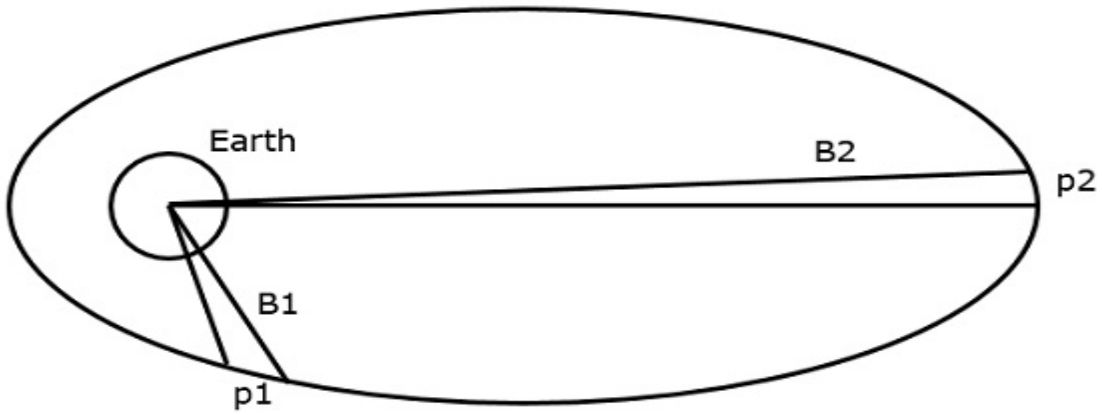
Kepler's 1st law

For an elliptical path, it is always desirable that the eccentricity should lie in between 0 and 1, i.e. 0 < e < 1 because if **e** becomes zero, the path will be no more in elliptical shape rather it will be converted into a circular path.

Kepler's 2nd Law

Kepler's 2nd law states that, "For equal intervals of time, the area covered by the satellite is equal with respect to the center of the earth."

It can be understood by taking a look at the following figure.



Kepler's 2nd law

Suppose that the satellite covers **p1** and **p2** distances, in the same time interval, then the areas **B1** and **B2** covered in both instances respectively, are equal.

Kepler's 3rd Law

Kepler's 3rd law states that, "The square of the periodic time of the orbit is proportional to the cube of the mean distance between the two bodies."

This can be written mathematically as

$$T^{2}\:\alpha\:\:a^{3}$$

Which implies

$$T^{2} = \frac{4\pi ^{2}}{GM}a^{3}$$

Where $\frac{4\pi ^{2}}{GM}$ is the proportionality constant (according to Newtonian Mechanics)

$$T^{2} = \frac{4\pi ^{2}}{\mu}a^{3} $$

Where μ = the earth's geocentric gravitational constant, i.e. M = 3.986005 × 10^{14} m^3/sec^2

$$1 = \left (\frac{2\pi}{T} \right)^{2}\frac{a^{3}}{\mu}$$

$$1 = n^{2}\frac{a^{3}}{\mu}\:\:\:\Rightarrow \:\:\:a^{3} = \frac{\mu}{n^{2}}$$

Where **n** = the mean motion of the satellite in radians per second

The orbital functioning of satellites is calculated with the help of these Kepler's laws.

Along with these, there is an important thing which has to be noted. A satellite, when it revolves around the earth, undergoes a pulling force from the earth which is the gravitational force. Also, it experiences some pulling force from the sun and the moon. Hence, there are two forces acting on it. They are −

- **Centripetal force** − The force that tends to draw an object moving in a trajectory path, towards itself is called as **centripetal force**.
- **Centrifugal force** − The force that tends to push an object moving in a trajectory path, away from its position is called as **centrifugal force**.

So, a satellite has to balance these two forces to keep itself in its orbit.

Earth Orbits

A satellite when launched into space, needs to be placed in a certain orbit to provide a particular way for its revolution, so as to maintain accessibility and serve its purpose whether scientific, military, or commercial. Such orbits which are assigned to satellites, with respect to earth are called as **Earth Orbits**. The satellites in these orbits are Earth **Orbit Satellites**.

The important kinds of Earth Orbits are –

- Geo Synchronous Earth Orbit
- Medium Earth Orbit
- Low Earth Orbit

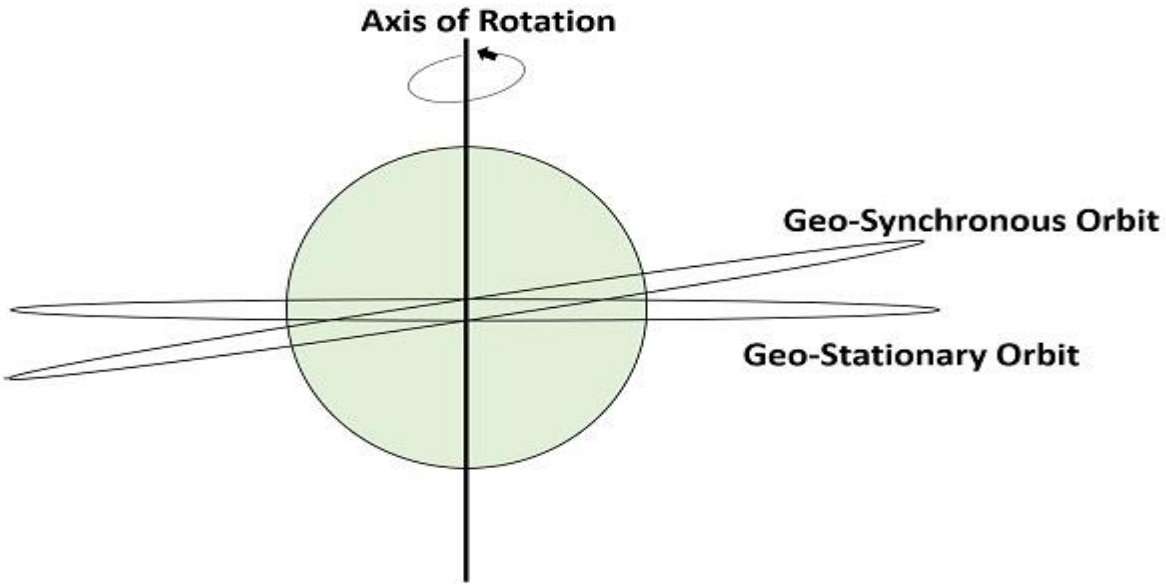
Geosynchronous Earth Orbit Satellites

A **Geo-Synchronous Earth Orbit (GEO)** satellite is one which is placed at an altitude of 22,300 miles above the Earth. This orbit is synchronized with a **side real day** (i.e., 23hours 56minutes). This orbit can **have inclination and eccentricity**. It may not be circular. This orbit can be tilted at the poles of the earth. But it appears stationary when observed from the Earth.

The same geo-synchronous orbit, if it is circular and in the plane of equator, it is called as **geo-stationary orbit**. These satellites are placed at 35,900kms (same as geosynchronous) above the Earth's Equator and they keep on rotating with respect to earth's direction (west to east). These satellites are considered stationary with respect to earth and hence the name implies.

Geo-Stationary Earth Orbit Satellites are used for weather forecasting, satellite TV, satellite radio and other types of global communications.

The following figure shows the difference between Geo-synchronous and Geo-stationary orbits. The axis of rotation indicates the movement of Earth.



Note – Every geo-stationary orbit is a geo-synchronous orbit. But every geo-synchronous orbit is NOT a Geo-stationary orbit.

Medium Earth Orbit Satellites

Medium Earth Orbit (MEO) satellite networks will orbit at distances of about 8000 miles from the earth's surface. Signals transmitted from a MEO satellite travel a shorter distance. This translates to improved signal strength at the receiving end. This shows that smaller, more lightweight receiving terminals can be used at the receiving end.

Since the signal is travelling a shorter distance to and from the satellite, there is less transmission delay. **Transmission delay** can be defined as the time it takes for a signal to travel up to a satellite and back down to a receiving station.

For real-time communications, the shorter the transmission delay, the better will be the communication system. As an example, if a GEO satellite requires 0.25 seconds for a round trip, then MEO satellite requires less than 0.1 seconds to complete the same trip. MEOs operates in the frequency range of 2 GHz and above.

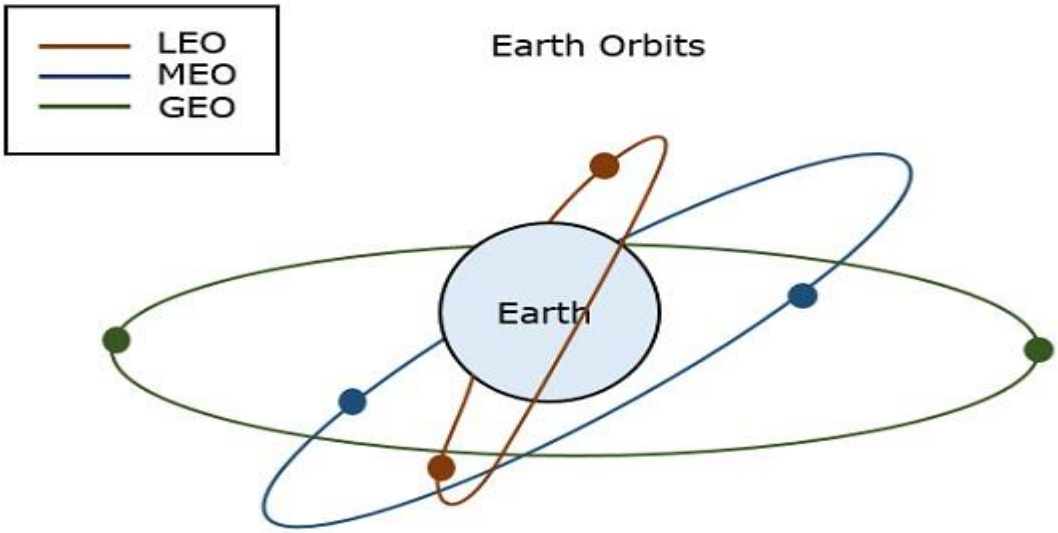
Low Earth Orbit Satellites

The Low Earth Orbit (LEO) satellites are mainly classified into three categories namely, little LEOs, big LEOs, and Mega-LEOs. LEOs will orbit at a distance of 500 to 1000 miles above the earth's surface.

This relatively short distance reduces transmission delay to only 0.05 seconds. This further reduces the need for sensitive and bulky receiving equipment. Little LEOs will operate in the 800 MHz (0.8 GHz) range. Big LEOs will operate in the 2 GHz or above range, and Mega-LEOs operates in the 20-30 GHz range.

The higher frequencies associated with **Mega-LEOs** translates into more information carrying capacity and yields to the capability of real-time, low delay video transmission scheme.

The following figure depicts the paths of LEO, MEO, and GEO.



Wireless Networks

Computer networks that are not connected by cables are called wireless networks. They generally use radio waves for communication between the network nodes. They allow devices to be connected to the network while roaming around within the network coverage.



Types of Wireless Networks

- Wireless LANs − Connects two or more network devices using wireless distribution techniques.
- Wireless MANs − Connects two or more wireless LANs spreading over a metropolitan area.
- Wireless WANs − Connects large areas comprising LANs, MANs and personal networks.

Advantages of Wireless Networks

- It provides clutter-free desks due to the absence of wires and cables.
- It increases the mobility of network devices connected to the system since the devices need not be connected to each other.
- Accessing network devices from any location within the network coverage or Wi-Fi hotspot becomes convenient since laying out cables is not needed.
- Installation and setup of wireless networks are easier.
- New devices can be easily connected to the existing setup since they needn't be wired to the present equipment. Also, the number of equipment that can be added or removed to the system can vary considerably since they are not limited by the cable capacity. This makes wireless networks very scalable.
- Wireless networks require very limited or no wires. Thus, it reduces the equipment and setup costs.

Examples of wireless networks

- Mobile phone networks
- Wireless sensor networks
- Satellite communication networks
- Terrestrial microwave networks

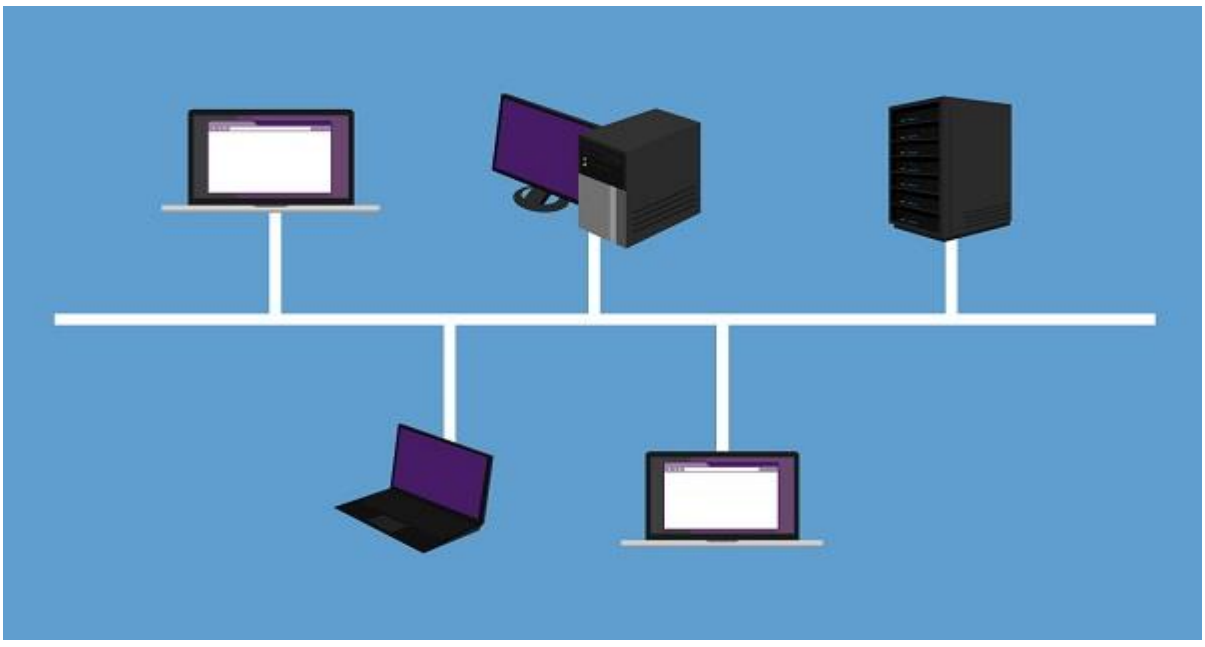
Topologies

The way in which devices are interconnected to form a network is called network topology. Some of the factors that affect choice of topology for a network are −

- **Cost** − Installation cost is a very important factor in overall cost of setting up an infrastructure. So cable lengths, distance between nodes, location of servers, etc. have to be considered when designing a network.
- **Flexibility** − Topology of a network should be flexible enough to allow reconfiguration of office set up, addition of new nodes and relocation of existing nodes.
- **Reliability** − Network should be designed in such a way that it has minimum down time. Failure of one node or a segment of cabling should not render the whole network useless.
- **Scalability** − Network topology should be scalable, i.e. it can accommodate load of new devices and nodes without perceptible drop in performance.
- **Ease of installation** − Network should be easy to install in terms of hardware, software and technical personnel requirements.
- **Ease of maintenance** − Troubleshooting and maintenance of network should be easy.

Bus Topology

Data network with bus topology has a **linear transmission cable**, usually **coaxial**, to which many **network devices** and **workstations** are attached along the length. **Server** is at one end of the bus. When a workstation has to send data, it transmits **packets** with **destination address** in its header along the bus.



The data travels in both the directions along the bus. When the destination terminal sees the data, it copies it to the local disk.

Advantages of Bus Topology

These are the advantages of using bus topology −

- Easy to install and maintain
- Can be extended easily
- Very reliable because of single transmission line

Disadvantages of Bus Topology

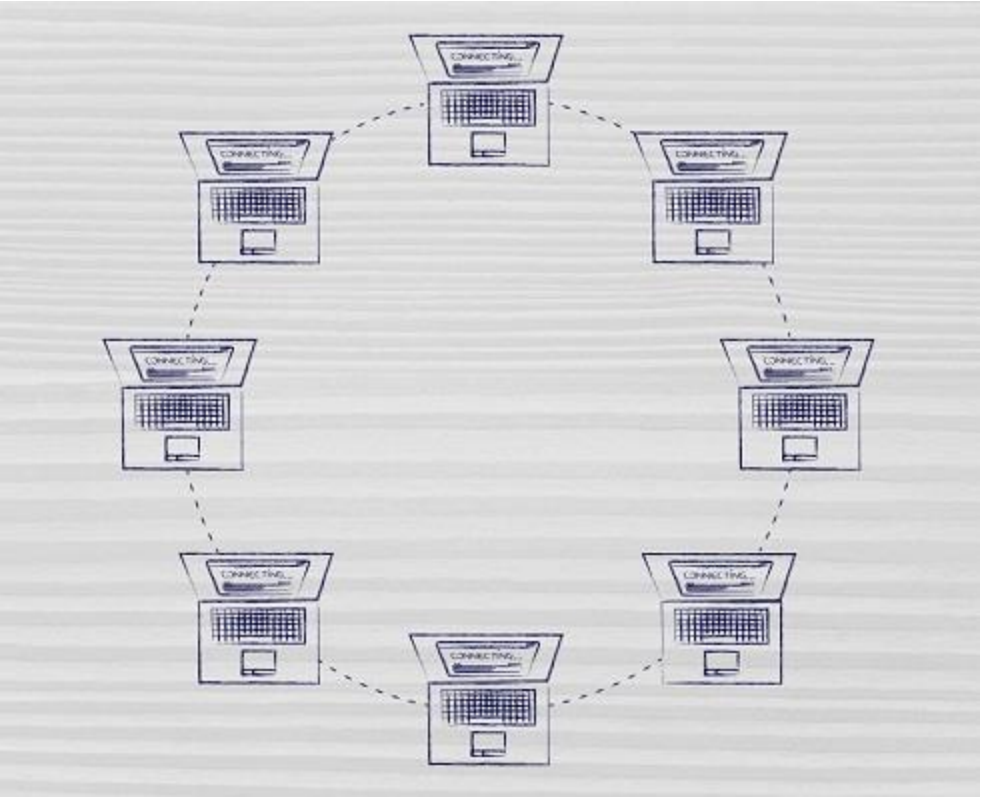
These are some disadvantages of using bus topology −

- Troubleshooting is difficult as there is no single point of control
- One faulty node can bring the whole network down
- Dumb terminals cannot be connected to the bus

Ring Topology

In **ring topology** each terminal is connected to exactly **two nodes**, giving the network a circular shape. Data travels in only one pre-determined direction.

DIWAKAR



When a terminal has to send data, it transmits it to the neighboring node which transmits it to the next one. Before further transmission data may be amplified. In this way, data raverses the network and reaches the destination node, which removes it from the network. If the data reaches the sender, it removes the data and resends it later.

Advantages of Ring Topology

These are the advantages of using ring topology −

- Small cable segments are needed to connect two nodes
- Ideal for optical fibres as data travels in only one direction
- Very high transmission speeds possible

Disadvantages of Ring Topology

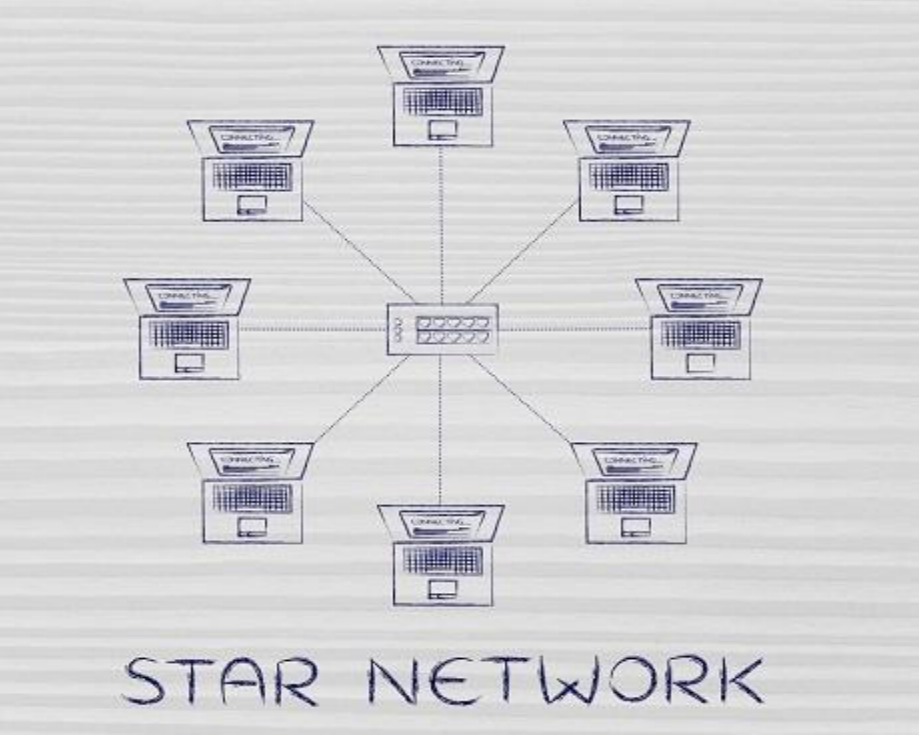
These are some the disadvantages of using ring topology −

- Failure of single node brings down the whole network

- Troubleshooting is difficult as many nodes may have to be inspected before faulty one is identified
- Difficult to remove one or more nodes while keeping the rest of the network intact

Star Topology

In star topology, server is connected to each node individually. Server is also called the central node. Any exchange of data between two nodes must take place through the server. It is the most popular topology for information and voice networks as central node can process data received from source node before sending it to the destination node.



Advantages of Star Topology

These are the advantages of using star topology −

- Failure of one node does not affect the network
- Troubleshooting is easy as faulty node can be detected from central node immediately

- Simple access protocols required as one of the communicating nodes is always the central node

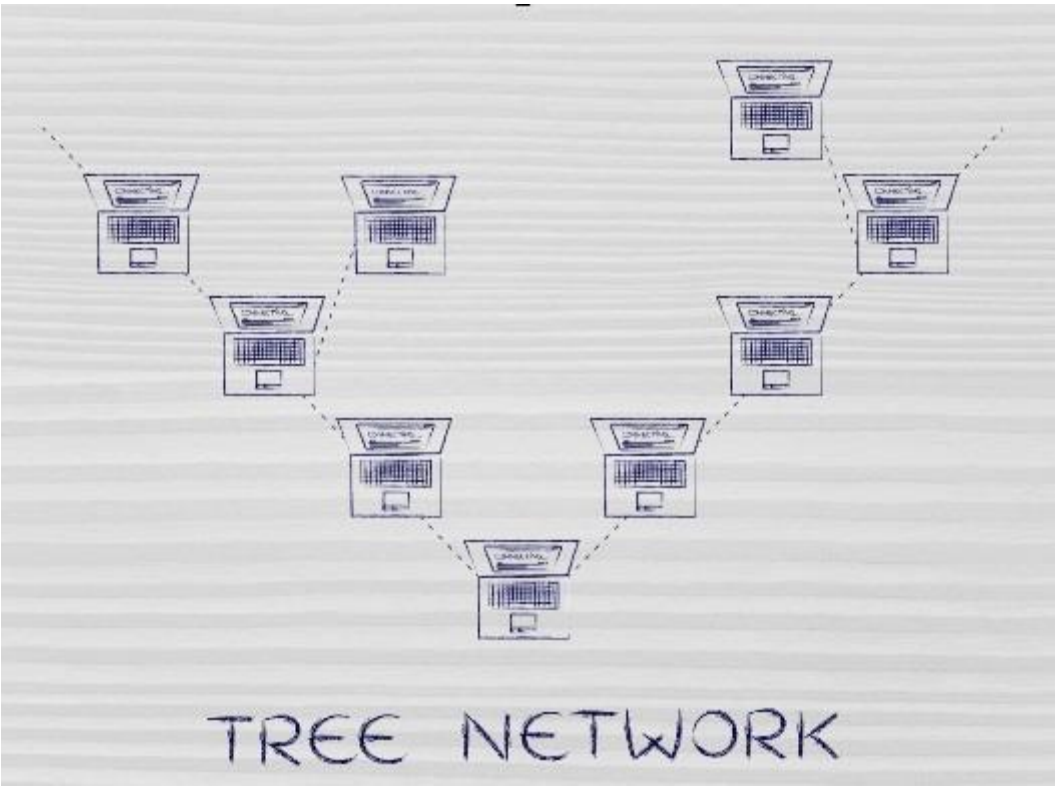
Disadvantages of Star Topology

These are the disadvantages of using star topology −

- Long cables may be required to connect each node to the server
- Failure of central node brings down the whole network

Tree Topology

Tree topology has a group of star networks connected to a linear bus backbone cable. It incorporates features of both star and bus topologies. Tree topology is also called hierarchical topology.



Advantages of Tree Topology

These are some of the advantages of using tree topology –

- Existing network can be easily expanded
- Point-to-point wiring for individual segments means easier installation and maintenance
- Well suited for temporary networks

Disadvantages of Tree Topology

These are some of the disadvantages of using tree topology −

- Technical expertise required to configure and wire tree topology
- Failure of backbone cable brings down entire network
- Insecure network
- Maintenance difficult for large networks

Ad Hoc Networks

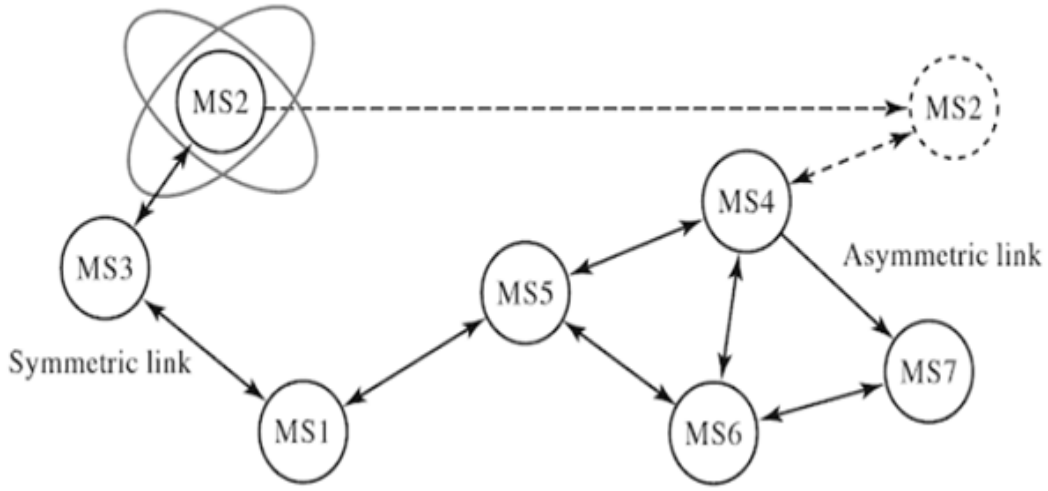
An ad hoc network is one that is spontaneously formed when devices connect and communicate with each other. The term ad hoc is a Latin word that literally means "for this," implying improvised or impromptu.

Ad hoc networks are mostly wireless local area networks (LANs). The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer co-ordination. Each device participates in routing activity, by determining the route using the routing algorithm and forwarding data to other devices via this route.

- A MANET consists of a number of mobile devices that come together to form a network as needed, without any support from any existing internet infrastructure or any other kind of fixed stations.
- A MANET can be defined as an autonomous system of nodes or MSs(also serving as routers) connected by wireless links, the union of which forms a communication network modeled in the form of an arbitrary communication graph.
- This is in contrast to the well-known single hop cellular network model that supports the needs of wireless communication between two mobile nodes relies on the wired backbone and fixed base stations.
- In a MANET, no such infrastructure exists and network topology may be changed dynamically in an unpredictable manner since nodes are free to

move and each node has limiting transmitting power, restricting access to the node only in the neighboring range.

- MANETs are basically peer-to-peer, multi-hop wireless networks in which information packets are transmitted in a store and forward manner from a source to an arbitrary destination, via intermediate nodes as given in the figure:



- As nodes move, the connectivity may change based on relative locations of other nodes. The resulting change in the network topology known at the local level must be passed on to other nodes so that old topology information can be updated.
- For example, as MS2 in the figure changes its point of attachment from MS3 to MS4, other nodes that are part of the network should use this new route to forward packets to MS2. In the figure, we assume that it is not possible to have all nodes within each other's radio range. In case all nodes are closed by within each other's radio range, there are no routing issues to be addressed.
- In figures raise another issue, that of symmetric and asymmetric (bidirectional) and asymmetric (unidirectional) links. Consider symmetric links with associative radio range; for example, if MS1 is within radio range of MS3, then MS3 is also within radio range of MS1. The communication links are symmetric. This assumption is not always valid because of differences in transmitting power levels and the terrain. Routing in

asymmetric networks is relatively hard task. In certain cases, it is possible to find routes that exclude asymmetric links, since it is cumbersome to find the return path. The issue of efficient is one of the several challenges encountered in a MANET.

- The other issue is varying the mobility patterns of different nodes. Some other nodes are highly mobile, while others are primarily stationary. It is difficult to predict a node's movement and direction of movement and numerous studies have been performed to evaluate their performance using different simulators.

Characteristics of MANET

Some characteristics of adhoc network are as follows:

- **Dynamic topologies:** nodes are free to move arbitrarily; thus the network topology may be changed randomly and unpredictably and primarily consists of bidirectional links. In some cases where the transmission power of two nodes is different, a unidirectional link may exist.
- **Bandwidth-constrained and variable capacity links:** wireless links continue to have significantly lower capacity than infrastructure networks.
- **Energy-constrained operation:** some or all of the MSs in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes or devices, the most important system design optimization criteria may be energy conservation.
- **Limited physical security:** MANETs are generally more prone to physical security threats than wire line networks. The increased possibility of eavesdropping, spoofing, and denial of services (DoS) attacks should be considered carefully. To reduce security threats, many existing link security techniques are often applied within wireless networks.

Applications of MANET

Some specific applications of ad hoc networks include industrial and commercial applications involving cooperative mobile data exchange. There are many existing and future military networking requirements for robust, IP-compliant data services within mobile wireless communication networks, with many of these networks consist of highly dynamic autonomous topology segments. Advanced

DIWAKAR EDUCATION HUB

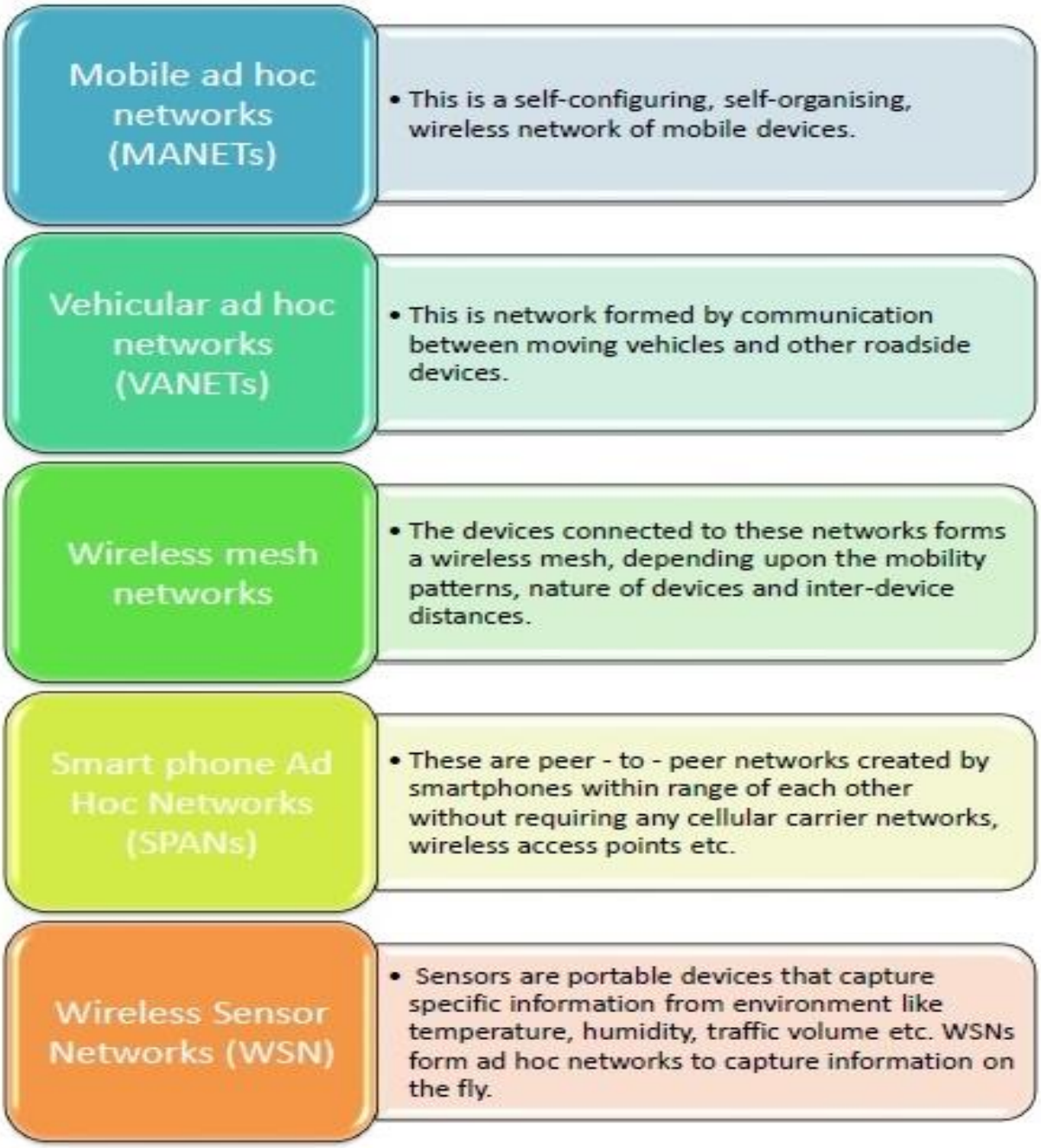
features of Mobile ad hoc networks, including data rates compatible with multimedia applications global roaming capability, and coordination with other network structures are enabling new applications.

- **Defense applications:** Many defense applications require on the fly communications set-up, and ad hoc/sensor networks are excellent candidates for use in battlefield management.
- **Crisis management applications:** These arise, for example, as a result of natural disasters in which the entire communication infrastructure is in disarray. Restoring communications quickly is essential.
- **Telemedicine:** The paramedic assisting the victim of a traffic accident in a remote location must access medical records (e.g. X-rays) and may need video conference assistance from a surgeon for an emergency intervention. In fact, the paramedic may need to instantaneously relay back to the hospital the victim's X-rays and other diagnostic tests from the site of the accident.
- **Tele-geoprocessing application:** The combination of GPS, GIS (Geographical Information Systems), and high-capacity wireless mobile systems enables a new type of application referred to as tele- geo processing.
- **Virtual Navigation:** A remote database contains the graphical representation of building, streets, and physical characteristics of a large metropolis. They may also "virtually" see the internal layout of buildings, including an emergency rescue plan, or find possible points of interest.
- **Education via the internet:** Educational opportunities available on the internet or remote areas because of the economic infeasibility of providing expensive last-mile wire line internet access in these areas to all subscribers.
- **Vehicular area network:** This a growing and very useful application of adhoc network in providing emergency services and other information. This is equally effective in both urban and rural setup. The basic and exchange necessary data that is beneficial in a given situation.

