# COMPUTER NETWORKS

**UNIT I:**

**INTRODUCTION:** Network Topologies WAN, LAN, MAN. Reference models- The OSI Reference Model the TCP/IP Reference Model - A Comparison of the OSI and TCP/IP Reference Models.

**PHYSICAL LAYER** –Introduction to physical layer-Data and Signals, Periodic analog signals, digital signals, transmission impairment, ,Data rate limits, performance -Introduction to Guided Media- Twisted-pair cable, Coaxial cable and Fiber optic cable and Unguided media: Wireless-Radio waves, microwaves, infrared.

**THE DATA LINK LAYER** - Services Provided to the Network Layer – Framing – Error Control – Flow Control, Error Detection and Correction – Error-Correcting Codes – Error Detecting Codes. Elementary

**UNIT II**

**DATA LINK PROTOCOLS-** A Utopian Simplex Protocol-A Simplex Stop and Wait Protocol for an Error free channel-A Simplex Stop and Wait Protocol for a Noisy Channel, Sliding Window Protocols-A One Bit Sliding Window Protocol-A Protocol Using Go-Back-N- A Protocol Using Selective Repeat.

**THE MEDIUM ACCESS CONTROL SUBLAYER-**The Channel Allocation Problem-Static Channel Allocation Assumptions for Dynamic Channel Allocation, Multiple Access Protocols-Aloha-Pure aloha- slotted aloha-Carrier Sense Multiple Access Protocols- Collision-Free Protocols-Limited Contention Protocols.

**WIRELESS LAN PROTOCOLS-** Ethernet-Classic Ethernet Physical Layer-Classic Ethernet MAC Sub-layer Protocol-Ethernet Performance-Fast Ethernet- Wireless LANs-The 802.11 Architecture and Protocol Stack-The 802.11 Physical Layer-The802.11 MAC Sub-layer Protocol- The 805.11 Frame Structure Services.

**UNIT III**

**THE NETWORK LAYER DESIGN ISSUES –** Store and Forward Packet Switching-Services Provided to the Transport layer- Implementation of Connectionless Service-Implementation of Connection Oriented Service- Comparison of Virtual Circuit and Datagram Networks, Routing Algorithms-The Optimality principle-Shortest path, Flooding, Distance vector, Link state, Hierarchical**.**

**CONGESTION CONTROL ALGORITHMS-**General principles of congestion control, Congestion prevention policies, Approaches to Congestion Control-Traffic Aware Routing- Admission Control-Traffic Throttling-Load Shedding.

**INTERNET WORKING:** How networks differ- How networks can be connected- Tunneling, internetwork routing-, Fragmentation, network layer in the internet – IP protocols-IP Version 4 protocol-, IP addresses-, Subnets-IP Version 6-The main IPV6 header- Internet control protocols- ICMP-ARPDHCP.

**UNIT IV**

**THE TRANSPORT LAYER:** Transport layer protocols: Introduction-services- port number-User datagram protocol-User datagram-UDP services-UDP applications-Transmission control protocol: TCP services TCP features- Segment- A TCP connection- windows in TCP- flow control-Error control.

**APPLICATION LAYER –-** World Wide Web: HTTP , FTP-Two connections-control connection-Data connection-security of FTP-Electronic mail-Architecture- web based mail- email security- TELENET-local versus remote Logging.

**DOMAIN NAME SYSTEM:** Name Space, DNS in Internet, - Resolution-Caching- Resource Records- DNS messages- Registrars-security of DNS Name Servers.

**UNIT I**

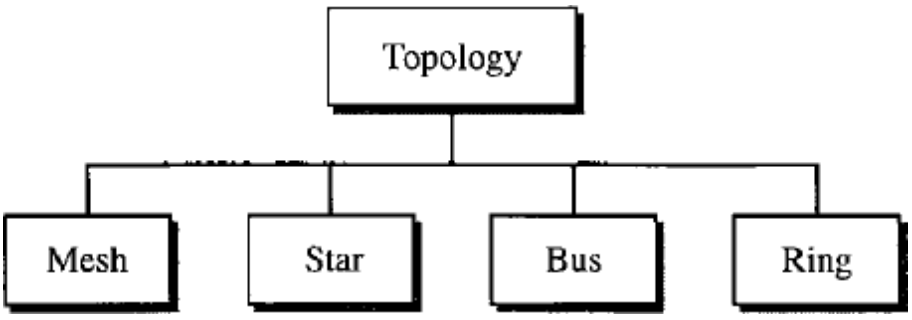
## Q).What is a NETWORKS

A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

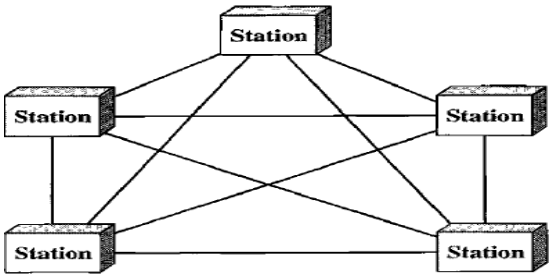
## Q).Write about Network Topology

The term *physical topology* refers to the way in which a network is laid out physically. One or more devices connect to a link; two or more links form a topology.

There are four basic topologies possible: mesh, star, bus, and ring




**Mesh:** In a mesh topology, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects.




*Advantages:*

1. A Mesh topology is a eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
3. It is provide privacy or security.

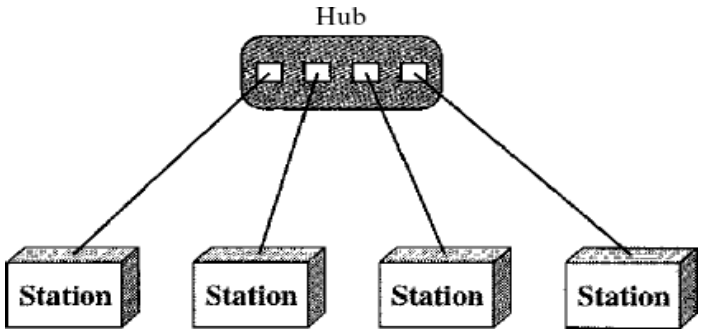
*Disadvantages:*

1. a mesh are related to the amount of cabling because every device must be connected to every other device, installation and reconnection are difficult.

2. the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

**Star Topology:**

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices.




Advantages

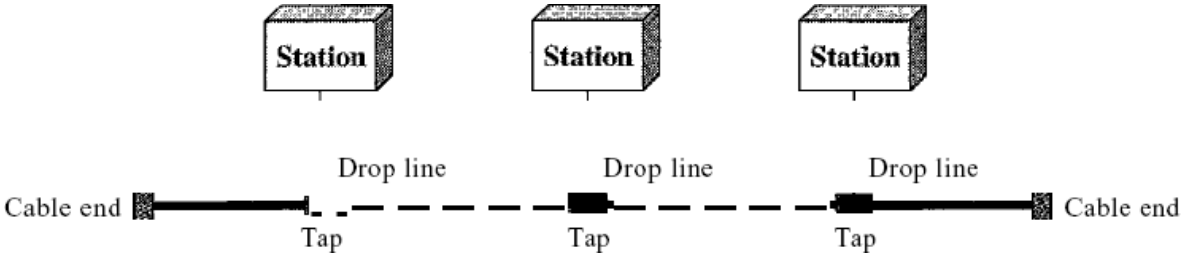
1. Star topology includes robustness. If one link fails, only that link is affected. All other links remain active.
2. A star topology is less expensive than a mesh topology.

Disadvantage

1. Star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

**Bus Topology:**

A bus topology is a multipoint. One long cable acts as a backbone to link all the devices in a network




Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.

Advantages:

- A Bus topology includes ease of installation.
- And Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.

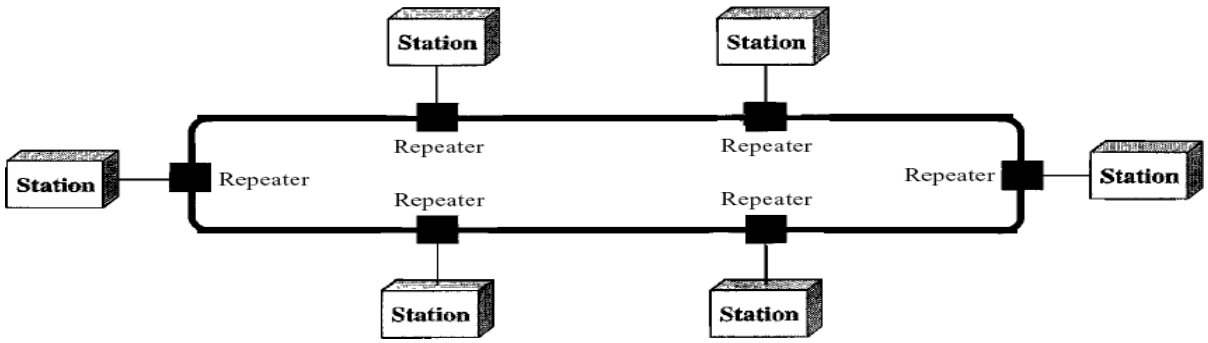
Disadvantages:

- It is difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation.
- It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality.

**Ring Topology**

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination.

Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along




A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

## Q) Explain various Categories of Networks

**Local Area Networks:**

Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.

LANs are distinguished from other kinds of networks by three characteristics:

(1) Their size,

(2) Their transmission technology, and

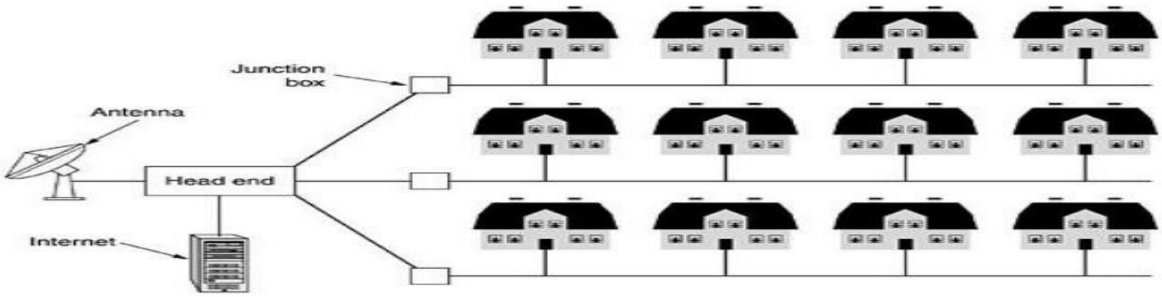
(3) Their topology.

LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance.


**Fig.1: Two broadcast networks . (a) Bus. (b) Ring.**

**Metropolitan Area Network:**

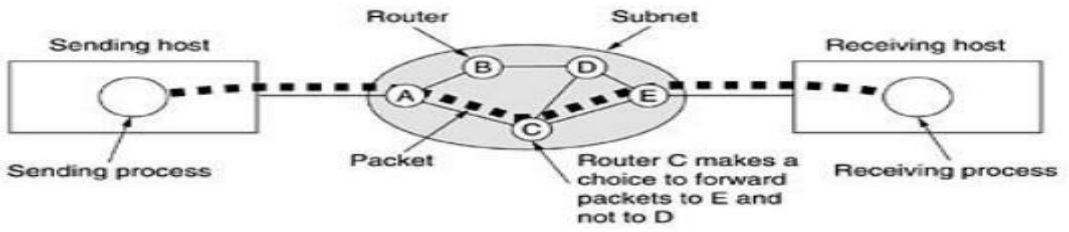
metropolitan area network, or MAN, covers a city. The best example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception.




In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses. At first, these were locally-designed, ad hoc systems. Then companies began jumping into the business, getting contracts from city governments to wire up an entire city.

**Wide Area Network:**

A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. These machines are called as hosts. The hosts are connected by a communication subnet, or just subnet for short. The hosts are owned by the customers (e.g., people's personal computers),




whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider.

The job of the subnet is to carry messages from host to host, just as the telephone system carries

## Q).Explain OSI Reference Model:

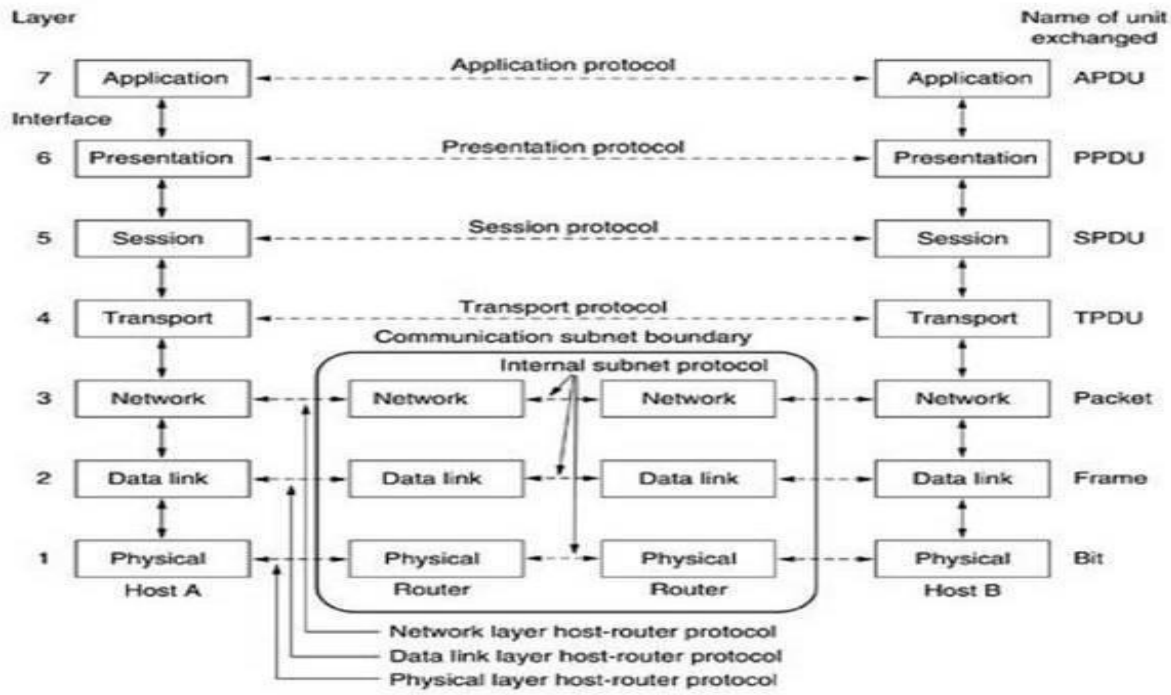



Fig: OSI REFERENCE MODEL

The OSI (Open Systems Interconnection) model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

**The Physical layer:**

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit.

**The Data Link Layer:**

The data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break up the input data into data frames (typically a few hundred or a few thousand bytes) and transmits the frames sequentially.

**The Network Layer:**

The network layer controls the operation of the subnet. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are ''wired into'' the network and rarely changed. They can also be determined at the start of each conversation, for example, a terminal session (e.g., a login to a remote machine). Finally, they can be highly dynamic, being determined anew for each packet, to reflect the current network load.

**The Transport Layer:**

The basic function of the transport layer is to accept data from above, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end.

**The Session Layer:**

The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management (preventing two parties from attempting the same critical operation at the same time), and synchronization (check pointing long transmissions to allow them to continue from where they were after a crash).

**The Presentation Layer:**

The presentation layer is concerned with the syntax and semantics of the information transmitted. In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used ''on the wire.''

**The Application Layer:**

The application layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (Hypertext Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back. Other application protocols are used for file transfer, electronic mail, and network news.

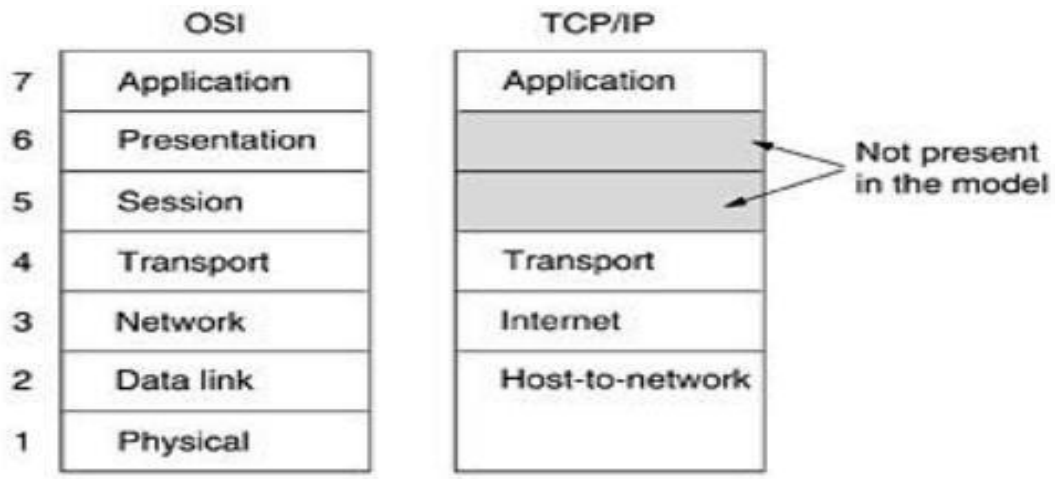
## Q).Explain about TCP/IP Reference Model

The TCP/IP reference model was developed prior to OSI model. The major design goals of this model were,

1. To connect multiple networks together so that they appear as a single network.
2. To survive after partial subnet hardware failures.
3. To provide a flexible architecture.

Unlike OSI reference model, TCP/IP reference model has only 4 layers. They are,

1. Host-to-Network Layer
2. Internet Layer
3. Transport Layer
4. Application Layer




**Host-to-Network Layer:**

The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host to host and network to network.

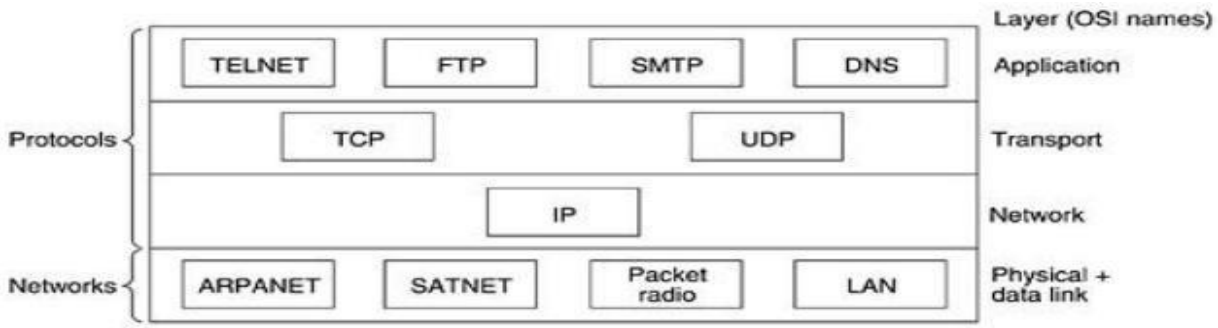
**Internet Layer:**

This layer, called the internet layer, is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have they travel independently to the destination (potentially on a different network). They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired. Note that ''internet'' is used here in a generic sense, even though this layer is present in the Internet.

**The Transport Layer:**

The layer above the internet layer in the TCP/IP model is now usually called the transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two end-to-end transport protocols have been defined here. The first one, TCP (Transmission Control Protocol), is a reliable connection- oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.

The second protocol in this layer, UDP (User Datagram Protocol), is an unreliable,



connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. The relation of IP, TCP, and UDP is shown in Fig.2. Since the model was developed, IP has been implemented on many other networks.

**The Application Layer:**

The TCP/IP model does not have session or presentation layers. On top of the transport layer is the application layer. It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP).

## Q).Differentiate between OSI and TCP/IP Reference Models

| OSI Model | TCP/IP Model |
|---|---|
| It stands for **Open System Interconnection.** | It stands for **Transmission Control Protocol.** |
| OSI model has been developed by ISO (International Standard Organization). | It was developed by ARPANET (Advanced Research Project Agency Network). |
| It is an independent standard and generic protocol used as a communication gateway between the network and the end user. | It consists of standard protocols that lead to the development of an internet. It is a communication protocol that provides the connection among the hosts. |
| In the OSI model, the transport layer provides a guarantee for the delivery of the packets. | The transport layer does not provide the surety for the delivery of packets. But still, we can say that it is a reliable model. |
| This model is based on a vertical approach. | This model is based on a horizontal approach. |
| In this model, the session and presentation layers are separated, i.e., both the layers are different. | In this model, the session and presentation layer are not different layers. Both layers are included in the application layer. |
| It is also known as a reference model through which various networks are built. For example, the TCP/IP model is built from the OSI model. It is also referred to as a guidance tool. | It is an implemented model of an OSI model. |
| In this model, the network layer provides both connection-oriented and connectionless service. | The network layer provides only connectionless service. |
| Protocols in the OSI model are hidden and can be easily replaced when the technology changes. | In this model, the protocol cannot be easily replaced. |
| It consists of 7 layers. | It consists of 4 layers. |

| | |
|---|---|
| OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them. It is protocol independent. | In the TCP/IP model, services, protocols, and interfaces are not properly separated. It is protocol dependent. |
| The usage of this model is very low. | This model is highly used. |
| It provides standardization to the devices like router, motherboard, switches, and other hardware devices. | It does not provide the standardization to the devices. It provides a connection between various computers. |

# PHYSICAL LAYER

## Q).what is meant by Analog and Digital Data

**Analog Data**:

The term **analog data** refers to information that is continuous; For example, an analog clock that has hour, minute, and second hands gives information in a continuous form; the movements of the hands are continuous. Analog data, such as the sounds made by a human voice, take on continuous values. When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal.