Classifications of Ad Hoc Networks

Ad hoc networks can be classified into several types depending upon the nature of their applications. The most prominent ad hoc networks that are commonly incorporated are illustrated in the diagram below −

DWAKAR EDUCATION HUB



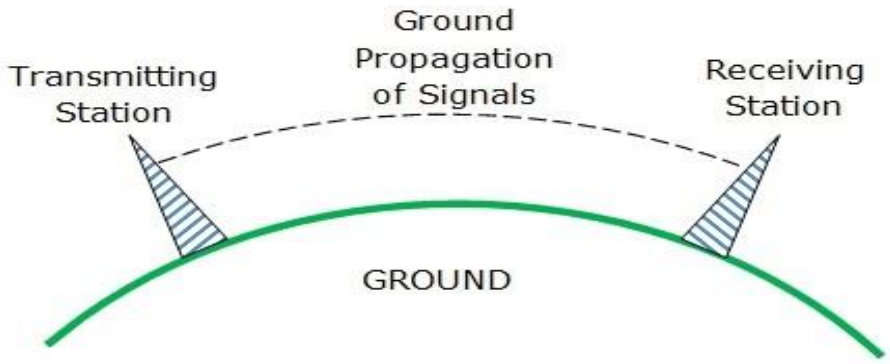
Wireless Transmission

In wireless transmission media, data is transmitted in the form of electromagnetic waves that do not require any physical conductors for transmission. The waves are broadcast through free space and any device who has permission to connect can receive them.

The three ways in which unguided signals travel are −

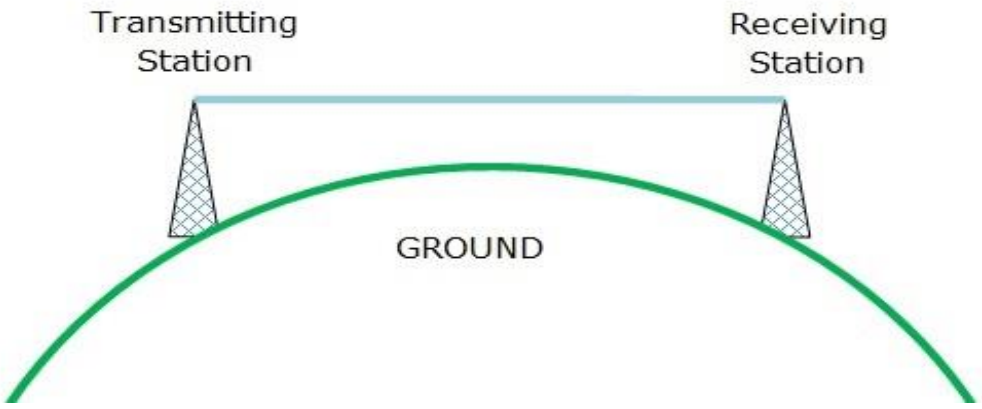
Ground Propagation:

It is a method of propagation, in which radio waves travel through the lowest layers of the atmosphere along the earth's surface, following the earth's curvature. The frequency of these signals is low (≤ 2MHz), and the distance they travel is directly proportional to the power in signal.



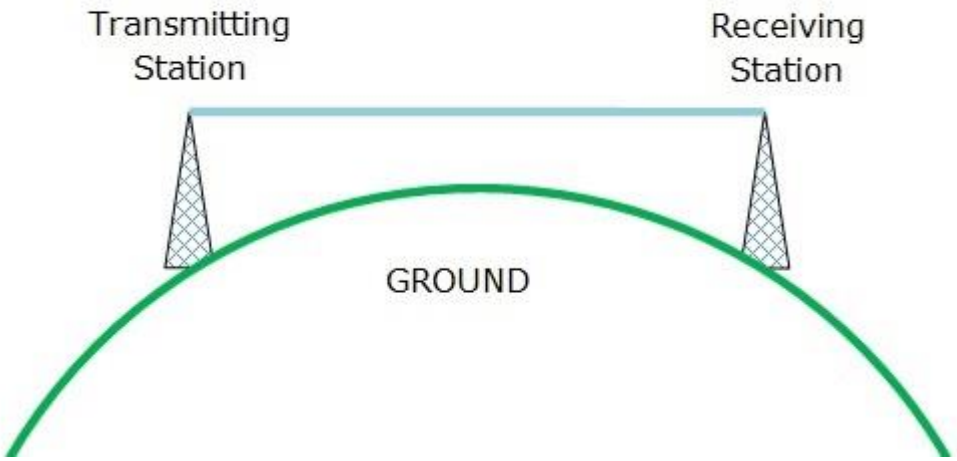
Sky Propagation:

In sky propagation, high frequency radio waves (2–30 MHz) are reflected back from the ionosphere towards the earth's surface. They can be used to transmit signals over a large geographical area since their distance is not bounded by the earth's curvature.



Line – of – Sight Propagation

In line – of – sight propagation, very high frequency waves (> 30 MHz) travel at straight lines from the source antenna (transmitter) to the destination antenna (receiver). These waves are easily disrupted by present of objects in their path. So the antennas are placed tall enough above obstructions. They are unidirectional facing each other.



Wireless LANs

Wireless LANs (WLANs) are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN (Local Area Network). Users connected by wireless LANs can move around within this limited area such as home, school, campus, office building, railway platform, etc.

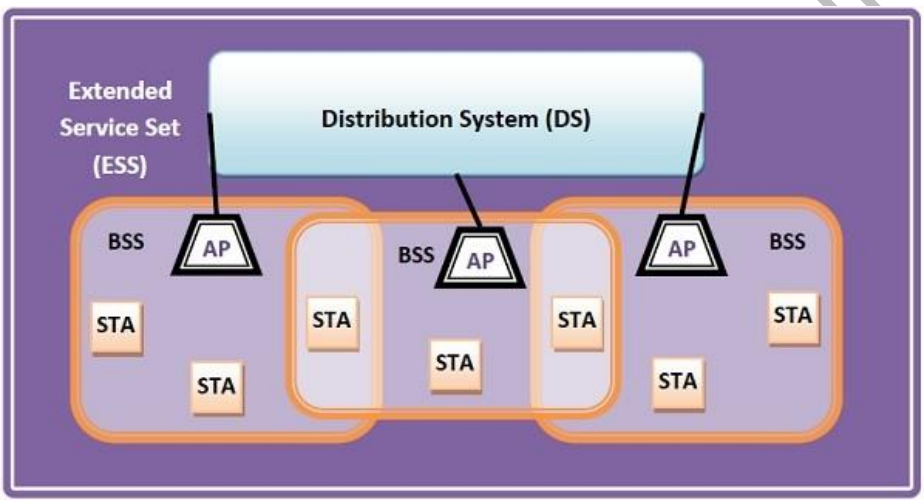
Most WLANs are based upon the standard IEEE 802.11 standard or WiFi.

Components of WLANs

The components of WLAN architecture as laid down in IEEE 802.11 are −

- **Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. Each station has a wireless network interface controller. A station can be of two types −

  - Wireless Access Point (WAP or AP)
  - Client
- **Basic Service Set (BSS)** − A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories −
  - Infrastructure BSS
  - Independent BSS
- **Extended Service Set (ESS)** − It is a set of all connected BSS.
- **Distribution System (DS)** − It connects access points in ESS.



Types of WLANS

WLANs, as standardized by IEEE 802.11, operates in two basic modes, infrastructure, and ad hoc mode.

- **Infrastructure Mode** − Mobile devices or clients connect to an access point (AP) that in turn connects via a bridge to the LAN or Internet. The client transmits frames to other clients via the AP.
- **Ad Hoc Mode** − Clients transmit frames directly to each other in a peer-to-peer fashion.

Advantages of WLANs

- They provide clutter-free homes, offices and other networked places.
- The LANs are scalable in nature, i.e. devices may be added or removed from the network at greater ease than wired LANs.

- The system is portable within the network coverage. Access to the network is not bounded by the length of the cables.
- Installation and setup are much easier than wired counterparts.
- The equipment and setup costs are reduced.

Disadvantages of WLANs

- Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
- Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
- WLANs are slower than wired LANs.

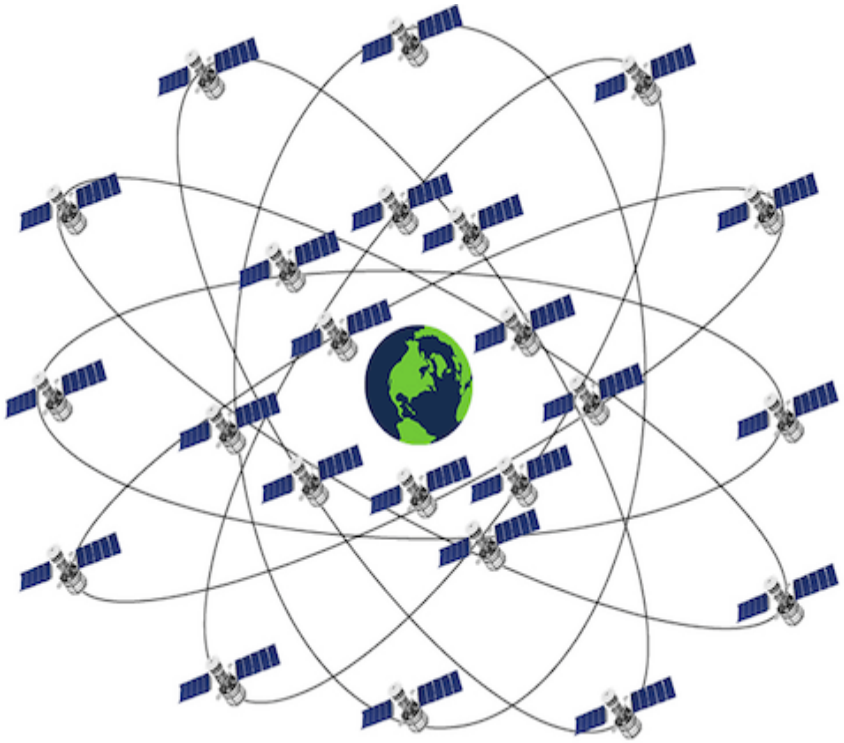
Global Positioning Systems (GPS)

Global Positioning Systems, widely known as GPSs, have a great importance since the days of World War II.

Although the initial focus was mainly on military targeting, fleet management, and navigation, commercial usage began finding relevance as the advantages of radiolocation were extended to (but not limited to) tracking down stolen vehicles and guiding civilians to the nearest hospital, gas station, hotel, and so on.

A GPS system consists of a network of 24 orbiting satellites, called **NAVSTAR** (Navigation System with Time and Ranging), and placed in space in six different orbital paths with four satellites in each orbital plane and covering the entire earth under their signal beams.

DIWAKAR EDUCATION



The orbital period of these satellites is twelve hours.

The satellite signals can be received anywhere and at any time in the world.

The spacing of the satellites is arranged such that a minimum of five satellites are in view from every point on the globe.

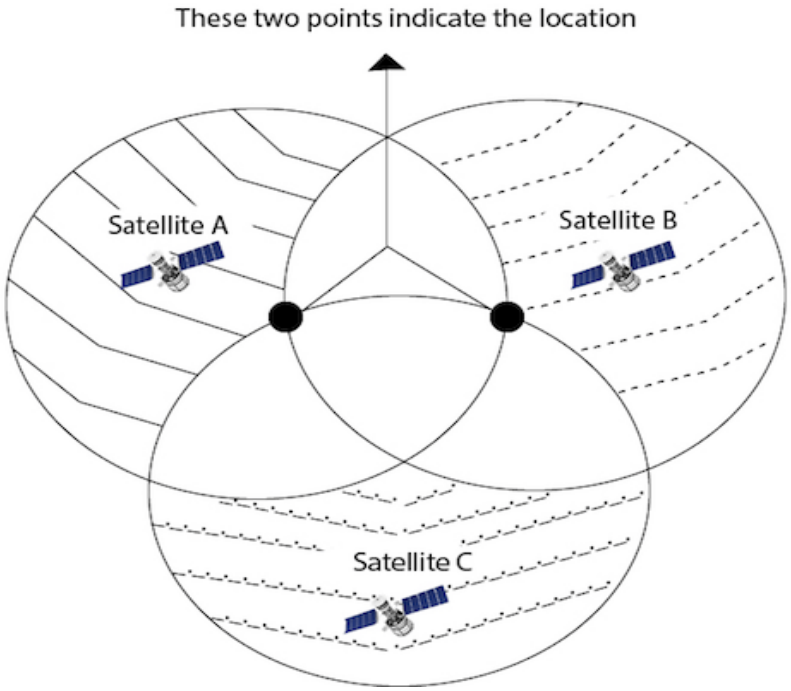
The first GPS satellite was launched in February 1978.

Each satellite is expected to last approx 7.5 years, and replacements are constantly being built and launched into orbit.

Each satellite is placed at an altitude of about 10,900 nautical miles and weights about 862 kg.

The satellites extend to about 5.2m (17ft) in space including the solar panels. Each satellite transmits on three frequencies.

The GPS is based on well known concept called the **triangulation technique**.



Consider the GPS receiver MS to be placed on an imaginary sphere. The radius of imaginary sphere is equal to the distance between satellite "A" and the receiver on the ground (with the satellite "A" as the center of the sphere).

Now the GPS receiver MS is also a point on another imaginary sphere with a second satellite "B" at its center. We can say that the GPS receiver is somewhere on the circle formed by the intersection of these two spheres.

Then, with a measurement of distance from a third satellite "C", the position of the receiver is narrowed down to just two points on the circle, one of which is imaginary and is eliminated from the calculations. As a result, the distance measured from three satellites suffices to determine the position of the GPS receiver on earth.

History of the Global Positioning System (GPS)

- 1957 - Soviet Union launched Sputnik I satellite.
- 1960s - U.S. Navy tracked U.S. submarines with satellite navigation.
- 1978 - NAVSTAR Block I GPS satellite was launched.

- 1983 - U.S. announced that it will make GPS available for civilian use after Korean Air flight 007 shot down.
- 1989 - Magellan introduced NAV 1000, the first hand-held GPS device. First Block II satellite is launched.
- 1993 - Constellation of 24 satellite system became operational.
- 1995 - Full Operational Capability (FOC) declared.
- 2000 - Selective Availability discontinued by the U.S. Government.
- 2004 - Qualcomm successfully completed test of live assisted GPS on a mobile phone.
- 2008 - Block II satellite launched.
- 2016 - GPS IIF satellite launched.

Beneficiaries of GPS

- At the start, more than 1000 portable commercial GPS receivers were purchased for military use.
- They were carried by soldiers and attached to vehicles, helicopters, and aircraft instrument panels.
- GPS receivers were used in several aircrafts, including B-2 bombers and F-16 fighters etc. Navy ships used them for rendezvous, minesweeping, and aircraft operations.
- GPS has become important for all military operations and weapons systems. In additions, GPS benefits nonmilitary operations.
- GPS is used on satellites to obtain highly accurate orbit data and to control spacecraft orientation.
- GPS has a various applications on land, at sea, and in the air.
- GPS can be used everywhere except indoors and places where a GPS signal cannot be received because of natural or man-made obstructions.
- Both military and commercial aircraft use GPS for navigation purposes. It is also used by commercial fisherman and boaters to aid in navigation.
- The precision timing capability provided by GPS is used by the scientific community for research purposes. The GPS enables survey units to help surveyors to set up their survey sites fairly quickly.
- GPS is also used for noncommercial purposes by car racers, hikers, hunters, mountain bikers, and cross-country skiers.

DIWAKAR EDUCATION HUB

- GPS also helps in providing emergency roadside assistance, by allowing an accident victim to transmit his or her position to the nearest response center at the push of a button.
- GPS is also helping to save lives. Many police, fire, and emergency medical service units are using GPS receivers to determine the location of a police car, a fire truck, or an ambulance nearest to an emergency, enabling the quickest possible response in death or life situations.
- Automobile manufacturers are offering moving map displays, guided by GPS receivers as an option on new vehicles.

Limitations of GPS

- There are several factors that introduce error into GPS position calculations and prevent us from achieving the best possible accuracy.
- A major source of error in GPS arises from the fact that the speed of the radio signals is constant only in a vacuum which means that distance measurements may vary as the values of the speed of signal vary in the atmosphere.
- The atmosphere, as we know, is composed of the ionosphere and the troposphere. The presence of the troposphere essentially composed of water vapor) is known to cause errors due to variation of temperature and pressure, and the particles in the ionosphere are known to cause significant measurement errors (as would be the case with bad clocks!).

Factors affecting the accuracy of GPS position are given below:

Error Factor	**Accuracy level (in meters)**	
	Standard GPS	**Differential GPS (DGPS)**
Atmospheric conditions (troposphere)	0.5-0.7	0.2

KARE EDUCATION HUB

Atmospheric conditions (ionosphere)	5-7	0.4
Multipath fading and shadowing effects	0.6-1.2	0.6
Receiver Noise	0.3-1.5	0.3
Selective availability	24-30	0
Atomic clock errors	1.5	0
Ephemeris errors	2.5	0

GPRS

The full form of GPRS is **General Packet Radio Service**. The GPRS is a non-voice high-speed packet switching system developed for GSM networks. GPRS is a packet-aligned, wireless communication service that transmits a mobile signal on 3 G and 2 G cellular transmission networks.

GPRS works based on the technique of modulation, also called GMSK (Gaussian Minimum Shift Keying). To allow GPRS to be deployed on a TDMA (Time Division Multiple Access) or GSM (Global System For Mobile Communications) or network, we must have two main modules that are named as

- GGSN (Gateway GPRS Service Node)
- SGSN (Serving GPRS Service Node)

GPRS can be used to communicate using internet protocols that support a wide range of companies as well as industrial applications.

History of GPRS

- GPRS was introduced in the year 2000 as a packet-switched data service incorporated into the channel switched cellular radio network GSM. GPRS

DIWAKAR EDUCATION

extends the reach of the Fixed Internet by connecting mobile terminals all over the world.

- The CELLPAC protocol established in 1991-1993 was the primary trigger for beginning in 1993 configuration of standard GPRS by ETSI SMG. In particular, the CELLPAC Voice & Data functions introduced in a 1993 ETSI Workshop dedication anticipate what later became known as GPRS roots.
- The workshop input is cited in 22 GPRS-related US-Patents. Successor systems to GSM / GPRS such as W-CDMA (UMTS) and LTE, as implemented by CELLPAC, depend on critical GPRS operations for mobile Internet access.
- As per research on the history of GPRS growth, the inventors of GPRS are Bernhard Walke and his student Peter Decker, the first to make the system access to mobile internet globally.

Requirements to use GPRS

Due to the more advanced infrastructure than traditional 2 G wireless technology, GPRS is considered as 2.5 G technology, but it does not satisfy the need for 3 G developments.

- A service that includes GPRS modem.
- A network of GSM / GPRS.
- A GPRS-aided SIM card.
- A remote location that has internet connectivity or a GPRS network.

Benefits of GPRS

- GPRS gives higher speed of data transfer compared with fixed telecommunication networks. Its prime speed is 171.2 kbps, almost three times the speed of set-telecommunications.
- It provides immediate fast communication and quick transfer of information.
- GPRS is highly cost efficient.
- GPRS applications are unique and of high standard. It offers web apps over mobile phones and also makes web surfing, IM messages, e-commerce and so on simpler.
- It allows people to connect to the web even when other service providers, including 3 G or HSDPA, are not accessible.

DIWAKAR EDUCATION HUB

SMS: Short Message Service

SMS is an acronym for Short Message Service. It is *a communication protocol that allows to exchange text messages between mobile devices*.

You can send SMS by mobile phones, smart phones, computer systems with web, handheld devices etc. All telecommunication companies like Idea, Vodafone, Airtel, Aircel, BSNL etc. provide the facility of sending SMS.

SMS is the most widely used data application with an estimated 3.5 billion active users. It was originally designed as a part of GSM, but is now available on the CDMA phones also. The maximum length of an individual message goes up to 160 alpha-numeric 7 bits characters. (In the case of 5-bit mode, it supports 224 characters).

Initial concept of SMS

Initial concept of SMS came in exist in early 1980s. It was developed in the Franco-German GSM cooperation in 1984 by Friedhelm Hillebrand and Bernard Ghillebiert. Then, the CEPT group GSM introduced a plan to include the exchange of text messages between mobile stations via message handling systems in use at that time.

Advantages

- It is a very reliable and attested platform for sending important information which ensures a guaranteed delivery of the information.
- It is a more discrete form of sending information in comparison to a phone call.
- It is provided automatically to all mobile devices and there is no requirement for an internet connection.
- The conversations among people are automatically stored until deleted by the people themselves.
- It does not require any app to be downloaded as it is already provided in all the mobile devices.

Disadvantages

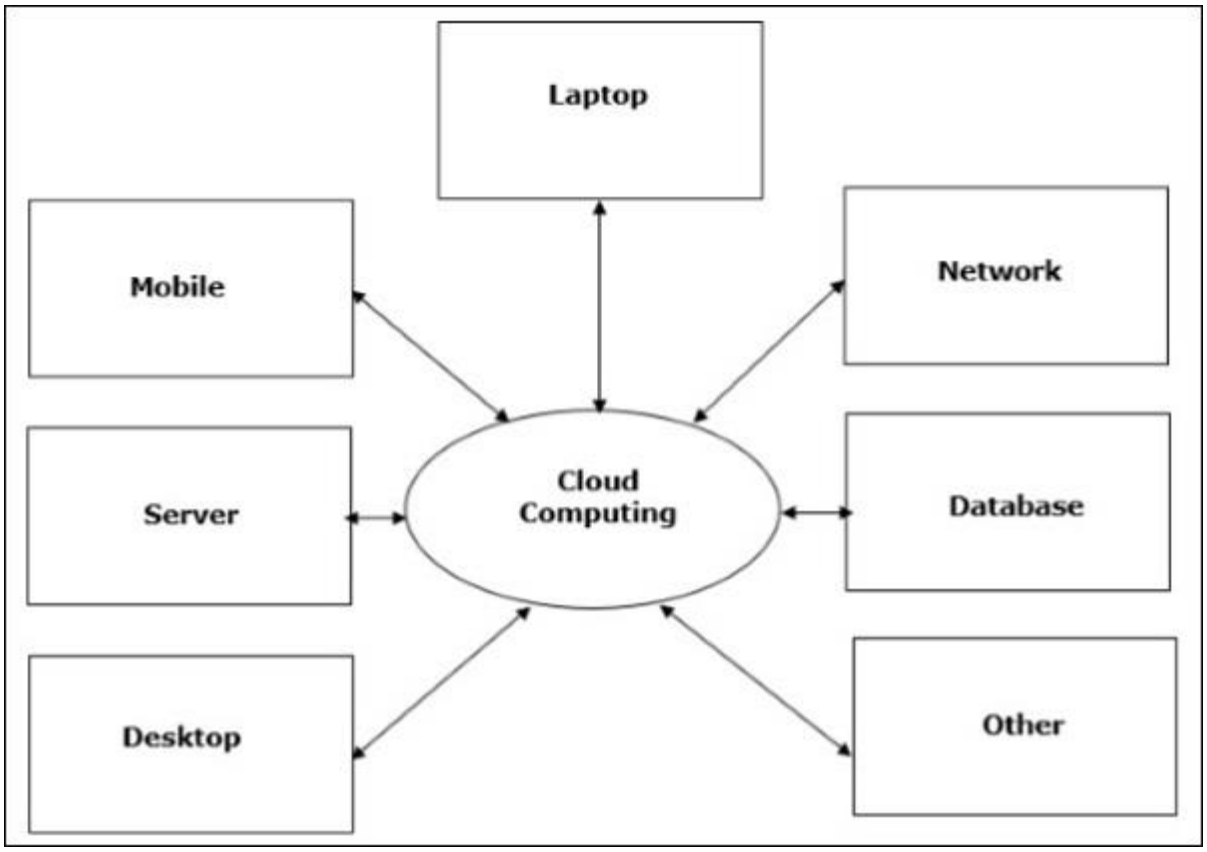
DIWAKAR EDUCATION HUB

- It has a limited length as it provides only 160 characters per text message.
- In order to send a text message one has to pay the cost for sending it as SMS facility is not free of cost.
- There is no possibility to unsend a message once sent.

Cloud Computing

The popular trend in today's technology driven world is 'Cloud Computing'. Cloud computing can be referred to as the storing and accessing of data over the internet rather than your computer's hard drive. This means you don't access the data from either your computer's hard drive or over a dedicated computer network (home or office network). Cloud computing means data is stored at a remote place and is synchronized with other web information.

One prominent example of cloud computing is Office 365 which allows users to store, access, edit their MS Office documents online (in browser) without installing the actual program on their device.



Architecture of Cloud Computing

The architecture of cloud computing comprises of the following components −

- Front-end device
- Back-end platform
- Cloud-based delivery
- Network

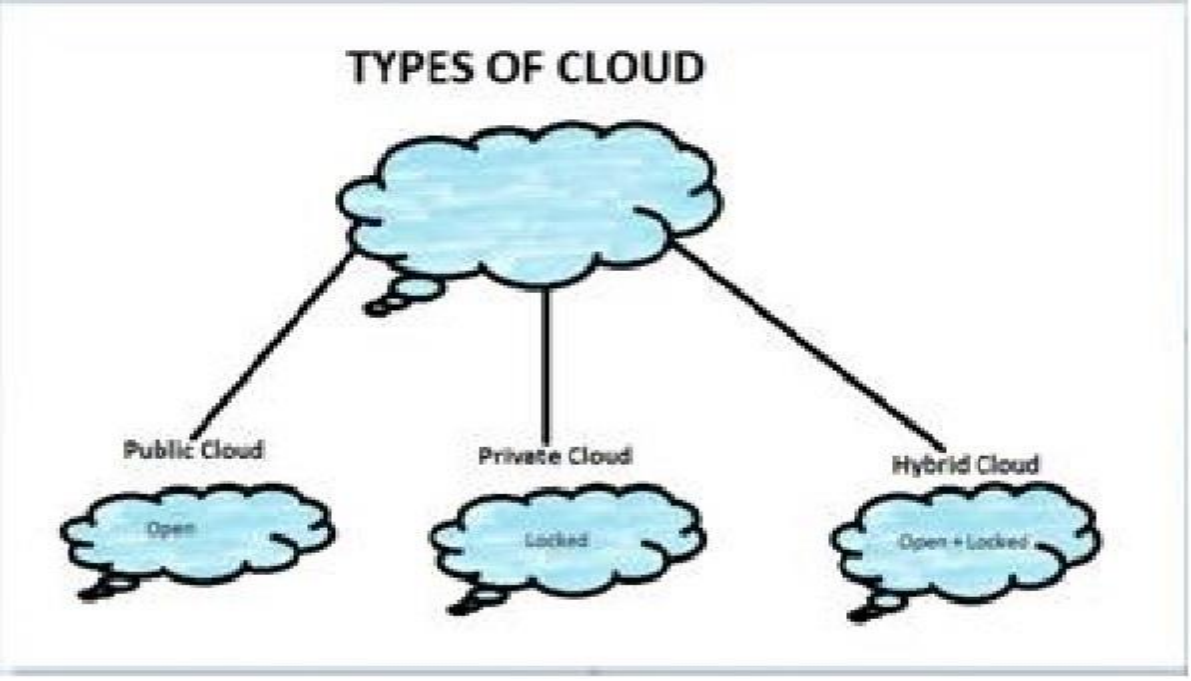
Front-end Devices − These are basically the devices that are used by clients to access the data or program using the browser or special applications.

Back-end Platform − There are various computers, servers, virtual machines, etc. that combine to become a back-end platform.

Types of Cloud

The storage options on cloud is in 3 forms −

- Public
- Private
- Hybrid



Public Cloud − A service provider makes the clouds available to the general public which is termed as a public cloud. These clouds are accessed through internet by users. These are open to public and their infrastructure is owned and operated by service providers as in case of Google and Microsoft.

Private Cloud − These clouds are dedicated to a particular organization. That particular organization can use the cloud for storing the company's data, hosting business application, etc. The data stored on private cloud can't be shared with other organizations. The cloud is managed either by the organization itself or by the third party.

Hybrid Cloud − When two or more clouds are bound together to offer the advantage of both public and private clouds, they are termed as Hybrid Cloud. Organizations can use private clouds for sensitive application, while public clouds for non-sensitive applications. The hybrid clouds provide flexible, scalable and cost-effective solutions to the organizations.

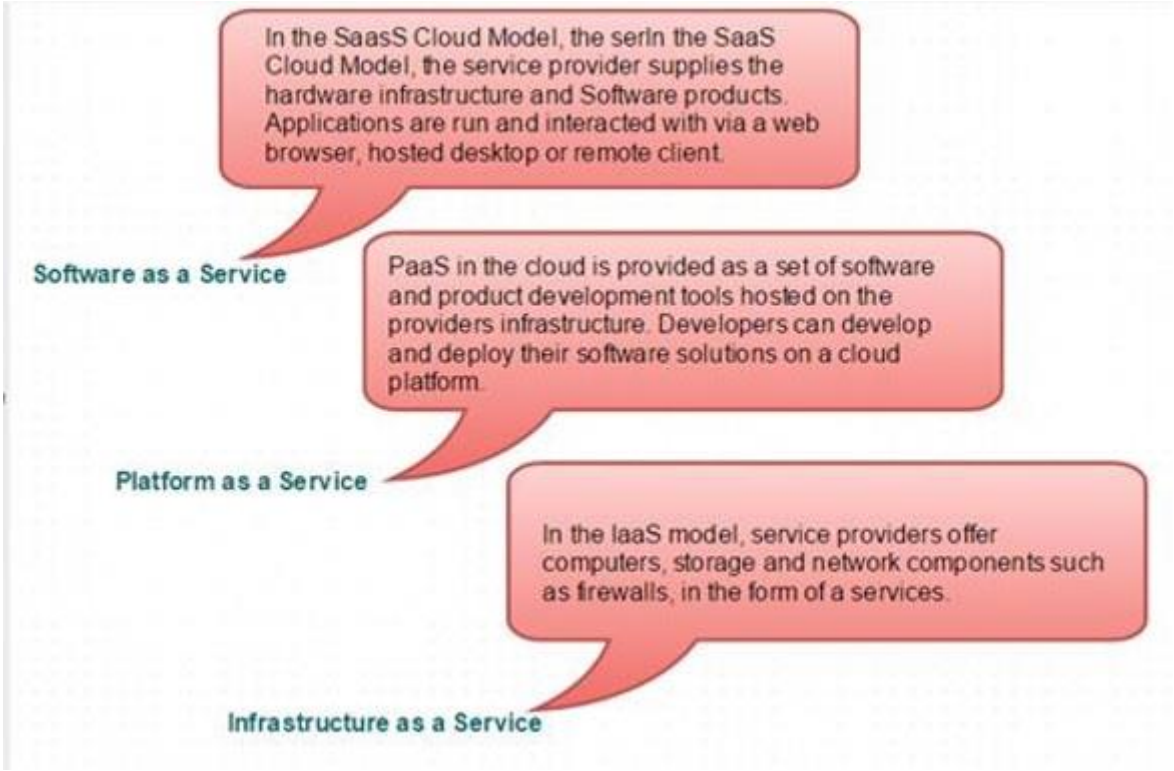
Benefits of Cloud

There are many benefits of clouds. Some of them are listed below.

- Cloud service offers scalability. Allocation and de-allocation of resources is dynamically as per demand.
- It saves on cost by reducing capital infrastructure.
- It allows the user to access the application independent of their location and hardware configuration.
- It simplifies the network and lets the client access the application without buying license for individual machine.
- Storing data on clouds is more reliable as it is not lost easily.

SPI

Next comes how cloud services are categorized. S stand for Software, P stands for Platform and I for Infrastructure in SPI. SaaS is Software as a service; PaaS is Platform as a service and IaaS is Infrastructure as a Service.



Following are the live examples of these models.

- **SAAS Model** – E-mail (Gmail, Yahoo, etc.)
- **PAAS Model** – Microsoft Azure
- **IAAS Model** – Amazon S3

Internet Of Things(IoT)

Internet of Things(IoT) is a network of physical objects or people called "things" that are embedded with software, electronics, network, and sensors that allows these objects to collect and exchange data. The goal of IoT is to extend to internet connectivity from standard devices like computer, mobile, tablet to relatively dumb devices like a toaster.

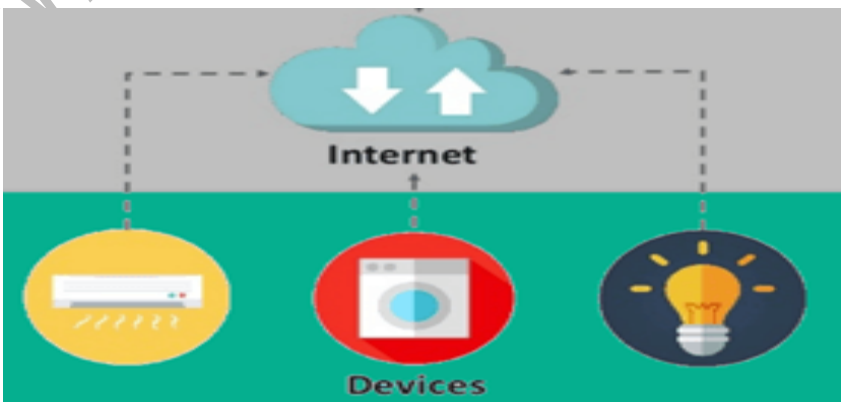
IoT makes virtually everything "smart," by improving aspects of our life with the power of data collection, AI algorithm, and networks. The thing in IoT can also be a person with a diabetes monitor implant, an animal with tracking devices, etc.



History of IOT

- 1970- The actual idea of connected devices was proposed
- 1990- John Romkey created a toaster which could be turned on/off over the Internet
- 1995- Siemens introduced the first cellular module built for M2M
- 1999- The term "Internet of Things" was used by Kevin Ashton during his work at P&G which became widely accepted
- 2004 - The term was mentioned in famous publications like the Guardian, Boston Globe, and Scientific American
- 2005-UN's International Telecommunications Union (ITU) published its first report on this topic.
- 2008- The Internet of Things was born
- 2011- Gartner, the market research company, include "The Internet of Things" technology in their research

How IOT works?



NAKAR EDUCATION

The entire IOT process starts with the devices themselves like smartphones, smartwatches, electronic appliances like TV, Washing Machine which helps you to communicate with the IOT platform.