**Digital Data:**

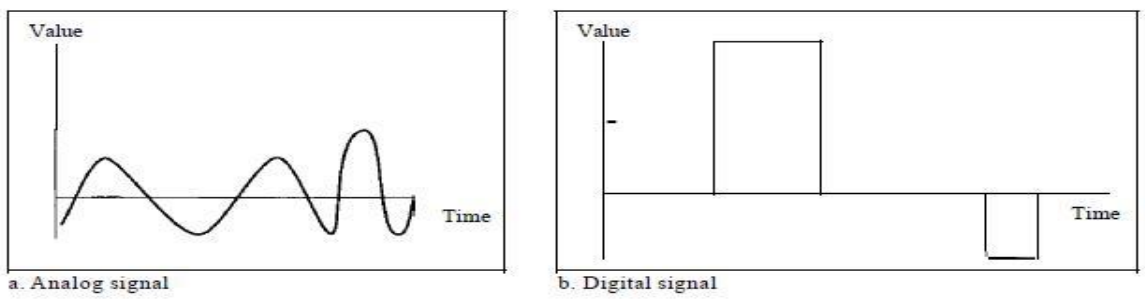
**Digital data** refers to information that has discrete states. For example, a digital clock that reports the hours and the minutes will change suddenly from 8:05 to 8:06. Digital data takes on discrete values. For example, data are stored in computer memory in the form of Os and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.

## Q).what is meant by Analog and Digital Signals.

**Analog and Digital Signals:**

Like the data they represent, signals can be either analog or digital. An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value *A* to value *B,* it passes through and includes an infinite number of values along its path. A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and O.

Figure 3.1 *Comparison of analog and digital signals*




a. Analog signal

b. Digital signal

## Q).what is meant by Periodic and Nonperiodic Signals

**Periodic and Nonperiodic Signals:**

A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A nonperiodic signal changes without exhibiting a pattern or cycle that repeats over time.

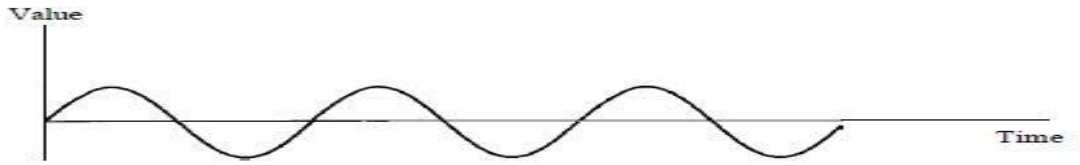
**PERIODIC ANALOG SIGNALS:**

Periodic analog signals can be classified as simple or composite. A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves.

## Sine Wave

The sine wave is the most fundamental form of a periodic analog signal. When we visualize it as a simple oscillating curve, its change over the course of a cycle is smooth and consistent, a continuous, rolling flow. Figure below shows a sine wave. Each cycle consists of a single arc above the time axis followed by a single arc below it.

*A sine wave*




## Characteristics of Signals:

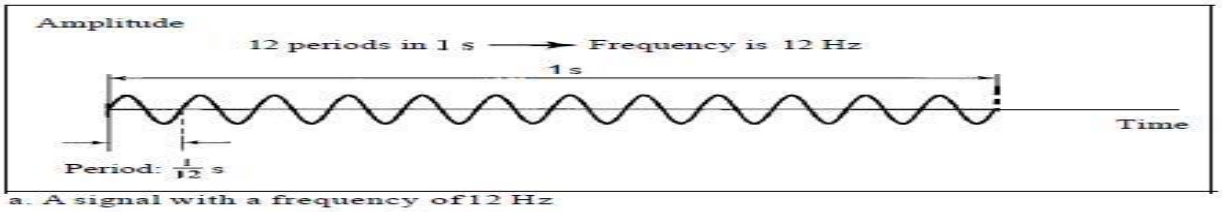
1. ***Peak Amplitude***

The peak amplitude of a signal is the absolute value of its highest intensity, proportional to the energy it carries. For electric signals, peak amplitude is normally measured in *volts.* Figure below shows two signals and their peak amplitudes.

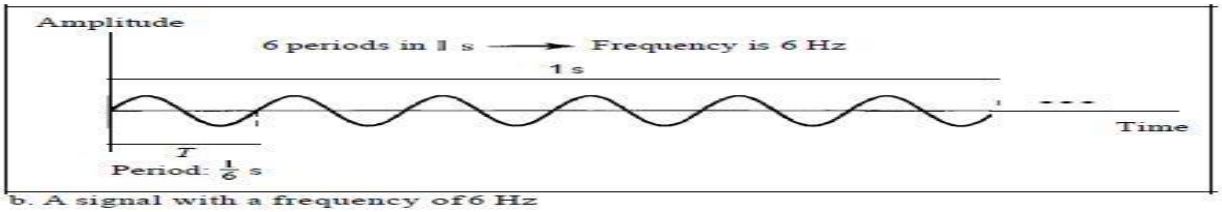
***2.Period and Frequency***

Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle. Frequency refers to the number of periods in I s. Period is formally expressed in seconds. Frequency is formally expressed in Hertz (Hz), which is cycle per second.

*Two signals with the same amplitude and phase, but different frequencies*




a. A signal with a frequency of 12 Hz

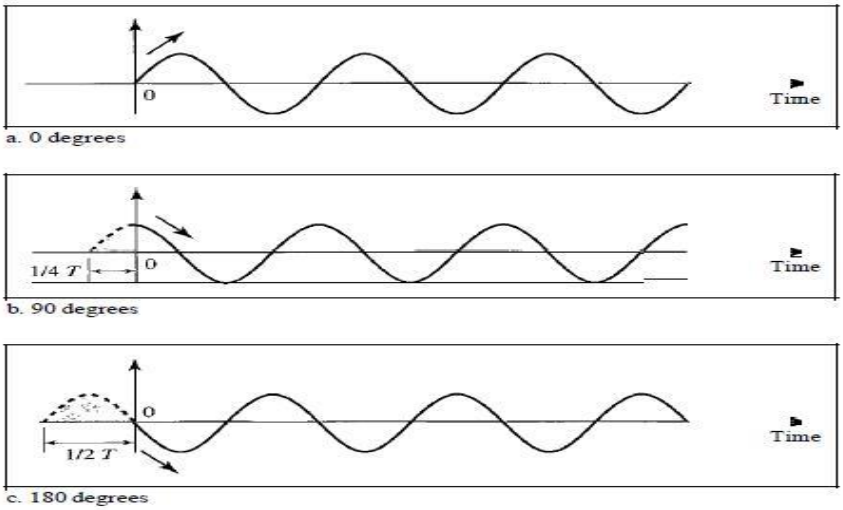



b. A signal with a frequency of 6 Hz

3. ***Phase***

The term phase describes the position of the waveform relative to time O. Phase is measured in degrees or radians [360° is *2n* rad; 1° is *2n/360* rad, and 1 rad is *360/(2n)].*

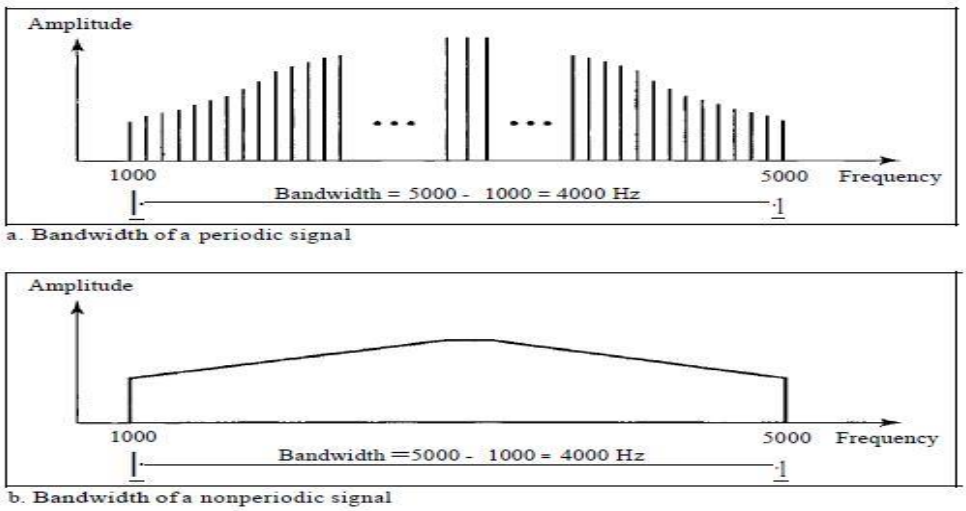
*Three sine waves with the same amplitude andfrequency, but different phases*




## Bandwidth

The range of frequencies contained in a composite signal is its bandwidth. The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 - 1000, or 4000. Figure 3.12 shows the concept of bandwidth. The figure depicts two composite signals, one periodic and the other nonperiodic. The bandwidth of the periodic signal contains all integer frequencies between 1000 and 5000 (1000, 100 I, 1002, ...). The bandwidth of the nonperiodic signals has the same range, but the frequencies are continuous.

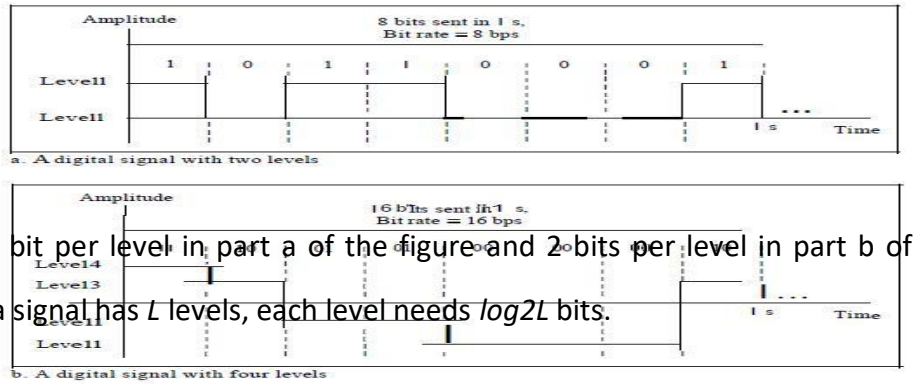
Figure 3.12 *The bandwidth ofperiodic and nonperiodic composite signals*



## Q). Explain Digital Signals in Detail.

In addition to being represented by an analog signal, information can also be represented by a digital signal. For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage. A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level. Figure 3.16 shows two signals, one with two levels and the other with four.

Figure 3.16 *Two digital signals: one with two signal levels and the other with four signal levels*




We send 1 bit per level in part a of the figure and 2 bits per level in part b of the figure. In general, if a signal has *L* levels, each level needs *log2L* bits.

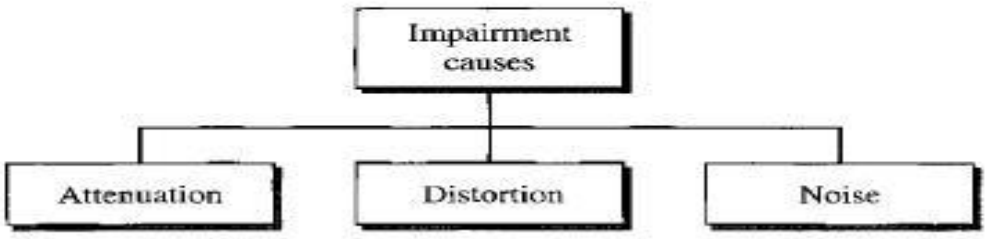
## Bit Rate

Most digital signals are nonperiodic, and thus period and frequency are not appropriate characteristics. Another *term-bit rate is* used to describe digital signals. The bit rate is the number of bits sent in 1s, expressed in bits per second (bps). Figure 3.16 shows the bit rate for two signals.

## Q). Explain Transmission Impairment.

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise.

*Causes of impairment*



## 1. **Attenuation**

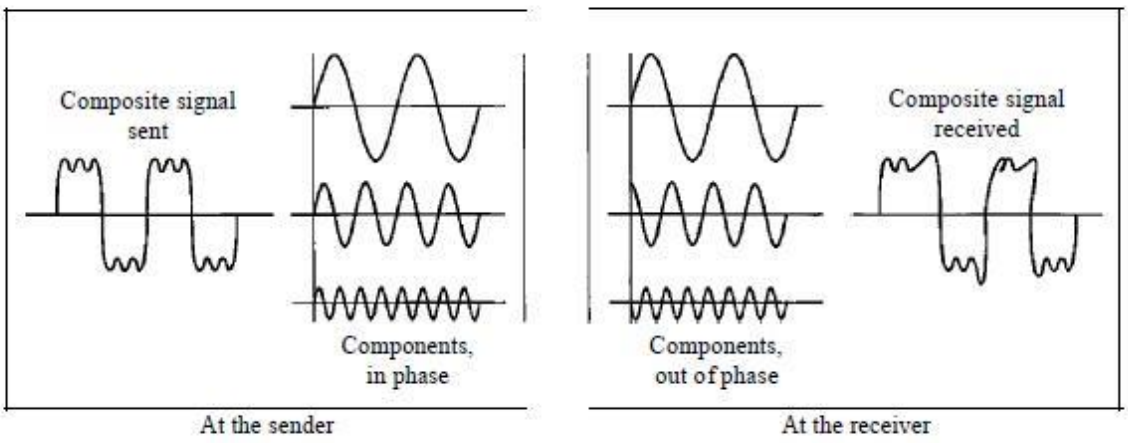
Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal. Attenuation is measured in terms of Decibels.

## 2. **Distortion**:

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propogation speed through a medium and therefore

~~component has its own propagation speed through a medium and, therefore, its own delay in~~ arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration. In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same. Figure 3.28 shows the effect of distortion on a composite signal.

Figure 3.28 *Distortion*




## 3. **Noise**

Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal. Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter. Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna. Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna. Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.

# Q). Write about Data Rate Limits.

A very important consideration in data communications is how fast we can send data, in bits per second. over a channel. Data rate depends on three factors:

1. The bandwidth available

2. The level of the signals we use

3. The quality of the channel (the level of noise)

Two theoretical formulas were developed to calculate the data rate: one by **Nyquist** for a noiseless channel. another by **Shannon** for a noisy channel.

## Noiseless Channel: Nyquist Bit Rate

For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate **BitRate = 2 x bandwidth x 10g2 *L***

In this formula, bandwidth is the bandwidth of the channel, *L* is the number of signal levels used to represent data, and BitRate is the bit rate in bits per second.

## Noisy Channel: Shannon Capacity

In reality, we cannot have a noiseless channel; the channel is always noisy. In 1944, Claude Shannon introduced a formula, called the Shannon capacity, to determine the theoretical highest data rate for a noisy channel:

**Capacity =bandwidth x log2 (1 +SNR)**

In this formula, bandwidth is the bandwidth of the channel, SNR is the signal-to-noise ratio, and capacity is the capacity of the channel in bits per second.

# Q).Explain Guided transmission Media.

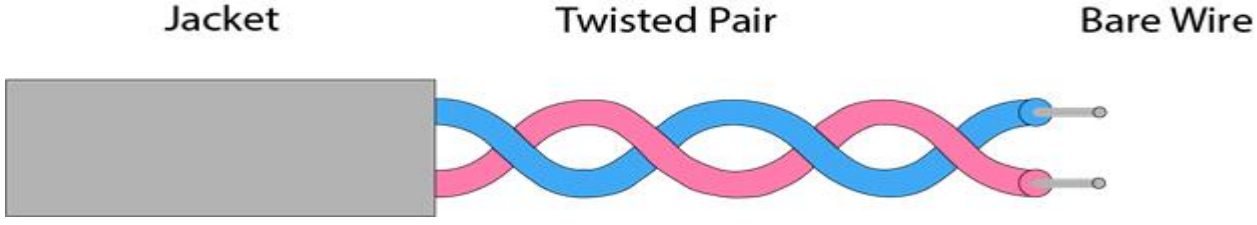
It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

**Types Of Guided media:**

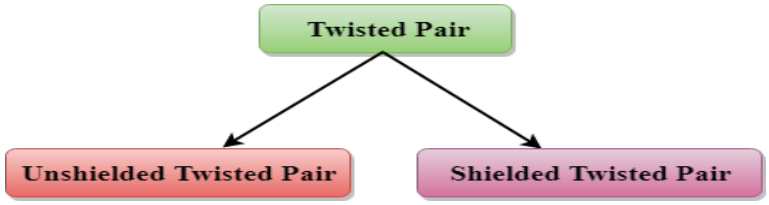
1. **Twisted pair:**

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:

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

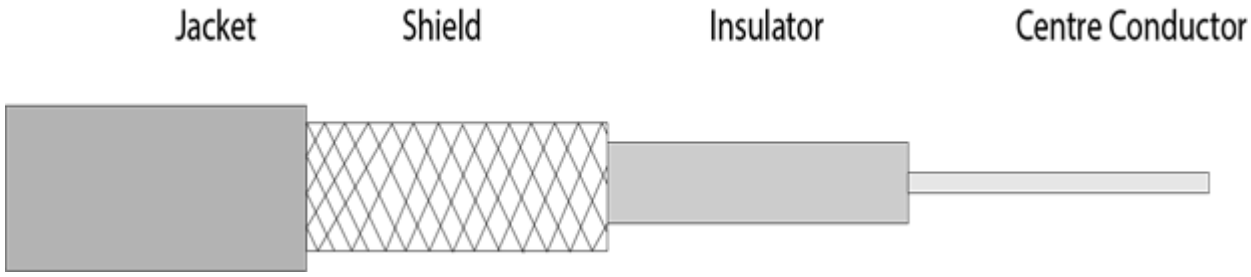
A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

**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.

## 2. Coaxial Cable

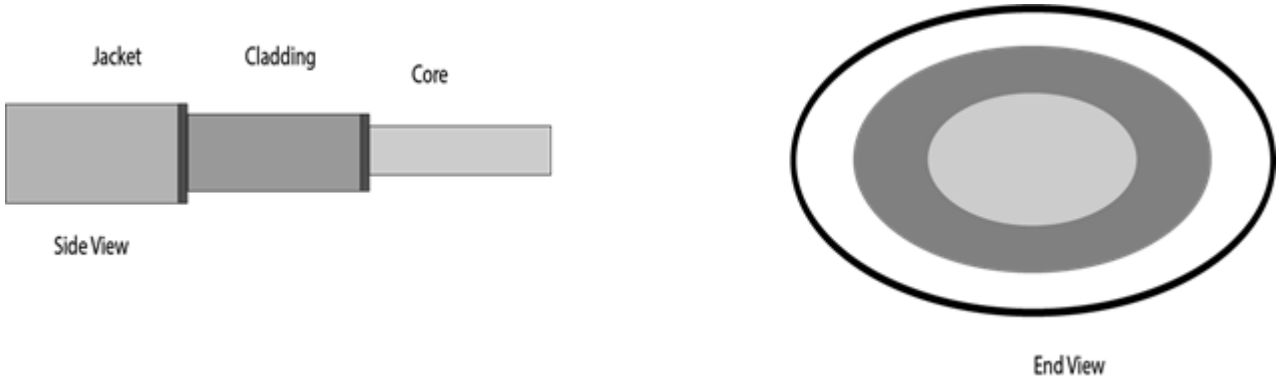
- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable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




## 3. Fibre Optic

- 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.

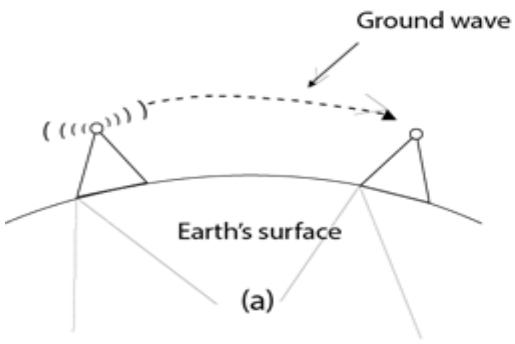
## Q).Explain about UnGuided Transmission media.

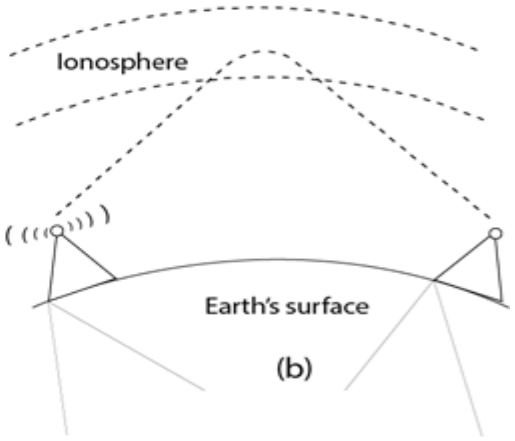
- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

### 1. Radio waves

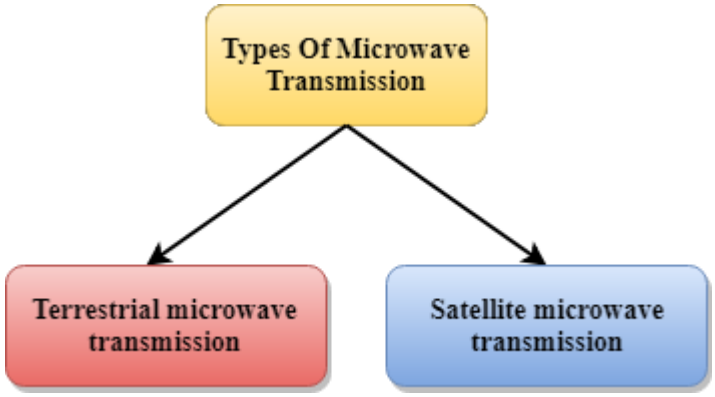
- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and 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**.



## 2. Microwaves

- 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.




Microwaves are of two types:

Terrestrial microwave

- 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.

### 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.

### 3. Infrared

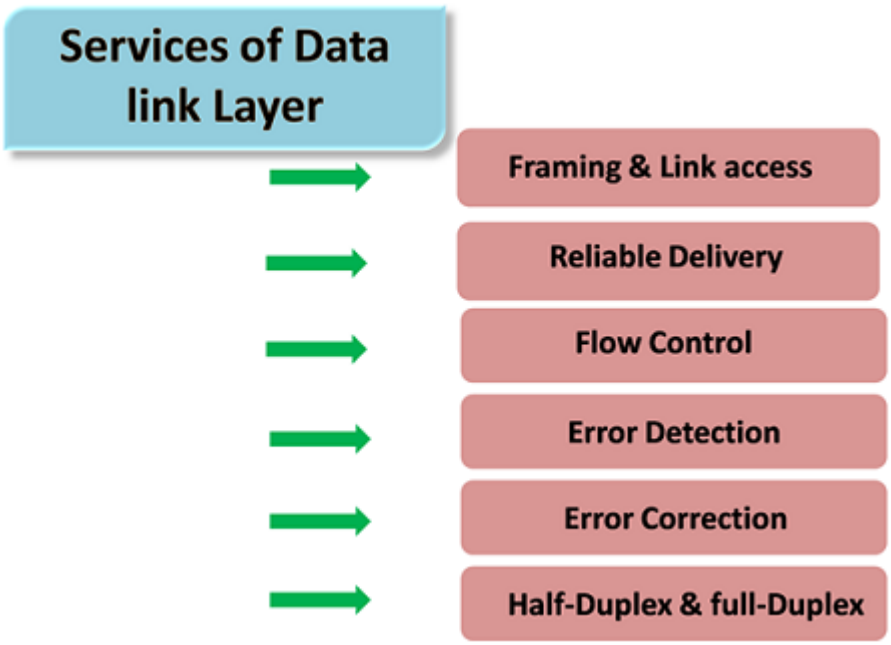
- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer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

## Data Link Layer

**Q).What is Data link Layer. Explain the service of data link layer**

- The Data link layer protocol defines the format of the packet exchanged across the nodes as well as the actions such as Error detection, retransmission, flow control, and random access.
- The Data Link Layer protocols are Ethernet, token ring, FDDI and PPP.

Following services are provided by the Data Link Layer:




- **Framing & Link access:** Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.

- **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements.
- **Flow control:** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.
- **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.
- **Error correction:** Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.
- **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

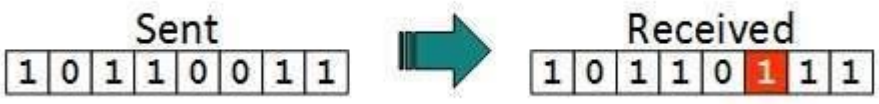
## Q).What is Error Detection ? Explain types of Errors

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

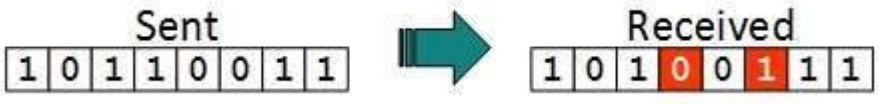
There may be three types of errors:

- **Single bit error**



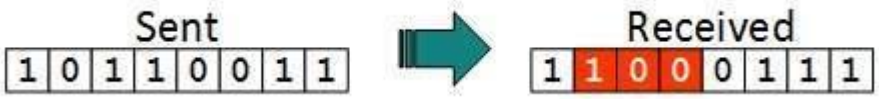

In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**




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

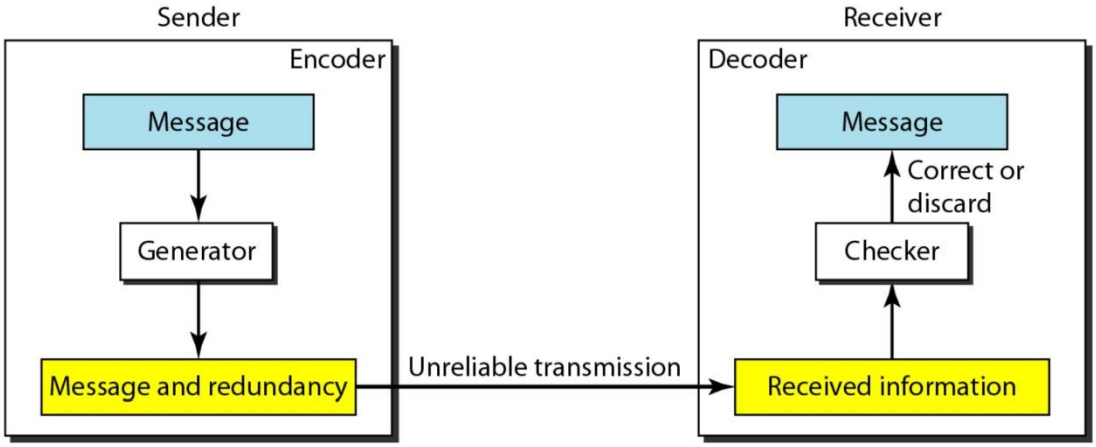
- **Burst error**




Frame contains more than1 consecutive bits corrupted.

**Define Redundancy?**

To be able to detect or correct errors , we need to send some extra bits with our data. These extra bits are called Redndancy.

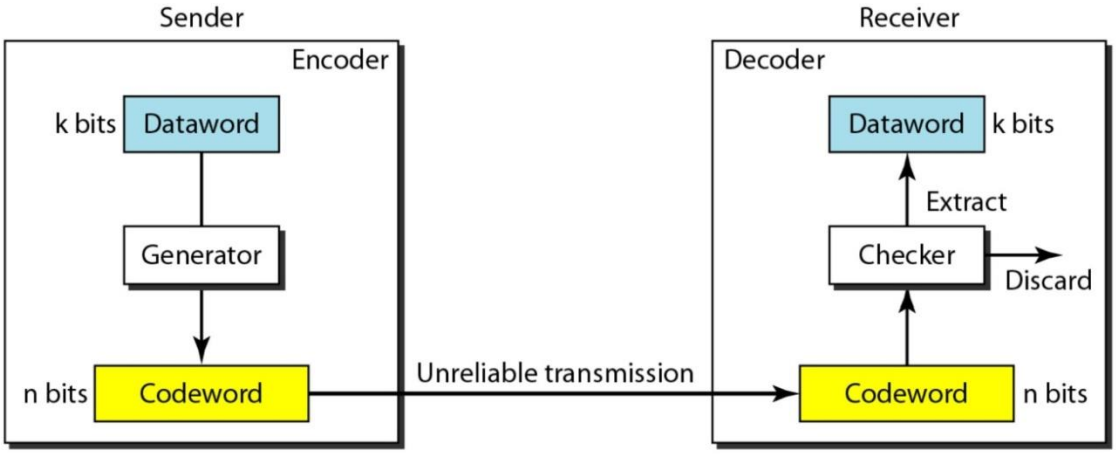



## Q.)Write about Error Detection and Error Correction.

**Error Detection**

Errors can be detected when the following two conditions are met.

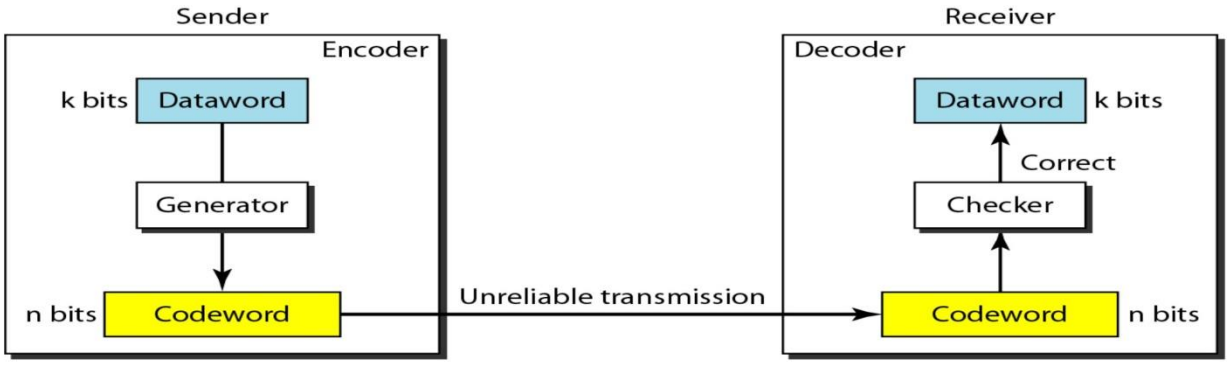
i. The receiver has a list of valid code words
ii. The original codeword has changed to an invalid one.



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.

**Error correction:**

In error correction the receiver needs to find the original codeword sent. We can say that we need more redundant bits for error correction than for error detection.




Error correction can be done in two ways:

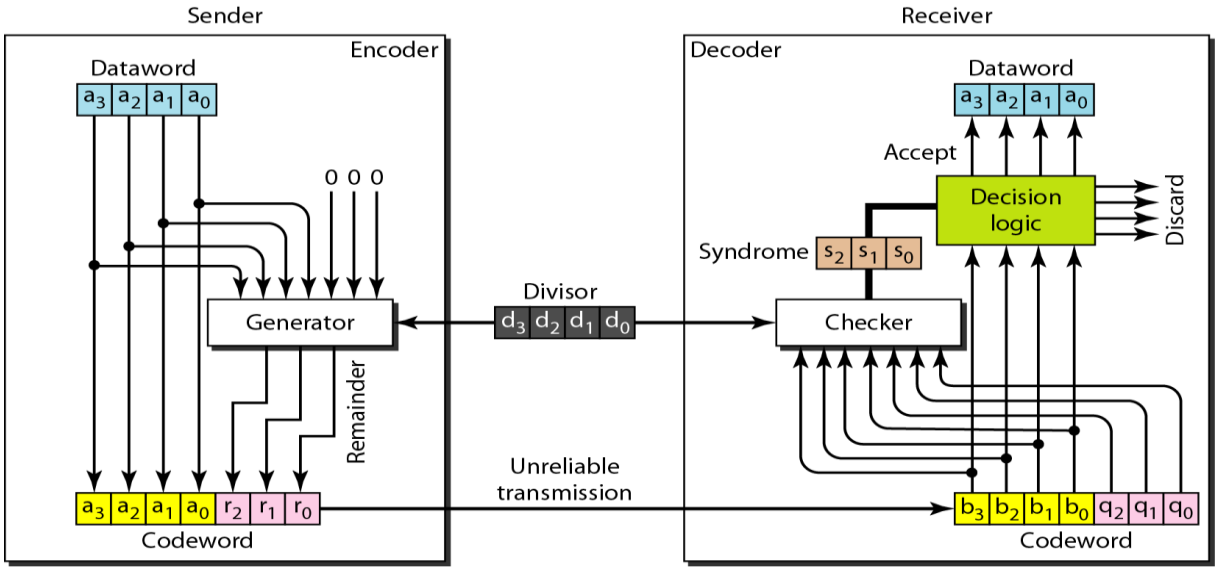
- **Backward Error Correction or retransmission** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

## Q). Explain Cyclic Codes in Data Link Layer.

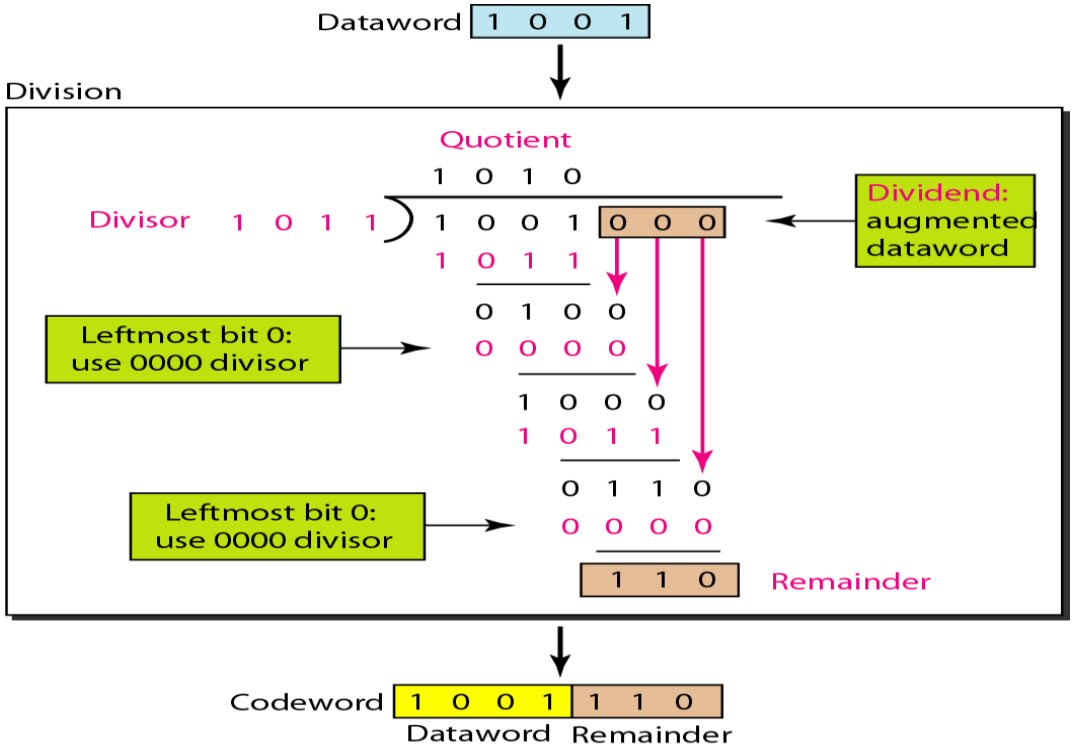
Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.

**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.

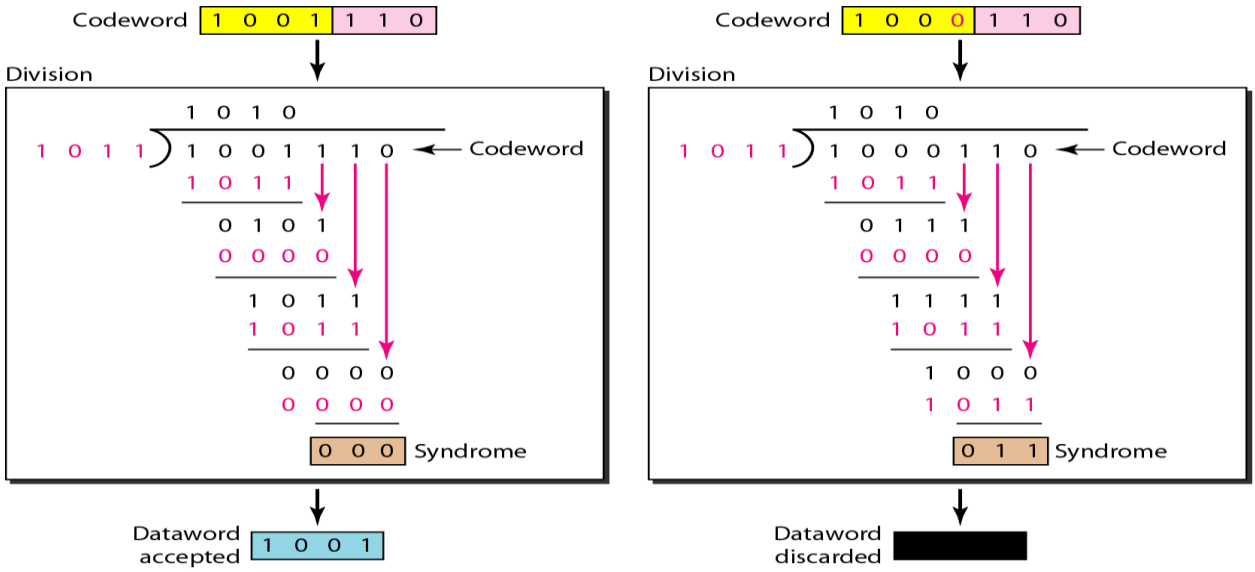



## CRC ENCODER




## CRC DECODER

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.




## Q).Explain Check Sum Error detection Mechanism.

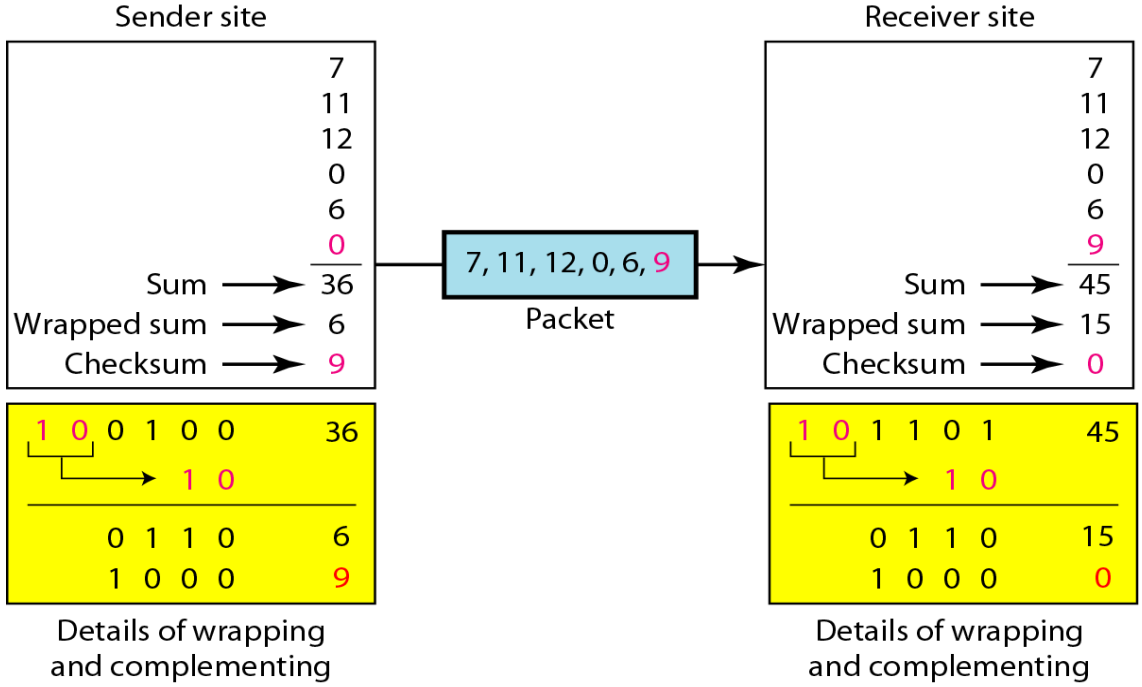
*The last error detection method we discuss here is called the checksum. The checksum is used in the Internet by several protocols although not at the data link layer.*

**Sender site:**

1. The message is divided into 16-bit words.
2. The value of the checksum word is set to 0.
3. All words including the checksum are added using one's complement addition.
4. The sum is complemented and becomes the checksum.
5. The checksum is sent with the data.

**Receiver site:**

1. The message (including checksum) is divided into 16-bit words.
2. All words are added using one's complement addition.
3. The sum is complemented and becomes the new checksum.
4. If the value of checksum is 0, the message is accepted; otherwise, it is rejected.



# Unit –II

# Data Link Protocols

### Q). Write a short notes on Flow control and Error Control.

The most important responsibilities of data link layer are Flow control and Error Control. Collectively these functions are known as data link control.

**Flow control:**

Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment

**Error Control:**

Error control in the data link layer is based on automatic repeat request, which is the retransmission of data. Any time an error is detected in an exchange, specified frames are retransmitted. This process is called Automatic Repeat Request(ARQ).

## Q). Explain Utopain Simplex Protocols.

There is one direction data transmission only from sender to receiver. Here we assume the communication channel to be error-free and the receiver will infinitely quickly process the input. The sender pumps out the data onto the line as fast as it can.

This protocol has two different procedures, a sender and a receiver. MAX_SEQ is not needed because no sequence numbers or acknowledgments are used. The only event type possible is frame arrival (i.e. the arrival of an undamaged frame).