Here, are four fundamental components of an IoT system:

1) Sensors/Devices: Sensors or devices are a key component that helps you to collect live data from the surrounding environment. All this data may have various levels of complexities. It could be a simple temperature monitoring sensor, or it may be in the form of the video feed.

A device may have various types of sensors which performs multiple tasks **apart** from sensing. Example, A mobile phone is a device which has multiple sensors like GPS, camera but your smartphone is not able to sense these things.

2) Connectivity: All the collected data is sent to a cloud infrastructure. The sensors should be connected to the cloud using various mediums of communications. These communication mediums include mobile or satellite networks, Bluetooth, WI-FI, WAN, etc.

3) Data Processing: Once that data is collected, and it gets to the cloud, the software performs processing on the gathered data. This process can be just checking the temperature, reading on devices like AC or heaters. However, it can sometimes also be very complex like identifying objects, using computer vision on video.

4)User Interface: The information needs to be available to the end-user in some way which can be achieved by triggering alarms on their phones or sending them notification through email or text message. The user sometimes might need an interface which actively checks their IOT system. For example, the user has a camera installed in his home. He wants to access video recording and all the feeds with the help of a web server.

However, it's not always one-way communication. Depending on the IoT application and complexity of the system, the user may also be able to perform an action which may create cascading effects.

DIWAKAR EDUCATION HUB

For example, if a user detects any changes in the temperature of the refrigerator, with the help of IOT technology the user should able to adjust the temperature with the help of their mobile phone.

IoT Applications



IoT Applications

IoT solutions are widely used in numerous companies across industries. Some most common IoT applications are given below:

Application type	Description
Smart Thermostats	Helps you to save resource on heating bills by knowing your usage patterns.
Connected Cars	IOT helps automobile companies handle billing, parking, insurance, and other related stuff automatically.
Activity Trackers	Helps you to capture heart rate pattern, calorie expenditure, activity

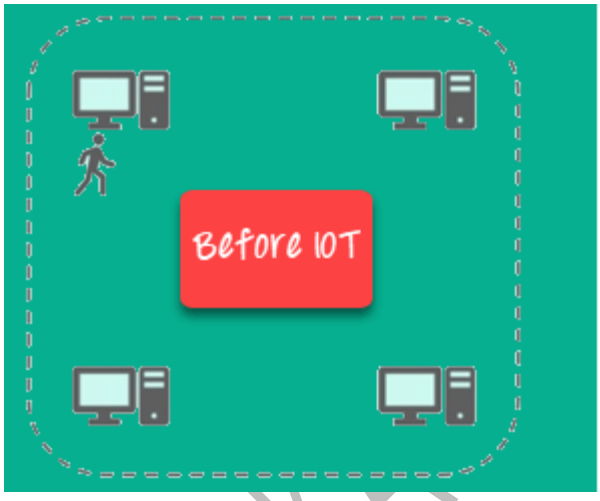
	levels, and skin temperature on your wrist.
Smart Outlets	Remotely turn any device on or off. It also allows you to track a device's energy level and get custom notifications directly into your smartphone.
Parking Sensors	IOT technology helps users to identify the real-time availability of parking spaces on their phone.
Connect Health	The concept of a connected health care system facilitates real-time health monitoring and patient care. It helps in improved medical decision-making based on patient data.
Smart City	Smart city offers all types of use cases which include traffic management to water distribution, waste management, etc.
Smart home	Smart home encapsulates the connectivity inside your homes. It includes smoke detectors, home appliances, light bulbs, windows, door locks, etc.
Smart supply chain	Helps you in real time tracking of goods while they are on the road, or getting suppliers to exchange inventory information.

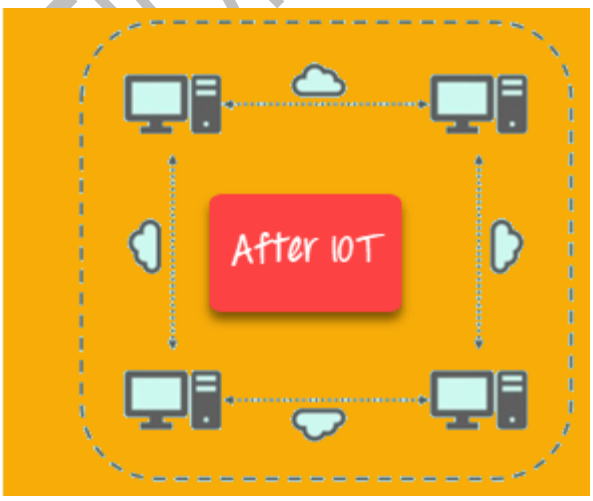
Challenges of IoT

At present IoT is faced with many challenges, such as:

- Insufficient testing and updating
- Concern regarding data security and privacy
- Software complexity
- Data volumes and interpretation
- Integration with AI and automation
- Devices require a constant power supply which is difficult
- Interaction and short-range communication

Advantages of IoT





Key benefits of IoT technology are as follows:

- **Technical Optimization:** IoT technology helps a lot in improving technologies and making them better. Example, with IoT, a manufacturer is able to collect data from various car sensors. The manufacturer analyzes them to improve its design and make them more efficient.
- **Improved Data Collection:** Traditional data collection has its limitations and its design for passive use. IoT facilitates immediate action on data.
- **Reduced Waste:** IoT offers real-time information leading to effective decision making & management of resources. For example, if a manufacturer finds an issue in multiple car engines, he can track the

manufacturing plan of those engines and solves this issue with the manufacturing belt.

- **Improved Customer Engagement:** IoT allows you to improve customer experience by detecting problems and improving the process.

Disadvantages IOT

- **Security:** IoT technology creates an ecosystem of connected devices. However, during this process, the system may offer little authentication control despite sufficient security measures.
- **Privacy:** The use of IOT, exposes a substantial amount of personal data, in extreme detail, without the user's active participation. This creates lots of privacy issues.
- **Flexibility:** There is a huge concern regarding the flexibility of an IoT system. It is mainly regarding integrating with another system as there are many diverse systems involved in the process.
- **Complexity:** The design of the IOT system is also quite complicated. Moreover, it's deployment and maintenance also not very easy.
- **Compliance:** IOT has its own set of rules and regulations. However, because of its complexity, the task of compliance is quite challenging.

IOT Best Practices

- Design products for reliability and security
- Use strong authentication and security protocols
- Disable non-essential services
- Ensure Internet-managed, and IoT management hubs & services are secured
- Energy efficient algorithms should be designed for the system to be active longer.

Cloud Computing Software as a Service (SaaS)

Software-as–a-Service (SaaS) model allows to provide software application as a service to the end users. It refers to a software that is deployed on a host service and is accessible via Internet. There are several SaaS applications listed below:

- Billing and invoicing system

DIWAKAR EDUCATION HUB

- Customer Relationship Management (CRM) applications
- Help desk applications
- Human Resource (HR) solutions

Some of the SaaS applications are not customizable such as **Microsoft Office Suite.** But SaaS provides us **Application Programming Interface (API),** which allows the developer to develop a customized application.

Characteristics

Here are the characteristics of SaaS service model:

- SaaS makes the software available over the Internet.
- The software applications are maintained by the vendor.
- The license to the software may be subscription based or usage based. And it is billed on recurring basis.
- SaaS applications are cost-effective since they do not require any maintenance at end user side.
- They are available on demand.
- They can be scaled up or down on demand.
- They are automatically upgraded and updated.
- SaaS offers shared data model. Therefore, multiple users can share single instance of infrastructure. It is not required to hard code the functionality for individual users.
- All users run the same version of the software.

Benefits

Using SaaS has proved to be beneficial in terms of scalability, efficiency and performance. Some of the benefits are listed below:

- Modest software tools
- Efficient use of software licenses
- Centralized management and data
- Platform responsibilities managed by provider
- Multitenant solutions

Modest software tools

The SaaS application deployment requires a little or no client side software installation, which results in the following benefits:

- No requirement for complex software packages at client side
- Little or no risk of configuration at client side
- Low distribution cost

Efficient use of software licenses

The customer can have single license for multiple computers running at different locations which reduces the licensing cost. Also, there is no requirement for license servers because the software runs in the provider's infrastructure.

Centralized management and data

The cloud provider stores data centrally. However, the cloud providers may store data in a decentralized manner for the sake of redundancy and reliability.

Platform responsibilities managed by providers

All platform responsibilities such as backups, system maintenance, security, hardware refresh, power management, etc. are performed by the cloud provider. The customer does not need to bother about them.

Multitenant solutions

Multitenant solutions allow multiple users to share single instance of different resources in virtual isolation. Customers can customize their application without affecting the core functionality.

Issues

There are several issues associated with SaaS, some of them are listed below:

- Browser based risks
- Network dependence
- Lack of portability between SaaS clouds

Browser based risks

If the customer visits malicious website and browser becomes infected, the subsequent access to SaaS application might compromise the customer's data.

To avoid such risks, the customer can use multiple browsers and dedicate a specific browser to access SaaS applications or can use virtual desktop while accessing the SaaS applications.

Network dependence

The SaaS application can be delivered only when network is continuously available. Also network should be reliable but the network reliability cannot be guaranteed either by cloud provider or by the customer.

Lack of portability between SaaS clouds

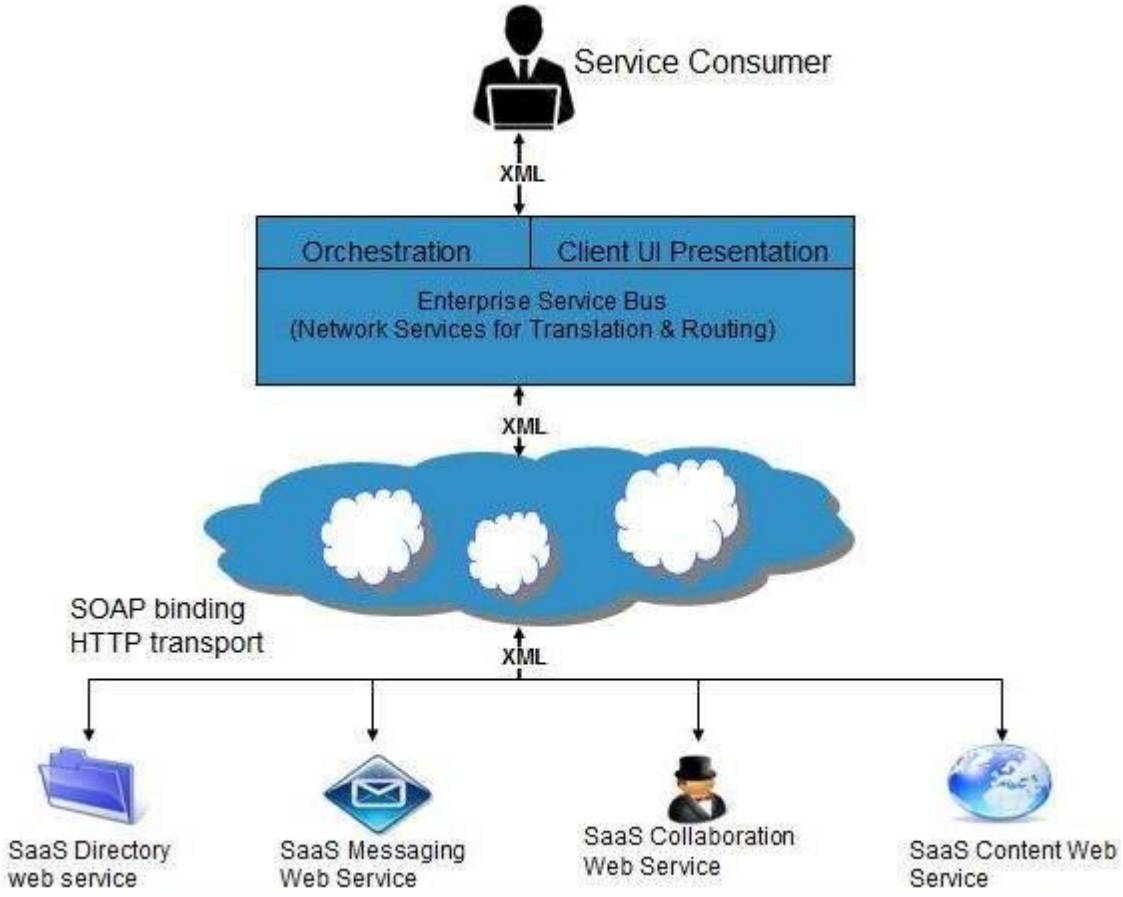
Transferring workloads from one SaaS cloud to another is not so easy because work flow, business logics, user interfaces, support scripts can be provider specific.

Open SaaS and SOA

Open SaaS uses those SaaS applications, which are developed using open source programming language. These SaaS applications can run on any open source operating system and database. Open SaaS has several benefits listed below:

- No License Required
- Low Deployment Cost
- Less Vendor Lock-in
- More portable applications
- More Robust Solution

The following diagram shows the SaaS implementation based on SOA:



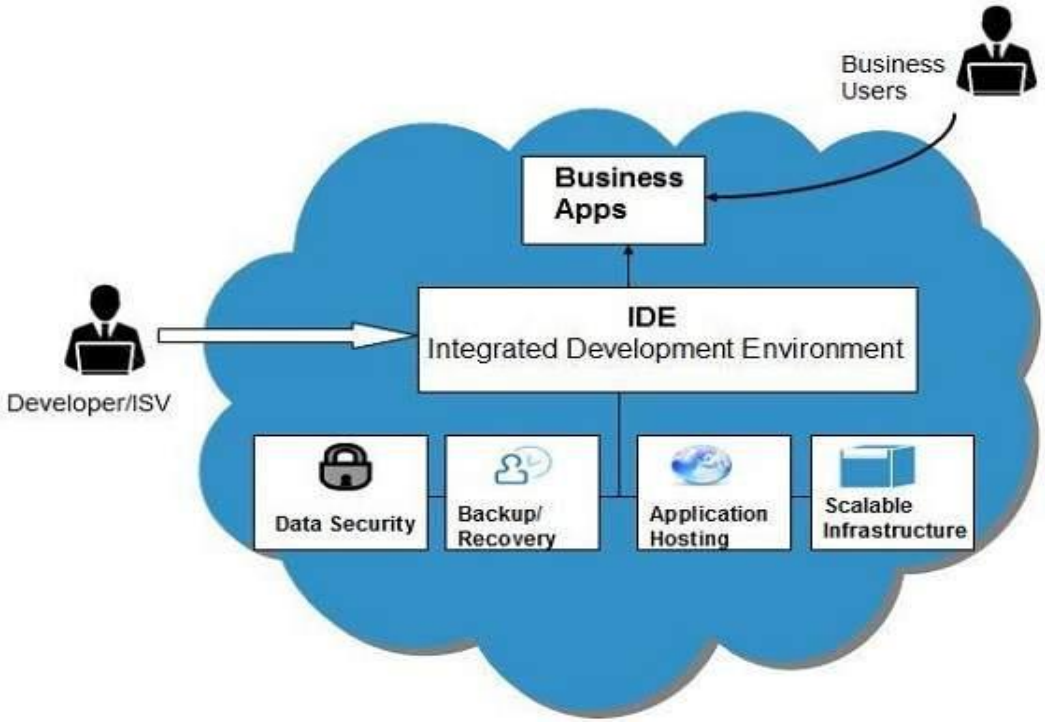
Cloud Computing Platform as a Service (PaaS)

Platform-as-a-Service offers the runtime environment for applications. It also offers development and deployment tools required to develop applications. PaaS has a feature of **point-and-click** tools that enables non-developers to create web applications.

App Engine of Google and **Force.com** are examples of PaaS offering vendors. Developer may log on to these websites and use the **built-in API** to create web-based applications.

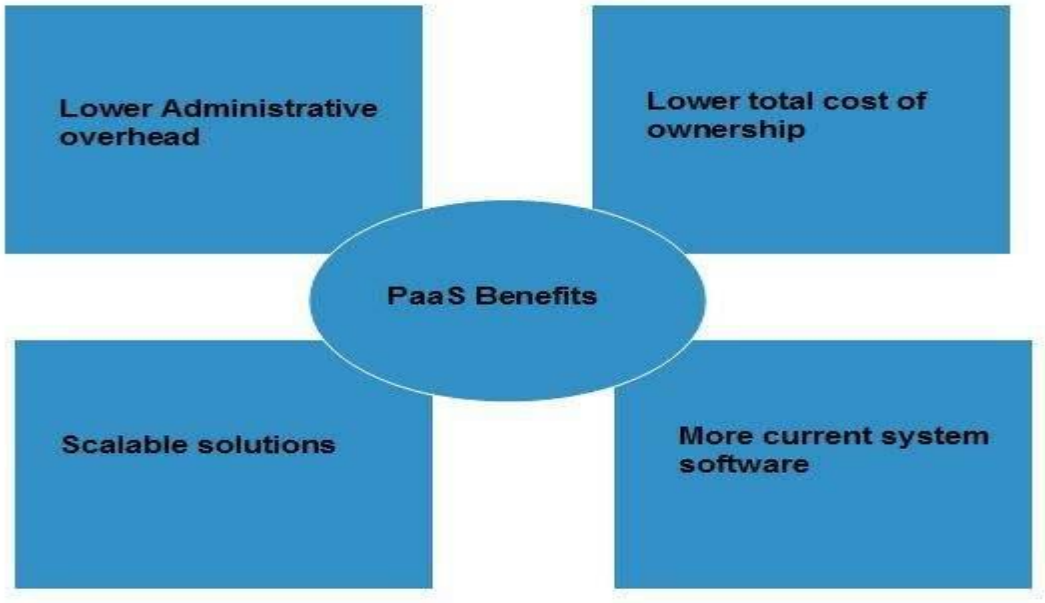
But the disadvantage of using PaaS is that, the developer **locks-in** with a particular vendor. For example, an application written in Python against API of Google, and using App Engine of Google is likely to work only in that environment.

The following diagram shows how PaaS offers an API and development tools to the developers and how it helps the end user to access business applications.



Benefits

Following are the benefits of PaaS model:



Lower administrative overhead

Customer need not bother about the administration because it is the responsibility of cloud provider.

Lower total cost of ownership

Customer need not purchase expensive hardware, servers, power, and data storage.

Scalable solutions

It is very easy to scale the resources up or down automatically, based on their demand.

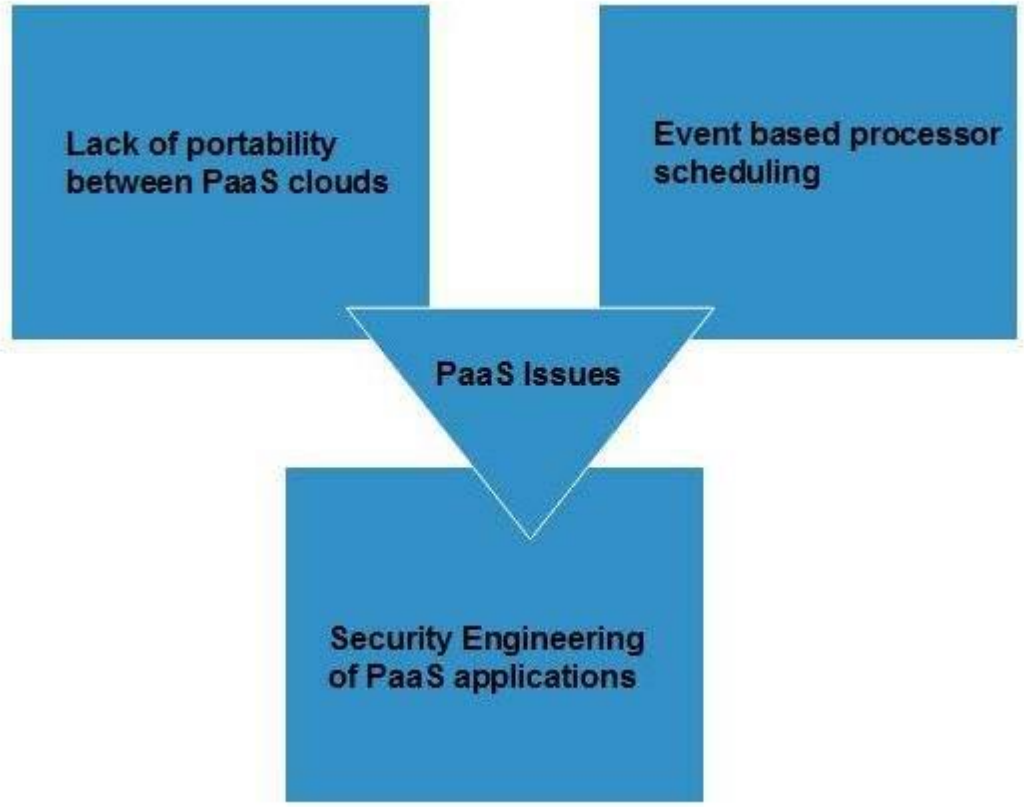
More current system software

It is the responsibility of the cloud provider to maintain software versions and patch installations.

Issues

Like **SaaS, PaaS** also places significant burdens on customer's browsers to maintain reliable and secure connections to the provider's systems. Therefore, PaaS shares many of the issues of SaaS. However, there are some specific issues associated with PaaS as shown in the following diagram:

DIWAKAR



Lack of portability between PaaS clouds

Although standard languages are used, yet the implementations of platform services may vary. For example, file, queue, or hash table interfaces of one platform may differ from another, making it difficult to transfer the workloads from one platform to another.

Event based processor scheduling

The PaaS applications are event-oriented which poses resource constraints on applications, i.e., they have to answer a request in a given interval of time.

Security engineering of PaaS applications

Since PaaS applications are dependent on network, they must explicitly use cryptography and manage security exposures.

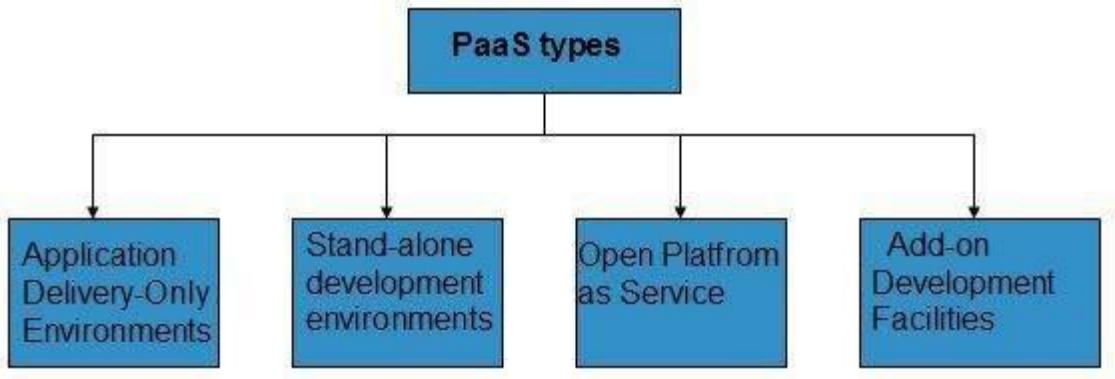
Characteristics

Here are the characteristics of PaaS service model:

- PaaS offers **browser based development environment.** It allows the developer to create database and edit the application code either via Application Programming Interface or point-and-click tools.
- PaaS provides **built-in security, scalability,** and **web service interfaces.**
- PaaS provides built-in tools for defining **workflow, approval processes,** and business rules.
- It is easy to integrate PaaS with other applications on the same platform.
- PaaS also provides web services interfaces that allow us to connect the applications outside the platform.

PaaS Types

Based on the functions, PaaS can be classified into four types as shown in the following diagram:



Stand-alone development environments

The **stand-alone PaaS** works as an independent entity for a specific function. It does not include licensing or technical dependencies on specific SaaS applications.

Application delivery-only environments

The **application delivery PaaS** includes **on-demand scaling** and **application security.**

Open platform as a service

Open PaaS offers an **open source software** that helps a PaaS provider to run applications.

Add-on development facilities

The **add-on PaaS** allows to customize the existing SaaS platform.

Infrastructure as a Service | IaaS

Iaas is also known as **Hardware as a Service (HaaS)**. It is one of the layers of the cloud computing platform. It allows customers to outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources. Customers access these resources on the Internet using a pay-as-per use model.

In traditional hosting services, IT infrastructure was rented out for a specific period of time, with pre-determined hardware configuration. The client paid for the configuration and time, regardless of the actual use. With the help of the IaaS cloud computing platform layer, clients can dynamically scale the configuration to meet changing requirements and are billed only for the services actually used.

IaaS cloud computing platform layer eliminates the need for every organization to maintain the IT infrastructure.

aaS is offered in three models: public, private, and hybrid cloud. The private cloud implies that the infrastructure resides at the customer-premise. In the case of public cloud, it is located at the cloud computing platform vendor's data center, and the hybrid cloud is a combination of the two in which the customer selects the best of both public cloud or private cloud.

IaaS provider provides the following services -

1. **Compute:** Computing as a Service includes virtual central processing units and virtual main memory for the Vms that is provisioned to the end- users.
2. **Storage:** IaaS provider provides back-end storage for storing files.
3. **Network:** Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the Vms.

DIWAKAR EDUCATION HUB

4. **Load balancers:** It provides load balancing capability at the infrastructure layer.



Advantages of IaaS cloud computing layer

There are the following advantages of IaaS computing layer -

1. Shared infrastructure

IaaS allows multiple users to share the same physical infrastructure.

2. Web access to the resources

Iaas allows IT users to access resources over the internet.

3. Pay-as-per-use model

IaaS providers provide services based on the pay-as-per-use basis. The users are required to pay for what they have used.

4. Focus on the core business

IaaS providers focus on the organization's core business rather than on IT infrastructure.

DIWAKAR EDUC

5. On-demand scalability

On-demand scalability is one of the biggest advantages of IaaS. Using IaaS, users do not worry about to upgrade software and troubleshoot the issues related to hardware components.

Disadvantages of IaaS cloud computing layer

1. Security

Security is one of the biggest issues in IaaS. Most of the IaaS providers are not able to provide 100% security.

2. Maintenance & Upgrade

Although IaaS service providers maintain the software, but they do not upgrade the software for some organizations.

3. Interoperability issues

It is difficult to migrate VM from one IaaS provider to the other, so the customers might face problem related to vendor lock-in.

Some important point about IaaS cloud computing layer

IaaS cloud computing platform cannot replace the traditional hosting method, but it provides more than that, and each resource which are used are predictable as per the usage.

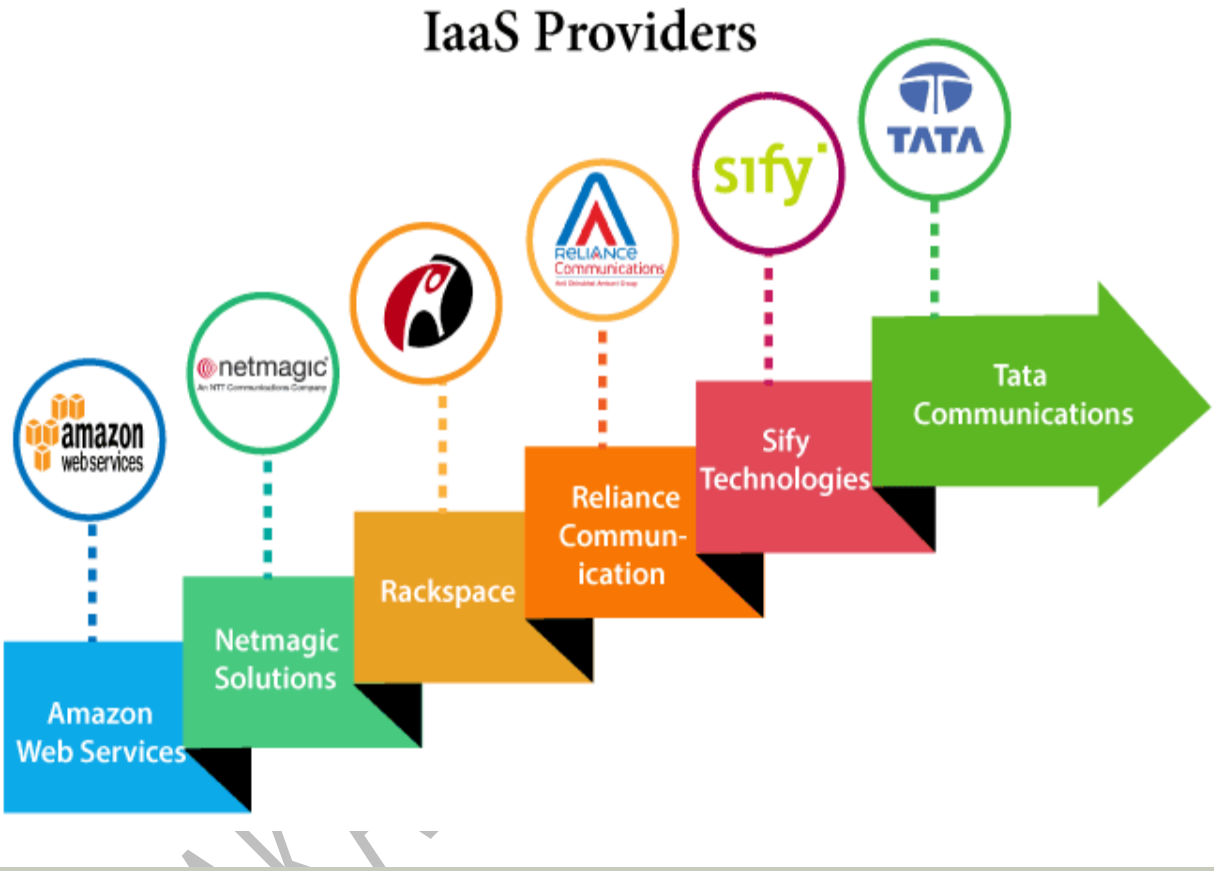
IaaS cloud computing platform may not eliminate the need for an in-house IT department. It will be needed to monitor or control the IaaS setup. IT salary expenditure might not reduce significantly, but other IT expenses can be reduced.

Breakdowns at the IaaS cloud computing platform vendor's can bring your business to the halt stage. Assess the IaaS cloud computing platform vendor's stability and finances. Make sure that SLAs (i.e., Service Level Agreement) provide backups for data, hardware, network, and application failures. Image portability and third-party support is a plus point.

DIWAKAR EDUCATION HUB

The IaaS cloud computing platform vendor can get access to your sensitive data. So, engage with credible companies or organizations. Study their security policies and precautions.

Top Iaas Providers who are providing IaaS cloud computing platform



IaaS Vendor	Iaas Solution	Details
Amazon Web Services	Elastic, Elastic Compute Cloud (EC2) MapReduce, Route 53, Virtual Private Cloud, etc.	The cloud computing platform pioneer, Amazon offers auto scaling, cloud monitoring, and load balancing features as part of its portfolio.

Netmagic Solutions	Netmagic IaaS Cloud	Netmagic runs from data centers in Mumbai, Chennai, and Bangalore, and a virtual data center in the United States. Plans are underway to extend services to West Asia.
Rackspace	Cloud servers, cloud files, cloud sites, etc.	The cloud computing platform vendor focuses primarily on enterprise-level hosting services.
Reliance Communications	Reliance Internet Data Center	RIDC supports both traditional hosting and cloud services, with data centers in Mumbai, Bangalore, Hyderabad, and Chennai. The cloud services offered by RIDC include IaaS and SaaS.
Sify Technologies	Sify IaaS	Sify's cloud computing platform is powered by HP's converged infrastructure. The vendor offers all three types of cloud services: IaaS, PaaS, and SaaS.
Tata Communications	InstaCompute	InstaCompute is Tata Communications' IaaS offering. InstaCompute data centers are located in Hyderabad and Singapore, with operations in both countries.

Cloud computing is an Internet-based computing in which shared the pool of resources are available over a broad network access, these resources can e

provisioned or released with minimum management efforts and service provider interaction.

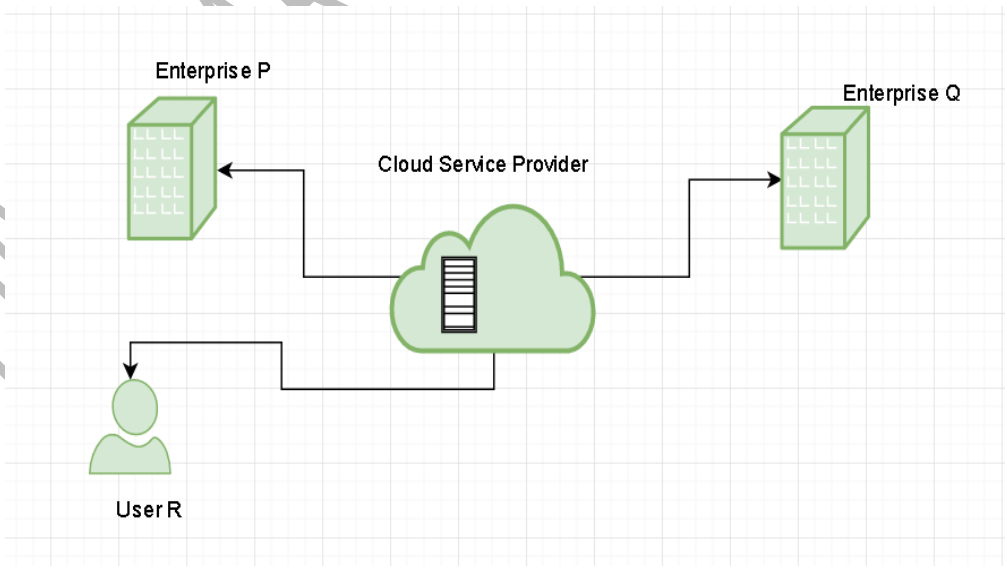
There are four types of cloud:

1. Public cloud
2. Private cloud
3. Hybrid cloud
4. Community cloud

Public cloud:

Public cloud are managed by third parties which provide cloud services over the internet to public, these services are available as pay-as-you-go billing mode. They offer solutions for minimizing IT infrastructure costs and act as a good option for handling peak loads on the local infrastructure. They are a goto option for small enterprises, which are able to start their businesses without large upfront investments by completely relying on public infrastructure for their IT needs.

A fundamental characteristic of public clouds is **multitenancy**. A public cloud is meant to serve multiple users, not a single customer. A user requires a virtual computing environment that is separated, and most likely isolated, from other users.



DINESH REDDY EDUCATION HUB

Computing in which service provider makes all resources public over the internet. It is connected to the public Internet. Service provider serves resources such as virtual machines, applications, storage, etc to the general public over the internet. It may be free of cost or with minimal pay-per-usage. It is available for public display, Google uses the cloud to run some of its applications like google docs, google drive or YouTube, etc.
It is the most common way of implementing cloud computing. External cloud service provider owns, operates and delivers it over the public network.
It is best for the companies which need an infrastructure to accommodate large number of customers and working on projects which has diverse organisation i.e. research institution and NGO etc.