The sender pumps out the data in an infinite while loop as fast as it can. The loop body consists of three actions and they are –

- Fetch a packet from the network layer,
- Construct an outbound frame using the variable s,
- Send the frame on its way.

Other fields have to do with error and flow control and there are no errors or flow control restrictions here so only the info field is used here.

The receiver is equally simple. The procedure wait_for_event returns when the frame arrives and the event set to frame arrival. The newly arrived frame from the hardware buffer is removed by the call from_physical_layer and puts in the variable r, so that receiver can get it. The data link layer settles back to wait for the next frame when the data portion is passed on to the network layer, suspending itself until the frame arrives. It does not handle either flow control or error correction therefore it is unrealistic.

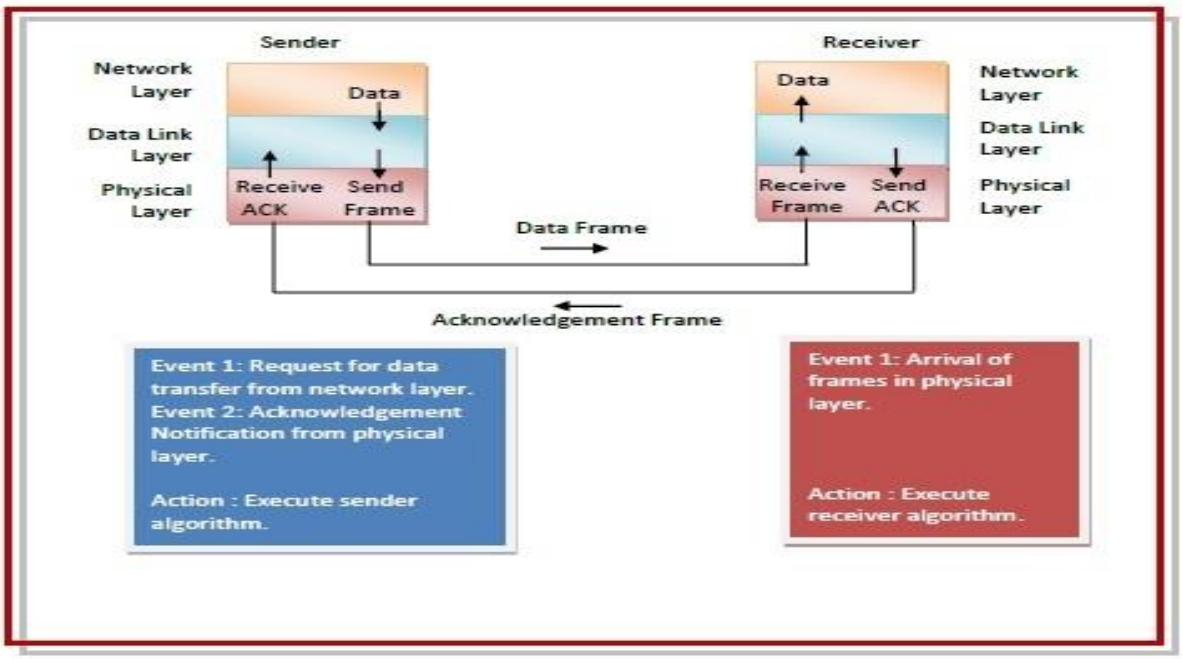
## Q). Explain A Simplex Stop-and-Wait Protocol for an Error-Free Channel.

Stop – and – Wait protocol is data link layer protocol for transmission of frames over noiseless channels. It provides unidirectional data transmission with flow control facilities but without error control facilities.

This protocol takes into account the fact that the receiver has a finite processing speed. If data frames arrive at the receiver's end at a rate which is greater than its rate of processing, frames be dropped out. In order to avoid this, the receiver sends an acknowledgement for each frame upon its arrival. The sender sends the next frame only when it has received a positive acknowledgement from the receiver that it is available for further data processing.

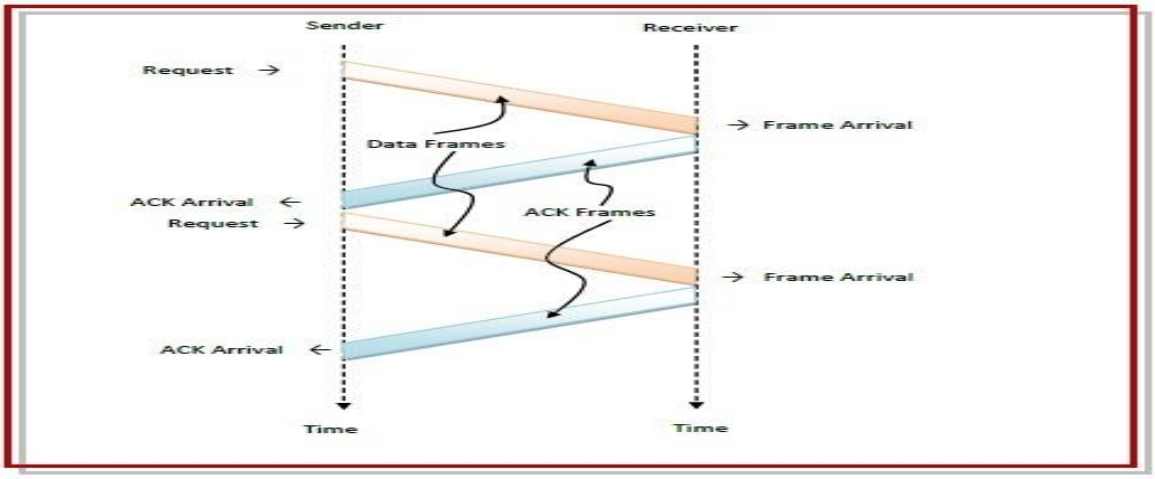
## Design

- **Sender Site**: The data link layer in the sender site waits for the network layer for a data packet. It then checks whether it can send the frame. If it receives a positive notification from the physical layer, it makes frames out of the data and sends it. It then waits for an acknowledgement before sending the next frame.
- **Receiver Site**: The data link layer in the receiver site waits for a frame to arrive. When it arrives, the receiver processes it and delivers it to the network layer. It then sends an acknowledgement back to the sender.




## Flow Diagram

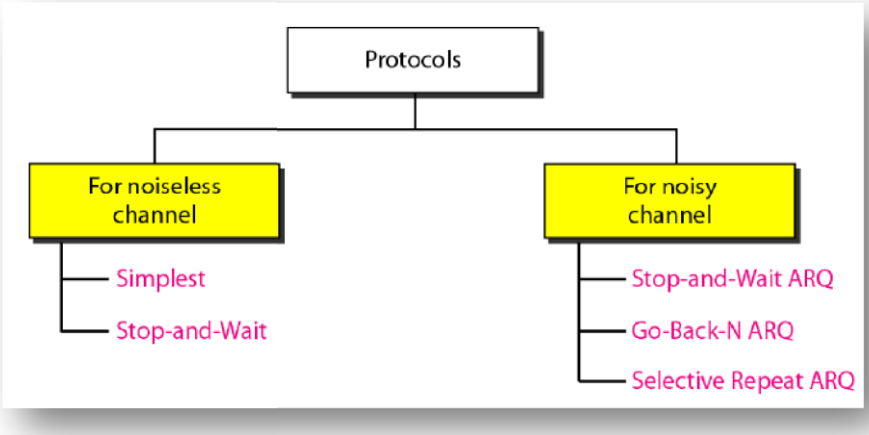
The following flow diagram depicts communication via simplex stop – and – wait protocol for noiseless channel:



## Q). Protocols for Error Control and Flow Control

Protocols at Data link Layer for flow and error control can be categorized into two types:

- Protocol for noiseless (error-free) channels
- Protocol for noisy (error-prone) channels.



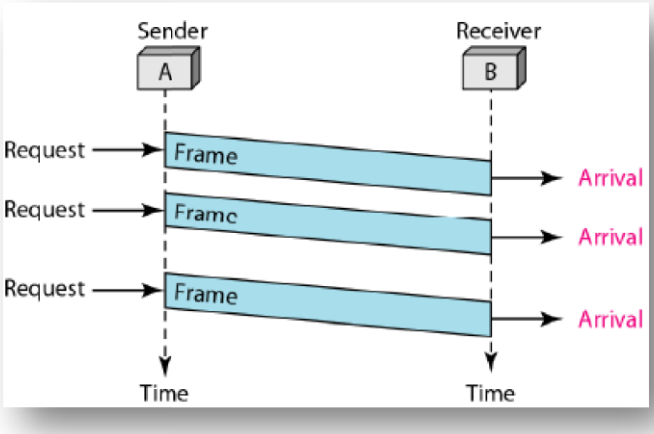

## Q). Protocols for Noiseless Channels

Noiseless protocols are

- Simplest
- Stop-and-wait

## Simplest Protocol

- It is a unidirectional protocol in which data frames are traveling in only one direction- from the sender to receiver.
- Receiver has infinite buffer space and infinite processing speed.
- In other words, the receiver can never be overwhelmed with incoming frames.
- Thus No flow or error control needed.



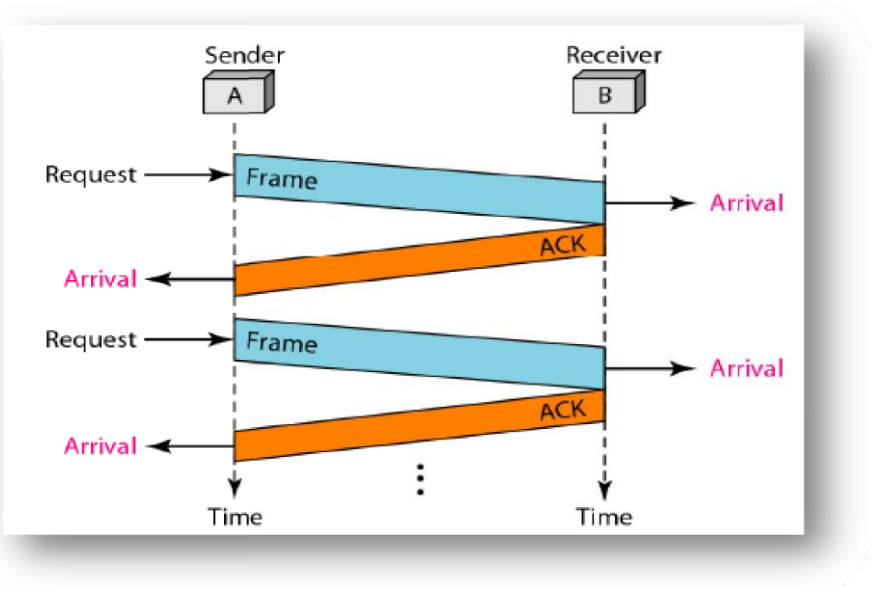

### Stop-and-Wait Protocol

- Receiver has finite buffer space and infinite processing speed.
- In other words, the receiver can be overwhelmed with incoming frames.

- Thus no error control but flow control is needed.

If data frames arrive at the receiver site faster than they can be processed, the frames must be stored until their use. Normally, the receiver does not have enough storage space, especially if it is receiving data from many sources. This may result in either the discarding of frames or denial of service. To prevent the receiver from becoming overwhelmed with frames, we somehow need to tell the sender to slow down. There must be feedback from the receiver to the sender.

The protocol is called the Stop-and-Wait Protocol because the sender sends one frame, stops until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame.




## Q). Protocol for Noisy Channels

There are three protocols in noisy channels that use error control.

i) Stop and Wait ARQ

ii) Go-Back-N ARQ

iii) Selective Repeat ARQ

**i) <u>Stop –and-wait Automatic Repeat Request</u>**

To detect and correct corrupted frames , we need to add redundancy bits to our data frame. When the frame arrives at the receiver site, it is checked and if it is corrupted , it is silently discarded by the receiver.Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires.

*a) <u>Sequence numbers</u>*

In Stop-and-Wait ARQ, we use sequence numbers to number the frames. The sequence numbers are based on modulo-2 arithmetic

### b) *Acknowledgement numbers*

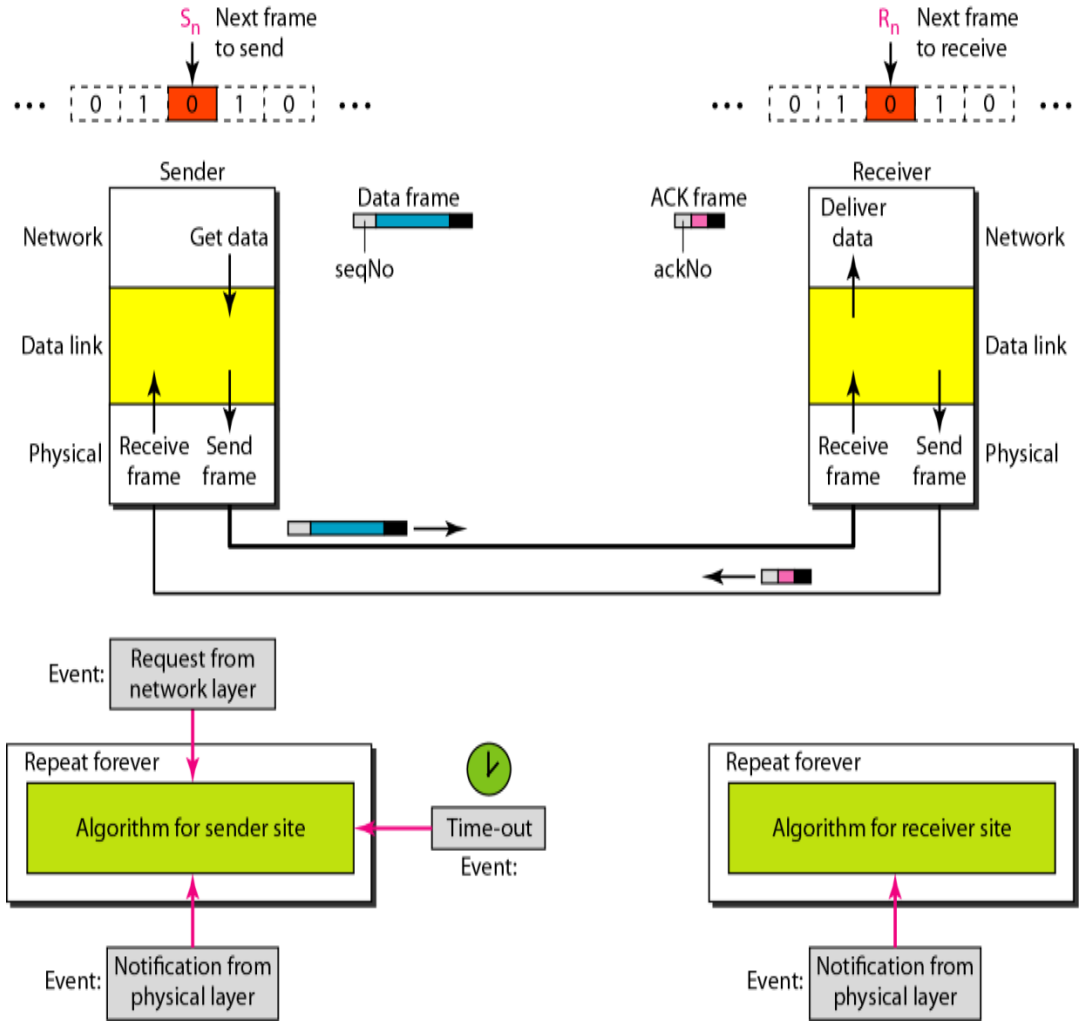
In Stop-and-Wait ARQ, the acknowledgment number always announces in modulo-2 arithmetic the sequence number of the next frame expected.

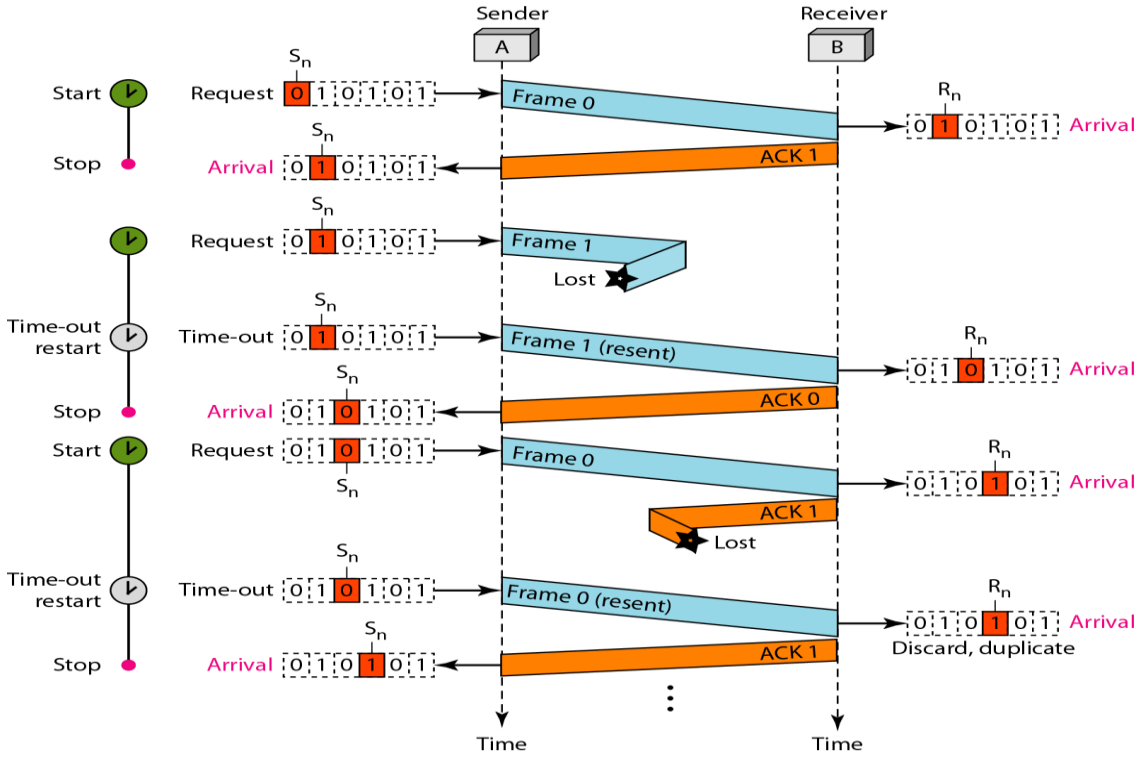
### c) *Design of stop and wait*

Below figure shows the design of stop and wait ARQ protocol. the sending device keeps a copy of the last frame transmitted until it receives an acknowledgment for that frame.

A data frame uses sequence number and ACK frame uses an ackno. The sender has a control variable $S_n$ that holds sequence number and the receiver has a control variable $R_n$ that holds the number of the next frame expected.

Example






Above figure is an example how stop and wait ARQ. Frame0 is sent and acknowledged. Frame1 is lost and resent after the time-out. The resent frame1 is acknowledged and the timer stops. Frame0 is sent and acknowledged, but the acknowledgement s lost. The sender has no idea if the frame or the acknowledgement is lost, so after time-out , it resends frame0, which is acknowledged.

### ii) Go-Back-N ARQ

In this protocol we can send several frames before receiving acknowledgment, we keep a copy of these frames until the acknowledgement arrive.

*a) Sequence numbers:*

Frames from a sending station are numbered sequentially. If the header allows m bits for the sequence number, the sequence numbers range from 0 to $2^m$-1.In the Go-Back-N Protocol, the sequence numbers are modulo $2^m$, where m is the size of the sequence number field in bits.

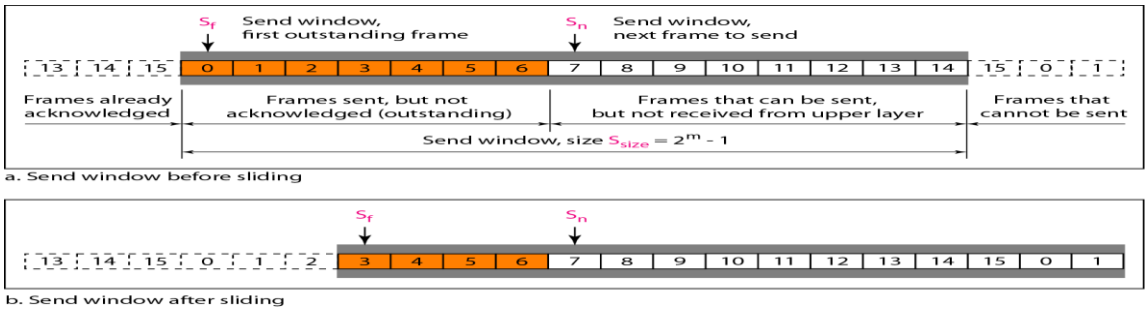
Eg: if m=3 then sequence numbers are

0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7.....

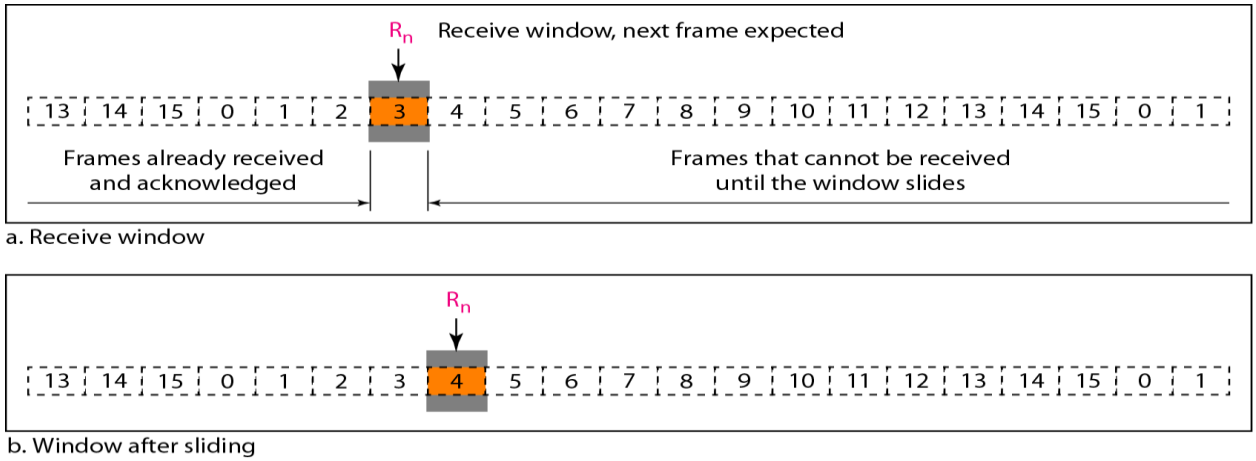
b) *Sliding window*

In this protocol , the sliding window is an abstract concept that defines the range of sequence numbers that is the concern of the sender and the receiver. The range which is the concern of the sender is called **sender sliding window ;** the range which is concern of the receiver is called the **receiver sliding window.**

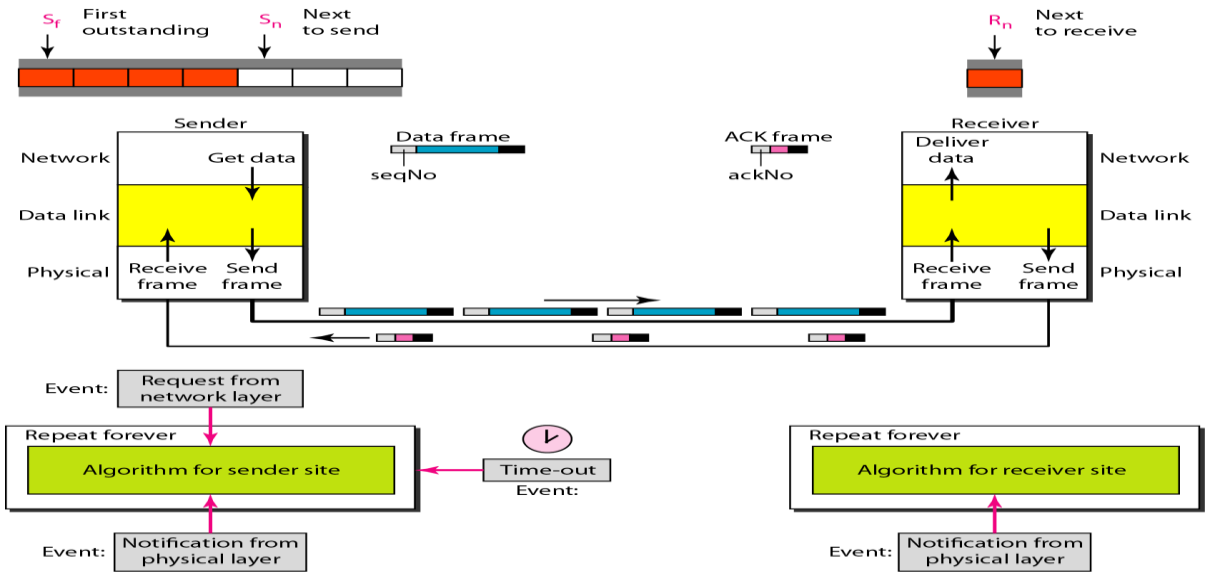
Sender sliding window




Receiver sliding window




c) Design:

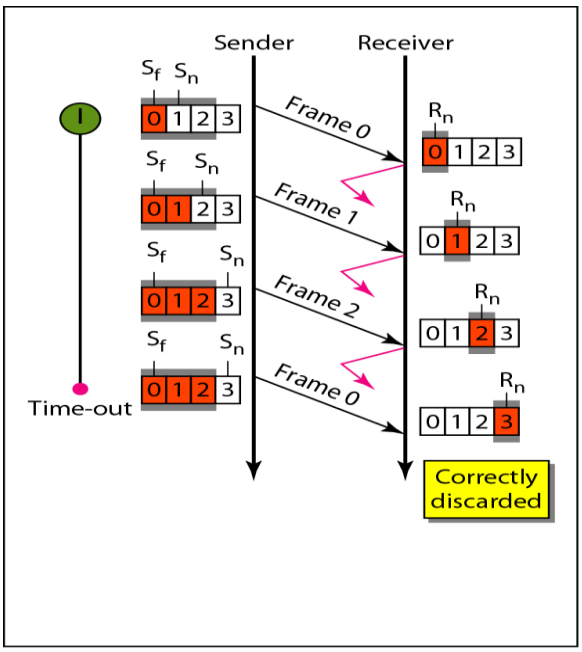



Above figure shows the design for this protocol. As we can see , multiple frames can be in transit in the forward direction , and multiple acknowledgements in the reverse direction .

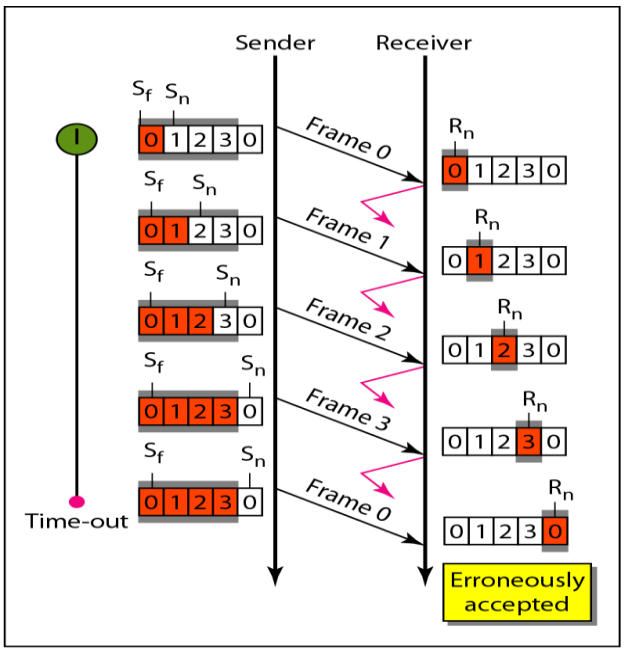
the idea is similar to stop and wait ARQ; the difference is that the send window allows us to have as many frames in transition as there are slots in the send window.

*d) send window size*

In Go-Back-N ARQ, the size of the send window must be less than $2^m$;the size of the receiver window is always 1.




a. Window size < $2^m$




b. Window size = $2^m$

**iii) Selective Repeat ARQ:**

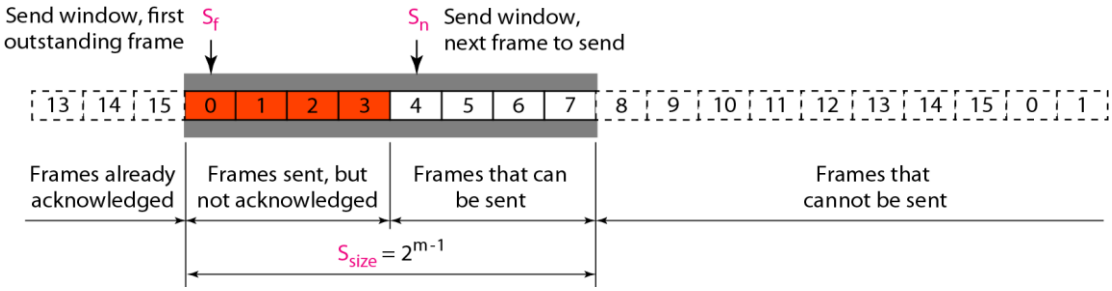
Go-Back-N ARQ simplifies the process at receiver site. But in ta nosy ink a frame has a higher probability of damage , which means the resending of multiple frames. This resending uses up the bandwidth and slows down the transmission. For noisy links, there is another mechanism that does not resend N frames when just one frame is damaged; only the damaged one is resent. This mechanism is called **Selective Repeat ARQ**

***a)*** *Window:*

Selective repeat protocol uses two windows : a sender window and a receiver window.

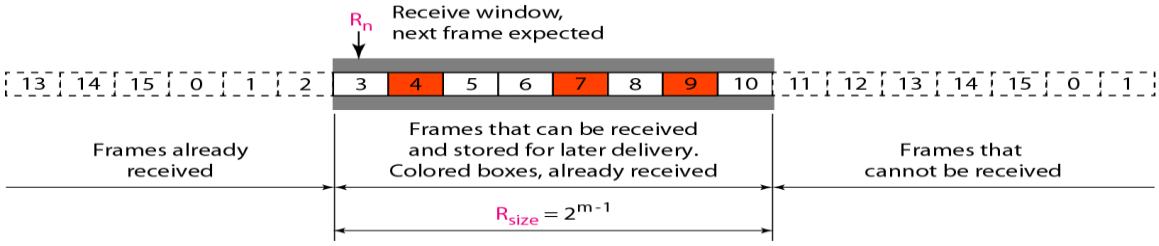
*Sender window:*

The size of the sender window is much smaller; it is $2^{m-1}$. The receiver window size is same as the sender window size.



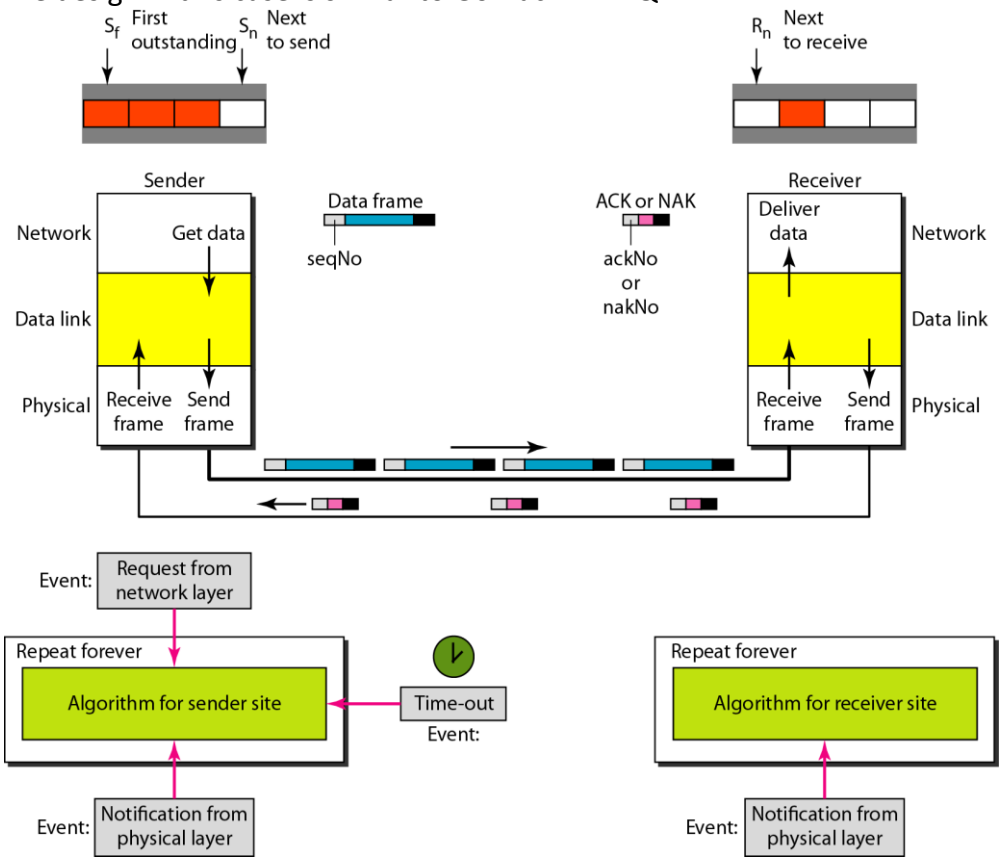

*Receiver window:*

The size of receiver window size is same as the sender window size($2^{m-1}$). The selective repeat protocol allows as many frames as the size of the window to arrive out of order and be kept until there is a set of in-order frames to be delivered to the network layer.

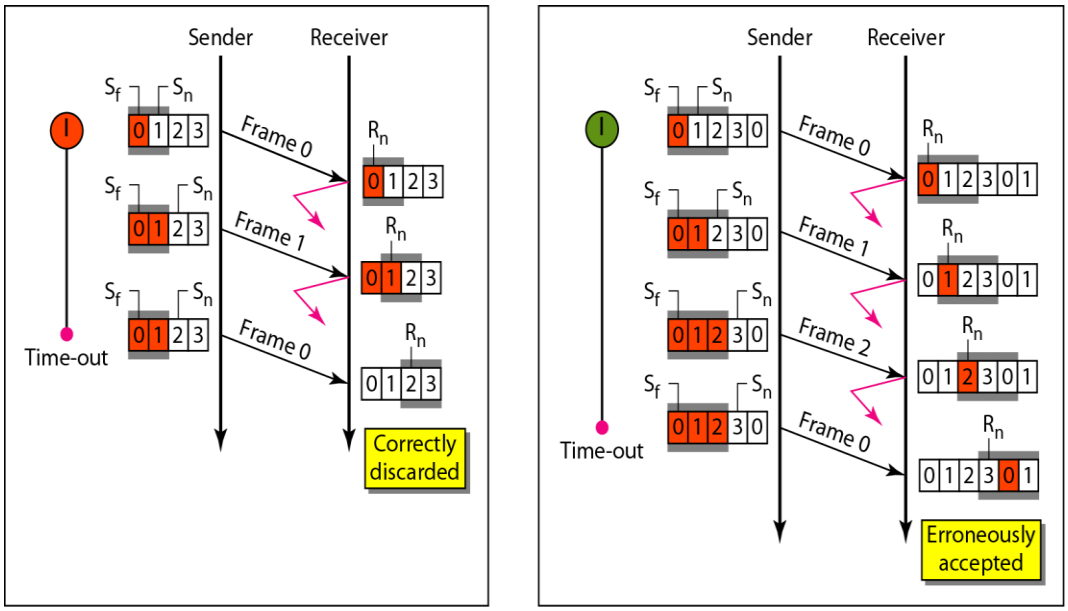



***b)*** *Design*

The design in this case is similar to Go-Back-N ARQ



***c)*** ***Window sizes:***




a. Window size = $2^{m-1}$ b. Window size > $2^{m-1}$

In Selective Repeat ARQ, the size of the sender and receiver window must be at most one-half of $2^m$.

## Q).Explain A One-Bit 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 these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.

In one – bit sliding window protocol, the size of the window is 1. So the sender transmits a frame, waits for its acknowledgment, then transmits the next frame. Thus it uses the concept of stop and waits for the protocol. This protocol provides for full – duplex communications. Hence, the acknowledgment is attached along with the next data frame to be sent by piggybacking.

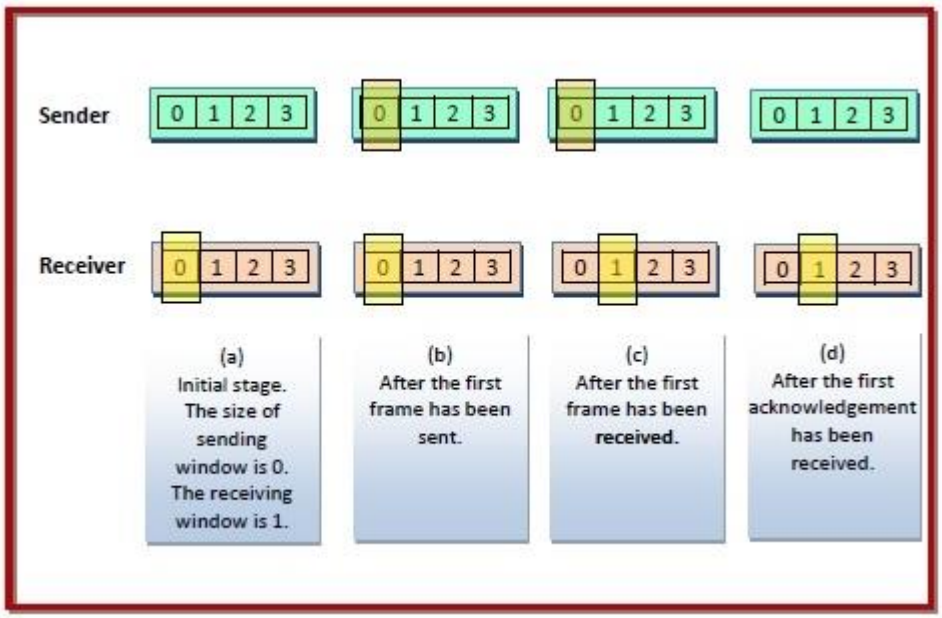
## Working Principle

The data frames to be transmitted additionally have an acknowledgment field, *ack* field that is of a few bits length. The *ack* field contains the sequence number of the last frame received without error. If this sequence number matches with the sequence number of the frame to be sent, then it is inferred that there is no error and the frame is transmitted. Otherwise, it is inferred that there is an error in the frame and the previous frame is retransmitted.

Since this is a bi-directional protocol, the same algorithm applies to both the communicating parties.

## Illustrative Example

The following diagram depicts a scenario with sequence numbers 0, 1, 2, 3, 0, 1, 2 and so on. It depicts the sliding windows in the sending and the receiving stations during frame transmission.




## THE MEDIUM ACCESS CONTROL SUBLAYER

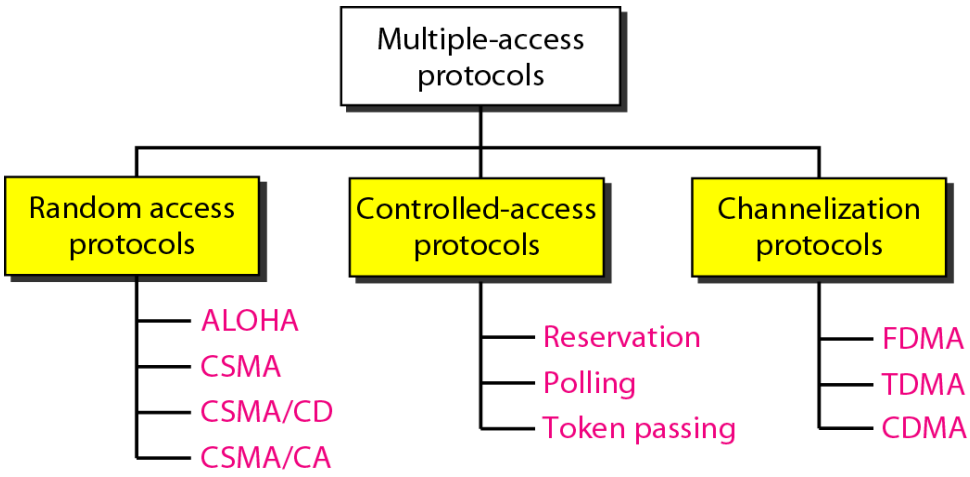
### Q).Write a short notes on Multiple Access Protocols?

When nodes or stations are connected and use a common link , called a multipoint or broadcast link, we need a multiple access protocol to coordinate access to a link. ***So*** the *Data link layer was divided into two sublayers . the* upper sublayer is responsible for data link control and the lower sublayer is *res for resolving access to the shared media.*

1.Data link Control
2.Multiple Accesse Resolution

But IEEE made this division for LANS. The Upper layer is responsible for flow and error control is called the Logical link control(LLC) layer ; the lower layer that is mostly responsible for multiple access resolution is called the medium access control(MAC) layer.

Many formal protocols have been devised to handle access to a shared link.



## Random Access Protocols:

In a Random Access method, each station has the right to the medium without being controlled by any other station. But, If more than one station tries to send , there is an access conflict-**collision**

### 1) ALOHA:

**ALOHA is a** very simple procedure called multiple access(MA). It was designed for radio LAN, but it can be used on any shared medium.

#### i) Pure ALOHA :

In pure ALOHA each station sends a frame whenever it has a frame to send.