Private cloud :
Private clouds are distributed systems that work on a private infrastructure and providing the users with dynamic provisioning of computing resources. Instead of a pay-as-you-go model as in public clouds, there could be other schemes in that take into account the usage of the cloud and proportionally billing the different departments or sections of an enterprise.

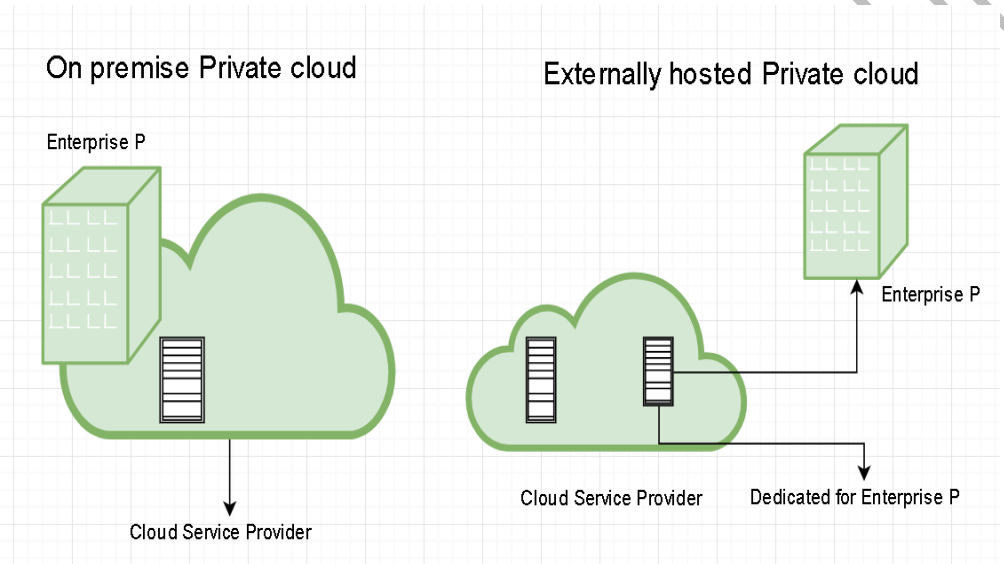
Computing in which service provider makes all resources public over the internet. It only supports connectivity over the private network. It has only authentic users and single-occupant architecture. Google back-end data of the applications like Google Drive, Google docs or YouTube, etc is not available to the public, these types of data and applications run on a private cloud.
The infrastructure and services are maintained and deployed over a private network; hardware and software are dedicated only to a private company i.e. members of the special entity .
It is best for the companies which need an infrastructure which has high performance, high security and privacy due to it's best adaptability and flexibility.

The advantages of using a private cloud are:

1. **Customer information protection:** In private cloud security concerns are less since customer data and other sensitive information does not flow out of a private infrastructure.

DIWAKAR EDUCATION HUB

2. **Infrastructure ensuring SLAs:** Private cloud provides specific operations such as appropriate clustering, data replication, system monitoring and maintenance, and disaster recovery, and other uptime services.
3. **Compliance with standard procedures and operations:** Specific procedures have to be put in place when deploying and executing applications according to third-party compliance standards.This is not possible in case of public cloud.



Below is a table of differences between Public Cloud and Private Cloud:

PUBLIC CLOUD	PRIVATE CLOUD
Cloud Computing infrastructure shared to public by service provider over the internet. It supports multiple customers i.e, enterprises.	Cloud Computing infrastructure shared to private organisation by service provider over the internet. It supports one enterprise.

PUBLIC CLOUD	PRIVATE CLOUD
Multi-Tenancy i.e, Data of many enterprise are stored in shared environment but are isolated. Data is shared as per rule, permission and security.	Single Tenancy i.e, Data of single enterprise is stored.
Cloud service provider provides all the possible services and hardware as the user-base is world. Different people and organization may need different services and hardware. Services provided must be versatile.	Specific hardware and hardware as per need of enterprise are available in private cloud.
It is hosted at Service Provider site.	It is hosted at Service Provider site or enterprise.
It is connected to the public internet.	It only supports connectivity over the private network.
Scalability is very high, and reliability is moderate.	Scalability is limited, and reliability is very high.
Cloud service provider manages cloud and customers use them.	Managed and used by single enterprise.
It is cheaper than private cloud.	It is costlier than public cloud.
Security matters and dependent on service provider.	It gives high class of security.
Performance is low to medium.	Performance is high.

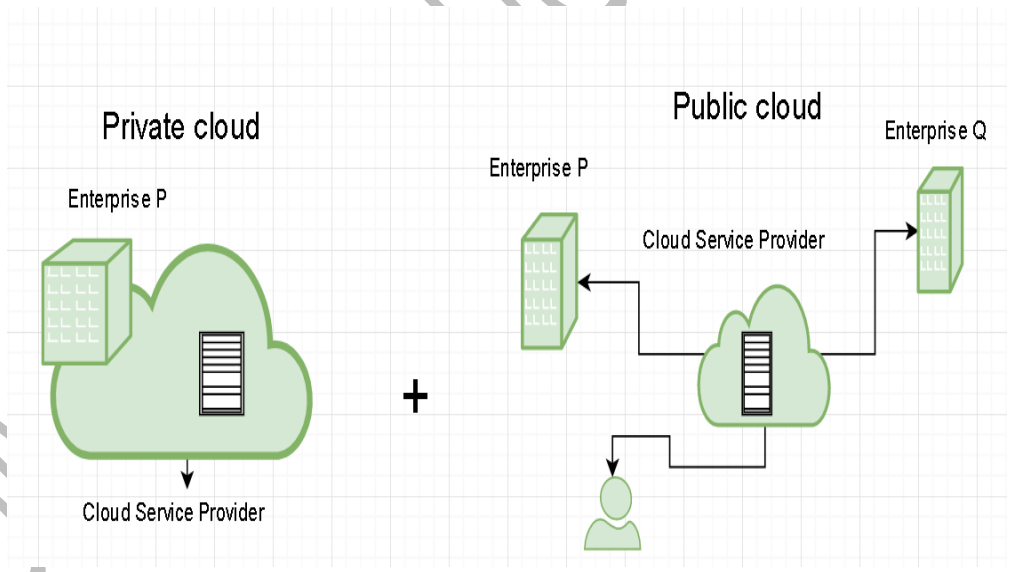
DIWAKAR EDUCATION HUB

PUBLIC CLOUD	PRIVATE CLOUD
It has shared servers.	It has dedicated servers.
Example : Amazon web service (AWS) and Google AppEngine etc.	Example : Microsoft KVM, HP, Red Hat & VMWare etc.

Hybrid cloud:

Hybrid cloud is a heterogeneous distributed system resulted by combining facilities of public cloud and private cloud. For this reason they are also called **heterogeneous clouds.**

A major drawback of private deployments is the inability to scale on demand and to efficiently address peak loads. Here public clouds are needed. Hence, a hybrid cloud takes advantages of both public and private cloud.



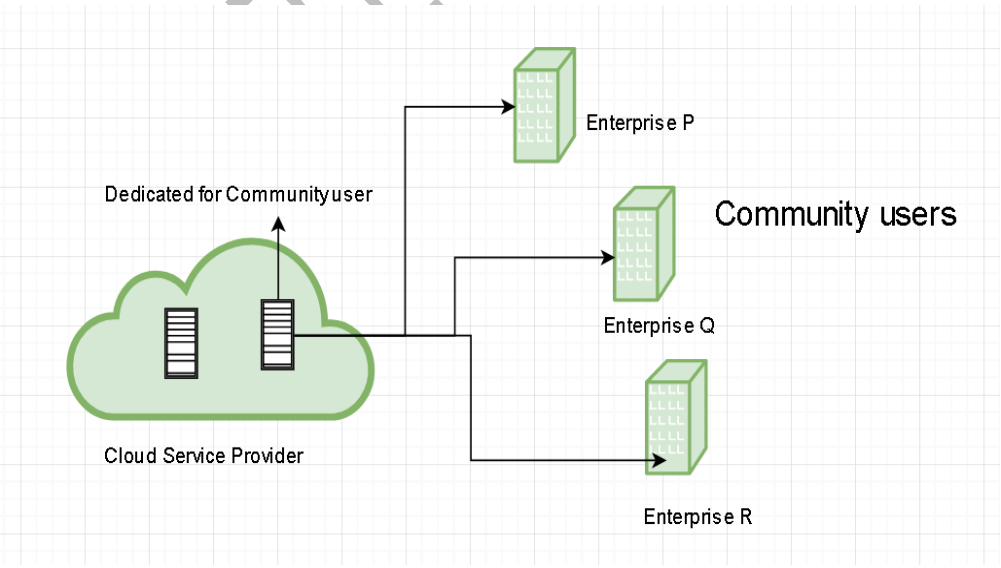
Community cloud:

Community clouds are distributed systems created by integrating the services of different clouds to address the specific needs of an industry, a community, or a

business sector.
In community cloud, the infrastructure is shared between organization which have shared concerns or tasks. The cloud may be managed by an organization or a third party.

Sectors that use community clouds are:

1. **Media industry:** Media companies are looking for quick, simple, low-cost way for increasing efficiency of content generation.Most media productions involve an extended ecosystem of partners. In particular, the creation of digital content is the outcome of a collaborative process that includes movement of large data, massive compute-intensive rendering tasks, and complex workflow executions.
2. **Healthcare industry:** In healthcare industry community clouds are used to share information and knowledge on the global level with sensitive data in the private infrastructure.
3. **Energy and core industry:** In these sectors, the community cloud is used to cluster set of solution which collectively addresses management, deployment, and orchestration of services and operations.
4. **Scientific research:** In this organization with common interests of science share large distributed infrastructure for scientific computing.



Virtualization

Virtualization is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources".

In other words, Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded.

What is the concept behind the Virtualization?

Creation of a virtual machine over existing operating system and hardware is known as Hardware Virtualization. A Virtual machine provides an environment that is logically separated from the underlying hardware.

The machine on which the virtual machine is going to create is known as **Host Machine** and that virtual machine is referred as a **Guest Machine**

Types of Virtualization:

1. Hardware Virtualization.
2. Operating system Virtualization.
3. Server Virtualization.
4. Storage Virtualization.

1) Hardware Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is directly installed on the hardware system* is known as hardware virtualization.

The main job of hypervisor is to control and monitoring the processor, memory and other hardware resources.

After virtualization of hardware system we can install different operating system on it and run different applications on those OS.

Usage:

DIWAKAR EDUCATION HUB

Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

2) Operating System Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is installed on the Host operating system* instead of directly on the hardware system is known as operating system virtualization.

Usage:

Operating System Virtualization is mainly used for testing the applications on different platforms of OS.

3) Server Virtualization:

When the virtual machine software or virtual machine manager *(VMM) is directly installed on the Server system* is known as server virtualization.

Usage:

Server virtualization is done because a single physical server can be divided into multiple servers on the demand basis and for balancing the load.

4) Storage Virtualization:

Storage virtualization is the *process of grouping the physical storage from multiple network storage devices so that it looks like a single storage device*.

Storage virtualization is also implemented by using software applications.

Usage:

Storage virtualization is mainly done for back-up and recovery purposes.

How does virtualization work in cloud computing?

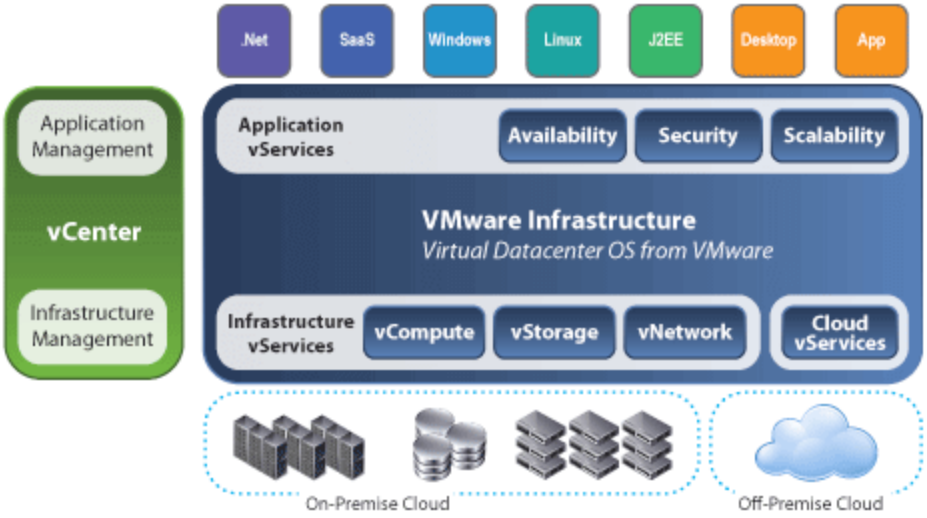
Virtualization plays a very important role in the cloud computing technology, normally in the cloud computing, users share the data present in the clouds like

DIWAKAR EDUCATION HUB

application etc, but actually with the help of virtualization users shares the Infrastructure.

The **main usage of Virtualization Technology** is to provide the applications with the standard versions to their cloud users, suppose if the next version of that application is released, then cloud provider has to provide the latest version to their cloud users and practically it is possible because it is more expensive.

To overcome this problem we use basically virtualization technology, By using virtualization, all severs and the software application which are required by other cloud providers are maintained by the third party people, and the cloud providers has to pay the money on monthly or annual basis.



Conclusion

Mainly Virtualization means, running multiple operating systems on a single machine but sharing all the hardware resources. And it helps us to provide the pool of IT resources so that we can share these IT resources in order get benefits in the business.

Server Virtualization

Server Virtualization is the process of dividing a physical server into several virtual servers, called **virtual private servers**. Each virtual private server can run independently.

The concept of Server Virtualization widely used in the IT infrastructure to minimizes the costs by increasing the utilization of existing resources.

Types of Server Virtualization

1. Hypervisor

In the Server Virtualization, Hypervisor plays an important role. It is a layer between the operating system (OS) and hardware. There are two types of hypervisors.

- Type 1 hypervisor (also known as bare metal or native hypervisors)
- Type 2 hypervisor (also known as hosted or Embedded hypervisors)

The hypervisor is mainly used to perform various tasks such as allocate physical hardware resources (CPU, RAM, etc.) to several smaller independent virtual machines, called "**guest**" on the host machine.

2. Full Virtualization

Full Virtualization uses a **hypervisor** to directly communicate with the CPU and physical server. It provides the best isolation and security mechanism to the virtual machines.

The biggest disadvantage of using hypervisor in full virtualization is that a hypervisor has its own processing needs, so it can slow down the application and server performance.

VMWare ESX server is the best example of full virtualization.

3. Para Virtualization

Para Virtualization is quite similar to the Full Virtualization. The advantage of using this virtualization is that it is **easier to use**, **Enhanced performance**, and **does not require emulation overhead**. Xen primarily and UML use the Para Virtualization.

The difference between full and pare virtualization is that, in para virtualization hypervisor does not need too much processing power to manage the OS.

DIWAKAR EDUCATION HUB

4. Operating System Virtualization

Operating system virtualization is also called as system-lever virtualization. It is a **server virtualization technology** that divides one operating system into multiple isolated user-space called **virtual environments**. The biggest advantage of using server visualization is that it reduces the use of physical space, so it will save money.

Linux OS Virtualization and **Windows OS Virtualization** are the types of Operating System virtualization.

FreeVPS, **OpenVZ**, and **Linux Vserver** are some examples of System-Level Virtualization.

Note: OS-Level Virtualization never uses a hypervisor.

5. Hardware Assisted Virtualization

Hardware Assisted Virtualization was presented by **AMD and Intel**. It is also known as **Hardware virtualization**, **AMD virtualization**, and **Intel virtualization**. It is designed to increase the performance of the processor. The advantage of using Hardware Assisted Virtualization is that it requires less hypervisor overhead.

6. Kernel-Level Virtualization

Kernel-level virtualization is one of the most important types of server virtualization. It is an **open-source virtualization** which uses the Linux kernel as a hypervisor. The advantage of using kernel virtualization is that it does not require any special administrative software and has very less overhead.

User Mode Linux (UML) and **Kernel-based virtual machine** are some examples of kernel virtualization.

Advantages of Server Virtualization

There are the following advantages of Server Virtualization -

1. Independent Restart

DIWAKAR EDUCATION HUB

In Server Virtualization, each server can be restart independently and does not affect the working of other virtual servers.

2. Low Cost

Server Virtualization can divide a single server into multiple virtual private servers, so it reduces the cost of hardware components.

3. Disaster Recovery<

Disaster Recovery is one of the best advantages of Server Virtualization. In Server Virtualization, data can easily and quickly move from one server to another and these data can be stored and retrieved from anywhere.

4. Faster deployment of resources

Server virtualization allows us to deploy our resources in a simpler and faster way.

5. Security

It allows uses to store their sensitive data inside the data centers.

Disadvantages of Server Virtualization

There are the following disadvantages of Server Virtualization -

1. The biggest disadvantage of server virtualization is that when the server goes offline, all the websites that are hosted by the server will also go down.
2. There is no way to measure the performance of virtualized environments.
3. It requires a huge amount of RAM consumption.
4. It is difficult to set up and maintain.
5. Some core applications and databases are not supported virtualization.
6. It requires extra hardware resources.

Uses of Server Virtualization

A list of uses of server virtualization is given below -

DIWAKAR EDUCATION HUB

- Server Virtualization is used in the testing and development environment.
- It improves the availability of servers.
- It allows organizations to make efficient use of resources.
- It reduces redundancy without purchasing additional hardware components.

Cloud Computing Data Storage

Cloud Storage is a service that allows to save data on offsite storage system managed by third-party and is made accessible by a **web services API.**

Storage Devices

Storage devices can be broadly classified into two categories:

- Block Storage Devices
- File Storage Devices

Block Storage Devices

The **block storage devices** offer raw storage to the clients. These raw storage are partitioned to create volumes.

File Storage Devices

The **file Storage Devices** offer storage to clients in the form of files, maintaining its own file system. This storage is in the form of Network Attached Storage (NAS).

Cloud Storage Classes

Cloud storage can be broadly classified into two categories:

- Unmanaged Cloud Storage
- Managed Cloud Storage

Unmanaged Cloud Storage

Unmanaged cloud storage means the storage is preconfigured for the customer. The customer can neither format, nor install his own file system or change drive properties.

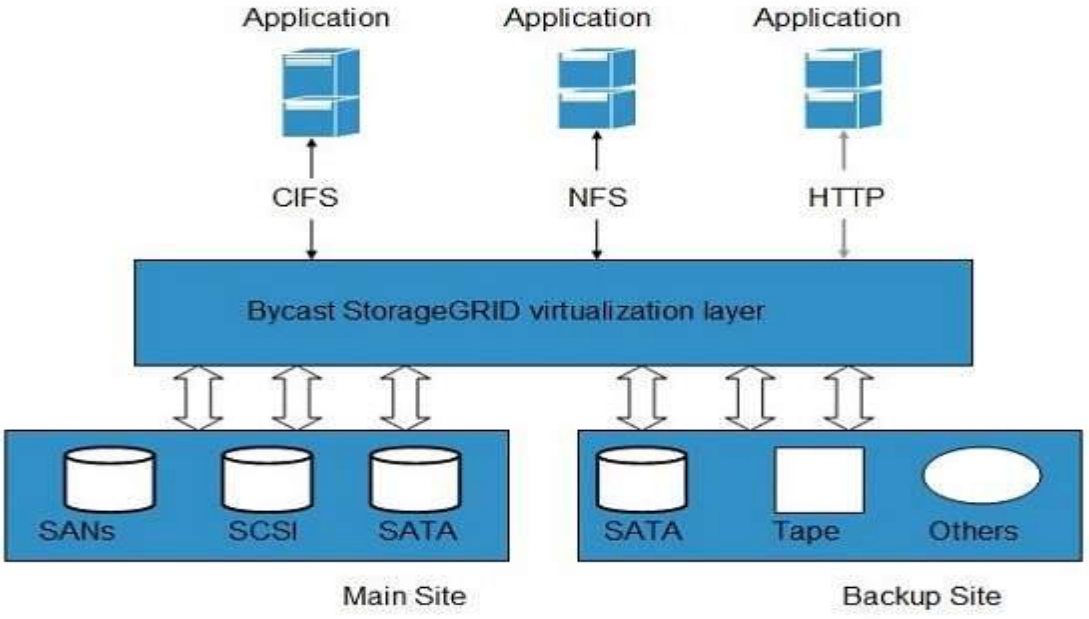
Managed Cloud Storage

Managed cloud storage offers online storage space on-demand. The managed cloud storage system appears to the user to be a raw disk that the user can partition and format.

Creating Cloud Storage System

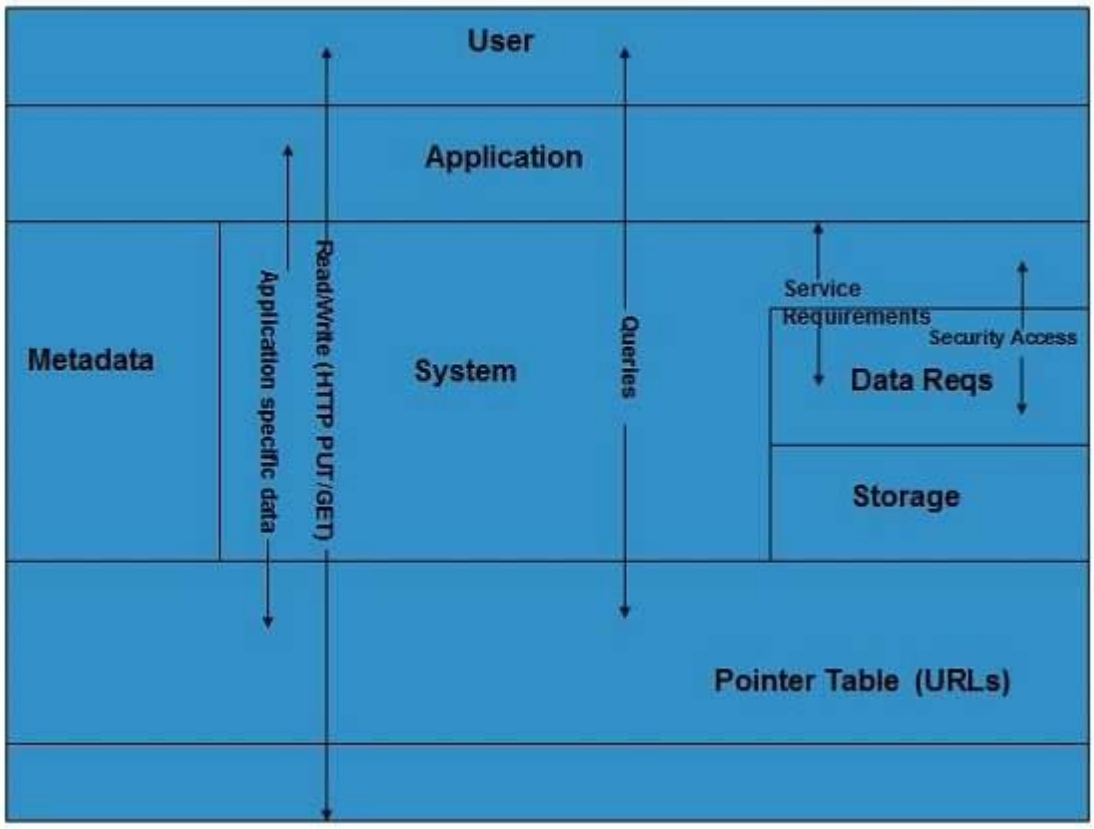
The cloud storage system stores multiple copies of data on multiple servers, at multiple locations. If one system fails, then it is required only to change the pointer to the location, where the object is stored.

To aggregate the storage assets into cloud storage systems, the cloud provider can use storage virtualization software known as **StorageGRID.** It creates a virtualization layer that fetches storage from different storage devices into a single management system. It can also manage data from **CIFS** and **NFS** file systems over the Internet. The following diagram shows how StorageGRID virtualizes the storage into storage clouds:



Virtual Storage Containers

The **virtual storage containers** offer high performance cloud storage systems. **Logical Unit Number (LUN)** of device, files and other objects are created in virtual storage containers. Following diagram shows a virtual storage container, defining a cloud storage domain:



Challenges

Storing the data in cloud is not that simple task. Apart from its flexibility and convenience, it also has several challenges faced by the customers. The customers must be able to:

- Get provision for additional storage on-demand.
- Know and restrict the physical location of the stored data.
- Verify how data was erased.
- Have access to a documented process for disposing of data storage hardware.

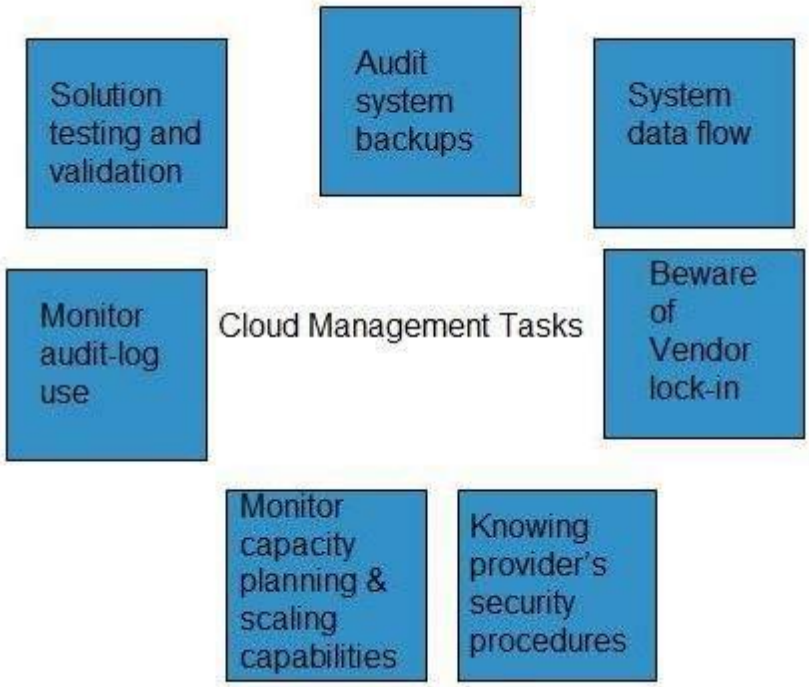
- Have administrator access control over data.

Cloud Computing Management

It is the responsibility of cloud provider to manage resources and their performance. Management of resources includes several aspects of cloud computing such as load balancing, performance, storage, backups, capacity, deployment, etc. The management is essential to access full functionality of resources in the cloud.

Cloud Management Tasks

The cloud provider performs a number of tasks to ensure efficient use of cloud resources. Here, we will discuss some of them:



Audit System Backups

It is required to audit the backups timely to ensure restoring of randomly selected files of different users. Backups can be performed in following ways:

- Backing up files by the company, from on-site computers to the disks that reside within the cloud.
- Backing up files by the cloud provider.

It is necessary to know if cloud provider has encrypted the data, who has access to that data and if the backup is taken at different locations then the user must know the details of those locations.

Data Flow of the System

The managers are responsible to develop a diagram describing a detailed process flow. This process flow describes the movement of data belonging to an organization throughout the cloud solution.

Vendor Lock-In Awareness and Solutions

The managers must know the procedure to exit from services of a particular cloud provider. The procedures must be defined to enable the cloud managers to export data of an organization from their system to another cloud provider.

Knowing Provider's Security Procedures

The managers should know the security plans of the provider for the following services:

- Multitenant use
- E-commerce processing
- Employee screening
- Encryption policy

Monitoring Capacity Planning and Scaling Capabilities

The managers must know the capacity planning in order to ensure whether the cloud provider is meeting the future capacity requirement for his business or not.

The managers must manage the scaling capabilities in order to ensure services can be scaled up or down as per the user need.

Monitor Audit Log Use

In order to identify errors in the system, managers must audit the logs on a regular basis.

Solution Testing and Validation

When the cloud provider offers a solution, it is essential to test it in order to ensure that it gives the correct result and it is error-free. This is necessary for a system to be robust and reliable.

Service level agreements

A **Service Level Agreement (SLA)** is the bond for performance negotiated between the cloud services provider and the client. Earlier, in cloud computing all Service Level Agreements were negotiated between a client and the service consumer. Nowadays, with the initiation of large utility-like cloud computing providers, most Service Level Agreements are standardized until a client becomes a large consumer of cloud services. Service level agreements are also defined at **different levels** which are mentioned below:

- Customer-based SLA
- Service-based SLA
- Multilevel SLA

Few Service Level Agreements are enforceable as contracts, but mostly are agreements or contracts which are more along the lines of an Operating Level Agreement (OLA) and may not have the restriction of law. It is fine to have an attorney review the documents before making a major agreement to the cloud service provider. Service Level Agreements usually specify **some parameters** which are mentioned below:

1. Availability of the Service (uptime)
2. Latency or the response time
3. Service components reliability
4. Each party accountability
5. Warranties

In any case, if a cloud service provider fails to meet the stated targets of minimums then the provider has to pay the penalty to the cloud service consumer

DIWAKAR EDUCATION HUB

as per the agreement. So, Service Level Agreements are like insurance policies in which the corporation has to pay as per the agreements if any casualty occurs. Microsoft publishes the Service Level Agreements linked with the Windows Azure Platform components, which is demonstrative of industry practice for cloud service vendors. Each individual component has its own Service Level Agreements. Below are two **major Service Level Agreements (SLA)** described:

1. **Windows Azure SLA –**
   Window Azure has different SLA's for compute and storage. For compute, there is a guarantee that when a client deploys two or more role instances in separate fault and upgrade domains, client's internet facing roles will have external connectivity minimum 99.95% of the time. Moreover, all of the role instances of the client are monitored and there is guarantee of detection 99.9% of the time when a role instance's process is not runs and initiates properly.
2. **SQL Azure SLA –**
   SQL Azure clients will have connectivity between the database and internet gateway of SQL Azure. SQL Azure will handle a "Monthly Availability" of 99.9% within a month. Monthly Availability Proportion for a particular tenant database is the ratio of the time the database was available to customers to the total time in a month. Time is measured in some intervals of minutes in a 30-day monthly cycle. Availability is always remunerated for a complete month. A portion of time is marked as unavailable if the customer's attempts to connect to a database are denied by the SQL Azure gateway.

Service Level Agreements are based on the usage model. Frequently, cloud providers charge their pay-as-per-use resources at a premium and deploy standards Service Level Agreements only for that purpose. Clients can also subscribe at different levels that guarantees access to a particular amount of purchased resources. The Service Level Agreements (SLAs) attached to a subscription many times offer various terms and conditions. If client requires access to a particular level of resources, then the client need to subscribe to a service. A usage model may not deliver that level of access under peak load condition.

Wireless Networks

DIWAKAR EDUCATION HUB

Computer networks that are not connected by cables are called wireless networks. They generally use radio waves for communication between the network nodes. They allow devices to be connected to the network while roaming around within the network coverage.



Types of Wireless Networks

- Wireless LANs − Connects two or more network devices using wireless distribution techniques.
- Wireless MANs − Connects two or more wireless LANs spreading over a metropolitan area.
- Wireless WANs − Connects large areas comprising LANs, MANs and personal networks.

Advantages of Wireless Networks

- It provides clutter-free desks due to the absence of wires and cables.
- It increases the mobility of network devices connected to the system since the devices need not be connected to each other.

- Accessing network devices from any location within the network coverage or Wi-Fi hotspot becomes convenient since laying out cables is not needed.
- Installation and setup of wireless networks are easier.
- New devices can be easily connected to the existing setup since they needn't be wired to the present equipment. Also, the number of equipment that can be added or removed to the system can vary considerably since they are not limited by the cable capacity. This makes wireless networks very scalable.
- Wireless networks require very limited or no wires. Thus, it reduces the equipment and setup costs.

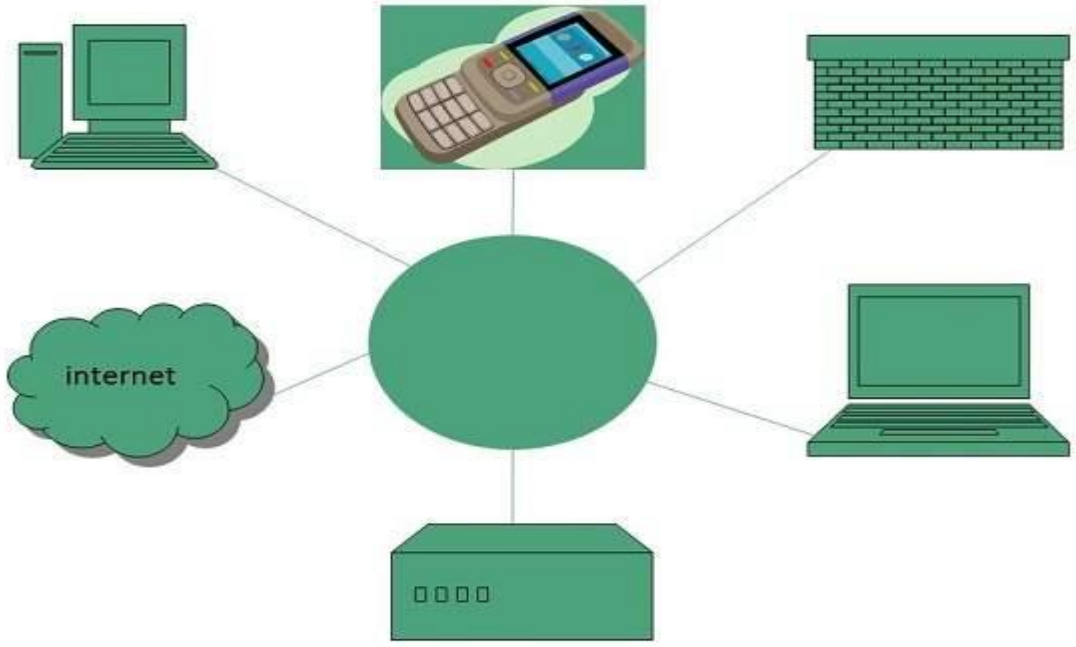
Examples of wireless networks

- Mobile phone networks
- Wireless sensor networks
- Satellite communication networks
- Terrestrial microwave networks

Internet

Internet is defined as an Information super Highway, to access information over the web. However, It can be defined in many ways as follows:

- Internet is a world-wide global system of interconnected computer networks.
- Internet uses the standard Internet Protocol (TCP/IP).
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.
- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.
- For example, a DNS server will resolve a name **http://www.tutorialspoint.com** to a particular IP address to uniquely identify the computer on which this website is hosted.
- Internet is accessible to every user all over the world.