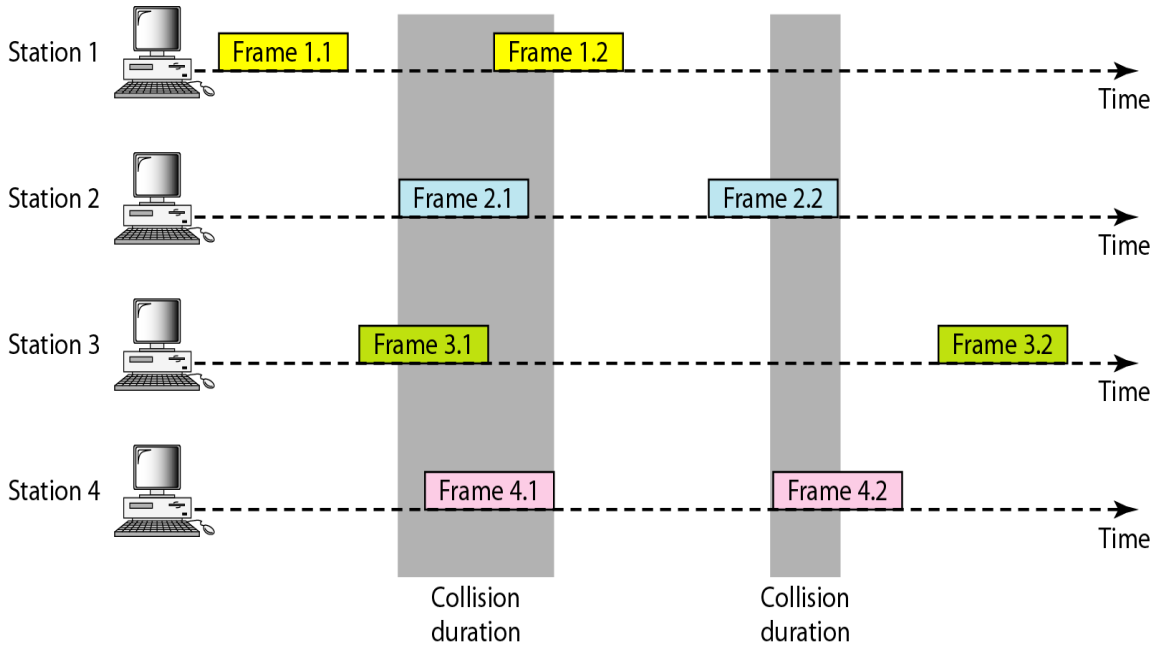
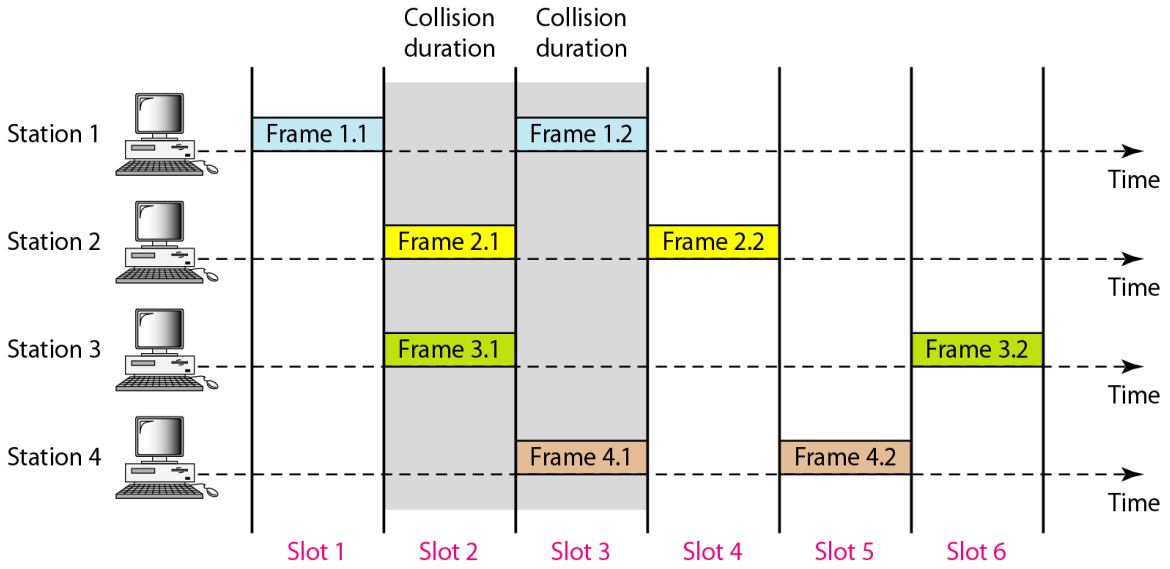



Figure shows that each station sends two frames ; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention of shared medium.

#### ii) Slotted ALOHA :

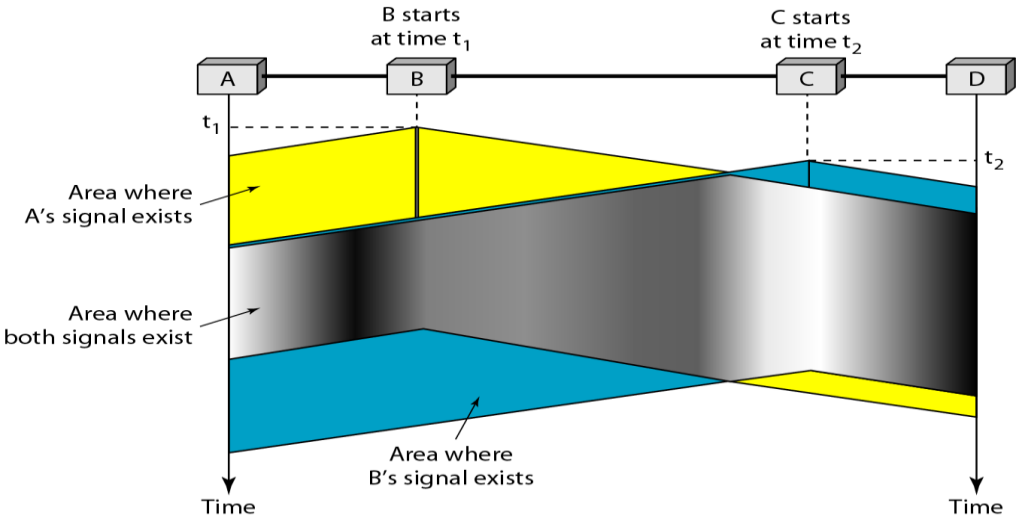
In slotted ALOHA we divide the time into slots of $T_{fr}$ s and force the station to send only at the beginning of the time slot.




**2) Carrier Sense Multiple Access(CSMA)**

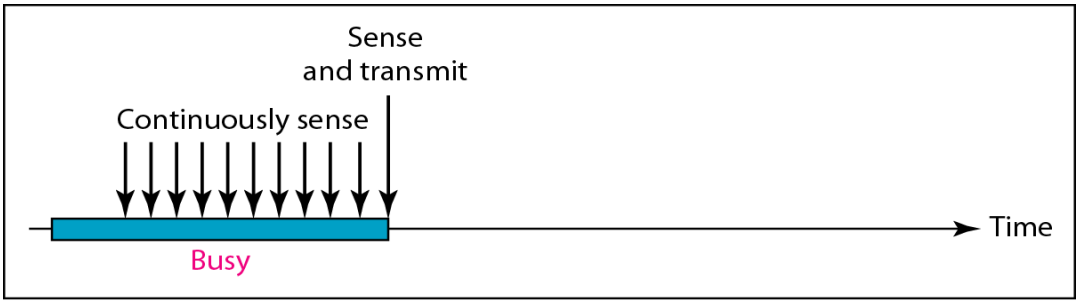
To minimize the chance of collision and increase the performance, the CSMA method was developed. CSMA requires that each station first listen to the medium before sending. The station senses the medium before trying to use it.

CSMA can reduce collisions, but it cannot eliminate. When station sends a frame , it still take time for the first bit to reach every station.

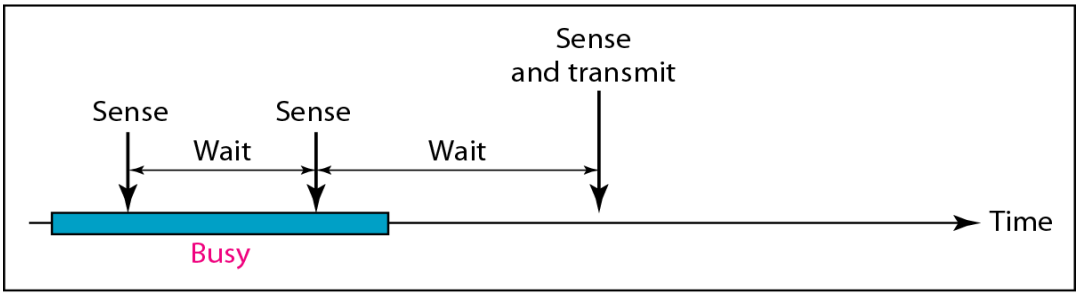



*a) Persistence Methods:*

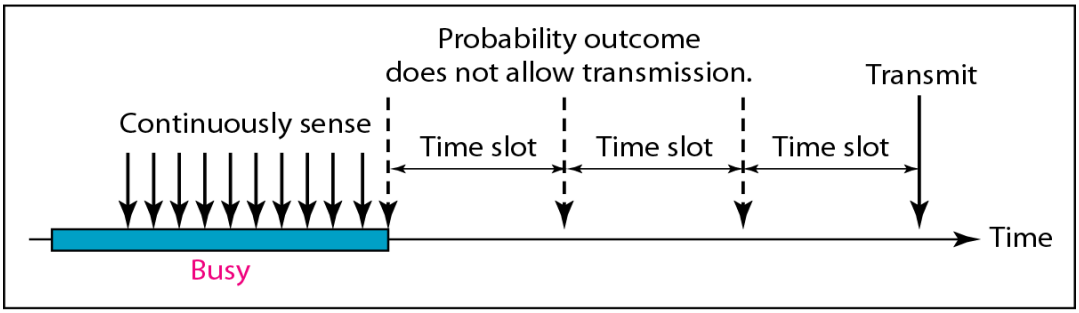
What should a station do if the channel is busy. Three methods have been defined to answer this question: 1-persistent, Nonpersistent and P- Persistent methods




a. 1-persistent




b. Nonpersistent

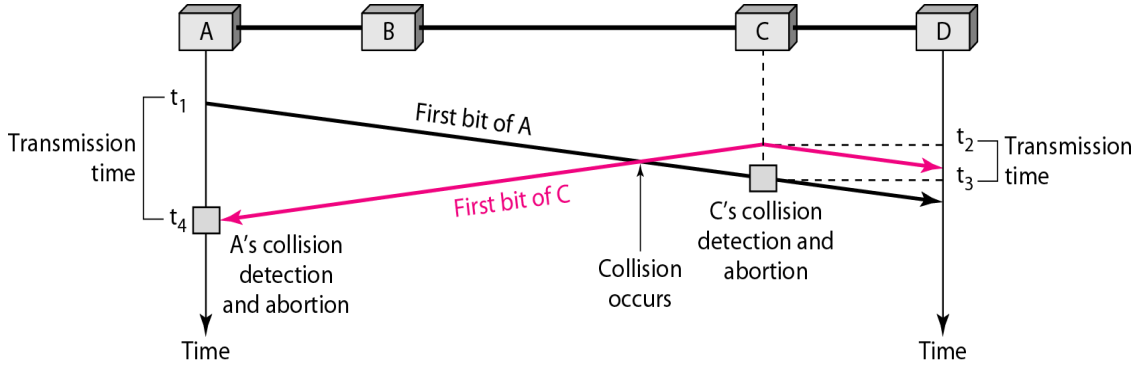



c. p-persistent

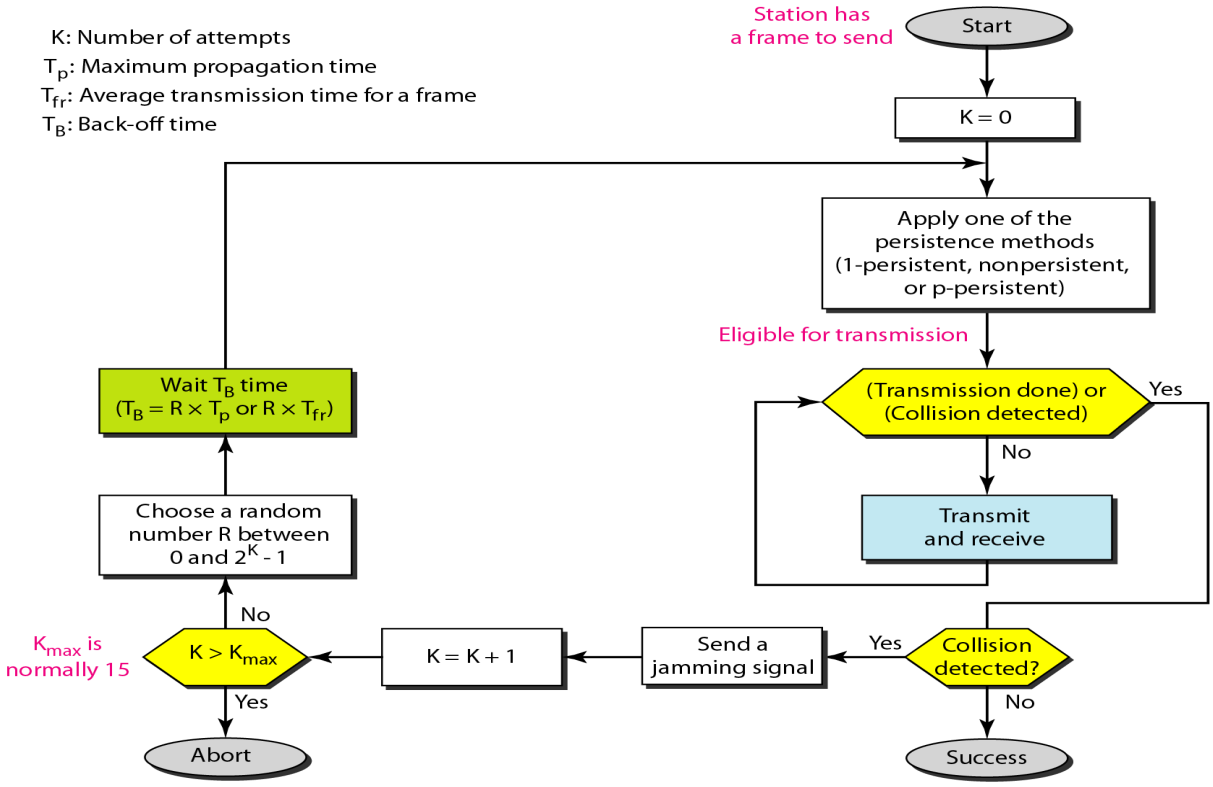
- 1-persistent: if the station find line is idle , it sends the frame immediately, highest collision.
- Non persistent: a station that has a frame to send senses the line, if the line is idle ,it sends immedately, otherwise it waits a random amount of time and sense again.
- P-persistent:is used if he channel has time slots. it reduces the chane of collision and improves efficiency

**3) Carrier Sense Multiple Access with Collision Detection(CSMA/CD)**

CSMA/CD augments the algorithm to handle the collision. In this method the station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If there is a collision , the frame is sent again.

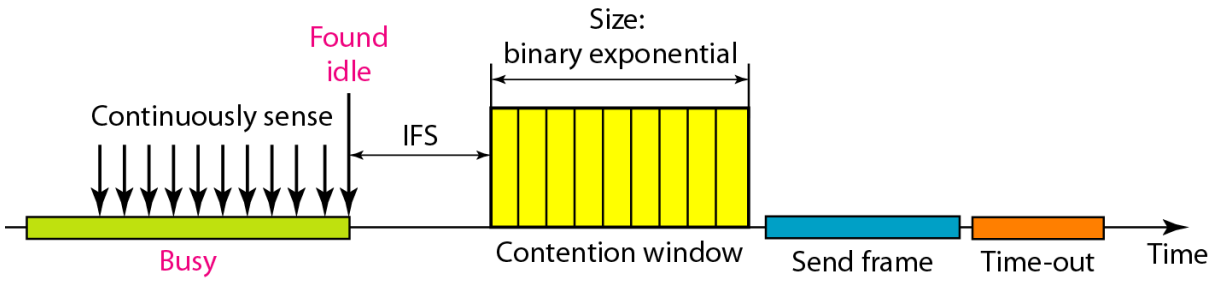



Flow diagram for the CSMA/CD




### 4) Carrier Sense Multiple Access with Collision Aviodane(CSMA/CA)

We need to avoid collisions on wireless medium because they cannot be detected, CSMA/CA was invented for this network. Collisions are avoided using three strategies: the Interframe space(IFS), the Contention window and the acknowledgement.



*Interframe space(IFS):*

First ,collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station doesnot send immediately. It waits for a period of time called **interframe space**(IFS)

*Contention window:*

In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window;it stops the timer and restarts it when the channel becomes idle.

*Acknowedgement:*

The positive acknowledgment and the time-out timer can help guarantee that the receiver .

## Q). The channel allocation problem

The channel allocation problem can be classified into 2 types. They are

- Static channel allocation
- Dynamic channel allocation

**Static channel allocation :**

The traditional way of allocating a channel among multiple competing users is FDM: if there are N users, the bandwidth is divided into N equal sized partitions. If the number of users is fixed and each has a heavy (buffered) load (e.g. switching offices of telephone companies) FDM is a simple and efficient allocation strategy. If however the number of users vary problems arise. If fewer than N users want to communicate, part of the available bandwidth is not used. If there are more than N users, some of them can not be served, even if some of the served users hardly transmit or receive anything. Even if the number of users is somehow kept constant, bandwidth can be wasted because data traffic is often bursty, peak to mean traffic ratio's of 1000:1 are quite common. These problems also apply to TDM.

Some queuing theory calculations to show the inefficiency of FDM. Suppose a channel with a capacity of C bps, frames arriving according a Poisson distribution with a mean of frames/sec, each having a length drawn from an exponential pdf (probability density function) with mean 1/ bits/frame. The mean time T a packet has to wait before it can be send is then: T = 1 / ( C - ). Now the channel is divided into N independent channels with capacity C/N bps, the mean input rate for each of the subchannels is then /N. Then TFDM = 1 / ( (C/N) -(/N) ) = N/ ( C

- ) = NT. The mean time delay for a packet to be send using FDM is thus N times worse than if all the frames were somehow magically arranged orderly in a big central queue.

**Dynamic channel allocation:**

Several assumptions are used in dynamic channel allocation. Station model. There are N independent stations, each with a program or user that generates frames for transmission. Usually the pdf of frame generation is taken to be a poisson distribution with mean frames/sec. The size of a frame is either constant or from an exponential distribution.

**Single channel:** A single channel is available, all stations can transmit on it and receive from it. As far as the hardware is concerned all stations are equal, although protocol software may assign priorities to them.

**Collision:** If two frames are transmitted simultaneously, the resulting signal is garbled. All stations can detect collisions.

**Time:** With continuous time, frame transmission can begin at any instant. With slotted time, time is divided into discrete intervals called slots, frame transmission always begin at the start of a slot. A slot may contain 0 (idle), 1 (successful transmission) or more (a collision) frames.

**Carrier sense**: Stations can either tell if the channel is in use or not. If they can, they do not send when the carrier is in use. If they can not, they just go ahead and send. LAN's usually have carrier sense possibilities.

## Q). what is an Ethernet Network?

Ethernet network is used to create local area network and connect multiple computers or other devices such as printers, scanners, and so on. In a wired network, this is done with the help of fiber optic cables, while in a wireless network, it is done through wireless network technology. An Ethernet network uses various topologies such as star, bus, ring, and more.

**Various Types of Ethernet Networks :**

Fiber optic media converters connect an Ethernet device with CAT5/CAT6 copper cables to a fiber optic cable. An Ethernet network usually is active in a 10-km periphery. This extension to fiber optic cable significantly increases the distance covered by the network. Here are some types of Ethernet networks:

- **Fast Ethernet**: As the term suggests, this is quite a high-speed internet, and can transmit or receive data at about 100 Mbps. This type of network is usually supported by a twisted pair or CAT5 cable. If a laptop, camera, or any other device is connected to a network, they operate at 10/100Base Ethernet and 100Base on the fiber side of the link.
- **Gigabit Ethernet**: This type of network transfers data at an even higher speed of about 1000 Mbps or 1Gbps. Gigabit speed is an upgrade from Fast Ethernet which is slowly being phased out. In this type of network, all the four pairs in the twisted pair cable contribute to the data transfer speed.

- **10-Gigabit Ethernet**: This is an even more advanced and high speed network type with a data transfer rate of 10 Gigabit/second. It is supported by CAT6a or CAT7 twisted pair cables, as well as fiber optic cables. By using a fiber optic cable, this network area can be extended up to around 10,000 meters.
- **Switch Ethernet**: This type of network requires a switch or hub. Also, instead of a twisted pair cable, a normal network cable is used in this case. Network switches are used for data transfer from one device to the other, without interrupting any other devices in the network.

## Q). Classic Ethernet Physical Layer

Classic Ethernet snaked around the building as a single long cable to which all the computers were attached. This architecture is shown in Fig. 4-13. The first variety, popularly called **thick Ethernet,** resembled a yellow garden hose, with markings every 2.5 meters to show where to attach computers. It was succeeded by **thin Ethernet,** which bent more easily and made connections using industry-standard BNC connectors. Thin Ethernet was much cheaper and easier to install, but it could run for only 185 meters per segment (instead of 500 m with thick Ethernet), each of which could handle only 30 machines (instead of 100).