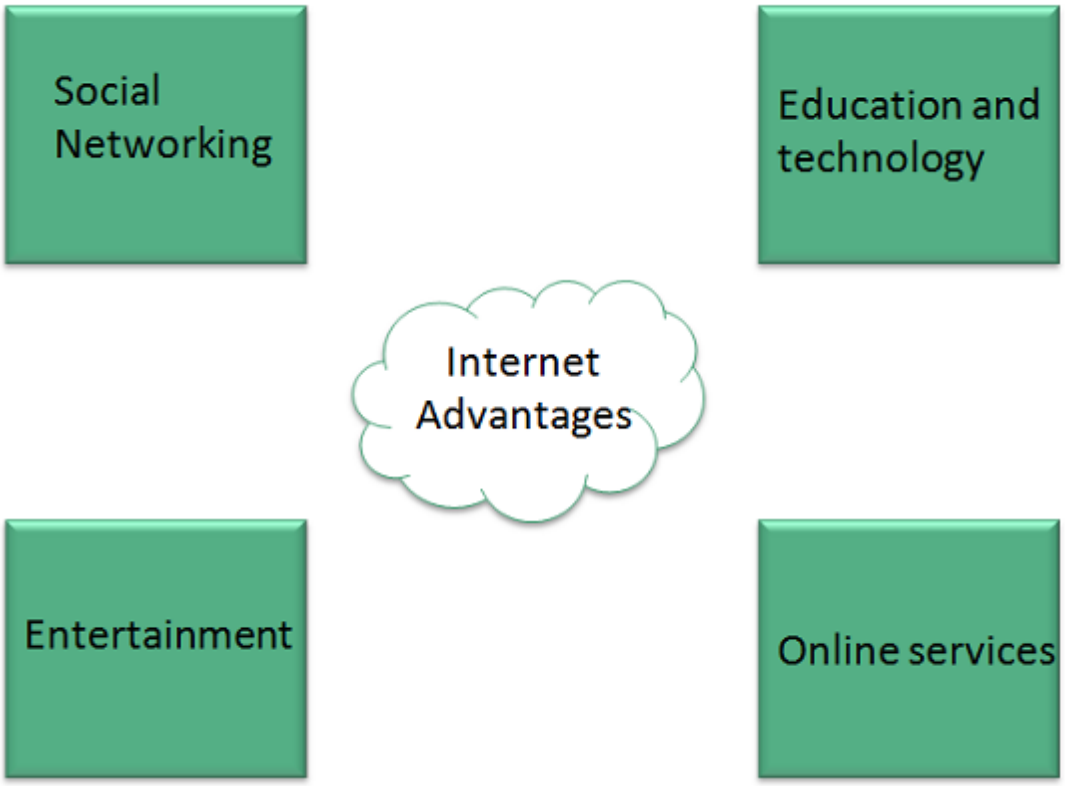
Evolution

The concept of Internet was originated in 1969 and has undergone several technological & Infrastructural changes as discussed below:

- The origin of Internet devised from the concept of **Advanced Research Project Agency Network (ARPANET).**
- **ARPANET** was developed by United States Department of Defense.
- Basic purpose of ARPANET was to provide communication among the various bodies of government.
- Initially, there were only four nodes, formally called **Hosts.**
- In 1972, the **ARPANET** spread over the globe with 23 nodes located at different countries and thus became known as **Internet.**
- By the time, with invention of new technologies such as TCP/IP protocols, DNS, WWW, browsers, scripting languages etc.,Internet provided a medium to publish and access information over the web.

Advantages

Internet covers almost every aspect of life, one can think of. Here, we will discuss some of the advantages of Internet:

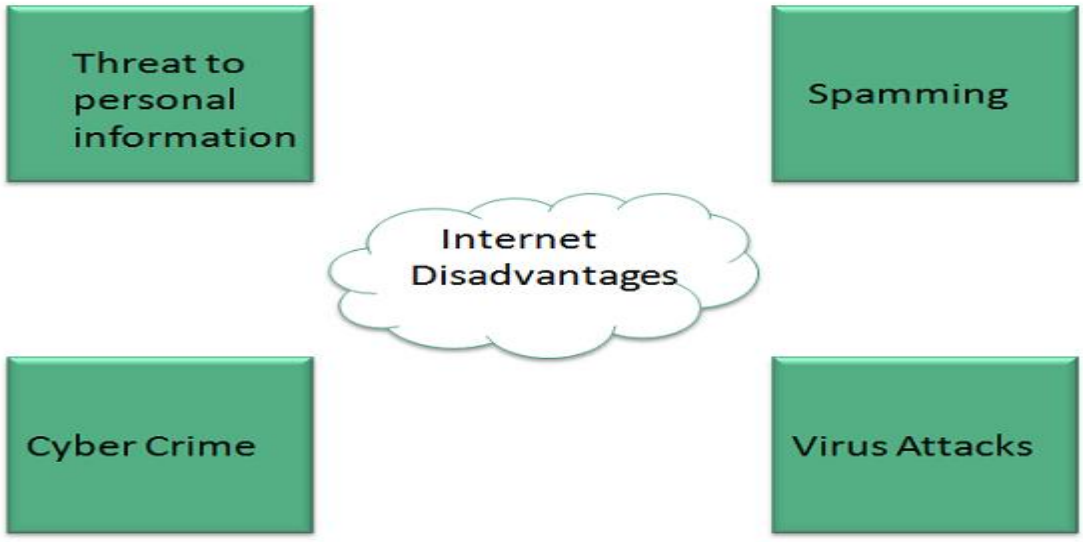


- Internet allows us to communicate with the people sitting at remote locations. There are various apps available on the wed that uses Internet as a medium for communication. One can find various social networking sites such as:
    - Facebook
    - Twitter
    - Yahoo
    - Google+
    - Flickr
    - Orkut
- One can surf for any kind of information over the internet. Information regarding various topics such as Technology, Health & Science, Social Studies, Geographical Information, Information Technology, Products etc can be surfed with help of a search engine.
- Apart from communication and source of information, internet also serves a medium for entertainment. Following are the various modes for entertainment over internet.

  - Online Television
  - Online Games
  - Songs
  - Videos
  - Social Networking Apps
- Internet allows us to use many services like:
  - Internet Banking
  - Matrimonial Services
  - Online Shopping
  - Online Ticket Booking
  - Online Bill Payment
  - Data Sharing
  - E-mail
- Internet provides concept of **electronic commerce**, that allows the business deals to be conducted on electronic systems

Disadvantages

However, Internet has prooved to be a powerful source of information in almost every field, yet there exists many disadvanatges discussed below:



- There are always chances to loose personal information such as name, address, credit card number. Therefore, one should be very careful while

sharing such information. One should use credit cards only through authenticated sites.

- Another disadvantage is the **Spamming**.Spamming corresponds to the unwanted e-mails in bulk. These e-mails serve no purpose and lead to obstruction of entire system.
- **Virus** can easily be spread to the computers connected to internet. Such virus attacks may cause your system to crash or your important data may get deleted.
- Also a biggest threat on internet is pornography. There are many pornographic sites that can be found, letting your children to use internet which indirectly affects the children healthy mental life.
- There are various websites that do not provide the authenticated information. This leads to misconception among many people.

DIWAKAR EDUCATION

DIWAKAR EDUCATION HUB

Data Communication and Computer Networks Unit – 9 MCQs

As per updated syllabus

DIWAKAR EDUCATION HUB

2020

THE LEARN WITH EXPERTIES

1) Which of these is a standard interface for serial data transmission?

a) ASCII
b) RS232C
c) 2
d) Centronics

Answer: (b) RS232C

Explanation: The RS232C is a standard interface for serial data transmission that defines the protocol and physical interface for transmitting serial data fairly easily between associated appliances and computers.

2) Which type of topology is best suited for large businesses which must carefully control and coordinate the operation of distributed branch outlets?

a) Ring
b) Local area
c) Hierarchical
d) Star

Answer: (d) Star

Explanation: The star topology is the best network topology for large businesses because it is simple to control and coordinate from the central computer.

3) Which of the following transmission directions listed is not a legitimate channel?

a) Simplex
b) Half Duplex
c) Full Duplex
d) Double Duplex

Hide Answer Workspace

Answer: (d) Double Duplex

Explanation: Double duplex is not a legitimate channel for transmission in computer network.

4) "Parity bits" are used for which of the following purposes?

a) Encryption of data
b) To transmit faster
c) To detect errors
d) To identify the user

Answer: (c) To detect errors

Explanation: The parity bit is also known as the check bit, and has a value of 0 or 1. It is used for error detection for blocks of data.

5) What kind of transmission medium is most appropriate to carry data in a computer network that is exposed to electrical interferences?

a) Unshielded twisted pair
b) Optical fiber
c) Coaxial cable
d) Microwave

Answer: (b) Optical fiber

Explanation: The optical fiber is made of glass or plastic. In this cable, the transmission of data occurs in the form of light rather than the electric current, so this cable provides higher data transfer speed than other cables.

6) A collection of hyperlinked documents on the internet forms the ?.?

a) World Wide Web (WWW)
b) E-mail system
c) Mailing list
d) Hypertext markup language

Answer: (a) World Wide Web (WWW)

Explanation: World Wide Web (WWW) creates a collection of hyperlinked documents on the Internet.

7) The location of a resource on the internet is given by its?

a) Protocol
b) URL
c) E-mail address
d) ICQ

Answer: (b) URL

Explanation: A URL (Uniform Resource Locator) is a database connection that describes the database's location on a computer network and the retrieval process. A URL is a different form of URI (Uniform Resource Identifier) although the two words are used interchangeably by many people.

8) The term HTTP stands for?

a) Hyper terminal tracing program
b) Hypertext tracing protocol
c) Hypertext transfer protocol
d) Hypertext transfer program

Answer: (c) Hypertext transfer protocol

Explanation: The term HTTP stands for Hypertext transfer protocol.

9) A proxy server is used as the computer?

a) with external access
b) acting as a backup
c) performing file handling
d) accessing user permissions

Answer: (a) with external access

Explanation: A proxy server is a computer that acts as a gateway between a user's computer and the Internet. The proxy server is also called application level gateway. By this the client computer can establish indirect network connection to another network.

10) Which one of the following would breach the integrity of a system?

a) Looking the room to prevent theft
b) Full access rights for all users
c) Fitting the system with an anti-theft device
d) Protecting the device against willful or accidental damage

Answer: (b) Full access rights for all users

Explanation: None

11) Which software prevents the external access to a system?

a) Firewall
b) Gateway
c) Router
d) Virus checker

Answer: (a) Firewall

Explanation: A firewall is a network securing software that prevents unauthorized users and dangerous

elements from accessing the network. Software firewall acts as a filter for our network which prevents harmful information.

12) The structure or format of data is called _____

a) Syntax
b) Semantics
c) Struct
d) Formatting

Answer: a
Explanation: The structure and format of data are defined using syntax. Semantics defines how a particular pattern to be interpreted, and what action is to be taken based on that interpretation. In programming languages, syntax of the instructions plays a vital role in designing of the program.

13) Which of the following best describes uploading information?

a) Sorting data on a disk drive
b) Sending information to a host computer
c) Receiving information from a host computer
d) Sorting data on a hard drive

Answer: (b) Sending information to a host computer

Explanation: None

14) Which one of the following is the most common internet protocol?

a) HTML
b) NetBEUI
c) TCP/IP
d) IPX/SPX

Answer: (c) TCP/IP

Explanation: TCP/IP is the most common internet protocol because it is the most widely used network protocol.

15) Software programs that allow you to legally copy files and give them away at no cost are called which of the following?

a) Probe ware
b) Timeshare
c) Shareware
d) Public domain

Answer: (d) Public domain

Explanation: Public domain software can be modified, distributed or sold by anyone without any attention, but no one can ever own it.

16) The term FTP stands for?

a) File transfer program
b) File transmission protocol
c) File transfer protocol
d) File transfer protection

Answer: (c) File transfer protocol

Explanation: The term FTP stands for File transfer protocol.

17) At what speed does tele-computed refer?

a) Interface speed
b) Cycles per second
c) Baud rate

d) Megabyte load

Hide Answer Workspace

Answer: (c) Baud rate

Explanation: In telecommunication, baud rate is a specific unit of the speed rate. It is one of the significant functions that determine the speed of the communication over the data channel.

18) Which one of the following is not a network topology?

a) Star

b) Ring

c) Bus

d) Peer to Peer

Answer: (d) Peer to Peer

Explanation: Peer to Peer network is a network to which all computers are used the same resources and rights as other computers. Its network designed primarily for the small local area.

19) The maximum length (in bytes) of an IPv4 datagram is?

a) 32
b) 1024
c) 65535
d) 512

Answer: (c) 65535

Explanation: None

20) Which of the following statements could be valid with respect to the ICMP (Internet Control Message Protocol)?

a) It reports all errors which occur during transmission.
b) A redirect message is used when a router notices that a packet seems to have been routed wrongly.
c) It informs routers when an incorrect path has been taken.
d) The "destination unreachable" type message is used when a router cannot locate the destination.

Answer: (b) A redirect message is used when a router notices that a packet seems to have been routed wrongly.

Explanation: None

21) The IP network 192.168.50.0 is to be divided into 10 equal sized subnets. Which of the following subnet masks can be used for the above requirement?

a) 255.243.240
b) 255.255.0.0
c) 255.255.0
d) 255.255.255

Answer: (c) 255.255.255.0

Explanation: This address belongs to class C, so 8 bits are reserved for the host ID. 24 bits are reserved for network ID.

22) When the mail server sends mail to other mail servers it becomes ___ ?

a) SMTP client
b) SMTP server

c) Peer
d) Master

Answer: (a) SMTP client

Explanation: The SMTP client is an organization that allows sending emails using the SMTP server. SMTP servers can't send emails to other SMTP servers separately. It is based on client-server architecture.

23) The length of an IPv6 address is?

a) 32 bits
b) 64 bits
c) 128 bits
d) 256 bits

Answer: (c) 128 bits

Explanation: An IPv6 address is 128 bits long, which has 2^128 address space.

24) Consider the following:

1. Twisted pair cables
2. Microwaves and Satellite Signals
3. Repeaters
4. Analog Transmissions
5. Fiber optics

Which of the above is consider as (a) signal transmission medium is data communications?

a. (1) and (5)

b. (1) and (2)

c. (1) (2) and (5)

d. (1) (2) (3) and (5)

Answer: (c) (1) (2) and (5)

Explanation: None

25) Which of the following address belongs class A?

a) 121.12.12.248
b) 130.12.12.248
c) 128.12.12.248
d) 129.12.12.248

Answer: (a) 121.12.12.248

Explanation: 121.12.12.248 address belongs the class A because the first octet value of this address lies between 0 and 127.

26) Which of the following is correct IPv4 address?

a) 124.201.3.1.52
b) 01.200.128.123
c) 300.142.210.64
d) 10110011.32.16.8
e) 128.64.0.0

Answer: (e) 128.64.0.0

Explanation: 128.64.0.0 is correct IPv4 address because IPv4 is a standard numbering system that uses four integers from 0 to 255. The IP address is a group of numbers that identify user system on the network.

27) Which of the following IP addresses can be used as (a) loop-back addresses?

a) 0.0.0.0

b) 127.0.0.1
c) 255.255.255.255
d) 0.255.255.255

Answer: (b) 127.0.0.1

Explanation: A loopback address is a special IP address whose IP address is between 127.0.0.1 to 127.255.255.255. It is reserved for loopback. It doesn't require a physical connection to a network.

28) The term WAN stands for?

a) Wide Area Net
b) Wide Access Network
c) Wide Area Network
d) Wide Access Net

Answer: (c) Wide Area Network

Explanation: The term WAN stands for Wide Area Network.

29) Which of the following cannot be used as a medium for 802.3 ethernet?

a) A thin coaxial cable
b) A twisted pair cable
c) A microwave link
d) A fiber optical cable

Answer: (c) A microwave link

Explanation: A microwave link cannot be used as a medium for 802.3 ethernets, because a microwave link is a transmission network that utilizes a beam of radio waves in the microwave frequency spectrum to relay video, audio, or data between two places.

30) What IP address class allocates 8 bits for the host identification part?

a) Class A
b) Class B
c) Class C
d) Class D

Answer: (c) Class C

Explanation: In class C only, 8 bits are reserved for the host ID, and 24 bits are reserved for network ID.

31) The term IANA stands for?

a) Internet Assigned Numbers Authority
b) Internal Assigned Numbers Authority
c) Internet Associative Numbers Authoritative
d) Internal Associative Numbers Authority

Answer: (a) Internet Assigned Numbers Authority

Explanation: The term IANA stands for Internet Assigned Numbers Authority.

32) How many versions available of IP?

a. 6 version

b. 4 version

c. 2 version

d. 1 version

Answer: (c) 2 version

Explanation: There are only two IP versions are avilable in the present: IP version 4 (IPv4) and IP version 6 (IPv6).

33) Which layer of the TCP / IP stack corresponds to the OSI model transport layer?

a) Host to host
b) Application
c) Internet
d) Network Access

Answer: (a) Host to Host

Explanation: The host to host layer conforms the transport layer of the OSI model. This layer is responsible for the final correspondence and error-free distribution of data.

34) An Aloha network uses an 18.2 kbps channel for sending message packets of 100 bits long size. Calculate the maximum throughput.

a) 5999
b) 6900
c) 6027
d) 5027

Answer: (c) 0.6027

Explanation: In Pure Aloha, Efficiency = 18.4%

Usable bandwidth for 18.2 kbps = 18.2 * 0.18 = 3.276 kbps

Therefore, the maximum throughput of Pure Aloha

= 1/2e * 3.276

= (18.4 * 3.276) / 100

= **0.6027**

35) On a simplex data link, which of the following is a possible error recovery technique?

a) Backward error correction (BEC)
b) The use of hamming codes
c) Automatic Repeat Request (ARQ)
d) Downward error correction (DEC)

Answer: (b) The use of hamming codes

Explanation: The hamming codes is an error recovery technique that can be used to detect and correct the errors. It was developed by R.W. Hamming.

36) Which of the statement is correct with regard to Time Division Multiplexing (TDM) and its variants?

a) Statistical TDM makes efficient use of the bandwidth only if the arrival pattern of the data stream is probabilistic.
b) TDM requires the transmitter and receiver to be synchronized periodically.
c) TDM performs efficiently if the arrival pattern of the data stream is probabilistic.
d) Statistical TDM is efficient if the data stream is deterministic.

Answer: (a) and (b)

Explanation: None

37) The term IPv4 stands for?

a) Internet Protocol Version 4
b) Internet Programming Version 4
c) International Programming Version4
d) None of these

Answer: (a) Internet Protocol Version 4

Explanation: The term IPv4 stands for Internet Protocol Version 4.

38) The term LAN stands for?

a) Local Area Net
b) Local Aera Network
c) Local Array Network
d) Local Array Net

Answer: (b) Local Area Network

Explanation: The term LAN stands for Local Area Network.

39) Which of the through is share the data of two computer?

a) Library
b) Network
c) Grouping
d) Integrated system

Answer: (b) Network

Explanation: There are many ways to share data between two computers, but a network connection is established before data sharing.

40) In specific, if the systems use separate protocols, which one of the following devices is used to link two systems?

a) Repeater
b) Gateway
c) Bridge
d) Hub

Answer: (b) Gateway

Explanation: If the system used separate protocols, gateway device is used to link two systems.

41) How many digits of the Data Network Identification Code (DNIC) identify the country?

a) first three
b) first four
c) first five
d) first six
e) None of the above

Answer: (a) first three

Explanation: The first three digits of the Data Network Identification Code (DNIC) is identify the country (first digit to identify a zone and other two digits to identify the country within the zone).

42) Which of the following methods is used to broadcast two packets on the medium at a time?

a) Collision
b) Synchronous
c) Asynchronous
d) None of the above

Answer: (a) Collision

Explanation: A collision occurs when two or more computers are attempting to transfer data across a network at a time.

43) Which of the following is true with regard to the ping command?

a) Ping stands for Packet Internet Generator.
b) The ping command checks the port level connectivity between source destinations end points.
c) Ping summarizes the packet loss and round-trip delay between two IP end points.
d) The ping command activates the RARP protocol of the IP layer.

Answer: (c) Ping summarizes the packet loss and round-trip delay between two IP end points.

Explanation: None

44) The private key in asymmetric key cryptography is kept by?

a) Sender
b) Receiver
c) Sender and Receiver
d) None of the these

Answer: (b) Receiver

Explanation: Only the receiver keeps the private key. Its purpose is to ensure that the message can only be decrypted by the intended receiver.

45) Which of the following algorithms is not used in asymmetric-key cryptography?

a) RSA algorithm
b) Diffie-Hellman algorithm
c) Electronic code book algorithm
d) None of the mentioned

Answer: (c) Electronic code book algorithm

Explanation: An electronic code book algorithm is a mode of operation for a block cipher, where each frame of text in an encrypted document refers to a data field. In other terms, the same plaintext value would also give the same value for ciphertext.

46) In the cryptography, the sequence of the letters is rearranged by?

a) Transposition ciphers
b) Substitution ciphers
c) Both a and b
d) None of these

Answer: (a) Transposition ciphers

Explanation: A predefined technique shuffles the sequence of letters in a plaintext message in the transposition ciphers.

47) What is the maximum efficiency of pure aloha at G = 1/2?

a) 1.89
b) 17.99
c) 18.999
d) 18.4

Answer: (d) 18.4

Explanation: The maximum efficiency of pure aloha formula is $G * e^{-2G}$.

Given, G =1/2

=1/2 x e-2 x 1/2

= 1 / 2e

= 0.184

= 18.4%

48) What is the maximum efficiency of slotted aloha at G = 1?

a) 36.8
b) 35.8
c) 35.5
d) 37.8

Answer: (a) 36.8

Explanation: The maximum efficiency of slotted aloha formula is G * e^{-G}.

Given, G = 1

= 1 x e-1

= 1 / e

= 0.368

= 36.8%

49) Which of the following statement is true about error detection techniques used on communications link?

a) Cyclic Redundancy Check (CRC) sequence can detect as well as correct errors.
b) Error detection cannot be used on simplex links.
c) Hamming code can detect up to 3-bit errors.
d) All of the these

Answer: (d) All of the these

Explanation: None

50) The correct order of corresponding OSI layers for having functionalities of routing and reconciling machine representation differences with shared access resolution and ASCII test protocol is?

a) Network, Physical, Transport, Data link
b) Network, Physical, Data link, Application
c) Network, Presentation, Data link, Application
d) Network, Presentation, Physical, Transport

Answer: (c) Network, Presentation, Data link, Application

Explanation: None

51. The IETF standards documents are called _____
a) RFC
b) RCF
c) ID
d) DFC

Answer: a
Explanation: RFC stands for Request For Comments and they are documents that describe methods, behaviors, research, or innovations applicable to the working of the Internet.

52. In the layer hierarchy as the data packet moves from the upper to the lower layers, headers are _____
a) Added
b) Removed
c) Rearranged
d) Modified

Answer: a
Explanation: Each layer adds its own header to the packet from the previous layer. For example, in the Internet layer, the IP header is added over the TCP header on the data packet that came from the transport layer.

53. Communication between a computer and a keyboard involves _____ transmission.
a) Automatic
b) Half-duplex
c) Full-duplex
d) Simplex

Answer: d
Explanation: In simplex transmission, data flows in single direction which in this case refers to the data flowing from the keyboard to the computer. Another example would be of the mouse where the data flows from the mouse to the computer only.

54. The first Network was called _____
a) CNNET
b) NSFNET
c) ASAPNET
d) ARPANET

Answer: d
Explanation: ARPANET stands for Advanced Research Projects Agency Networks. It was the first network to be implemented which used the TCP/IP protocol in the year 1969.

55. A _____ is the physical path over which a message travels.
a) Path
b) Medium
c) Protocol
d) Route

Answer: b
Explanation: Messages travel from sender to receiver via a physical path called the medium using a set of methods/rules called protocol. Mediums can be guided (wired) or unguided (wireless).

56. When collection of various computers seems a single coherent system to its client, then it is called _____
a) computer network
b) distributed system
c) networking system
d) mail system

Answer: b
Explanation: A Computer network is defined as a collection of interconnected computers which uses a single technology for connection.
A distributed system is also the same as computer network but the main difference is that the whole collection of computers appears to its users as a single coherent system.
Example:- World wide web

57. Two devices are in network if _____
a) a process in one device is able to exchange information with a process in another device
b) a process is running on both devices
c) PIDs of the processes running of different devices are same
d) a process is active and another is inactive

Answer: a
Explanation: A computer network, or data network, is a digital telecommunications network which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections between nodes. The nodes have certain processes which enable them to share a specific type of data using a distinct protocol.

58. Which of the following computer networks is built on the top of another network?
a) prior network
b) chief network
c) prime network
d) overlay network

Answer: d
Explanation: An overlay network is a computer network that is built on top of another network. Some examples of an overlay network are Virtual Private Networks (VPN) and Peer-to-Peer Networks (P2P).

59. In computer network nodes are _____
a) the computer that originates the data
b) the computer that routes the data
c) the computer that terminates the data
d) all of the mentioned

Answer: d
Explanation: In a computer network, a node can be anything that is capable of sending data or receiving data or even routing the data to its destination. Routers, Computers and Smartphones are some examples of network nodes.

60. Communication channel is shared by all the machines on the network in _____
a) broadcast network
b) unicast network
c) multicast network
d) anycast network

Answer: a
Explanation: In a broadcast network, information is sent to all stations in a network whereas in a multicast network the data or information is sent to a group of stations in the network. In unicast network, information is sent to only one specific station. The broadcast address of the network is the last assigned address of the network.

61. Bluetooth is an example of _____
a) personal area network
b) local area network
c) virtual private network
d) wide area network

Answer: a
Explanation: Bluetooth is a wireless technology used to create a wireless personal area network for data transfer up to a distance of 10 meters. It operates on 2.45 GHz frequency band for transmission.

62. A _____ is a device that forwards packets between networks by processing the routing information included in the packet.
a) bridge
b) firewall

c) router
d) hub

Answer: c
Explanation: A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. They make use of routing protocols like RIP to find the cheapest path to the destination.

63. A list of protocols used by a system, one protocol per layer, is called _____
a) protocol architecture
b) protocol stack
c) protocol suite
d) protocol system

Answer: b
Explanation: A protocol stack refers to a group of protocols that are running concurrently that are employed for the implementation of network protocol suite. Each layer in the network model has to use one specific protocol from the protocol stack.

64. Network congestion occurs _____
a) in case of traffic overloading
b) when a system terminates
c) when connection between two nodes terminates
d) in case of transfer failure

Answer: a
Explanation: Network congestion occurs when traffic in the network is more than the network could handle. To avoid network congestion, the network management uses various open-loop and closed-loop congestion control techniques.

65. Which of the following networks extends a private network across public networks?
a) local area network
b) virtual private network
c) enterprise private network
d) storage area network

Answer: b
Explanation: A virtual private network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.VPN provides enhanced security and online anonymity to users on the internet. It is also used to unblock websites which are unavailable in certain regions.

66. Which of this is not a constituent of residential telephone line?
a) A high-speed downstream channel
b) A medium-speed downstream channel
c) A low-speed downstream channel
d) An ultra-high speed downstream channel

Answer: c
Explanation: A low-speed downstream channel is not a constituent of a residential telephone line. But it might be just a two-way telephone channel. Internet can be provided through a high-speed downstream channel in a residential telephone line.

67. How many layers are present in the Internet protocol stack (TCP/IP model)?

a) 5
b) 7
c) 6
d) 10

Answer: a
Explanation: There are five layers in the Internet Protocol stack. The five layers in Internet Protocol stack is Application, Transport, Network, Data link and Physical layer. The internet protocol stack model is also called the TCP/IP model and it's used in modern Internet Communication.

68. The number of layers in ISO OSI reference model is _____
a) 5
b) 7
c) 6
d) 10

Answer: b
Explanation: The seven layers in ISO OSI reference model is Application, Presentation, Session, Transport, Network, Data link and Physical layer. OSI stands for Open System Interconnect and it is a generalized model.

69. Which of the following layers is an addition to OSI model when compared with TCP IP model?
a) Application layer
b) Presentation layer
c) Session layer
d) Session and Presentation layer

Answer: d
Explanation: The only difference between OSI model and TCP/IP model is that the functions of Presentation and Session layer in the OSI model are handled by the transport layer itself in TCP/IP. OSI is a generalized model and TCP/IP is an application specific model.

70. Application layer is implemented in _____
a) End system
b) NIC
c) Ethernet
d) Packet transport

Answer: a
Explanation: Not only application layer, but presentation layer, session layer and transport layer are also implemented in the end system. The layers below are implemented outside the end system, for example, the network layer is implemented on the routers and the physical layer is implemented for the medium.

71. Transport layer is implemented in _____
a) End system
b) NIC
c) Ethernet
d) Signal transmission

Answer: a
Explanation: Application, Presentation, Session and Transport layer are implemented in the end system. The transport layer handles the process to process delivery of the packet through ports.

72. The functionalities of the presentation layer include _____

a) Data compression
b) Data encryption
c) Data description
d) All of the mentioned

Answer: d
Explanation: Some functions of the presentation layer include character-code translation, data conversion, data encryption and decryption, and data translation. It connects the application layer with the layers below converting the human readable text and media to machine readable format and vice-versa.

73. Delimiting and synchronization of data exchange is provided by _____
a) Application layer
b) Session layer
c) Transport layer
d) Link layer

Answer: b
Explanation: The session layer provides the mechanism for opening, closing and managing a session between end-user application processes. The session layer 5 is responsible for establishing managing synchronizing and terminating sessions. In TCP/IP protocol stack, the functions of the session layer are handled by the transport layer itself and thus the session layer is missing from the TCP/IP model.

74. In OSI model, when data is sent from device A to device B, the 5th layer to receive data at B is _____
a) Application layer
b) Transport layer
c) Link layer
d) Session layer

Answer: d
Explanation: In OSI reference model, the fifth layer is Session layer. Session layer provides the mechanism for opening, closing and managing a session between end-user application processes. In TCP/IP protocol stack, the functions of the session layer are handled by the transport layer itself and thus the session layer is missing from the TCP/IP model.

75. In TCP IP Model, when data is sent from device A to device B, the 5th layer to receive data at B is _____
a) Application layer
b) Transport layer
c) Link layer
d) Session layer

Answer: a
Explanation: In TCP/IP model, the fifth layer is application layer. When data is sent from device A to device B, the 5th layer to receive data at B is application layer. Application layer provides the interface between applications and the network. The user interacts with only this layer.

76. In the OSI model, as a data packet moves from the lower to the upper layers, headers are _____
a) Added
b) Removed
c) Rearranged
d) Randomized

Answer: b
Explanation: In OSI reference model, when data packet moves from lower layers to higher layer, headers get removed. Whereas when the data packet moves from higher layer to lower layers, headers are added. These headers contain the essential control information for the protocols used on the specific layer.

77. Which of the following statements can be associated with OSI model?
a) A structured way to discuss and easier update system components
b) One layer may duplicate lower layer functionality
c) Functionality at one layer no way requires information from another layer
d) It is an application specific network model

Answer: c
Explanation: One layer may use the information from another layer, for example timestamp value. The information is contained in the header inserted by the previous layer. The headers are added as the packet moves from higher layers to the lower layers.

78. OSI stands for _____
a) open system interconnection
b) operating system interface
c) optical service implementation
d) open service Internet

Answer: a
Explanation: OSI is the abbreviation for Open System Interconnection. OSI model provides a structured plan on how applications communicate over a network, which also helps us to have a structured plan for troubleshooting. It is recognized by the ISO as the generalized model for computer network i.e. it can be modified to design any kind of computer network.

79. The number of layers in ISO OSI reference model is _____
a) 4
b) 5
c) 6
d) 7

Answer: d
Explanation: In OSI reference model, there are 7 layers namely Application, Presentation, Session, Transport, Network, Data Link and Physical layer. Each layer uses a protocol to perform its designated function, for example, the data link layer uses error detection protocols for error control functions.

80. TCP/IP model does not have _____ layer but OSI model have this layer.
a) session layer
b) transport layer
c) application layer
d) network layer

Answer: a
Explanation: In OSI reference model, there are two layers which are not present in TCP/IP model. They are Presentation and Session layer. The functions of Presentation and Session layer in the OSI model are handled by the transport layer itself in TCP/IP.

81. Which layer is used to link the network support layers and user support layers?
a) session layer
b) data link layer
c) transport layer
d) network layer

Answer: c
Explanation: Physical, data link and network layers are network support layers and session, presentation and application layers are user support layers. The transport layer links these layers by segmenting and rearranging the data. It uses protocols like TCP and UDP.

82. Which address is used on the internet for employing the TCP/IP protocols?
a) physical address and logical address
b) port address
c) specific address
d) all of the mentioned

Answer: d
Explanation: The physical, logical, port and specific addresses are used in TCP/IP protocol. All the addressing schemes, that is physical (MAC) and logical address, port address and specific address are employed in both TCP/IP model and OSI model. In TCP/IP, the addresses are more focused on the internet implementation of these addresses.

83. TCP/IP model was developed _____ the OSI model.
a) prior to
b) after
c) simultaneous to
d) with no link to

Answer: a
Explanation: Several TCP/IP prototypes were developed at multiple research centers between 1978 and 1983, whereas OSI reference model was developed in the year 1984. TCP/IP was developed with the intention to create a model for the Internet while OSI was intended to be a general network model.

84. Which layer is responsible for process to process delivery in a general network model?
a) network layer
b) transport layer
c) session layer
d) data link layer

Answer: b
Explanation: The role of Transport layer (Layer 4) is to establish a logical end to end connection between two systems in a network. The protocols used in Transport layer is TCP and UDP. The transport layer is responsible for segmentation of the data. It uses ports for the implementation of process-to-process delivery.

85. Which address is used to identify a process on a host by the transport layer?
a) physical address
b) logical address
c) port address
d) specific address

Answer: c
Explanation: A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server. Some

examples of port numbers are port 20 which is used for FTP data, port 22 which is used for SSH remote login ,and port 23 which is used for TELNET.

86. Which layer provides the services to user?
a) application layer
b) session layer
c) presentation layer
d) physical layer

Answer: a
Explanation: In networking, a user mainly interacts with application layer to create and send information to other computer or network. Application layer provides the interface between applications and the network. It is the top-most layer in both the TCP/IP and the OSI model.

87. Transmission data rate is decided by _____
a) network layer
b) physical layer
c) data link layer
d) transport layer

Answer: b
Explanation: Physical layer is a layer 1 device which deals with network cables or the standards in use like connectors, pins, electric current used etc. Basically the transmission speed is determined by the cables and connectors used. Hence it is physical layer that determines the transmission speed in network. Some of the cables used for high speed data transmission are optical fiber cables and twisted pair cables.

88. The physical layer is concerned with _____
a) bit-by-bit delivery
p) process to process delivery
c) application to application delivery
d) port to port delivery

Answer: a
Explanation: Physical layer deals with bit to bit delivery in networking. The data unit in the physical layer is bits. Process to process delivery or the port to port delivery is dealt in the transport layer. The various transmission mediums aid the physical layer in performing its functions.

89. Which transmission media provides the highest transmission speed in a network?
a) coaxial cable
b) twisted pair cable
c) optical fiber
d) electrical cable

Answer: c
Explanation: Fiber optics is considered to have the highest transmission speed among the all mentioned above. The fiber optics transmission runs at 1000Mb/s. It is called as 1000Base-Lx whereas IEEE standard for it is 802.3z. It is popularly used for modern day network connections due to its high transmission rate.

90. Bits can be sent over guided and unguided media as analog signal by _____
a) digital modulation
b) amplitude modulation
c) frequency modulation
d) phase modulation

Answer: a
Explanation: In analog modulation, digital low frequency baseband signal (digital bit stream) is transmitted over a higher frequency. Whereas in digital modulation the only difference is that the base band signal is of discrete amplitude level. The bits are represented by only two frequency levels, one for high and one for low.

91. The portion of physical layer that interfaces with the media access control sublayer is called _____
a) physical signalling sublayer
b) physical data sublayer
c) physical address sublayer
d) physical transport sublayer

Answer: a
Explanation: The portion of physical layer that interfaces with the medium access control sublayer is Physical Signaling Sublayer. The main function of this layer is character encoding, reception, decoding and performs optional isolation functions. It handles which media connection the signal should be forwarded to physically.

92. The physical layer provides _____
a) mechanical specifications of electrical connectors and cables
b) electrical specification of transmission line signal level
c) specification for IR over optical fiber
d) all of the mentioned

Answer: d
Explanation: Anything dealing with a network cable or the standards in use – including pins, connectors and the electric current used is dealt in the physical layer (Layer 1). Physical layer deals with bit to bit delivery of the data aided by the various transmission mediums.

93. The data link layer takes the packets from _____ and encapsulates them into frames for transmission.
a) network layer
b) physical layer
c) transport layer
d) application layer

Answer: a
Explanation: In computer networks, the data from application layer is sent to transport layer and is converted to segments. These segments are then transferred to the network layer and these are called packets. These packets are then sent to data link layer where they are encapsulated into frames. These frames are then transferred to physical layer where the frames are converted to bits. Error control and flow control data is inserted in the frames at the data link layer.

94. Which of the following tasks is not done by data link layer?
a) framing
b) error control
c) flow control
d) channel coding

Answer: d
Explanation: Channel coding is the function of physical layer. Data link layer mainly deals with framing, error control and flow control. Data link layer is the layer where the packets are encapsulated into frames.

95. Which sublayer of the data link layer performs data link functions that depend upon the type of medium?
a) logical link control sublayer
b) media access control sublayer
c) network interface control sublayer
d) error control sublayer

Answer: b
Explanation: Media access control (MAC) deals with transmission of data packets to and from the network-interface card, and also to and from another remotely shared channel. The MAC sublayer also prevents collision using protocols like CSMA/CD.

96. Header of a frame generally contains _____
a) synchronization bytes
b) addresses
c) frame identifier
d) all of the mentioned

Answer: d
Explanation: In a frame, the header is a part of the data that contains all the required information about the transmission of the file. It contains information like synchronization bytes, addresses, frame identifier etc. It also contains error control information for reducing the errors in the transmitted frames.

97. Automatic repeat request error management mechanism is provided by _____
a) logical link control sublayer
b) media access control sublayer
c) network interface control sublayer
d) application access control sublayer

Answer: a
Explanation: The logical link control is a sublayer of data link layer whose main function is to manage traffic, flow and error control. The automatic repeat request error management mechanism is provided by the LLC when an error is found in the received frame at the receiver's end to inform the sender to re-send the frame.

98. The network layer is concerned with _____ of data.
a) bits
b) frames
c) packets
d) bytes

Answer: c
Explanation: In computer networks, the data from the application layer is sent to the transport layer and is converted to segments. These segments are then transferred to the network layer and these are called packets. These packets are then sent to data link layer where they are encapsulated into frames. These frames are then transferred to physical layer where the frames are converted to bits.

99. Which one of the following is not a function of network layer?
a) routing
b) inter-networking
c) congestion control
d) error control

Answer: d
Explanation: In the OSI model, network layer is the third layer and it provides data routing paths for network communications.

Error control is a function of the data link layer and the transport layer.

100. A 4 byte IP address consists of _____

a) only network address
b) only host address
c) network address & host address
d) network address & MAC address

Answer: c
Explanation: An ip address which is 32 bits long, that means it is of 4 bytes and is composed of a network and host portion and it depends on address class. The size of the host address and network address depends upon the class of the address in classful IP addressing.

101. When displaying a web page, the application layer uses the _____

a) HTTP protocol
b) FTP protocol
c) SMTP protocol
d) TCP protocol

Answer: a
Explanation: HTTP is abbreviation for hypertext transfer protocol. It is the foundation of data communication for world wide web. This protocol decides how the message is formatted and transmitted etc.

102. The number of objects in a Web page which consists of 4 jpeg images and HTML text is _____

a) 4
b) 1
c) 5
d) 7

Answer: c
Explanation: 4 jpeg images + 1 base HTML file.

103. Multiple objects can be sent over a TCP connection between client and server in a persistent HTTP connection.

a) True
b) False

Answer: a
Explanation: Persistent connections are kept active after completing transaction so that multiple objects can be sent over the same TCP connection.

104. FTP server listens for connection on port number _____

a) 20
b) 21
c) 22
d) 23

Answer: b
Explanation: Port 20 is used for FTP data. Port 22 is used for SSH remote login. Port 23 is used for TELNET.

105. In FTP protocol, client contacts server using ____ as the transport protocol.

a) transmission control protocol
b) user datagram protocol
c) datagram congestion control protocol
d) stream control transmission protocol

Answer: a
Explanation: The clients use the Transmission Control Protocol for FTP as it's

more reliable than UDP, DCCP, and SCTP, and reliability of file transfer is required to be as high as possible for FTP.

106. In Active mode FTP, the client initiates both the control and data connections.
a) True
b) False

Answer: b
Explanation: In Passive mode of FTP, the client initiates both data and control connections, while in Active mode, the client initiates the control connection and then the server initiates the data connection.

107. The File Transfer Protocol is built on _____
a) data centric architecture
b) service oriented architecture
c) client server architecture
d) connection oriented architecture

Answer: c
Explanation: The FTP connection includes a Server and a Client which wish to share files. The server can have multiple clients at the same time while the client communicates with only one server at a time.

108. In File Transfer Protocol, data transfer cannot be done in _____
a) stream mode
b) block mode
c) compressed mode
d) message mode

Answer: d
Explanation: In Stream mode, the data is transferred in a continuous stream. In Block mode, data is transferred after being divided into smaller blocks. In Compressed mode, data is transferred after being compressed using some compression algorithm.

109. Expansion of FTP is _____
a) Fine Transfer Protocol
b) File Transfer Protocol
c) First Transfer Protocol
d) Fast Transfer Protocol

Answer: b
Explanation: File Transfer Protocol is an application layer protocol used to share "files" between a server and a client. The protocol uses two separate ports for data and control connections: port 20 for data and port 21 for control.

110. FTP is built on _____ architecture.
a) Client-server
b) P2P
c) Data centric
d) Service oriented

Answer: a
Explanation: An FTP connection includes a Server and a Client which wish to share a number of data files. The server can transfer files with multiple clients at the same time while the client communicates with only one server at a time.

111. FTP uses _____ parallel TCP connections to transfer a file.
a) 1
b) 2

c) 3
d) 4

Answer: b
Explanation: Control connection using FTP port: 21, and data connection using FTP port: 20. The FTP session is started or ended using port 21 and the actual data i.e. files are sent through port 20.

112. Identify the incorrect statement regarding FTP.
a) FTP stands for File Transfer Protocol
b) FTP uses two parallel TCP connections
c) FTP sends its control information in-band
d) FTP sends exactly one file over the data connection

Answer: c
Explanation: FTP is out-of-band because the data connection is done separately through port 20 and control connection is done separately through port 21.

113. If 5 files are transferred from server A to client B in the same session. The number of TCP connections between A and B is

_____
a) 5
b) 10
c) 2
d) 6

Answer: d
Explanation: The client would first initiate the TCP control connection through port 21. Then for every file transfer, a separate connection would be made through port 20. Now, since we have five files to be transferred, 1 control connection + 5 data connections = 6 total TCP connections.

114. When the mail server sends mail to other mail servers it becomes

_____
a) SMTP server
b) SMTP client
c) Peer
d) Master

Answer: b
Explanation: SMTP clients are the entities that send mails to other mail servers. The SMTP servers cannot send independent mails to other SMTP servers as an SMTP server. There are no masters or peers in SMTP as it is based on the client-server architecture.

115. If you have to send multimedia data over SMTP it has to be encoded into

_____
a) Binary
b) Signal
c) ASCII
d) Hash

Answer: c
Explanation: Since only 7-bit ASCII codes are transmitted through SMTP, it is mandatory to convert binary multimedia data to 7-bit ASCII before it is sent using SMTP.

116. Expansion of SMTP is _____
b) Simple Message Transfer Protocol
c) Simple Mail Transmission Protocol
d) Simple Message Transmission Protocol

Answer: a
Explanation: SMTP or Simple Mail Transfer

Protocol is an application layer protocol used to transport e-mails over the Internet. Only 7-bit ASCII codes can be sent using SMTP.

117. In SMTP, the command to write receiver's mail address is written with the command _____
a) SEND TO
b) RCPT TO
c) MAIL TO
d) RCVR TO

Answer: b
Explanation: RCPT TO command is followed by the recipient's mail address to specify where or to whom the mail is going to through the internet. If there is more than one receiver, the command is repeated for each address continually.

118. The underlying Transport layer protocol used by SMTP is _____
a) TCP
b) UDP
c) Either TCP or UDP
d) IMAP

Answer: a
Explanation: TCP is a reliable protocol, and Reliability is a mandatory requirement in e-mail transmission using SMTP.

119. Simple mail transfer protocol (SMTP) utilizes _____ as the transport layer protocol for electronic mail transfer.
a) TCP
b) UDP
c) DCCP
d) SCTP

Answer: a
Explanation: Since TCP is a reliable protocol, it's more efficient to use TCP protocol for e-mail transfer. TCP also provides more security than other transport layer protocols.

120. SMTP connections secured by SSL are known as _____
a) SMTPS
b) SSMTP
c) SNMP
d) STARTTLS

Answer: a
Explanation: SSMTP is a simple mail transfer program to send mail from a local PC to a mail host. SNMP is a network management protocol. STARTTLS connections are secured by TLS.

121. SMTP uses which of the following TCP port?
a) 22
b) 23
c) 21
d) 25

Answer: d
Explanation: Port 21 is used for FTP control connection, port 22 is used by SSH, and port 23 is used by TELNET.

122. Which one of the following protocol is used to receive mail messages?
a) SMTP
b) Post Office Protocol (POP)
c) Internet Message Access Protocol (IMAP)
d) FTP

Answer: d
Explanation: FTP is used to share files. SMTP, POP and IMAP are the protocols used to send and receive mails on the internet.

123. What is on-demand mail relay (ODMR)?
a) protocol for SMTP security
b) an SMTP extension
c) protocol for web pages
d) protocol for faster mail transfer

Answer: b
Explanation: ODMR is an extension to SMTP, in which mails are relayed to the receivers after they are authenticated. It allows only the authorized receivers to receive the mail.

124. The entire hostname has a maximum of _____
a) 255 characters
b) 127 characters
c) 63 characters
d) 31 characters

Answer: a
Explanation: An entire hostname can have a maximum of 255 characters. Although each label must be from 1 to 63 characters long. Host name is actually a label that is given to a device in a network.

125. A DNS client is called _____
a) DNS updater
b) DNS resolver
c) DNS handler
d) none of the mentioned

Answer: b
Explanation: DNS client also known as DNS resolver also known as DNS lookup helps to resolve DNS requests using an external DNS server.

126. Servers handle requests for other domains _____
a) directly
b) by contacting remote DNS server
c) it is not possible
d) none of the mentioned

Answer: b
Explanation: Whenever a request is received at server from other domains, it handles this situation by contacting remote DNS server.

127. DNS database contains _____
a) name server records
b) hostname-to-address records
c) hostname aliases
d) all of the mentioned

Answer: d
Explanation: Domain Name system not only deals with mapping IP addresses with the hostname but also deals with exchange of information in the server.

128. If a server has no clue about where to find the address for a hostname then _____
a) server asks to the root server
b) server asks to its adjcent server
c) request is not processed
d) none of the mentioned

Answer: a
Explanation: Root name servers are actually

very important and critical as they are the first step in translating human readable hostnames into IP addresses for carrying out communication.

129. Which one of the following allows client to update their DNS entry as their IP address change?
a) dynamic DNS
b) mail transfer agent
c) authoritative name server
d) none of the mentioned

Answer: a
Explanation: Dynamic DNS or in short DDNS or DynDNS helps in automatically updating a name server in the DNS. This does not require manual editing.

130. Wildcard domain names start with label _____
a) @
b) *
c) &
d) #

Answer: b
Explanation: A wildcard DNS record matches requests to a non existent domain name. This wildcard DNS record is specified by using asterisk "*" as the starting of a domain name.

131. The right to use a domain name is delegated by domain name registers which are accredited by _____
a) internet architecture board
b) internet society
c) internet research task force
d) internet corporation for assigned names and numbers

Answer: d
Explanation: The ICANN (Internet Corporation for Assigned Names and Numbers) deals with IP address space allocation, protocol identifier assignment, generic and country code Top Level domain name system management (gTLD and ccTLD).

132. The domain name system is maintained by _____
a) distributed database system
b) a single server
c) a single computer
d) none of the mentioned

Answer: a
Explanation: A domain name system is maintained by a distributed database system. It is a collection of multiple, logically interrelated databases distributed over a computer network.

133. Which one of the following is not true?
a) multiple hostnames may correspond to a single IP address
b) a single hostname may correspond to many IP addresses
c) a single hostname may correspond to a single IP address
d) none of the mentioned

Answer: c
Explanation: It need not be that a single hostname will correspond to a ip address. For example facebook.com and fb.com both correspond to same ip address. So there

can be multiple hostnames for a single ip address.

134. IPSec is designed to provide security at the _____
a) Transport layer
b) Network layer
c) Application layer
d) Session layer

Answer: b
Explanation: IPSec is a set of protocols used to provide authentication, data integrity and confidentiality between two machines in an IP network. In the TCP/IP model, it provides security at the IP layer i.e. the network layer.

135. A _____ is an extension of an enterprise's private intranet across a public network such as the internet, creating a secure private connection.
a) VNP
b) VPN
c) VSN
d) VSPN

Answer: b
Explanation: VPN provides enhanced security and online anonymity to users on the internet. It is also used to unblock websites that are unavailable in certain regions.

136. When were VPNs introduced into the commercial world?
a) Early 80's
b) Late 80's
c) Early 90's
d) Late 90's

Answer: d
Explanation: VPNs were first introduced in the year 1996. Then as the internet started to get popularized, the need for connection security increased. VPN was a great solution to this, and that's when VPNs were implemented in the commercial world.

137. What protocol is NOT used in the operation of a VPN?
a) PPTP
b) IPsec
c) YMUM
d) L2TP

Answer: c
Explanation: PPTP is a tunneling protocol which was initially used for the creation of VPNs. IPSec is used in encrypting the traffic flowing in the VPN. L2TP is used to tunnel all the L2 traffic on the VPN.

138. Which of the following statements is NOT true concerning VPNs?
a) Financially rewarding compared to leased lines
b) Allows remote workers to access corporate data
c) Allows LAN-to-LAN connectivity over public networks
d) Is the backbone of the Internet

Answer: d
Explanation: VPNs are not the backbone of the Internet as they are just a method to create private intranets on the internet. They are used for enhancing the connection security for the users.

139. Traffic in a VPN is NOT _____
a) Invisible from public networks
b) Logically separated from other traffic
c) Accessible from unauthorized public networks
d) Restricted to a single protocol in IPsec

Answer: c
Explanation: Traffic in a VPN is not accessible from any unauthorized public networks because it is secured with the masking IP address. This provides the benefit of access to blocked resources to the users.

140. VPNs are financially speaking _____
a) Always more expensive than leased lines
b) Always cheaper than leased lines
c) Usually cheaper than leased lines
d) Usually more expensive than leased lines

Answer: c
Explanation: The services of a VPN are cheaper for moderate to large scale institutional networks than the services of leased lines. Though for a small scale network, it does not prove to be as beneficial as the costs are not reduced to a great degree as compared to leased lines.

141. Which layer 3 protocols can be transmitted over an L2TP VPN?
a) Only IP
b) Only IPX
c) Only ICMP
d) IP and IPX

Answer: d
Explanation: L2TP stands for Layer 2 Tunneling Protocol. It is used to tunnel all the L2 traffic on an IP network and is able to transmit network layer's IP and IPX protocol data.

142. The application layer protocol used by a Telnet application is _____
a) Telnet
b) FTP
c) HTTP
d) SMTP

Answer: a
Explanation: Telnet is an application layer protocol that provides access to the command-line interface on a remote host. Telnet stands for teletype network.

143. Which amongst the following statements is correct for "character at a time" mode?
a) Character processing is done on the local system under the control of the remote system
b) Most text typed is immediately sent to the remote host for processing
c) All text is echoed locally, only completed lines are sent to the remote host
d) All text is processed locally, and only confirmed lines are sent to the remote host

Answer: b
Explanation: In character at a time mode, the typed text is sent immediately to the remote host while the user is typing. Another mode used in Telnet is "Old line by line" mode in which only completed lines are sent to the remote host.

144. _____ allows you to connect and login to a remote computer
a) Telnet
b) FTP
c) HTTP
d) SMTP

Answer: a
Explanation: Telnet provides access to the command-line interface on a remote computer. One can login to the computer from the command-line interface.

145. Telnet is used for _____
a) Television on net
b) Network of Telephones
c) Remote Login
d) Teleshopping site

Answer: c
Explanation: Telnet is an application layer protocol that provides access to the command line interface of a remote computer that can be used to perform remote login.

146. Which one of the following is not correct?
a) telnet is a general purpose client-server program
b) telnet lets user access an application on a remote computer
c) telnet can also be used for file transfer
d) telnet can be used for remote login

Answer: c
Explanation: File Transfer Protocol is used for file transfer. Telnet provides access to the command-line interface on a remote host.

147. Which operating mode of telnet is full duplex?
a) default mode
b) server mode
c) line mode
d) character mode

Answer: c
Explanation: In line mode, terminal character processing is done on the client side but editing is enabled on the server side. Line mode reduces the number of packets and is useful for long delay networks.

148. Telnet protocol is used to establish a connection to _____
a) TCP port number 21
b) TCP port number 22
c) TCP port number 23
d) TCP port number 25

Answer: c
Explanation: TCP port 21 is used for FTP, TCP port 22 is used for SSH and TCP port 25 is used for SMTP. Telnet provides access to a command line interface on a remote computer using the TCP port number 23.

149. Which one of the following is not true?
a) telnet defines a network virtual terminal (NVT) standard
b) client programs interact with NVT
c) server translates NVT operations
d) client can transfer files using to remote server using NVT

Answer: d
Explanation: The client can use the NVT only to interact with the programs already

present on the remote server, not to transfer files to it. To transfer files, an FTP connection has to be used.

150. All telnet operations are sent as _____
a) 4 bits
b) 8 bits
c) 16 bits
d) 32 bits

Answer: b
Explanation: Telnet provides a bi-directional, 8-bit byte oriented communications facility through which operations are sent as 8-bit bytes for the server to interpret.

151. AbsoluteTelnet is a telnet client for _____ Operating system.
a) windows
b) linux
c) mac
d) ubuntu

Answer: a
Explanation: AbsoluteTelnet was originally released in 1999. It was developed by Brian Pence of Celestial Software.

152. Which of the following is false with respect to TCP?
a) Connection-oriented
b) Process-to-process
c) Transport layer protocol
d) Unreliable

Answer: d
Explanation: TCP is a transport layer protocol that provides reliable and ordered delivery of a stream of bytes between hosts communicating via an IP network.

153. In TCP, sending and receiving data is done as _____
a) Stream of bytes
b) Sequence of characters
c) Lines of data
d) Packets

Answer: a
Explanation: TCP provides stream oriented delivery between hosts communicating via an IP network and there are no message boundaries. TCP can concatenate data from a number of send () commands into one stream of data and still transmit it reliably.

154. TCP process may not write and read data at the same speed. So we need _____ for storage.
a) Packets
b) Buffers
c) Segments
d) Stacks

Answer: b
Explanation: A TCP receiver has a receive buffer that is used to store the unprocessed incoming packets in case the sender is sending packets faster than the processing rate of the received packets.

155. TCP groups a number of bytes together into a packet called _____
a) Packet
b) Buffer
c) Segment
d) Stack

Answer: c
Explanation: A segment may be collection of data from many send () statements. TCP transmits each segment as a stream of bytes.

156. Communication offered by TCP is _____
a) Full-duplex
b) Half-duplex
c) Semi-duplex
d) Byte by byte

Answer: a
Explanation: Data can flow both the directions at the same time during a TCP communication hence, it is full-duplex. This is the reason why TCP is used in systems that require full-duplex operation such as e-mail systems.

157. The receiver of the data controls the amount of data that are to be sent by the sender is referred to as _____
a) Flow control
b) Error control
c) Congestion control
d) Error detection

Answer: a
Explanation: Flow control is done to prevent the receiver from being overflowed with data. It is done using various open-loop (prevention) methods and closed-loop (recovery) methods.

158. Size of TCP segment header ranges between _____
a) 16 and 32 bytes
b) 16 and 32 bits
c) 20 and 60 bytes
d) 20 and 60 bits

Answer: c
Explanation: The size of the header can be 20 bytes at a minimum if there are no options and can go up to 60 bytes at maximum with 40 bytes in the options field. The header contains all the control information required to ensure ordered, error-free and reliable delivery of the segment.

159. Connection establishment in TCP is done by which mechanism?
a) Flow control
b) Three-Way Handshaking
c) Forwarding
d) Synchronization

Answer: b
Explanation: A three-way handshake allows both, the server and the client to choose their Initial Sequence Number and inform about it to the other party. This won't be possible using the two-way handshake mechanism.

160. The server program tells its TCP that it is ready to accept a connection. This process is called _____
a) Active open
b) Active close
c) Passive close
d) Passive open

Answer: d
Explanation: This is the first step in the Three-Way Handshaking process and is started by the server. Then the Client picks

an ISN (Initial Sequence Number) and synchronizes (shares) it with the Server requesting a connection. The Server acknowledges the clients ISN, and then picks an ISN and synchronizes it with the Client. At last, the Client acknowledges the servers ISN.

161. A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server. The process is called _____
a) Active open
b) Active close
c) Passive close
d) Passive open

Answer: a
Explanation: This is the second step in the Three-Way Handshaking process and is done by the client once it finds the open server and picks an ISN. The Server acknowledges the clients request, and then picks an ISN and synchronizes it with the Client. At last, the Client acknowledges the servers ISN.

162. Which of the following is false with respect to UDP?
a) Connection-oriented
b) Unreliable
c) Transport layer protocol
d) Low overhead

Answer: a
Explanation: UDP is an unreliable, connectionless transport layer protocol that provides message-based data transmission. TCP is an example of connection-oriented protocols.

163. Return value of the UDP port "Chargen" is _____
a) String of characters
b) String of integers
c) Array of characters with integers
d) Array of zero's and one's

Answer: a
Explanation: Using Chargen with UDP on port 19, the server sends a UDP datagram containing a random number of characters every time it receives a datagram from the connecting host. The number of characters is between 0 and 512.

164. Beyond IP, UDP provides additional services such as _____
a) Routing and switching
b) Sending and receiving of packets
c) Multiplexing and demultiplexing
d) Demultiplexing and error checking

Answer: d
Explanation: De-multiplexing is the delivering of received segments to the correct application layer processes at the recipients end using UDP. Error checking is done through checksum in UDP.

165. What is the main advantage of UDP?
a) More overload
b) Reliable
c) Low overhead
d) Fast

Answer: c
Explanation: As UDP does not provide assurance of delivery of packet, reliability and other services, the overhead taken to provide these services is reduced in UDP's

operation. Thus, UDP provides low overhead, and higher speed.

166. Port number used by Network Time Protocol (NTP) with UDP is _____
a) 161
b) 123
c) 162
d) 124

Answer: b
Explanation: The Network Time Protocol is a clock synchronization network protocol implemented by using UDP port number 123 to send and receive time stamps.

167. What is the header size of a UDP packet?
a) 8 bytes
b) 8 bits
c) 16 bytes
d) 124 bytes

Answer: a
Explanation: The fixed size of the UDP packet header is 8 bytes. It contains four two-byte fields: Source port address, Destination port address, Length of packet, and checksum.

168. The port number is "ephemeral port number", if the source host is _____
a) NTP
b) Echo
c) Server
d) Client

Answer: d
Explanation: Port numbers from 1025 to 5000 are used as ephemeral port numbers in Windows Operating System. Ephemeral port numbers are short-lived port numbers which can be used for clients in a UDP system where there are temporary clients all the time.

169. "Total length" field in UDP packet header is the length of _____
a) Only UDP header
b) Only data
c) Only checksum
d) UDP header plus data

Answer: d
Explanation: Total length is the 16 bit field which contains the length of UDP header and the data. The maximum value of the Total length field and the maximum size of a UDP datagram is 65,535 bytes (8 byte header + 65,527 bytes of data).

170. Which is the correct expression for the length of UDP datagram?
a) UDP length = IP length – IP header's length
b) UDP length = UDP length – UDP header's length
c) UDP length = IP length + IP header's length
d) UDP length = UDP length + UDP header's length

Answer: a
Explanation: A user datagram is encapsulated in an IP datagram. There is a field in the IP header that defines the total length of the IP packet. There is another field in the IP header that defines the length of the header. So if we subtract the length of the IP header that is encapsulated in the

IP packet, we get the length of UDP datagram.

171. The _____ field is used to detect errors over the entire user datagram.
a) udp header
b) checksum
c) source port
d) destination port

Answer: b
Explanation: Checksum field is used to detect errors over the entire user datagram. Though it is not as efficient as CRC which is used in TCP, it gets the job done for the UDP datagram as UDP doesn't have to ensure the delivery of the packet.

172. Two broad categories of congestion control are
a) Open-loop and Closed-loop
b) Open-control and Closed-control
c) Active control and Passive control
d) Active loop and Passive loop

Answer: a
Explanation: Open loop congestion control techniques are used to prevent congestion before it even happens by enforcing certain policies. Closed loop congestion control techniques are used to treat congestion after it has happened.

173. In open-loop control, policies are applied to _____
a) Remove after congestion occurs
b) Remove after sometime
c) Prevent before congestion occurs
d) Prevent before sending packets

Answer: c
Explanation: Open loop congestion control techniques are used to prevent congestion before it even happens by enforcing certain policies. Retransmission policy, window policy and acknowledgement policy are some policies that might be enforced.

174. Retransmission of packets must not be done when _____
a) Packet is lost
b) Packet is corrupted
c) Packet is needed
d) Packet is error-free

Answer: d
Explanation: Retransmission refers to the sender having to resend the packet to the receiver. It needs to be done only when some anomaly occurs with the packet like when the packet is lost or corrupted.

175. In Go-Back-N window, when the timer of the packet times out, several packets have to be resent even some may have arrived safe. Whereas in Selective Repeat window, the sender resends _____
a) Packet which are not lost
b) Only those packets which are lost or corrupted
c) Packet from starting
d) All the packets

Answer: b
Explanation: In Selective Repeat, the sender side uses a searching algorithm to find the packets which need to be retransmitted based on the negative acknowledgements received and then resends only those packets thus saving bandwidth.

176. A piece of icon or image on a web page associated with another webpage is called _____
a) url
b) hyperlink
c) plugin
d) extension

Answer: b
Explanation: URLs are locators for resources present on the World Wide Web. A plugin provides extra functionality to the webpage. An extension provides modification allowance for the core functionality of a webpage. Hyperlink is piece of icon or image on a web page associated with another webpage.

177. Dynamic web page _____
a) is same every time whenever it displays
b) generates on demand by a program or a request from browser
c) both is same every time whenever it displays and generates on demand by a program or a request from browser
d) is different always in a predefined order

Answer: b
Explanation: A dynamic web page provides different content every time the user opens it based on some events like new additions or time of the day. Languages such as JavaScript are used to respond to client-side events while languages such as PHP as used to respond to server-side events.

178. What is a web browser?
a) a program that can display a web page
b) a program used to view html documents
c) it enables user to access the resources of internet
d) all of the mentioned

Answer: d
Explanation: A web browser is an application program that is used to access the World Wide Web resources, applications and websites. Some examples of web browsers are Google Chrome, Internet Explorer and Safari.

179. Common gateway interface is used to _____
a) generate executable files from web content by web server
b) generate web pages
c) stream videos
d) download media files

Answer: a
Explanation: CGI is an interface through servers can run execute console-based executable files on a web server that generates dynamic web pages. A CGI script executes only when a request is made. The script then generates HTML.

180. URL stands for _____
a) unique reference label
b) uniform reference label
c) uniform resource locator
d) unique resource locator

Answer: c
Explanation: The Uniform Resource Locator is a locator for the resource to be located by HTTP on the World Wide Web. The URL is derived from the Uniform Resource Identifier.

181. A web cookie is a small piece of data that is _____
a) sent from a website and stored in user's web browser while a user is browsing a website
b) sent from user and stored in the server while a user is browsing a website
c) sent from root server to all servers
d) sent from the root server to other root servers

Answer: a
Explanation: A web cookie is a small piece of data sent from a website and stored in user's web browser while a user is browsing the website and is used to remember stateful information about the user's operations on the website. This can help the website provide a better browsing experience to the user.

182. Which one of the following is not used to generate dynamic web pages?
a) PHP
b) ASP.NET
c) JSP
d) CSS

Answer: d
Explanation: CSS alone cannot be used to generate dynamic web pages as it does not provide many event handling functions. It can be used along with JavaScript to generate dynamic web pages which are visually compelling.

183. An alternative to JavaScript on windows platform is _____
a) VBScript
b) ASP.NET
c) JSP
d) PHP

Answer: a
Explanation: VBScript is a general-purpose, lightweight and active scripting language which can be used on Microsoft Visual Basic. It was first released in 1996.

184. What is document object model (DOM)?
a) convention for representing and interacting with objects in html documents
b) application programming interface
c) hierarchy of objects in ASP.NET
d) scripting language

Answer: a
Explanation: DOM is a hierarchical model i.e. a tree used to represent an HTML or XML document. Every node of the tree an object that represents a part of the document.

185. AJAX stands for _____
a) asynchronous javascript and xml
b) advanced JSP and xml
c) asynchronous JSP and xml
d) advanced javascript and xml

Answer: a
Explanation: AJAX is a group of technologies that works on the client-side to create asynchronous web applications. It is used to modify only a part of a webpage and not the whole webpage whenever some event occurs.

186. Which of the following is not applicable for IP?
a) Error reporting

b) Handle addressing conventions
c) Datagram format
d) Packet handling conventions
Answer: a
Explanation: The Internet Protocol is the networking protocol which establishes the internet by relaying datagrams across network boundaries. ICMP is a supporting protocol for IP which handles the Error Reporting functionality.

187. Which of the following field in IPv4 datagram is not related to fragmentation?
a) Flags
b) Offset
c) TOS
d) Identifier

Answer: c
Explanation: TOS-type of service identifies the type of packets. It is not related to fragmentation but is used to request specific treatment such as high throughput, high reliability or low latency for the IP packet depending upon the type of service it belongs to.

188. The TTL field has value 10. How many routers (max) can process this datagram?
a) 11
b) 5
c) 10
d) 1

Answer: c
Explanation: TTL stands for Time to Live. This field specifies the life of the IP packet based on the number of hops it makes (Number of routers it goes through). TTL field is decremented by one each time the datagram is processed by a router. When the value is 0, the packet is automatically destroyed.

189. If the value in protocol field is 17, the transport layer protocol used is

_____
a) TCP
b) UDP
c) ICMP
d) IGMP

Answer: b
Explanation: The protocol field enables the demultiplexing feature so that the IP protocol can be used to carry payloads of more than one protocol type. Its most used values are 17 and 6 for UDP and TCP respectively. ICMP and IGMP are network layer protocols.

190. The data field cannot carry which of the following?
a) TCP segment
b) UDP segment
c) ICMP messages
d) SMTP messages

Answer: c
Explanation: Data field usually has transport layer segments, but it can also carry ICMP messages. SMTP is an application layer protocol. First it must go through the transport layer to be converted into TCP segments and then it can be inserted into IP packets.

191. What should be the flag value to indicate the last fragment?
a) 0

b) 1
c) TTl value
d) Protocol field value

Answer: a
Explanation: The Flag field in the IP header is used to control and identify the fragments. It contains three bits: reserved, don't fragment and more fragments. If the more fragments bit is 0, it means that the fragment is the last fragment.

192. Which of these is not applicable for IP protocol?
a) is connectionless
b) offer reliable service
c) offer unreliable service
d) does not offer error reporting

Answer: b
Explanation: IP does not provide reliable delivery service for the data. It's dependent upon the transport layer protocols like TCP to offer reliability.

193. Which of the following demerits does Fragmentation have?
a) complicates routers
b) open to DOS attack
c) overlapping of fragments.
d) all of the mentioned

Answer: d
Explanation: Fragmentation makes the implementation of the IP protocol complex and can also be exploited by attackers to create a DOS attack such as a teardrop attack. Fragmentation won't be required if the transport layer protocols perform wise segmentation.

194. Which field helps to check rearrangement of the fragments?
a) offset
b) flag
c) ttl
d) identifer

Answer: a
Explanation: The Fragment Offset field specifies where the fragment fits in the original datagram. The offset of the first fragment will always be 0. The size of the field (13 bits) is 3-bits shorter than the size of the total length field (16 bits).

195. Which of these is not applicable for IP protocol?
a) Connectionless
b) Offer reliable service
c) Offer unreliable service
d) Does not offer error reporting

Answer: b
Explanation: IP does not provide reliable delivery service for the data. It's dependent upon the transport layer protocols like TCP to offer reliability.

196. Which of the following demerits does Fragmentation have?
a) Complicates routers
b) Open to DOS attack
c) Overlapping of fragments
d) All of the mentioned

Answer: d
Explanation: Fragmentation makes the implementation of the IP protocol complex and can also be exploited by attackers to create a DOS attack such as a teardrop

attack. Fragmentation won't be required if the transport layer protocols perform wise segmentation.

197. Which field helps to check rearrangement of the fragments?
a) Offset
b) Flag
c) TTL
d) Identifier

Answer: a
Explanation: The Fragment Offset field specifies where the fragment fits in the original datagram. The offset of the first fragment will always be 0. The size of the field (13 bits) is 3-bits shorter than the size of the total length field (16 bits).