Each version of Ethernet has a maximum cable length per segment (i.e., unamplified length) over which the signal will propagate. To allow larger net- works, multiple cables can be connected by **repeaters**. A repeater is a physical layer device that receives, amplifies (i.e., regenerates), and retransmits signals in both directions. As far as the software is concerned, a series of cable segments

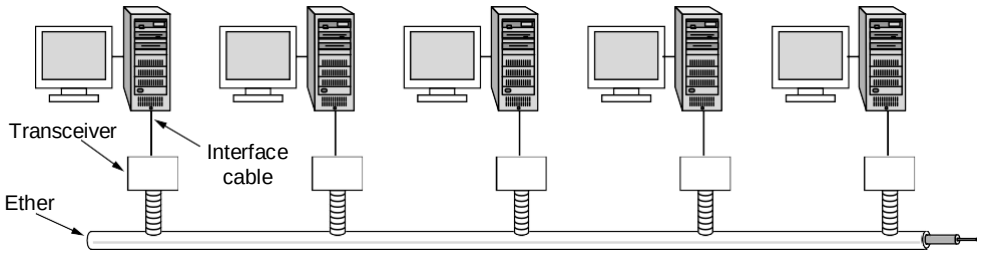



**Figure 4-13.** Architecture of classic Ethernet.

connected by repeaters is no different from a single cable (except for a small amount of delay introduced by the repeaters).

## Q). Classic Ethernet MAC Sublayer Protocol

The format used to send frames is shown in Fig. 4-14. First comes a *Pream- ble* of 8 bytes, each containing the bit pattern 10101010 (with the exception of the last byte, in which the last 2 bits are set to 11). This last byte is called the *Start of Frame* delimiter for 802.3. The Manchester encoding of this pattern produces a 10-MHz square wave for 6.4 sec to allow the receiver's clock to synchronize with the sender's. The last two 1 bits tell the receiver that the rest of the frame is about to start.

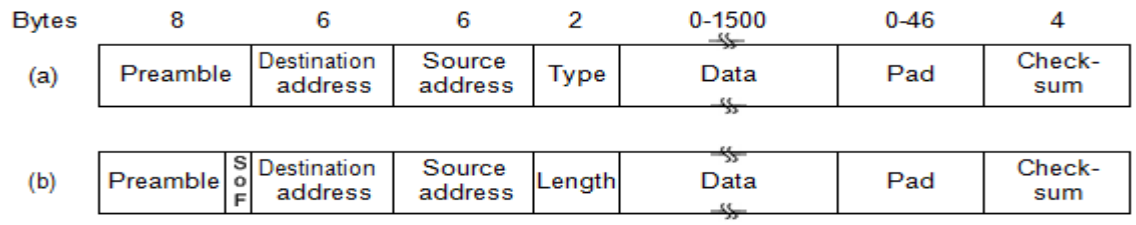



**Figure 4-14.** Frame formats. (a) Ethernet (DIX). (b) IEEE 802.3.

Next come two addresses, one for the destination and one for the source. They are each 6 bytes long. The first transmitted bit of the destination address is a 0 for ordinary addresses and a 1 for group addresses. Group addresses allow multiple stations to listen to a single address. When a frame is sent to a group address, all the stations in the group receive it. Sending to a group of stations is called **multi- casting.**

Next comes the *Type* or *Length* field, depending on whether the frame is Eth- Ethernet or IEEE 802.3. Ethernet uses a *Type* field to tell the receiver what to do with the frame.

IEEE 802.3, in its wisdom, decided that this field would carry the length of the frame, since the Ethernet length was determined by looking inside the data—a layering violation if ever there was one.

Next come the data, up to 1500 bytes. This limit was chosen somewhat arbitrarily at the time the Ethernet standard was cast in stone, mostly based on the fact that a transceiver needs enough RAM to hold an entire frame and RAM was expensive in 1978. A larger upper limit would have meant more RAM, and hence a more expensive transceiver.

The final field is the *Checksum*. It is a 32-bit CRC. This CRC is an error- detecting code that is used to determine if the bits of the frame have been received correctly. It just does error detection, with the frame dropped if an error isdetected.

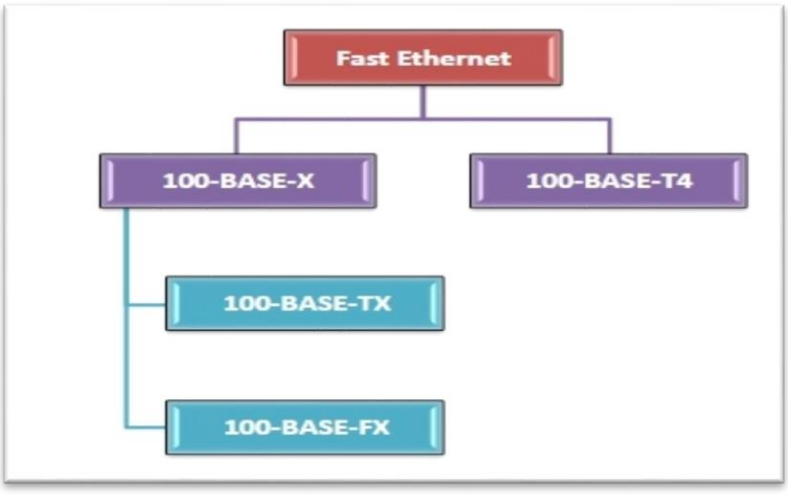
## Q). Fast Ethernet

In computer networks, Fast Ethernet is a variation of Ethernet standards that carry data traffic at 100 Mbps (Mega bits per second) in local area networks (LAN). It was launched as the IEEE 802.3u standard in 1995, and stayed the fastest network till the introduction of Gigabit Ethernet.

Fast Ethernet is popularly named as 100-BASE-X. Here, 100 is the maximum throughput, i.e. 100 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used, which is TX or FX.

## Varieties of Fast Ethernet

The common varieties of fast Ethernet are 100-Base-TX, 100-BASE-FX and 100-Base-T4.



- **100-Base-T4**
    - This has four pairs of UTP of Category 3, two of which are bi-directional and the other two are unidirectional.
    - In each direction, three pairs can be used simultaneously for data transmission.
    - Each twisted pair is capable of transmitting a maximum of 25Mbaud data. Thus the three pairs can handle a maximum of 75Mbaud data.
    - It uses the encoding scheme 8B/6T (eight binary/six ternary).
- **100-Base-TX**
    - This has either two pairs of unshielded twisted pairs (UTP) category 5 wires or two shielded twisted pairs (STP) type 1 wires. One pair transmits frames from hub to the device and the other from device to hub.
    - Maximum distance between hub and station is 100m.
    - It has a data rate of 125 Mbps.
    - It uses MLT-3 encoding scheme along with 4B/5B block coding.
- **100-BASE-FX**
    - This has two pairs of optical fibers. One pair transmits frames from hub to the device and the other from device to hub.
    - Maximum distance between hub and station is 2000m.
    - It has a data rate of 125 Mbps.
    - It uses NRZ-I encoding scheme along with 4B/5B block coding.

### Q) WIRELESS LANS

Wireless LANs are increasingly popular, and homes, offices, cafes, libraries, airports, zoos, and other public places are being outfitted with them to connect computers, PDAs, and smart phones to the Internet. Wireless LANs can also be used to let two or more nearby computers communicate without using the Inter- net.

## Q) The 802.11 Architecture and Protocol Stack

802.11 networks can be used in two modes. The most popular mode is to connect clients, such as laptops and smart phones, to another network, such as a company intranet or the Internet. This mode is shown in Fig. 4-23(a).

In infrastructure mode, each client is associated with an **AP** (**Access Point**) that is in turn connected to the other network. The client sends and receives its packets via the AP. Several access points may be connected together, typically by a wired network called a **distribution system**, to form an extended 802.11 network. In this case, clients can send frames to other clients via their APs.

The other mode, shown in Fig. 4-23(b), is an **ad hoc network**. This mode is a collection of computers that are associated so that they can directly send frames to each other. There is no access point. Since Internet access is the killer application for wireless, ad hoc networks are not very popular.

**Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. A station can be of two types−
Wireless Access Point (WAP) − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
Client. Clients are workstations, computers, laptops, printers, smartphones, etc.
Each station has a wireless network interface controller.
**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 depending upon the mode of operation−
Infrastructure BSS − Here, the devices communicate with other devices through access points.
Independent BSS − Here, the devices communicate in a peer-to-peer basis in an ad hoc manner.
**Extended Service Set (ESS)** − It is a set of all connected BSS.
**Distribution System (DS)** − It connects access points in ESS.

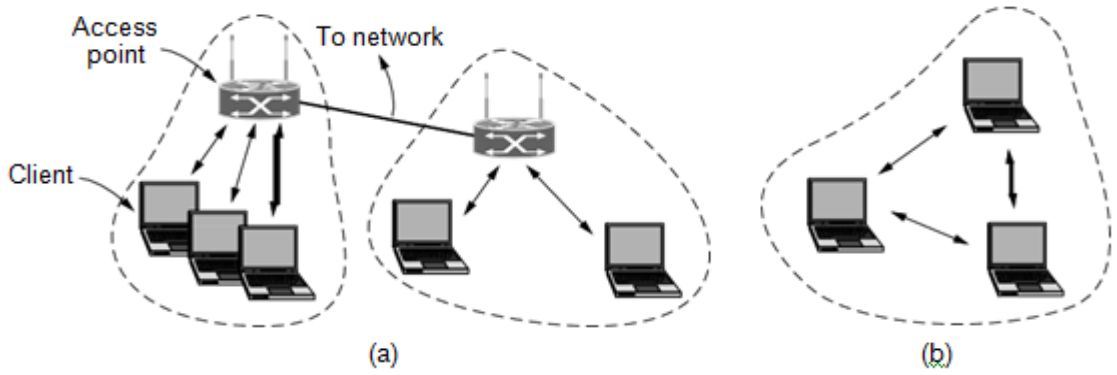



**Figure 4-23.** 802.11 architecture. (a) Infrastructure mode. (b) Ad-hoc mode.

A partial view of the 802.11 protocol stack is given in Fig. 4-24. The stack is the same for clients and APs. The physical layer corresponds fairly well to the OSI physical layer, but the data link layer in all the 802 protocols is split into two or more sublayers. In 802.11, the MAC (Medium Access Control) sublayer determines how the channel is allocated, that is, who gets to transmit next.

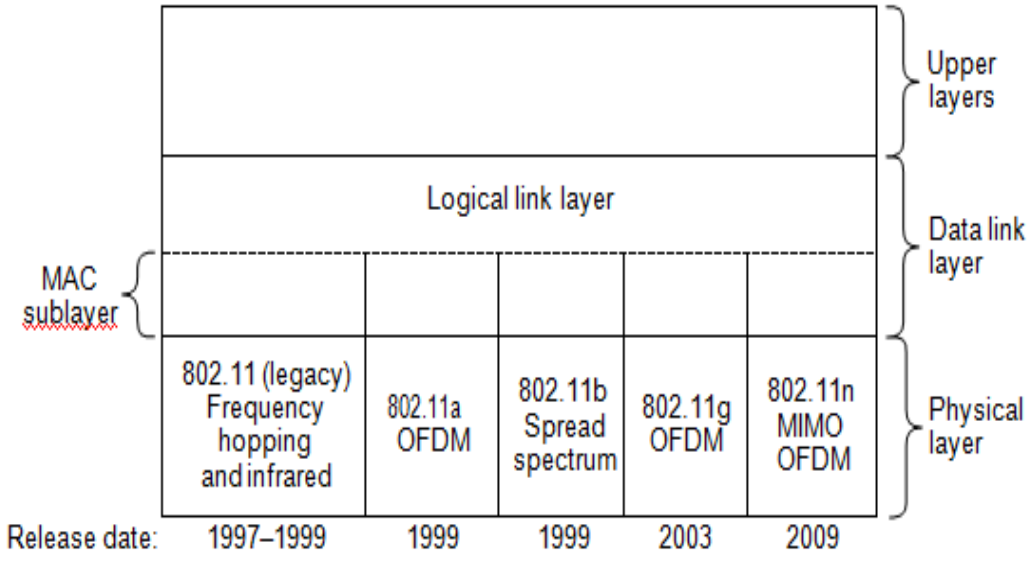
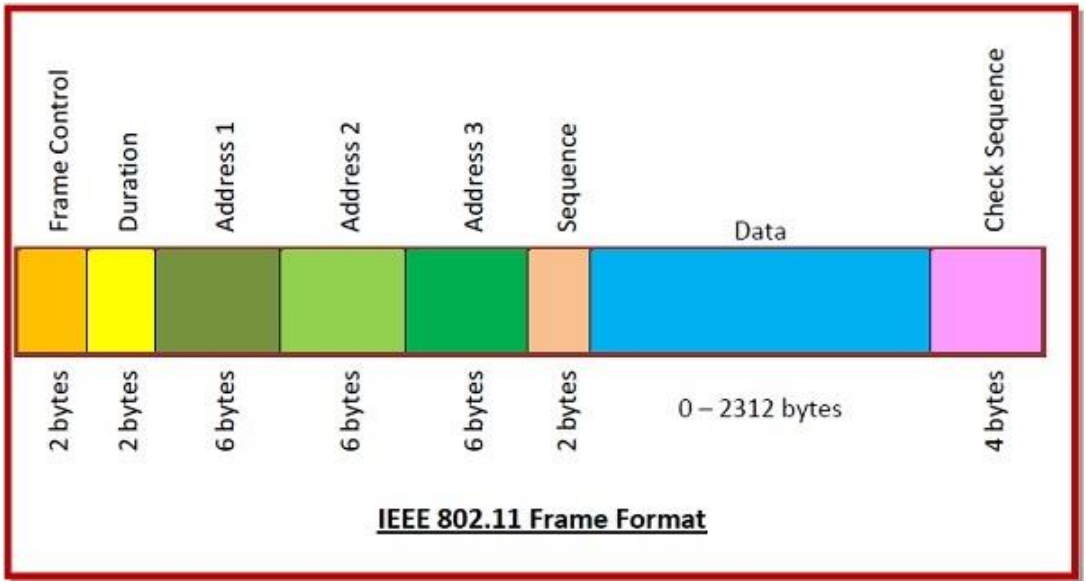



**Figure 4-24.** Part of the 802.11 protocol stack.

**Q) 802.11 frame structure**

The IEEE 802.11 standard, lays down the architecture and specifications of wireless local area networks (WLANs). WLAN or WiFi uses high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

The 802.11 MAC sublayer provides an abstraction of the physical layer to the logical link control sublayer and upper layers of the OSI network. It is responsible for encapsulating frames and describing frame formats.




**Frame Control** − It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.

**Duration** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.

**Address fields** − There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.

**Sequence** − It a 2 bytes field that stores the frame numbers.

**Data** − This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.

**Check Sequence** − It is a 4-byte field containing error detection information.

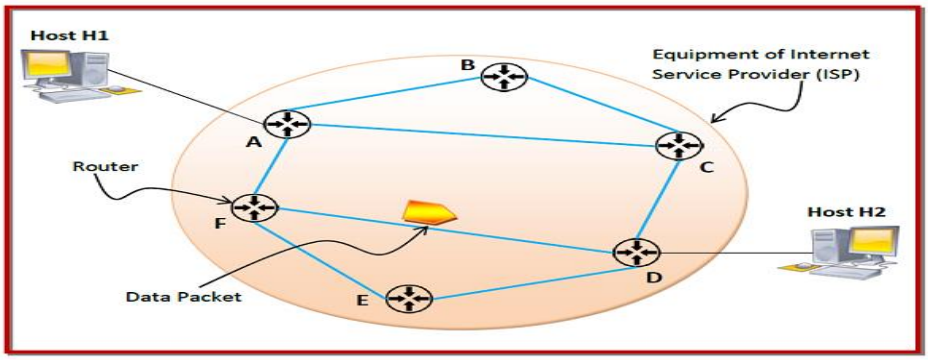
## Unit -III

### Q) Store – and – Forward Packet Switching

In telecommunications, store − and − forward packet switching is a technique where the data packets are stored in each intermediate node, before they are forwarded to the next node. The intermediate node checks whether the packet is error−free before transmitting, thus ensuring integrity of the data packets. In general, the network layer operates in an environment that uses store and forward packet switching.

### Working Principle

The node which has a packet to send, delivers it to the nearest node, i.e. router. The packet is stored in the router until it has fully arrived and its checksum is verified for error detection. Once, this is done, the packet is transmitted to the next router. The same process is continued in each router until the packet reaches its destination.




In the above diagram, we can see that the Internet Service Provider (ISP) has six routers (A to F) connected by transmission lines shown in blue lines. There are two hosts, host H1 is connected to router A, while host H2 is connected to router D. Suppose that H1 wants to send a data packet to H2. H1 sends the packet to router A. The packet is stored in router A until it has arrived fully. Router A verifies the checksum using CRC (cyclic redundancy check) code. If there is a CRC error, the packet is discarded, otherwise it is transmitted to the next hop, here router F. The same process is followed by router F which then transmits the packet to router D. Finally router D delivers the packet to host H2.

### Advantages and Disadvantages

Store − and forward packet switching ensures high quality data packet transmission. Since erroneous packets are discarded at each router, bad packets or invalid packets in the network are mostly eliminated.

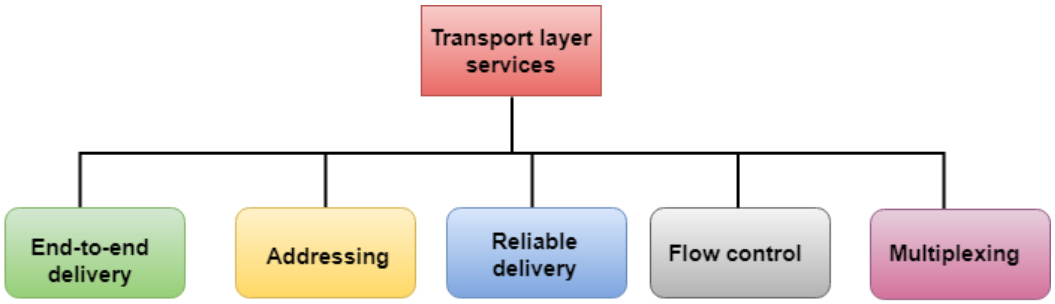
However, error − free packet transmission is achieved by compromising on the overall speed of transmission. Switch latency is introduced due to waiting for entire packet to arrive as well as computation of CRC. Though the latency at each router may seem small enough, the cumulative latency at all routers make it inappropriate for time − critical online applications.

### Services provided by the Transport Layer

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

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

- End-to-end delivery
- Addressing
- Reliable delivery
- Flow control
- Multiplexing




End-to-end delivery:

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

Reliable delivery:

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

**The reliable delivery has four aspects:**

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

**Error Control**

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

detects those errors that have been introduced between the beginning and end of the link. Therefore, the transport layer performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.

**Sequence Control**

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

**Loss Control**

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

**Duplication Control**

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

**Flow Control**

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

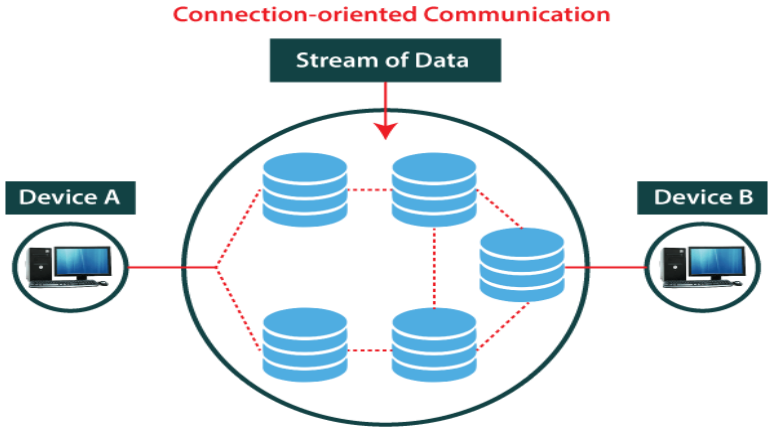
The transport layer uses the multiplexing to improve transmission efficiency.

**Multiplexing can occur in two ways:**

- **Upward multiplexing:** Upward multiplexing means multiple transport layer connections use the same network connection. To make more cost-effective, the transport layer sends several transmissions bound for the same destination along the same path; this is achieved through upward multiplexing.
- **Downward multiplexing:** Downward multiplexing means one transport layer connection uses the multiple network connections. Downward multiplexing allows the transport layer to split a connection among several paths to improve the throughput. This type of multiplexing is used when networks have a low or slow capacity.