198. In classless addressing, there are no classes but addresses are still granted in _____
a) IPs
b) Blocks
c) Codes
d) Sizes

Answer: b
Explanation: In classless addressing, there are no classes but addresses are still granted in blocks. The total number of addresses in a block of classless IP addresses = $2^{(32 - CIDR\_value)}$.

199. In IPv4 Addresses, classful addressing is replaced with _____
a) Classless Addressing
b) Classful Addressing
c) Classful Advertising
d) Classless Advertising

Answer: a
Explanation: Classful addressing is replaced with classless addressing as a large ratio of the available addresses in a class in calssful addressing is wasted. In classless addressing, one can reserve the number of IP addresses required by modifying the CIDR value and make sure that not many addresses are wasted.

200. In virtual circuit network each packet contains _____
a) full source and destination address
b) a short VC number
c) only source address
d) only destination address

Answer: b
Explanation: A short VC number also called as VCID (virtual circuit identifier) is a type of identifier which is used to distinguish between several virtual circuits in a connection oriented circuit switched network. Each virtual circuit is used to transfer data over a larger packet switched network.

201. Which of the following routing algorithms can be used for network layer design?
a) shortest path algorithm
b) distance vector routing
c) link state routing
d) all of the mentioned

Answer: d
Explanation: The routing algorithm is what decides where a packet should go next. There are several routing techniques like shortest path algorithm, static and dynamic

routing, decentralized routing, distance vector routing, link state routing, Hierarchical routing etc. The routing algorithms go hand in hand with the operations of all the routers in the networks. The routers are the main participants in these algorithms.

202. Transport layer aggregates data from different applications into a single stream before passing it to _____
a) network layer
b) data link layer
c) application layer
d) physical layer

Answer: a
Explanation: The flow of data in the OSI model flows in following manner Application -> Presentation -> Session -> Transport -> Network -> Data Link -> Physical. Each and every layer has its own set of functions and protocols to ensure efficient network performance.

203. Which of the following are transport layer protocols used in networking?
a) TCP and FTP
b) UDP and HTTP
c) TCP and UDP
d) HTTP and FTP

Answer: c
Explanation: Both TCP and UDP are transport layer protocol in networking. TCP is an abbreviation for Transmission Control Protocol and UDP is an abbreviation for User Datagram Protocol. TCP is connection oriented whereas UDP is connectionless.

204. User datagram protocol is called connectionless because _____
a) all UDP packets are treated independently by transport layer
b) it sends data as a stream of related packets
c) it is received in the same order as sent order
d) it sends data very quickly

Answer: a
Explanation: UDP is an alternative for TCP and it is used for those purposes where speed matters most whereas loss of data is not a problem. UDP is connectionless whereas TCP is connection oriented.

205. Transmission control protocol _____
a) is a connection-oriented protocol
b) uses a three way handshake to establish a connection
c) receives data from application as a single stream
d) all of the mentioned

Answer: d
Explanation: TCP provides reliable and ordered delivery of a stream of bytes between hosts communicating via an IP network. Major internet applications like www, email, file transfer etc rely on TCP. TCP is connection oriented and it is optimized for accurate delivery rather than timely delivery.

206. An endpoint of an inter-process communication flow across a computer network is called _____
a) socket

b) pipe
c) port
d) machine

Answer: a
Explanation: Socket is one end point in a two way communication link in the network. TCP layer can identify the application that data is destined to be sent by using the port number that is bound to socket.

207. Physical or logical arrangement of network is _____
a) Topology
b) Routing
c) Networking
d) Control

Answer: a
Explanation: Topology in networks is the structure or pattern in which each and every node in the network is connected. There are many topologies in networking like bus, tree, ring, star, mesh, and hybrid topology. There is no particular best topology and a suitable topology can be chosen based on the kind of application of the network .

208. Which network topology requires a central controller or hub?
a) Star
b) Mesh
c) Ring
d) Bus

Answer: a
Explanation: In star topology, no computer is connected to another computer directly but all the computers are connected to a central hub. Every message sent from a source computer goes through the hub and the hub then forwards the message only to the intended destination computer.

209. _____ topology requires a multipoint connection.
a) Star
b) Mesh
c) Ring
d) Bus

Answer: d
Explanation: In bus topology, there is a single cable to which all the network nodes are connected. So whenever a node tries to send a message or data to other nodes, this data passes through all other nodes in the network through the cable. It is really simple to install but it's not secure enough to be used in most of the computer network applications.

210. Data communication system spanning states, countries, or the whole world is _____
a) LAN
b) WAN
c) MAN
d) PAN

Answer: b
Explanation: WAN is the abbreviation for Wide Area Network. This network extends over a large geographical area. WANs are used to connect cities, states or even countries. A wireless connection is required to build a WAN. The best example of WAN is the Internet.

210. Data communication system within a building or campus is_____
a) LAN
b) WAN
c) MAN
d) PAN

Answer: a
Explanation: LAN is an abbreviation for Local Area Network. This network interconnects computers in a small area such as schools, offices, residence etc. It is the most versatile kind of data communication system where most of the computer network concepts can be visibly used.

211. WAN stands for _____
a) World area network
b) Wide area network
c) Web area network
d) Web access network

Answer: b
Explanation: WAN is the abbreviation for Wide Area Network. This network extends over a large geographical area. These are used to connect cities, states or even countries. They can be connected through leased lines or satellites.

212. In TDM, slots are further divided into _____
a) Seconds
b) Frames
c) Packets
d) Bits

Answer: b
Explanation: TDM is the abbreviation for Time division multiplexing. It is technique for combining several low rate channels to a single high rate channel. For a certain time slot, the several channels could use the maximum bandwidth. Each channel is inactive for a period of time too. Some other multiplexing techniques are Frequency division multiplexing and Phase division multiplexing.

213. _____ is the multiplexing technique that shifts each signal to a different carrier frequency.
a) FDM
b) TDM
c) Both FDM & TDM
d) PDM

Answer: a
Explanation: FDM is an abbreviation for Frequency Division Multiplexing. This technique is used when the bandwidth of the channel is greater than the combined bandwidth of all the signals which are to be transmitted. The channel is active at all times unless a collision occurs with another channel trying to use the same frequency. Some other multiplexing techniques are Time division multiplexing and Phase division multiplexing.

214. The sharing of a medium and its link by two or more devices is called _____
a) Fully duplexing
b) Multiplexing
c) Micropleixng
d) Duplexing

Answer: b
Explanation: Multiplexing is a method using

which one can send multiples signals through a shared medium at the same time. This helps in using less resources and thus saving the cost of sending messages.

215. Multiplexing is used in _____
a) Packet switching
b) Circuit switching
c) Data switching
d) Packet & Circuit switching

Answer: b
Explanation: Circuit switching is a switching method by which one can obtain a physical path between end points. Circuit switching method is also called a connection oriented network. Two nodes must be physically and logically connected to each other to create a circuit switching network.

216. Which multiplexing technique used to transmit digital signals?
a) FDM
b) TDM
c) WDM
d) FDM & WDM

Answer: b
Explanation: TDM abbreviation for Time Division Multiplexing is a method used for digital signals. Whereas FDM and WDM abbreviation for Frequency Division Multiplexing, and Wavelength Division Multiplexing, are used for analog signals. TDM is used in applications like ISDN (Integrated Services Digital Network) and PSTN (Public Switched Telephone Network).

217. If there are n signal sources of same data rate, then the TDM link has _____ slots.
a) n
b) n/2
c) n*2
d) 2^n

Answer: a
Explanation: In TDM, the total unit of time is divided equally among all the signal sources and each and every source has access to the complete channel bandwidth during its allotted time slot. When the time slot of the source is not active, it remains idle and waits for its slot to begin.

218. If link transmits 4000frames per second, and each slot has 8 bits, the transmission rate of circuit this TDM is _____
a) 32kbps
b) 500bps
c) 500kbps
d) 32bps

Answer: a
Explanation: Transmission rate= frame rate * number of bits in a slot.
Given: Frame rate = 4000/sec and number of bits in slot = 8
Thus, Transmission rate = (4000 * 8) bps
= 32000bps
= 32kbps

219. The state when dedicated signals are idle are called _____
a) Death period
b) Poison period
c) Silent period
d) Stop period

Answer: c
Explanation: There are instances when connection between two endpoints has been established, but no communication or transfer of messages occurs. This period of time is called silent period. The silent period ends when either of the two endpoints starts the communication.

220. Multiplexing provides _____
a) Efficiency
b) Privacy
c) Anti jamming
d) Both Efficiency & Privacy

Answer: d
Explanation: Multiplexing helps us to transfer our messages over a shared channel. This brings up the issue of privacy and efficiency. Fortunately, Multiplexing has high efficiency and high privacy when implemented because in the implementation, the transport layer of the OSI network model handles the function of multiplexing through interfaces called ports which provide the required efficiency and privacy.

221. In TDM, the transmission rate of a multiplexed path is always _____ the sum of the transmission rates of the signal sources.
a) Greater than
b) Lesser than
c) Equal to
d) Equal to or greater than

Answer: a
Explanation: In TDM the transmission rate provided by the path that is multiplexed will always be greater than the sum of transmission rates of the single sources. This happens because the transmission rate is provided to each source only for a small period of time.

222. In TDM, slots are further divided into _____
a) Seconds
b) Frames
c) Packets
d) Bits

Answer: b
Explanation: TDM is the abbreviation for Time division multiplexing. It is technique for combining several low rate channels to a single high rate channel. For a certain time slot, the several channels could use the maximum bandwidth. Each channel is inactive for a period of time too. Some other multiplexing techniques are Frequency division multiplexing and Phase division multiplexing.

223. The attacker using a network of compromised devices is known as _____
a) Internet
b) Botnet
c) Telnet
d) D-net

Answer: b
Explanation: Botnet is a network of compromised devices used by the attacker without the owner's knowledge to perform unethical activities such as spamming. The attacker usually uses the least secure devices to create the botnet.

224. Which of the following is a form of DoS attack?
a) Vulnerability attack
b) Bandwidth flooding
c) Connection flooding
d) All of the mentioned

Answer: d
Explanation: In a DoS attack, the attacker won't let the victims access the network by using a certain method that ensures that an essential network resource is unavailable to the victim. In vulnerability attack, the attacker exploits any obvious vulnerable entity in the network to deny the victim access into the network. In bandwidth flooding, the attacker floods the victim with a huge flow of packets and uses up all the bandwidth. In connection flooding, the attacker floods the victim network with a huge number of connections, so that, no other machine can connect to it.

225. The DoS attack, in which the attacker establishes a large number of half-open or fully open TCP connections at the target host is _____
a) Vulnerability attack
b) Bandwidth flooding
c) Connection flooding
d) UDP flooding

Answer: c
Explanation: In Vulnerability attack, the attacker exploits the vulnerable control points of the network to deny access to the victims. In Bandwidth flooding, the attacker intentionally uses up all the bandwidth by flooding the victim with a deluge of packets and makes sure that the victim can't use any bandwidth. In UDP flooding, too many UDP packets are sent by the attacker to the victim at random ports.

226. Which of this is not a guided media?
a) Fiber optical cable
b) Coaxial cable
c) Wireless LAN
d) Copper wire

Answer: c
Explanation: Wireless LAN is unguided media.

227. UTP is commonly used in _____
a) DSL
b) FTTP
c) HTTP
d) None of the mentioned

Answer: a
Explanation: Unshielded twisted pair(UTP) is commonly used in home access.

228. A local telephone network is an example of a _____ network.
a) Packet switched
b) Circuit switched
c) Bit switched
d) Line switched

Answer: b
Explanation: Circuit switching is connection oriented switching technique, whereas in the case of packet switching, it is connectionless. Circuit switching is implemented in the Physical layer, whereas packet switching is implemented in the Network layer. Internet too is based on the concept of circuit switching.

229. Most packet switches use this principle
_____
a) Stop and wait
b) Store and forward
c) Store and wait
d) Stop and forward

Answer: b
Explanation: The packet switch will not transmit the first bit to outbound link until it receives the entire packet. If the entire packet is not received and the time-out period expires, the packet switch will inform the sender to resend the part of packet or the entire packet based on the algorithm being used.

230. If there are N routers from source to destination, the total end to end delay in sending packet P(L-> number of bits in the packet R-> transmission rate) is equal to
_____
a) N
b) (N*L)/R
c) (2N*L)/R
d) L/R

Answer: b
Explanation: The equation to find the end to end delay when no. of bits, transmission rate and no. of routers is given by (N*L)/R. The total end to end delay, that is, nodal delay is the sum of all, the processing delay, queuing delay, transmission delay and propagation delay.

231. What are the Methods to move data through a network of links and switches?
a) Packet switching and Line switching
b) Circuit switching and Line switching
c) Line switching and bit switching
d) Packet switching and Circuit switching

Answer: d
Explanation: Packet switching and Circuit switching are two different types of switching methods used to connect the multiple communicating devices with one another. Packet switching is used in conventional LAN systems and circuit switching is used in telephonic systems.

232. The required resources for communication between end systems are reserved for the duration of the session between end systems in _____ method.
a) Packet switching
b) Circuit switching
c) Line switching
d) Frequency switching

Answer: b
Explanation: In circuit switching, a physical path between the sender and receiver is established. This path is maintained until the connection is needed. Circuit switching is implemented in the Physical layer and is used in telephonic systems.

233. As the resources are reserved between two communicating end systems in circuit switching, _____ is achieved.
a) authentication
b) guaranteed constant rate
c) reliability
d) store and forward

Answer: b
Explanation: Circuit switching is connection oriented and is always implemented in the

physical layer. Once a path is set, all transmission occurs through the same path. It is used since the early times in telephonic systems.

234. Which is not a application layer protocol?
a) HTTP
b) SMTP
c) FTP
d) TCP

Answer: d
Explanation: TCP is transport layer protocol.

235. The packet of information at the application layer is called _____
a) Packet
b) Message
c) Segment
d) Frame

Answer: b
Explanation: For Application, Presentation and Session layers there is no data format for message. Message is message as such in these three layers. But when it comes to Transport, Network, Data and Physical layer they have data in format of segments, packets, frames and bits respectively.

236. Which one of the following is an architecture paradigms?
a) Peer to peer
b) Client-server
c) HTTP
d) Both Peer-to-Peer & Client-Server

Answer: d
Explanation: HTTP is a protocol.

237. Application developer has permission to decide the following on transport layer side
a) Transport layer protocol
b) Maximum buffer size
c) Both Transport layer protocol and Maximum buffer size
d) None of the mentioned

Answer: c
Explanation: Application layer provides the interface between applications and the network. So application developer can decide what transport layer to use and what should be its maximum buffer size.

238. Application layer offers _____ service.
a) End to end
b) Process to process
c) Both End to end and Process to process
d) None of the mentioned

Answer: a
Explanation: End to End service is provided in the application layer. Whereas process to process service is provided at the transport layer.

239. E-mail is _____
a) Loss-tolerant application
b) Bandwidth-sensitive application
c) Elastic application
d) None of the mentioned

Answer: c
Explanation: Because it can work with available throughput.

240. The _____ translates internet domain and host names to IP address.

a) domain name system
b) routing information protocol
c) network time protocol
d) internet relay chat

Answer: a
Explanation: Domain name system is the way the internet domain names are stored and translated to IP addresses. The domain names systems matches the name of website to ip addresses of the website.

241. Which one of the following allows a user at one site to establish a connection to another site and then pass keystrokes from local host to remote host?
a) HTTP
b) FTP
c) Telnet
d) TCP

Answer: c
Explanation: Telnet is used for accessing remote computers. Using telnet a user can access computer remotely. With Telnet, you can log on as a regular user with whatever privileges you may have been granted to the specific application and data on the computer.

242. Application layer protocol defines _____
a) types of messages exchanged
b) message format, syntax and semantics
c) rules for when and how processes send and respond to messages
d) all of the mentioned

Answer: d
Explanation: Application layer deals with the user interface, what message is to be sent or the message format, syntax and semantics. A user has access to application layer for sending and receiving messages.

243. Which one of the following protocol delivers/stores mail to reciever server?
a) simple mail transfer protocol
b) post office protocol
c) internet mail access protocol
d) hypertext transfer protocol

Answer: a
Explanation: SMTP, abbreviation for Simple Mail Transfer Protocol is an application layer protocol. A client who wishes to send a mail creates a TCP connection to the SMTP server and then sends the mail across the connection.

244. The ASCII encoding of binary data is called
a) base 64 encoding
b) base 32 encoding
c) base 16 encoding
d) base 8 encoding

Answer: a
Explanation: Base64 is used commonly in a number of applications including email via MIME, and storing complex data in XML. Problem with sending normal binary data to a network is that bits can be misinterpreted by underlying protocols, produce incorrect data at receiving node and that is why we use this code.

245. Which one of the following is an internet standard protocol for managing devices on IP network?

a) dynamic host configuration protocol
b) simple network management protocol
c) internet message access protocol
d) media gateway protocol

Answer: b
Explanation: SNMP is a set of protocols for network management and monitoring. This protocol is included in the application layer. SNMP uses 7 protocol data units.

246. Which one of the following is not an application layer protocol?
a) media gateway protocol
b) dynamic host configuration protocol
c) resource reservation protocol
d) session initiation protocol

Answer: c
Explanation: Resource reservation protocol is used in transport layer. It is designed to reserve resources across a network for quality of service using the integrated services model.

247. Which protocol is a signaling communication protocol used for controlling multimedia communication sessions?
a) session initiation protocol
b) session modelling protocol
c) session maintenance protocol
d) resource reservation protocol

Answer: a
Explanation: SIP is a signaling protocol in which its function includes initiating, maintaining and terminating real time sessions. SIP is used for signaling and controlling multimedia sessions.

248. Which one of the following is not correct?
a) Application layer protocols are used by both source and destination devices during a communication session
b) HTTP is a session layer protocol
c) TCP is an application layer protocol
d) All of the mentioned

Answer: d
Explanation: HTTP is an application layer protocol. Whereas TCP is a transport layer protocol.

249. Discarding policy is mainly done by _____
a) Sender
b) Receiver
c) Router
d) Switch

Answer: c
Explanation: The discarding policy adopted by the routers mainly states that the routers discard sensitive or corrupted packets that it receives, thus controlling the integrity of the packet flow. The discarding policy is adopted as an open loop congestion control technique.

250. In classful addressing, a large part of available addresses are _____
a) Organized
b) Blocked
c) Wasted
d) Communicated

Answer: c
Explanation: In classful addressing, a large part of available addresses are wasted. Thus

to solve this classful addressing is replaced with classless addressing where one can reserve the number of IP addresses required by modifying the CIDR value and make sure that not many addresses are wasted.

251. Network addresses are a very important concept of _____
a) Routing
b) Mask
c) IP Addressing
d) Classless Addressing

Answer: c
Explanation: Network addresses are a very important concept of IP addressing. The first address in a block is used as network address that represents the organization. The network address can be found by AND'ing any address in the block or class by the default mask.

252. Which of this is not a class of IP address?
a) Class E
b) Class C
c) Class D
d) Class F

Answer: d
Explanation: Class F is not a class of IP addressing. There are only five classes of IP addresses: Class A (0.0.0.0 to 127.255.255.255), Class B (128.0.0.0 to 191.255.255.255), Class C (192.0.0.0 to 223.255.255.255), Class D (224.0.0.0 to 239.255.255.255), and Class E (240.0.0.0 to 255.255.255.255).

253. The size of an IP address in IPv6 is _____
a) 4 bytes
b) 128 bits
c) 8 bytes
d) 100 bits

Answer: b
Explanation: An IPv6 address is 128 bits long. Therefore, 2128 i.e. 340 undecillion addresses are possible in IPv6. IPv4 has only 4 billion possible addresses and IPv6 would be a brilliant alternative in case IPv4 runs out of possible new addresses.

254. The header length of an IPv6 datagram is _____
a) 10bytes
b) 25bytes
c) 30bytes
d) 40bytes

Answer: d
Explanation: IPv6 datagram has fixed header length of 40bytes, which results in faster processing of the datagram. There is one fixed header and optional headers which may or may not exist. The fixed header contains the mandatory essential information about the packet while the optional headers contain the optional "not that necessary" information.

255. In the IPv6 header, the traffic class field is similar to which field in the IPv4 header?
a) Fragmentation field
b) Fast-switching
c) ToS field
d) Option field

Answer: c
Explanation: The traffic class field is used to specify the priority of the IP packet which is a similar functionality to the Type of Service field in the IPv4 header. It's an 8-bit field and its values are not defined in the RFC 2460.

256. IPv6 does not use _____ type of address.
a) broadcast
b) multicast
c) anycast
d) unicast

Answer: a
Explanation: There is no concept of broadcast address in IPv6. Instead, there is an anycast address in IPv6 which allows sending messages to a group of devices but not all devices in a network. Anycast address is not standardized in IPv4.

257. Which among the following features is present in IPv6 but not in IPv4?
a) Fragmentation
b) Header checksum
c) Options
d) Anycast address

Answer: d
Explanation: There is an anycast address in IPv6 which allows sending messages to a group of devices but not all devices in a network. Anycast address is not standardized in IPv4.

258. Dual-stack approach refers to _____
a) Implementing Ipv4 with 2 stacks
b) Implementing Ipv6 with 2 stacks
c) Node has both IPv4 and IPv6 support
d) Implementing a MAC address with 2 stacks

Answer: c
Explanation: Dual-stack is one of the approaches used to support IPv6 in already existing systems. ISPs are using it as a method to transfer from IPv4 to IPv6 completely eventually due to the lower number of possible available addresses in IPv4.

259. Suppose two IPv6 nodes want to interoperate using IPv6 datagrams, but they are connected to each other by intervening IPv4 routers. The best solution here is _____
a) Use dual-stack approach
b) Tunneling
c) No solution
d) Replace the system

Answer: b
Explanation: The IPv4 routers can form a tunnel in which at the sender's side, the IPv6 datagram is encapsulated in to IPv4, and at the receiver's side of the tunnel, the IPv4 packet is stripped and the IPv6 packet is sent to the receiver.

260. Which layer is responsible for process-to-process delivery?
a) Physical layer
b) Network layer
c) Transport layer
d) Application layer

Answer: c
Explanation: The transport layer is responsible for process-to-process delivery, error control and flow control. It provides an interface for the implementation of process to process delivery through ports. There are 65,535 port numbers.

261. In process-to-process delivery, two processes communicate in which of the following methods?
a) Client/Server
b) Source/Destination
c) Message Transfer
d) Peer to Peer

Answer: a
Explanation: The most common method used for this communication is Client/Server. The client requests a service through a particular port number to the port of the server using its socket address. Then the server responds by giving the requested service to the client port.

262. Multiple processes on destinations at transport layer are identified by _____
a) Mac address
b) Port number
c) Host number
d) Host address

Answer: b
Explanation: Multiple processes on destinations are identified by a transport layer address also called as port number. The IP address along with the port number is called the socket address.

263. In cryptography, what is cipher?
a) algorithm for performing encryption and decryption
b) encrypted message
c) both algorithm for performing encryption and decryption and encrypted message
d) decrypted message

Answer: a
Explanation: Cipher is a method to implement encryption and decryption of messages travelling in a network. It's used to increase the confidentiality of the messages.

264. In asymmetric key cryptography, the private key is kept by _____
a) sender
b) receiver
c) sender and receiver
d) all the connected devices to the network

Answer: b
Explanation: The private key is kept only by the receiver of the message. Its aim is to make sure that only the intended receiver can decipher the message.

265. Which one of the following algorithm is not used in asymmetric-key cryptography?
a) rsa algorithm
b) diffie-hellman algorithm
c) electronic code book algorithm
d) dsa algorithm

Answer: c
Explanation: Electronic code book algorithm is a block cipher method in which each block of text in an encrypted message

corresponds to a block of data. It is not feasible for block sizes smaller than 40 bits.

266. In cryptography, the order of the letters in a message is rearranged by _____

a) transpositional ciphers
b) substitution ciphers
c) both transpositional ciphers and substitution ciphers
d) quadratic ciphers

Answer: a
Explanation: In transposition ciphers, the order of letters in a plaintext message is shuffled using a pre-defined method. Some of such ciphers are Rail fence cipher and Columnar transposition.

267. What is data encryption standard (DES)?
a) block cipher
b) stream cipher
c) bit cipher
d) byte cipher

Answer: a
Explanation: DES is a symmetric key block cipher in which the block size is 64 bits and the key size is 64 bits. It is vulnerable to some attacks and is hence not that popularly used.

268. Cryptanalysis is used _____
a) to find some insecurity in a cryptographic scheme
b) to increase the speed
c) to encrypt the data
d) to make new ciphers

Answer: a
Explanation: Cryptanalysis is a field of study in which a cryptographic scheme is intentionally tried to breach in order to find flaws and insecurities. It is used to make sure that the scheme is least vulnerable to attacks.

269. Which one of the following is a cryptographic protocol used to secure HTTP connection?
a) stream control transmission protocol (SCTP)
b) transport layer security (TLS)
c) explicit congestion notification (ECN)
d) resource reservation protocol

Answer: b
Explanation: TLS has strong message authentication and key-material generation to prevent eavesdropping, tampering and message forgery. It has been used since the year 1996.

270. Voice privacy in GSM cellular telephone protocol is provided by _____
a) A5/2 cipher
b) b5/4 cipher
c) b5/6 cipher
d) b5/8 cipher

Answer: a
Explanation: The A5/2 cipher was published in the year 1996 and was cryptanalysed in the same year within a month. It's use was discontinued from the year 2006 as it was really weak.

271. IPSec is designed to provide security at the _____

a) transport layer
b) network layer
c) application layer
d) session layer

Answer: b
Explanation: IPSec is a set of protocols used to provide authentication, data integrity and confidentiality between two machines in an IP network. In the TCP/IP model, it provides security at the IP layer i.e. the network layer.

272. Network layer firewall works as a _____
a) frame filter
b) packet filter
c) signal filter
d) content filter

Answer: b
Explanation: As you know, firewalls are available as hardware appliances, as software-only, or a combination of the two. In every case, the purpose of a firewall is to isolate your trusted internal network (or your personal PC) from the dangers of unknown resources on the Internet and other network connections that may be harmful. The firewall prevents unauthorized access to your internal, trusted network from outside threats.

273. Network layer firewall has two sub-categories called _____
a) stateful firewall and stateless firewall
b) bit oriented firewall and byte oriented firewall
c) frame firewall and packet firewall
d) network firewall and data firewall

Answer: a
Explanation: Most network layer firewalls can operate as stateful or stateless firewalls, creating two subcategories of the standard network layer firewall. Stateful firewalls have the advantage of being able to track packets over a period of time for greater analysis and accuracy — but they require more memory and operate more slowly. Stateless firewalls do not analyze past traffic and can be useful for systems where speed is more important than security, or for systems that have very specific and limited needs. For example, a computer that only needs to connect to a particular backup server does not need the extra security of a stateful firewall.

274. WPA2 is used for security in _____
a) ethernet
b) bluetooth
c) wi-fi
d) e-mail

Answer: c
Explanation: WPA2 or WiFi Protected Access 2 is a security protocol used to provide users and firms with strong data security and protection for their wireless networks (WiFi) to give them confidence that only authorized users can access their network.

275. An attempt to make a computer resource unavailable to its intended users is called _____
a) denial-of-service attack
b) virus attack

c) worms attack
d) botnet process

Answer: a
Explanation: In a Denial of Service attack, the attacker won't let the victims access the network by using a certain method that ensures that an essential network resource is unavailable to the victim. The methods that the attacker can use are vulnerability attack, bandwidth flooding and connection flooding.

276. Extensible authentication protocol is authentication framework frequently used in _____
a) wired personal area network
b) wireless networks
c) wired local area network
d) wired metropolitan area network

Answer: b
Explanation: The Extensible Authentication Protocol (EAP) is an authentication protocol used to connect a network node to the Internet. It designed through extending the methods used by the Point-to-Point Protocol for authentication.

277. Datagram switching is done at which layer of OSI model?
a) Network layer
b) Physical layer
c) Application layer
d) Transport layer

Answer: a
Explanation: Datagram switching is normally done at network layer. In datagram switching, the datagram stream need not be in order as each datagram can take different routes to the destination.

278. Packets in datagram switching are referred to as _____
a) Switches
b) Segments
c) Datagrams
d) Data-packets

Answer: c
Explanation: As the name suggests, in datagram switching packets are called as datagram. Each datagram/packet is treated as an individual entity and routed independently through the network.

279. Datagram networks mainly refers to _____
a) Connection oriented networks
b) Connection less networks
c) Telephone networks
d) Internetwork

Answer: b
Explanation: The switch does not keep the information about the connection state, hence it is connection less. There is no need for establishing a handshake to begin the transmission in such networks.

280. Datagrams are routed to their destinations with the help of _____
a) Switch table
b) Segments table
c) Datagram table
d) Routing table

Answer: c
Explanation: Routing table is used to route the packets to their destinations. The

packet/datagram header contains the destination header for the whole journey to source to the destination through the routers.

281. Network layer firewall works as a _____

a) Frame filter
b) Packet filter
c) Content filter
d) Virus filter

Answer: b
Explanation: As you know, firewalls are available as hardware appliances, as software-only, or a combination of the two. In every case, the purpose of a firewall is to isolate your trusted internal network (or your personal PC) from the dangers of unknown resources on the Internet and other network connections that may be harmful. The firewall prevents unauthorized access to your internal, trusted network from outside threats.

282. Network layer firewall has two sub-categories as _____

a) State full firewall and stateless firewall
b) Bit oriented firewall and byte oriented firewall
c) Frame firewall and packet firewall
d) Network layer firewall and session layer firewall

Answer: a
Explanation: Most network layer firewalls can operate as stateful or stateless firewalls, creating two subcategories of the standard network layer firewall. Stateful firewalls have the advantage of being able to track packets over a period of time for greater analysis and accuracy — but they require more memory and operate more slowly. Stateless firewalls do not analyze past traffic and can be useful for systems where speed is more important than security, or for systems that have very specific and limited needs. For example, a computer that only needs to connect to a particular backup server does not need the extra security of a stateful firewall.

283. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as _____

a) Chock point
b) Meeting point
c) Firewall point
d) Secure point

Answer: a
Explanation: A firewall can be a PC, a router, a midrange, a mainframe, a UNIX workstation, or a combination of these that determines which information or services can be accessed from the outside and who is permitted to use the information and services from outside. Generally, a firewall is installed at the point where the secure internal network and untrusted external network meet, which is also known as a chokepoint.

284. Which of the following is / are the types of firewall?

a) Packet Filtering Firewall
b) Dual Homed Gateway Firewall

c) Screen Host Firewall
d) Dual Host Firewall

Answer: a
Explanation: A firewall can be a PC, a midrange, a mainframe, a UNIX workstation, a router, or combination of these. Depending on the requirements, a firewall can consist of one or more of the following functional components: Packet-filtering router

285. A proxy firewall filters at _____
a) Physical layer
b) Data link layer
c) Network layer
d) Application layer

Answer: d
Explanation: The application firewall is typically built to control all network traffic on any layer up to the application layer. It is able to control applications or services specifically, unlike a stateful network firewall, which is – without additional software – unable to control network traffic regarding a specific application. There are two primary categories of application firewalls, network-based application firewalls and host-based application firewalls.

286. A packet filter firewall filters at _____
a) Physical layer
b) Data link layer
c) Network layer or Transport layer
d) Application layer

Answer: c
Explanation: In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.[2] Firewalls are often categorized as either network firewalls or host-based firewalls.

287. Complex networks today are made up of hundreds and sometimes thousands of _____
a) Documents
b) Components
c) Servers
d) Entities

Answer: b
Explanation: Complex networks today are made up of hundreds and sometimes thousands of components. For effective functioning of these thousands of components, good network management is essential.

288. Performance management is closely related to _____
a) Proactive Fault Management
b) Fault management
c) Reactive Fault Management
d) Preventive Fault Management

Answer: b
Explanation: Fault management is really closely related to performance management. It is important to ensure that

the network handles faults as effectively as it handles it's normal functioning to achieve better performance management.

289. Configuration management can be divided into two subsystems: reconfiguration and _____
a) Documentation
b) Information
c) Servers
d) Entity

Answer: a
Explanation: The documentation subsystem of configuration management handles the log making and reporting functions of the configuration management. It also reports the errors in the network caused by the configuration's failure.

290. In Network Management System, the term that is responsible for controlling access to network based on predefined policy is called _____
a) Fault Management
b) Secured Management
c) Active Management
d) Security Management

Answer: d
Explanation: In Network Management System, the term that is responsible for controlling access to the network based on predefined policy is called security management. The security management ensures authentication, confidentiality and integrity in the network.

291. What is the access point (AP) in a wireless LAN?
a) device that allows wireless devices to connect to a wired network
b) wireless devices itself
c) both device that allows wireless devices to connect to a wired network and wireless devices itself
d) all the nodes in the network

Answer: a
Explanation: Access point in a wireless network is any device that will allow the wireless devices to a wired network. A router is the best example of an Access Point.

292. In wireless ad-hoc network _____
a) access point is not required
b) access point is must
c) nodes are not required
d) all nodes are access points

Answer: a
Explanation: An ad-hoc wireless network is a decentralized kind of a wireless network. An access point is usually a central device and it would go against the rules of the ad-hoc network to use one. Hence it is not required.

293. Which multiple access technique is used by IEEE 802.11 standard for wireless LAN?
a) CDMA
b) CSMA/CA
c) ALOHA
d) CSMA/CD

Answer: b
Explanation: CSMA/CA stands for Carrier-sense multiple access/collision avoidance. It

is a multiple access protocol used by IEEE 802.11 standard for wireless LAN. It's based on the principle of collision avoidance by using different algorithms to avoid collisions between channels.

294. In wireless distribution system _____

a) multiple access point are inter-connected with each other
b) there is no access point
c) only one access point exists
d) access points are not required

Answer: a
Explanation: A Wireless Distribution System allows the connection of multiple access points together. It is used to expand a wireless network to a larger network.

295. A wireless network interface controller can work in _____

a) infrastructure mode
b) ad-hoc mode
c) both infrastructure mode and ad-hoc mode
d) WDS mode

Answer: c
Explanation: A wireless network interface controller works on the physical layer and the data link layer of the OSI model. Infrastructure mode WNIC needs access point but in ad-hoc mode access point is not required.

296. In wireless network an extended service set is a set of _____

a) connected basic service sets
b) all stations
c) all access points
d) connected access points

Answer: a
Explanation: The extended service set is a part of the IEEE 802.11 WLAN architecture and is used to expand the range of the basic service set by allowing connection of multiple basic service sets.

297. Mostly _____ is used in wireless LAN.

a) time division multiplexing
b) orthogonal frequency division multiplexing
c) space division multiplexing
d) channel division multiplexing
View Answer

Answer: b
Explanation: In orthogonal frequency division multiplexing, digital data is encoded on multiple carrier frequencies. It is also used in digital television and audio broadcasting in addition to Wireless LANs.

298. Which one of the following event is not possible in wireless LAN?

a) collision detection
b) acknowledgement of data frames
c) multi-mode data transmission
d) connection to wired networks

Answer: a
Explanation: Collision detection is not possible in wireless LAN with no extensions. Collision detection techniques for multiple access like CSMA/CD are used to detect collisions in Wireless LANs.

299. What is Wired Equivalent Privacy (WEP)?
a) security algorithm for ethernet
b) security algorithm for wireless networks
c) security algorithm for usb communication
d) security algorithm for emails

Answer: b
Explanation: WEP is a security algorithm for wireless network which intended to provide data confidentiality comparable to that of traditional wired networks. It was introduced in 1997.

300. What is WPA?
a) wi-fi protected access
b) wired protected access
c) wired process access
d) wi-fi process access

Answer: a
Explanation: WPA or WiFi Protected Access is a security protocol used to provide users and firms with strong data security and protection for their wireless networks (WiFi) to give them confidence that only authorized users can access their network.

301. What is internet?
a) a single network
b) a vast collection of different networks
c) interconnection of local area networks
d) interconnection of wide area networks

Answer: b
Explanation: Internet is nothing but an interconnected computer network providing a variety of communication facilities, consisting of a huge amount of small networks using standardized communication protocols.

302. To join the internet, the computer has to be connected to a _____
a) internet architecture board
b) internet society
c) internet service provider
d) different computer

Answer: c
Explanation: The ISPs (Internet Service Providers) are the main agents through which every computer is connected to the internet. They are licensed to allot public IP addresses to its customers in order to connect them to the internet.

303. Internet access by transmitting digital data over the wires of a local telephone network is provided by _____
a) leased line
b) digital subscriber line
c) digital signal line
d) digital leased line

Answer: b
Explanation: DSL (Digital Subscriber Line) is the technology designed to use the existing telephone lines to transport high-bandwidth data to service subscribers. DSL was used to allow the early users access to the internet and it provides dedicated, point-to-point, public network access.

304. ISP exchanges internet traffic between their networks by _____
a) internet exchange point
b) subscriber end point

c) isp end point
d) internet end point

Answer: a
Explanation: ISPs exchange internet traffic between their networks by using Internet Exchange Points. ISPs and CDNs are connected to each other at these physical locations are they help them provide better service to their customers.

305. Which of the following protocols is used in the internet?
a) HTTP
b) DHCP
c) DNS
d) DNS, HTTP and DNS

Answer: d
Explanation: HTTP is used to browse all the websites on the World Wide Web, DHCP is used to allot IPs automatically to the users on the internet, and DNS is used to connect the users to the host servers on the internet based on the Domain Name.

306. Bluetooth is the wireless technology for _____
a) local area network
b) personal area network
c) metropolitan area network
d) wide area network

Answer: b
Explanation: Bluetooth is a wireless technology used to create a wireless personal area network for data transfer up to a distance of 10 meters. It operates on 2.45 GHz frequency band for transmission.

307. Bluetooth uses _____
a) frequency hopping spread spectrum
b) orthogonal frequency division multiplexing
c) time division multiplexing
d) channel division multiplexing

Answer: a
Explanation: Frequency hopping spread spectrum is a method of transmitting radio signals by rapidly changing the carrier frequency and is controlled by the codes known to the sender and receiver only.

308. Which algorithm can be used to sign a message?
a) Public key algorithm
b) Private key algorithm
c) Public & Private key algorithm
d) None of the mentioned

Answer: a
Explanation: Public key algorithms are used to sign a message and private key algorithms are used to encrypt the messages.

309. Private key algorithm is used for _____ encryption and public key algorithm is used for _____ encryption.
a) Messages, session key
b) Session key, messages
c) Can be used for both
d) None of the mentioned

Answer: a
Explanation: Private key algorithm is used for encryption of messages and public key algorithm is used for encryption of session keys.

310. In public key cryptosystem which is kept as public?
a) Encryption keys
b) Decryption keys
c) Encryption & Decryption keys
d) None of the mentioned

Answer: a
Explanation: In public key cryptosystem, the encryption keys are kept as public where as decryption keys are kept as secret.

311. In public key cryptosystem _____ keys are used for encryption and decryption.
a) Same
b) Different
c) Encryption Keys
d) None of the mentioned
View Answer

Answer: b
Explanation: In conventional cryptosystem, same keys are used for encryption and decryption where as in public key cryptosystem different keys are used.

312. Which of the following is the world's first cellular system to specify digital modulation and network level architecture?
a) GSM
b) AMPS
c) CDMA
d) IS-54

Answer: a
Explanation: GSM was the world's first cellular system to specify digital modulation and level architectures and services. It is the world's most popular 2G technology. It was developed to solve the fragmentation problems of the first cellular systems in Europe.

313. Previously in 1980s, GSM stands for _____
a) Global system for mobile
b) Groupe special mobile
c) Global special mobile
d) Groupe system mobile

Answer: b
Explanation: In the mid-1980s GSM was called by the name Groupe special mobile. In 1992, GSM changed its name to Global System for Mobile Communication for marketing reasons.

314. Who sets the standards of GSM?
a) ITU
b) AT & T
c) ETSI
d) USDC

Answer: c
Explanation: The setting of standards for GSM is under the aegis of the European Technical Standards Institute (ETSI). GSM task was to specify a common mobile communication system for Europe in the 900 MHZ band.

315. Which of the following does not come under the teleservices of GSM?
a) Standard mobile telephony
b) Mobile originated traffic
c) Base originated traffic
d) Packet switched traffic

Answer: d
Explanation: GSM services follow ISDN guidelines and are classified as either

teleservices or data services. Teleservices include standard mobile telephony and mobile originated or base originated traffic.

316. Which of the following comes under supplementary ISDN services?
a) Emergency calling
b) Packet switched protocols
c) Call diversion
d) Standard mobile telephony

Answer: c
Explanation: Supplementary ISDN services are digital in nature. They include call diversion, closed user groups, and caller identification, and are not available in analog mobile networks. Supplementary services also include short messaging service (SMS).

317. US digital cellular system based on CDMA was standardized as _____
a) IS-54
b) IS-136
c) IS-95
d) IS-76

Answer: c
Explanation: A US digital cellular system based on CDMA was standardized as Interim Standard 95 (IS-95). It was standardized by US Telecommunication Industry Association (TIA) and promised increased capacity.

318. IS-95 was not compatible with existing AMPS frequency band.
a) True
b) False

Answer: b
Explanation: Like IS-136, IS-95 system was designed to be compatible with the existing US analog cellular system (AMPS) frequency band. Hence, mobile and base stations can be economically produced for dual mode operation.

319. Which of the following is used by IS-95?
a) DSSS
b) FHSS
c) THSS
d) Hybrid

Answer: a
Explanation: IS-95 uses a direct sequence spread spectrum CDMA system. It allows each user within a cell to use the same radio channel, and users in adjacent cell also use the same radio channel.

320. GPRS and EDGE supports which 2G standard?
a) GSM only
b) IS-136 only
c) GSM and IS-136 both
d) PDC

Answer: c
Explanation: GPRS (General Packet Radio Service) network provides a packet network on dedicated GSM or IS-136 radio channels. EDGE (Enhanced Data rates for GSM Evolution) is also developed keeping in desire both GSM and IS-136 operators.

321. How is HSCSD different from GPRS?
a) Infrastructure
b) Multiple Access Scheme

c) Modulation technique
d) Switching Technique

Answer: d
Explanation: GPRS is a packet based network. HSCSD dedicates circuit switched channels to specific users whereas GPRS supports many more users, but in a bursty manner.

322. What changes GPRS need to acquire while upgrading itself from GSM?
a) A whole new base station
b) New transceiver at base station
c) New channel cards
d) New packet overlay including routers and gateways

Answer: d
Explanation: GPRS requires a GSM operator to install new routers and Internet gateways at the base station along with new software upgrade. New base station RF hardware is not required.

323. How many types of protocols are important for instant messaging?
a) 2
b) 3
c) 4
d) All of the mentioned

Answer: b
Explanation: In an effort to create an interoperability standard between different IM clients, several instant messaging protocols have been created.

324. Point out the correct statement.
a) Every third-party IM clients aim to allow their users to connect to the different major IM services
b) SIP stands for Secure Initiation Protocol
c) XMPP stands for Extensible Messaging and Presence Protocol
d) All of the mentioned

Answer: c
Explanation: SIP stands for Session Initiation Protocol.

325. Which of the following protocol is adopted for interoperability by top three IM service providers?
a) SIP
b) SIMPLE
c) XMPP
d) IMPS

Answer: b
Explanation: They allow their users to connect with the other services' public users for a fee.

326. Which of the following systems allow short text messages to be exchanged?
a) SMS
b) IMS
c) JVS
d) All of the mentioned

Answer: a
Explanation: Twitter is described as the prototypical example of this type of service.

327. Point out the correct statement.
a) Aggregation also can be done within software creating a custom Web page
b) The Add Stuff link in iGoogle takes you to the content management system
c) When you return to iGoogle, the feed appears within an Ajax frame that can be

moved around on the page or moved to additional tabs that you can create
d) All of the mentioned

Answer: d
Explanation: iGoogle's syndication aggregation site is an example of a content management system.

328. _____ builds on the older concept of Internet chat to add a more immediate response to text messages between individuals and groups.
a) VM
b) IM
c) SM
d) None of the mentioned

Answer: b
Explanation: IM stands for instant messaging.

329. Which of the following is a virtual machine technology now owned by Oracle that can run various operating systems?
a) Vmachines
b) VirtualBox
c) ThoughtPolice
d) None of the mentioned

Answer: b
Explanation: VirtualBox serves as a host for a variety of virtual appliances.

330. Point out the correct statement.
a) JumpIt is an open-source virtual appliance installation and management service
b) Converting a virtual appliance from one platform to another is easy proposition
c) Nearly all major virtualization platform vendors support OVF, notably VMware, Microsoft, Oracle, and Citrix
d) All of the mentioned

Answer: c
Explanation: Efforts are underway to create file format standards for these types of objects that make the task easier.

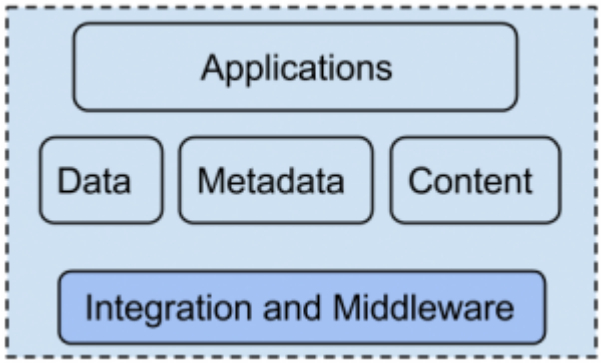
331. Which of the following lets a Web service advertise itself in terms of a collection of endpoints?
a) WSDL
b) VMc
c) SOAP
d) All of the mentioned

Answer: a
Explanation: The most commonly used model for discovery and description used with SOAP messaging is the Web Services Description Language (WSDL).

332. Which of the following is a specification for multicast discovery on a LAN?
a) WS-Agent
b) WS-Discovery
c) WS-SOAP
d) All of the mentioned

Answer: b
Explanation: WS-Discovery stands for Web Services Dynamic Discovery specification.

333. Which of the following content is allowed as per virtual appliance block diagram shown below?



a) Table
b) Image
c) Documents
d) All of the mentioned

Answer: d
Explanation: Content can be structured or unstructured in virtual appliance.

334. Point out the correct statement.
a) WS-+ services carried over XML messages using the SOAP protocol access remote server applications
b) REST stands for Representational State Transfer
c) A transaction following the rules of SOAP is considered to be RESTful
d) All of the mentioned

Answer: b
Explanation: REST assigns a global identifier to a resource so there is a uniform method for accessing information sources.

335. Which of the following is based on the IETF Session Initiation Protocol?
a) WSDL
b) SIMPLE
c) SOAP
d) All of the mentioned

Answer: b
Explanation: SIMPLE is an open standard protocol.

336. _____ offering provides the tools and development environment to deploy applications on another vendor's application.
a) PaaS
b) IaaS
c) CaaS
d) All of the mentioned

Answer: b
Explanation: PaaS tool is a fully integrated development environment.

337. Point out the correct statement.
a) Platforms cannot be based on specific types of development languages, application frameworks, or other constructs
b) PaaS systems offer a way to create user interfaces
c) In a CaaS model, customers may interact with the software to enter and retrieve data
d) All of the mentioned

Answer: b
Explanation: PaaS systems support standards such as HTML, JavaScript, or other rich media technologies.

338. Which of the following is associated with considerable vendor lock-in?
a) PaaS
b) IaaS
c) CaaS
d) SaaS

Answer: a
Explanation: The difficulty with PaaS is that

it locks the developer (and the customer) into a solution that is dependent upon the platform vendor.

339. _____ serves as a PaaS vendor within Google App Engine system.
a) Google
b) Amazon
c) Microsoft
d) All of the mentioned

Answer: a
Explanation: Google offers many of its Web service applications to customers as part of this service model.

340. Point out the wrong statement.
a) The customer takes no responsibility for maintaining the hardware, the software, or the development of the applications
b) The vendor is responsible for all the operational aspects of the service
c) Google's App Engine platform is IaaS offering
d) None of the mentioned

Answer: c
Explanation: The customer is responsible only for his interaction with the platform.

341. Which of the following can be considered PaaS offering?
a) Google Maps
b) Gmail
c) Google Earth
d) All of the mentioned

Answer: a
Explanation: The vendor of the PaaS solution is in most cases the developer, who is offering a complete solution to the customer.

342. Which of the following is the most complete cloud computing service model?
a) PaaS
b) IaaS
c) CaaS
d) SaaS

Answer: d
Explanation: The most complete cloud computing service model is one in which the computing hardware and software, as well as the solution itself, are provided by a vendor as a complete service offering.

343. Point out the correct statement.
a) Platforms can be based on specific types of development languages, application frameworks, or other constructs
b) SaaS is the cloud-based equivalent of shrink-wrapped software
c) Software as a Service (SaaS) may be succinctly described as software that is deployed on a hosted service
d) All of the mentioned

Answer: d
Explanation: SaaS can be accessed globally over the Internet, most often in a browser.

344. Which of the following aspect of the service is abstracted away?
a) Data escrow
b) User Interaction
c) Adoption drivers
d) None of the mentioned

Answer: b
Explanation: With the exception of the user

interaction with the software, all other aspects of the service are abstracted away.

345. Which of the following SaaS platform is with an exposed API?
a) salesforce.com
b) amazon.com
c) flipkart.com
d) all of the mentioned

Answer: a
Explanation: SaaS does not necessarily mean that the software is static or monolithic.

346. Point out the wrong statement.
a) SaaS applications come in all shapes and sizes
b) Every computer user is familiar with SaaS systems
c) SaaS software is not customizable
d) None of the mentioned

Answer: d
Explanation: Every computer user is familiar with SaaS systems, which are either replacements or substitutes for locally installed software.

347. The storage structure which do not survive system crashes are _____
a) Volatile storage
b) Non-volatile storage
c) Stable storage
d) Dynamic storage

Answer: a
Explanation: Volatile storage, is a computer memory that requires power to maintain the stored information, in other words it needs power to reach the computer memory.

348. Storage devices like tertiary storage, magnetic disk comes under
a) Volatile storage
b) Non-volatile storage
c) Stable storage
d) Dynamic storage

Answer: b
Explanation: Information residing in nonvolatile storage survives system crashes.

349. For a transaction to be durable, its changes need to be written to _____ storage.
a) Volatile storage
b) Non-volatile storage
c) Stable storage
d) Dynamic storage

Answer: c
Explanation: Similarly, for a transaction to be atomic, log records need to be written to stable storage before any changes are made to the database on disk.

350. The unit of storage that can store one are more records in a hash file organization are
a) Buckets
b) Disk pages
c) Blocks
d) Nodes

Answer: a
Explanation: Buckets are used to store one or more records in a hash file organization.

351. _____ allows us to control electronic components
a) RETful API
b) RESTful API
c) HTTP
d) MQTT

Answer: a
Explanation: RETful API that allows us to control electronic components connected to our Intel Galileo Gen 2 board through HTTP requests.

352. MQTT stands for _____
a) MQ Telemetry Things
b) MQ Transport Telemetry
c) MQ Transport Things
d) MQ Telemetry Transport

Answer: d
Explanation: MQTT was known as MQ Telemetry Transport protocol. MQTT is a lightweight protocol that runs on top of the TCP/IP protocol.

353. MQTT is better than HTTP for sending and receiving data.
a) True
b) False

Answer: a
Explanation: We want to send and receive data in real time through internet and RESTful API is not the most appropriate option to do this. Instead, we will work on MQTT which is lighter than HTTP.

354. MQTT is _____ protocol.
a) Machine to Machine
b) Internet of Things
c) Machine to Machine and Internet of Things
d) Machine Things

Answer: c
Explanation: The MQTT protocol is a machine to machine and Internet of thing connectivity protocol.

355. Which protocol is lightweight?
a) MQTT
b) HTTP
c) CoAP
d) SPI

Answer: a
Explanation: MQTT is a lightweight protocol that runs on top of the TCP/IP protocol and works with publish subscribe mechanism.

356. PubNub publishes and subscribes _____ in order to send and receive messages.
a) Network
b) Account
c) Portal
d) Keys

Answer: d
Explanation: It is necessary to generate our PubNub publishes and subscribes keys in order to send and receive messages in the network.

357. By clicking which key the PubNub will display public, subscribe, and secret keys.
a) Pane
b) Demo Keyset
c) Portal
d) Network

Answer: b
Explanation: Click on Demo keyset pane and PubNub will display public, subscribe, and secret keys. We must copy and paste each of these keys to use them in our code that will publish messages and subscribe to them.

358. _____ is another data hiding technique which can be used in conjunction with cryptography for the extra-secure method of protecting data.
a) Cryptography
b) Steganography
c) Tomography
d) Chorography

Answer: b
Explanation: Steganography is the technique of hiding data in another raw data. Steganography is another data hiding technique which can be used in conjunction with cryptography for an extra-secure method of protecting data.

359. _____ is hiding of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.
a) Cryptography
b) Tomography
c) Steganography
d) Chorography

Answer: c
Explanation: Steganography helps in hiding any form of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

360. Steganography follows the concept of security through obscurity.
a) True
b) False

Answer: a
Explanation: Hiding of data within another data through obscurity is called steganography. It is another data hiding technique which can be used in conjunction with cryptography for an extra-secure method of protecting data.

361. The word _____is a combination of the Greek words ‘steganos’ which means “covered or concealed”, and ‘graphein’ which means “writing”.
a) Cryptography
b) Tomography
c) Steganography
d) Chorography

Answer: c
Explanation: The word steganography is a combination of the Greek words ‘steganos’ which means “covered or concealed”, and ‘graphein’ which means “writing”. Steganography is hiding of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

362. A _____ tool permits security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.
a) Cryptography
b) Tomography

c) Chorography
d) Steganography

Answer: d
Explanation: A steganography tool is a software tool that permits a security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

363. Frequency division multiple access (FDMA) assigns _____ channels to _____ users.
a) Individual, individual
b) Many, individual
c) Individual, many
d) Many, many

Answer: a
Explanation: Frequency division multiple access (FDMA) assigns individual channels to individual users. Each user is allocated a unique frequency band or channel. These channels are assigned on demand to users who request service.

364. During the period of call, other users can share the same channel in FDMA.
a) True
b) False

Answer: b
Explanation: In FDMA systems, no other user can share the same channel during the period of call. In FDD systems, the users are assigned a channel as a pair of frequencies; one is used for the forward channel while the other frequency is used for the reverse channel.

365. The FDMA channel carries _____ phone circuit at a time.
a) Ten
b) Two
c) One
d) Several

Answer: c
Explanation: The FDMA channel carries one phone circuit at a time. Each individual band or channel is wide enough to accommodate the signal spectra of the transmissions to be propagated.

366. If the FDMA channel is not in use, it can be used by other users.
a) True
b) False

Answer: b
Explanation: If an FDMA channel is not in use, it sits idle and cannot be used by other users to increase or share capacity. It is essentially a wasted resource.

367. TDMA systems transmit in a continuous way.
a) True
b) False

Answer: b
Explanation: TDMA systems transmit data in a buffer and burst method. Thus, the transmission for any user is not continuous.

368. Preamble contains _____
a) Address
b) Data
c) Guard bits
d) Trail bits

Answer: a
Explanation: TDMA frame is made up of a preamble, an information message and the trail bits. In a TDMA frame, the preamble contains the address and synchronization information that both the base station and the subscribers use to identify each other.

369. _____ are utilized to allow synchronization of the receivers between different slots and frames.
a) Preamble
b) Data
c) Guard bits
d) Trail bits

Answer: c
Explanation: Guard times are utilized to allow synchronization of the receivers between different slots and frames. TDMA/FDD systems intentionally induce several time slots of delay between the forward and reverse time slots for a particular user.

370. Which of the following is not true for TDMA?
a) Single carrier frequency for single user
b) Discontinuous data transmission
c) No requirement of duplexers
d) High transmission rates

Answer: a
Explanation: TDMA share a single carrier frequency with several users, where each user makes use of non-overlapping time slots. The number of time slots per frame depends on several factors, such as modulation technique, available bandwidth etc.

371. Which of the following is used for shaping the velocity of the satellite orbit?
a) User segment
b) Control segment
c) Ground segment
d) Space segment

Answer: b
Explanation: The entire process of GPS has been categorized into user segment, control segment. These are allocated with a certain part of the entire work. Control segment helps me monitoring the shape and velocity of satellite orbits.

372. Which waveforms are also called as line codes?
a) PCM
b) PAM
c) FM
d) AM

Answer: a
Explanation: When pulse modulation is applied to binary symbol we obtain pulse code modulated waveforms. These waveforms are also called as line codes.

373. When pulse code modulation is applied to non binary symbols we obtain waveform called as
a) PCM
b) PAM
c) M-ary
d) line codes

Answer: c
Explanation: When pulse code modulation is applied to binary symbols we get PCM waveforms and when it is applied to non

binary symbols we obtain M-ary waveforms.

374. First address in a block is used as network address that represents the _____
a) Class Network
b) Entity
c) Organization
d) Codes

Answer: c
Explanation: First address in a block is used as network address that represents the organization. The network address can be found by AND'ing any address in the block by the default mask. The last address in a block represents the broadcast address.

375. Protocol is a set of
a) Formats
b) Procedures
c) Formats & Procedures
d) None of the mentioned

Answer: c
Explanation: Protocol is a set of procedures and formats that entities use to communicate information.

376. The time required to transmit frame depends on
a) Frame size
b) Channel capacity
c) Frame size & Channel capacity
d) None of the mentioned

Answer: c
Explanation: The time to transmit frame is given by the ratio of frame size and channel capacity.

377. Window given the number of
a) Bytes
b) Frames
c) Bytes & Frames
d) None of the mentioned

Answer: c
Explanation: Window gives the number of frames or bytes that can be in transit unacknowledged.

378. Routing is
a) Static
b) Dynamic
c) Static & Dynamic
d) None of the mentioned

Answer: c
Explanation: Routing can be static and dynamic.

379. Routing is performed only centrally.
a) True
b) False

Answer: a
Explanation: Routing is performed centrally and also in fully distributed way.

380. Which is connection oriented and which is connection-less?
a) Datagrams, virtual circuits
b) Virtual circuits, datagrams
c) Datagrams
d) None of the mentioned

Answer: b
Explanation: Datagram is connection-less and virtual circuits are connection oriented.

381. Which uses UDP?
a) Echo
b) Time
c) Domain name server
d) All of the mentioned

Answer: d
Explanation: The protocols using UDP are echo, time, domain name server, network file system etc.

382. Which uses TCP?
a) Simple mail transfer protocol
b) Simple network management protocol
c) Simple mail transfer & network management protocol
d) None of the mentioned

Answer: a
Explanation: Some of the protocols using TCP are http, telnet, file transfer protocol, simple mail transfer protocol etc.

383. Which tells about low level transmission and framing?
a) V series
b) X series
c) G series
d) Q series

Answer: c
Explanation: G series tells about level transmission, modulation and framing.

384. Which tells about signalling?
a) V series
b) X series
c) G series
d) Q series

Answer: d
Explanation: Q series tells about signalling.

385. Which of the following module feature is provided by Drupal CMS?
a) Traffic management
b) OpenID authentication
c) User interface creation tools
d) All of the mentioned

Answer: d
Explanation: The Drupal core by itself contains a number of modules.

386. Which of the following programming language solves problems by acting on constraints and inputs?
a) 3GL
b) 4GL
c) 5GL
d) None of the mentioned

Answer: c
Explanation: Force.com uses a 4GL programming language environment.

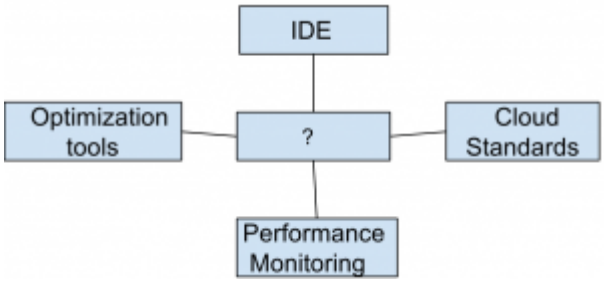
387. _____ PaaS application delivery platform creates SOA applications that work on several different IaaS vendors.
a) AppOne
b) Eccentex AppBase
c) Ez Publish
d) All of the mentioned

Answer: b
Explanation: Eccentex is a Culver City, California, company founded in 2005 that has a PaaS development platform for Web applications.

388. Which of the following AppBase tool allows you to assign access rights to different objects in the system?
a) Security Roles Management
b) Dashboard Designer
c) Report Builder
d) All of the mentioned

Answer: a
Explanation: Security roles can be assigned in groups without users, and users can be added later as the application is deployed.

389. Which of the following should be replaced with question mark in the figure?



a) CaaS
b) SaaS
c) IaaS
d) None of the mentioned

Answer: b
Explanation: A good PaaS system has certain desirable characteristics that are important in developing robust, scalable, and hopefully portable applications.

390. When you add a software stack, such as an operating system and applications to the service, the model shifts to _____ model.
a) SaaS
b) PaaS
c) IaaS
d) All of the mentioned

Answer: a
Explanation: Microsoft's Windows Azure Platform is best described as currently using SaaS model.

391. Which of the following is the most refined and restrictive service model?
a) IaaS
b) CaaS
c) PaaS
d) All of the mentioned

Answer: c
Explanation: When the service requires the client to use a complete hardware/software/application stack, it is using the most refined and restrictive service model.

392. _____ is a pay-as-you-go model matches resources to need on an ongoing basis.
a) Utility
b) Elasticity
c) Low barrier to entry
d) All of the mentioned

Answer: a
Explanation: This eliminates waste and has the added benefit of shifting risk from the client.

393. _____ feature allows you to optimize your system and capture all possible transactions.
a) scalability
b) reliability

c) elasticity
d) none of the mentioned

Answer: c
Explanation: You have the ability to right-size resources as required.

394. _____ enables batch processing, which greatly speeds up high-processing applications.
a) Scalability
b) Reliability
c) Elasticity
d) Utility

Answer: a
Explanation: This feature obviates the need for planning and provisioning.

395. _____ is a complete operating environment with applications, management, and user interface.
a) IaaS
b) SaaS
c) PaaS
d) All of the mentioned

Answer: b
Explanation: In the SaaS model, the application is provided to the client through a thin client interface.

396. How many types of service model are mainly present in Cloud?
a) 1
b) 2
c) 3
d) 4

Answer: c
Explanation: Three types of Service model exist.

397. The three different service models are together known as the _____ model of cloud computing.
a) SPI
b) SIP
c) CPI
d) All of the mentioned

Answer: a
Explanation: Many other service models are also present.

398. CaaS stands for _____ as service.
a) Compliance
b) Computer
c) Community
d) Communication

Answer: d
Explanation: Communication as a Service (CaaS), enables the consumer to utilize Enterprise level VoIP, VPNs, PBX and Unified Communications without the costly investment of purchasing, hosting and managing the infrastructure.

399. Which of the following is the IaaS service provider?
a) EC2
b) EC1
c) EC10
d) Hybrid

Answer: a
Explanation: On Amazon EC2, a client would

provision a computer in the form of a virtual machine image.

400. ARPANET stands for?
a) Advanced Research Project Agency Network
b) Advanced Research Programmed Auto Network
c) Advanced Research Project Automatic Network
d) Advanced Research Project Authorized Network

Answer: a
Explanation: ARPANET stands for Advanced Research Project Agency Network. It was developed in late 1960s under ARPA (Advanced Research Projects Agency).

401. Internet can help you find the shortest route.
a) True
b) False

Answer: a
Explanation: The statement is true. Obviously, Internet is so widespread; it can help us in all the possible ways. It can predict the weather, play music, etc.

402. In this technique, there is no direct contact between users and their programs during execution.
a) Time Sharing
b) Batch Processing
c) System Processing
d) Message Passing

Answer: b
Explanation: In the Batch Environment, there is no direct interaction between users and their programs during execution.

403. A technique that marked the beginning of computer communications.
a) Batch Environment
b) Message passing
c) User Environment
d) Time Sharing

Answer: d
Explanation: The answer is time sharing. In time sharing, Users were able to interact with the computer and could share its information processing resources.

404. A type of technique in which dumb terminals are connected to a central computer system.
a) Time Sharing
b) Message passing
c) Batch environment
d) User environment

Answer: a
Explanation: This happens in time sharing. In this, users were able to interact with the computer and could share its information processing resources.

405. TCP stands for?
a) Transmission control program
b) Transmission control protocol
c) Transfer control program
d) Transfer control protocol

Answer: b
Explanation: TCP stands for transmission control protocol. It basically allows different networks to interconnect.

406. The “Victorian internet” is actually?
a) Telegraph
b) Batch Environment
c) Unit Environment
d) System Environment

Answer: a
Explanation: It was a telegraph. Invented in the 1840s. Used extensively by the U.S. Government.

407. Packet switching was invented in?
a) 1960s
b) 1980s
c) 2000s
d) 1990s

Answer: a
Explanation: Packet switching was developed in 1964. In packet switching, the message is broken into parts and then sent over independently.

408. The probability of failure-free operation of a software application in a specified environment for a specified time.
a) Software Reliability
b) Software Quality
c) Software availability
d) Software Safety

Answer: a
Explanation: The answer is software reliability. It is estimated using historical and development data.

409. DARPA stands for?
a) Data Advanced Research Projects Agency
b) Defense Advanced Research Product Agency
c) Data based Advanced Research Product Agency
d) Defense Advanced Research Projects Agency

Answer: d
Explanation: DARPA (Defense Advanced Research Projects Agency) contracted with BBN (Bolt, Beranek & Newman) to create ARPAnet.

410. A network of physical objects or things embedded with electronics or softwares.
a) AI
b) ML
c) IOT
d) Internet

Answer: c
Explanation: IoT is a network of physical objects or things embedded with electronics or softwares. Iot allows objects to be controlled remotely across existing network.

411. RFID is a part of IoT.
a) True
b) False

Answer: a
Explanation: The statement is true. RFID is Radio frequency identification. Radio frequency identification is a part of IoT.

412. RFID stands for?
a) Random frequency identification
b) Radio frequency identification
c) Random frequency information
d) Radio frequency information

Answer: b
Explanation: Earlier, RFID or Radio

frequency identification was a prerequisite for Internet of Things.

413. Which of the following is not involved in working of IoT?
a) RFID
b) Sensor
c) Nano tech
d) Server

Answer: d
Explanation: IoT works from RFID to Sensor, to Smart tech and then to Nano tech.

414. Making the smaller and smaller things have the ability to connect and interact.
a) Micro Tech
b) Smart tech
c) Nano tech
d) RFID

Answer: c
Explanation: Nano Tech is the term used when smaller things are made to interact and communicate. It is involved in the working of Iot also.

415. Wi-Fi stands for?
a) Wireless fidelity
b) Wireless Flexibility
c) Wide Fidelity
d) WAN Flexibility

Answer: a
Explanation: Wi-Fi stands for Wireless Fidelity. It is widely used in both outdoor and indoor environments.

416. Diagnostics service for Cars.
a) MIPS
b) AutoBot
c) IoT Assistant
d) IoT

Answer: b
Explanation: Autobot is a diagnostics service for cars. This service is integrated with several web services.

417. The father of ioT.
a) Kevin Atrun
b) Kevin Atrhur
c) Kevin Ashton
d) Kevin Thomas

Answer: c
Explanation: Kevin Ashton is the father of IoT. He believed IoT could turn the world into data.

418. Collect->Communicate->_____->Act
a) Acknowledge
b) Analyze
c) Examine
d) Rectify

Answer: a
Explanation: The correct option is analyze. This shows the lifecycle of IoT. Collect->Communicate->Analyze->Act.

419. Several instructions execution simultaneously in?
a) processing
b) parallel processing
c) serial processing
d) multitasking

Answer: b
Explanation: In parallel processing, the several instructions are executed

simultaneously. Parallel processing system provides the concurrent data processing to increase the execution time.

420. What is A2DP (advanced audio distribution profile)?
a) a bluetooth profile for streaming audio
b) a bluetooth profile for streaming video
c) a bluetooth profile for security
d) a bluetooth profile for file management

Answer: a
Explanation: A2DP stands for Advanced Audio Distribution Profile is a transfer standard use to transmit high definition audio through Bluetooth. It is mainly used in Bluetooth speakers and wireless headphones.

421. In a piconet, one master device _____
a) can not be slave
b) can be slave in another piconet
c) can be slave in the same piconet
d) can be master in another piconet

Answer: b
Explanation: In a scatternet, a slave node of one piconet may act as a master in a piconet that is part of the scatternet. The scatternet uses this property to connect many piconets together to create a larger network.

422. Bluetooth transceiver devices operate in _____ band.
a) 2.4 GHz ISM
b) 2.5 GHz ISM
c) 2.6 GHz ISM
d) 2.7 GHz ISM

Answer: a
Explanation: Bluetooth operates on 2.45 GHz frequency ISM band for transmission. It is used to create a wireless personal area network for data transfer up to a distance of 10 meters.

423. Bluetooth supports _____
a) point-to-point connections
b) point-to-multipoint connection
c) both point-to-point connections and point-to-multipoint connection
d) multipoint to point connection

Answer: c
Explanation: In Bluetooth, each slave node communicates with the master of the piconet independently i.e. each master-slave connection is independent. The slave is not allowed to communicate with other slaves directly.

424. A scatternet can have maximum _____
a) 10 piconets
b) 20 piconets
c) 30 piconets
d) 40 piconets

Answer: a
Explanation: A scatternet can have maximum of 10 piconets and minimum of 2 piconets. To connect these piconets, a slave node of one piconet may act as a master in a piconet that is part of the scatternet.