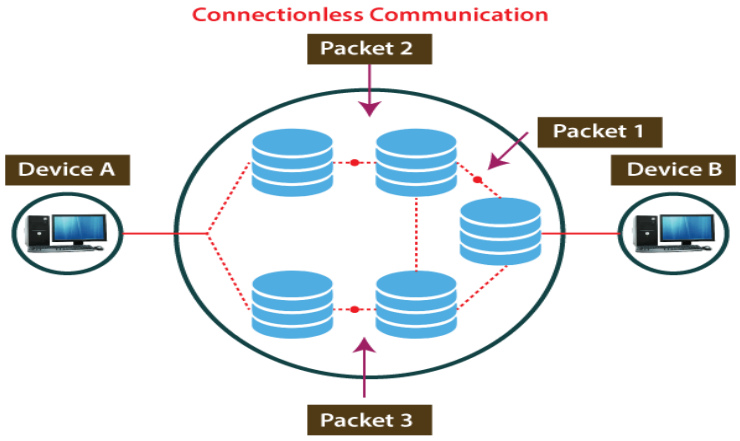
## Q) Connection-Oriented Service & Connectionless Service

A connection-oriented service is a network service that was designed and developed after the telephone system. A connection-oriented service is used to create an end to end connection between the sender and the receiver before transmitting the data over the same or different networks. In connection-oriented service, packets are transmitted to the receiver in the same order the sender has sent them. It uses a handshake method that creates a connection between the user and sender for transmitting the data over the network. Hence it is also known as a reliable network service.




## Connectionless Service

A connection is similar to a **postal system**, in which each letter takes along different route paths from the source to the destination address. Connectionless service is used in the network system to transfer data from one end to another end without creating any connection. So it does not require establishing a connection before sending the data from the sender to the receiver. It is not a reliable network service because it does not guarantee the transfer of data packets to the receiver, and data packets can be received in any order to the receiver. Therefore we can say that the data packet does not follow a **defined** path. In connectionless service, the transmitted data packet is not received by the receiver due to network congestion, and the data may be lost.



**Q) Comparison of Virtual Circuits and Datagram Networks**

| Virtual Circuits | Datagram Networks |
|---|---|
| Virtual circuits are connection-oriented, which means that there is a reservation of resources like buffers, bandwidth, etc. for the time during which the newly setup VC is going to be used by a data transfer session. | It is connectionless service. There is no need for reservation of resources as there is no dedicated path for a connection session. |
| A virtual circuit network uses a fixed path for a particular session, after which it breaks the connection and another path has to be set up for the next the next session. | A Datagram based network is a true packet switched network. There is no fixed path for transmitting data. |
| All the packets follow the same path and hence a global header is required only for the first packet of connection and other packets will not require it. | Every packet is free to choose any path, and hence all the packets must be associated with a header containing information about the source and the upper layer data. |
| Packets reach in order to the destination as data follows the same path. | Data packets reach the destination in random order, which means they need not reach in the order in which they were sent out. |
| Virtual Circuits are highly reliable. | Datagram networks are not as reliable as Virtual Circuits. |
| Implementation of virtual circuits is costly as each time a new connection has to be set up with reservation of resources and extra information handling at routers. | But it is always easy and cost-efficient to implement datagram networks as there is no need of reserving resources and making a dedicated path each time an application has to communicate. |

**Q) 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.

The Routing algorithm is divided into two categories:

- Adaptive Routing algorithm
- Non-adaptive Routing algorithm

### 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.

### Non-Adaptive Routing algorithm

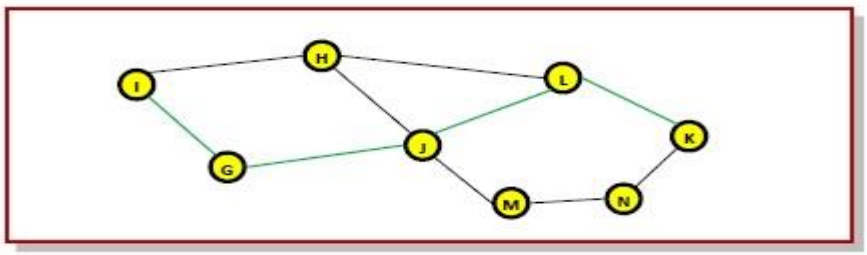
- Non Adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

**Q) Optimality Principle**

The purpose of a routing algorithm at a router is to decide which output line an incoming packet should go. The optimal path from a particular router to another may be the least cost path, the least distance path, the least time path, the least hops path or a combination of any of the above.
The optimality principle can be logically proved as follows −
If a better route could be found between router J and router K, the path from router I to router K via J would be updated via this route. Thus, the optimal path from J to K will again lie on the optimal path from I to K.

**Examples**

Consider a network of routers, {G, H, I, J, K, L, M, N} as shown in the figure. Let the optimal route from I to K be as shown via the green path, i.e. via the route I-G-J-L-K. According to the optimality principle, the optimal path from J to K with be along the same route, i.e. J-L-K.




**Shortest Path**

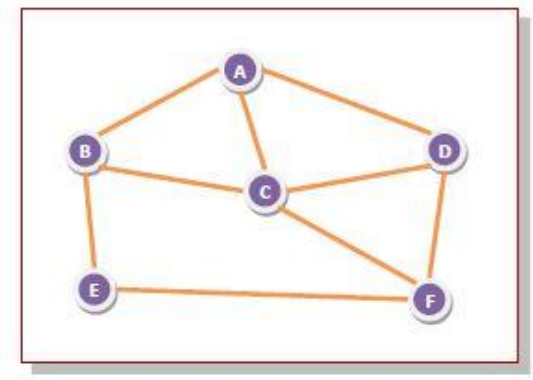
Consider that a network comprises of N vertices (nodes or network devices) that are connected by M edges (transmission lines). Each edge is associated with a weight,

representing the physical distance or the transmission delay of the transmission line. The target of shortest path algorithms is to find a route between any pair of vertices along the edges, so the sum of weights of edges is minimum. If the edges are of equal weights, the shortest path algorithm aims to find a route having minimum number of hops.

**Flooding**

Flooding is a non-adaptive routing technique following this simple method: when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on.

For example, let us consider the network in the figure, having six routers that are connected through transmission lines.




Using flooding technique –

- An incoming packet to A, will be sent to B, C and D.
- B will send the packet to C and E.
- C will send the packet to B, D and F.
- D will send the packet to C and F.
- E will send the packet to F.
- F will send the packet to C and E.

## Q) Distance Vector

- **Distributed:** It is distributed in that each node receives information from one or more of its directly attached neighbors, performs calculation and then distributes the result back to its neighbors.
- **Iterative:** It is iterative in that its process continues until no more information is available to be exchanged between neighbors.
- **Asynchronous:** It does not require that all of its nodes operate in the lock step with each other.

- The Distance vector algorithm is a dynamic algorithm.
- It is mainly used in ARPANET, and RIP.
- Each router maintains a distance table known as **Vector**.

## Q) Link State

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

**The three keys to understand the Link State Routing algorithm:**

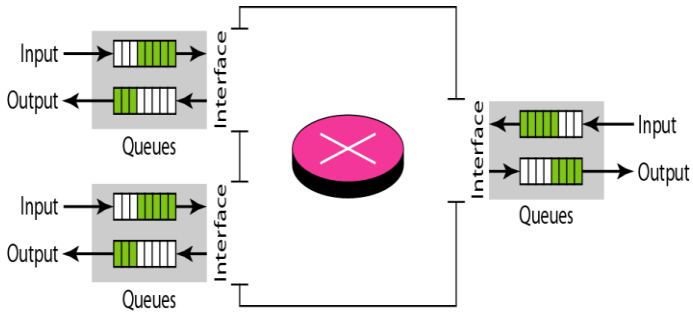
- **Knowledge about the neighborhood:** Instead of sending its routing table, a router sends the information about its neighborhood only. A router broadcast its identities and cost of the directly attached links to other routers.
- **Flooding:** Each router sends the information to every other router on the internetwork except its neighbors. This process is known as Flooding. Every router that receives the packet sends the copies to all its neighbors. Finally, each and every router receives a copy of the same information.
- **Information sharing:** A router sends the information to every other router only when the change occurs in the information.

**Hierarchical**

Hierarchical Routing is **the method of routing in networks that is based on hierarchical addressing**. Most transmission control protocol, Internet protocol (DCPIP). Routing is based on two level of hierarchical routing in which IP address is divided into a network, person and a host person.

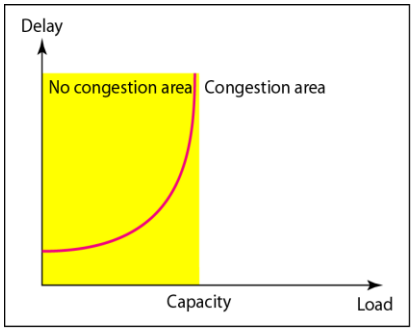
## Q).What is meant by congestion?

Congestion in a network may occur if the load on the network—the number of packets sent to the network—is greater than the capacity of the network—the number of packets a network can handle. Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

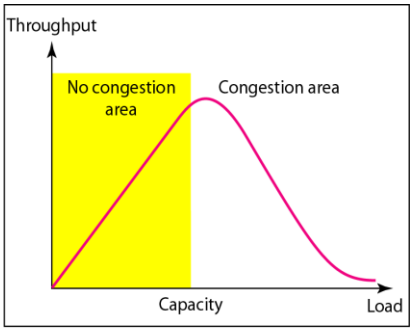



**Network Performance**

Congestion control involves two factors that measure the performance of a network : *delay and throughput*



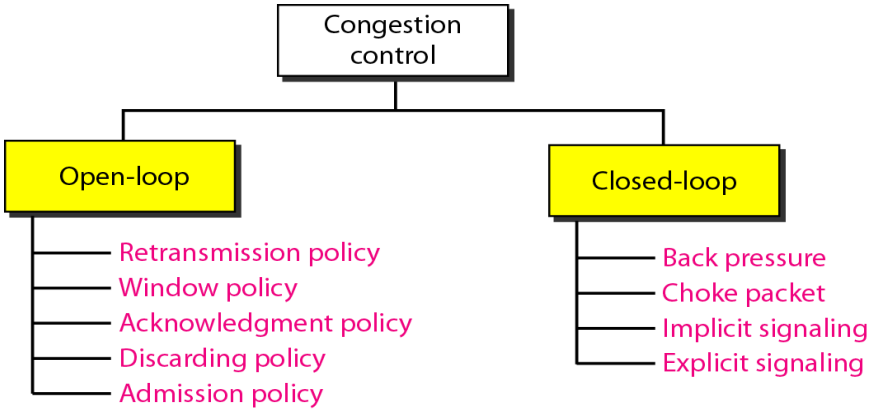
a. Delay as a function of load



b. Throughput as a function of load

## Q).What are the methods to control the congestion.

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal).




### i) Open-Loop Congestion Control

In open loop congestion control, policis are applied to prevent the congestion before it happens.

*a) Retransmission policy*: if the sender feels that a sent packet is lost, the packet needs to be retransmitted.

*b) Window policy:*
The type of window at the sender may also affect congestion.

c) *Acknowledgment policy* :
The acknowledgment policy imposed by the receiver may also affect congestion.

*d) Discarding policy:*
A good discarding policy by the router may prevent congestion and at the same time may not harm the integrity of the transmission.

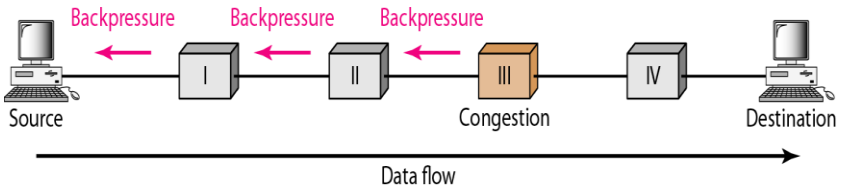
*e) Admission policy:*
Admission policy can also prevent congestion.

**ii) Closed-Loop Congestion Control**

closed loop congestion control mechanisms try to alleviate congestion after it happens.

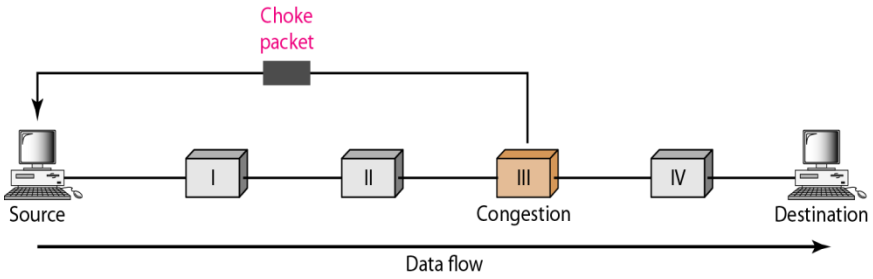
a)*Back pressure:*

the technique f backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes.




**b)***choke packet:*

a choke packet is a packet sent by a node to the source to inform it of congestion.




C) *implicit signalling:*

In implicit signalling, the source guesses that there is a congestion somewhere in the network from other system.

d)*Explicit signalling:*

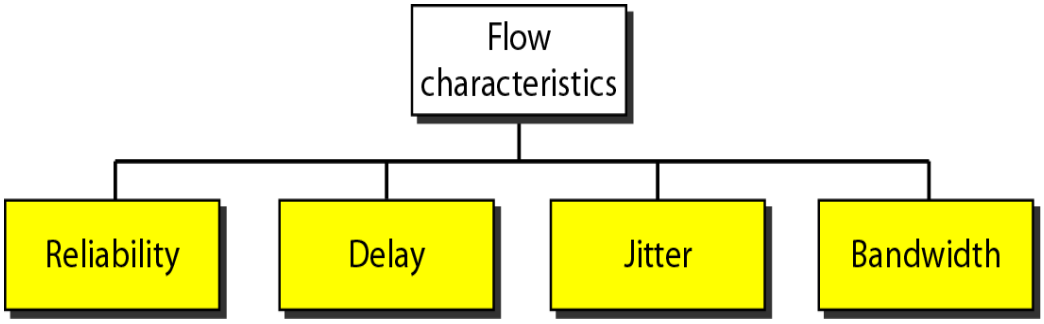
the node that experience congestion can explicitly send a signal to the source or destination. It can occur in either the forward or the backward direction.

**1. Define Quality of Service.**

Quality of service (QOS) is an internetworking issue that has been discussed more than defined. We can informally define quality of service as something a flow seeks to attain.

**i) Flow Characteristics**

**Four** types of characteristics are attributed to flow: reliability, delay, jitter and bandwidth.




**ii) Flow Classes**

Based on the flow characteristics, we can classify flows into groups or classes.

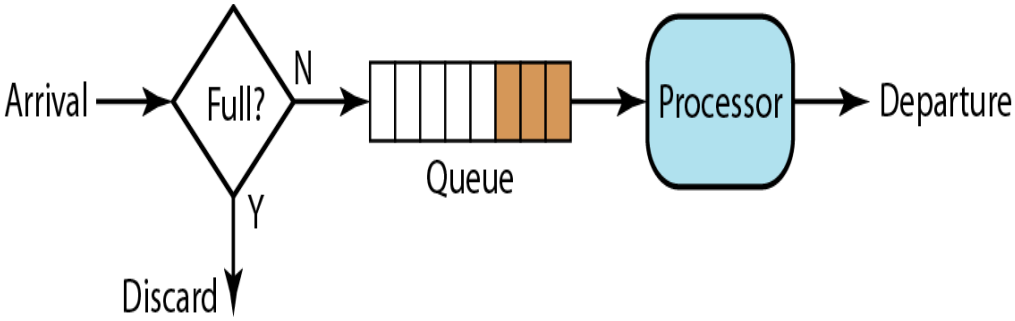
**2. Explain the Techniques to improve QOS.**

In this section, we discuss some techniques that can be used to improve the quality of service. We briefly discuss four common methods: scheduling, traffic shaping, admission control, and resource reservation.

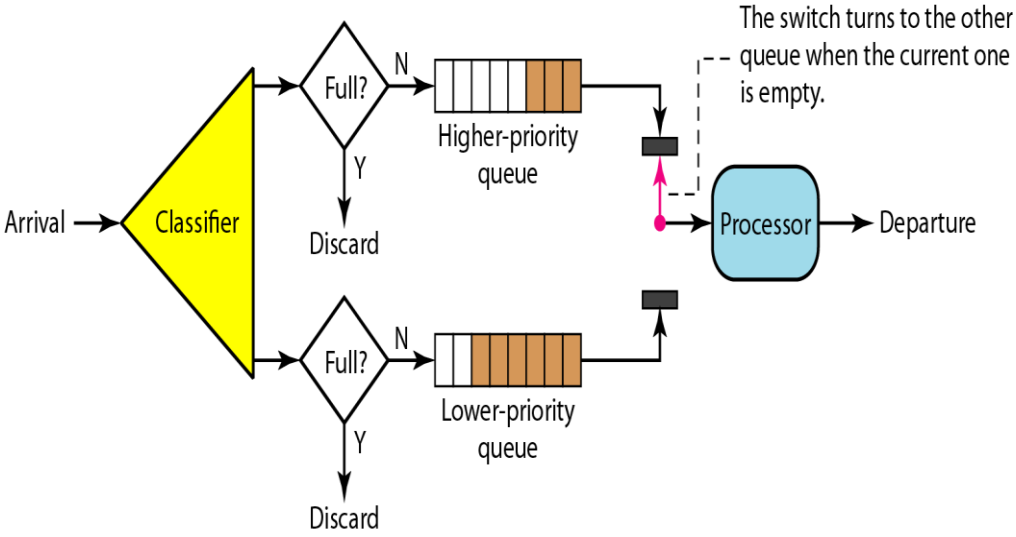
**i) Scheduling:**

A scheduling technique treats the different flows in fair and appropriate manner.

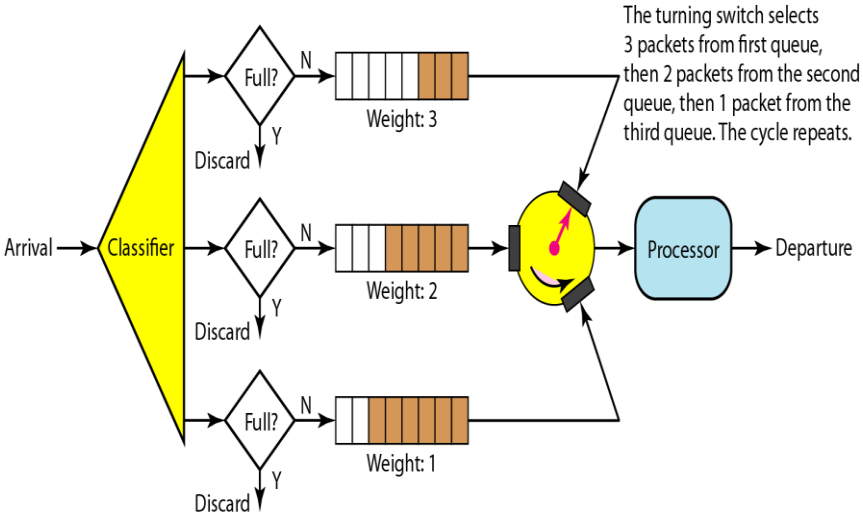
a)*FIFO Queuing:*




b)*Priority Queuing :*



c)*weighted fair queuing :*

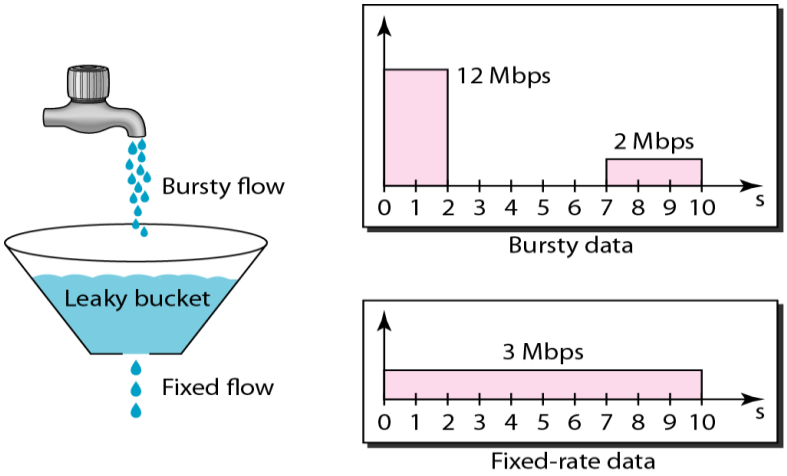



**ii) Traffic Shaping :**

Traffic shaping is a mechanism to control the amount and rate of the traffic sent to the network.

*a) Leaky Bucket :*

The input rate can vary, but the output rate remains constant.




**iii) Resource Reservation :**

The quality of service is improved if the resources are reservered beforehand.

**iv) Admission Control:**

Admission control refers to the mechanism used by a router or switch to accept or reject a fow based on predefined parameters called flow specifications.

**Q).Explain Integrated services in QOS.**

Integrated service is a flow baed QOS model, which means that a user needs to create a flow , a kind of virtual circuit, from the source to destination and inform all routers of the resource requirements.

**i) Signaling:**

The signaling protocol runs over IP that provides the signaling mechanism for making reservation called Resource Reservation Protocol(RSVP).

**ii) Flow Specification :**

When a source makes reservation, it needs to define a flow specification. A flow specification has two parts Rspec(Resource Specificiation) and Tspec(Traffic Specifcation)

**iii) Admission :**

After a router receives the flow specifications from the application, it decides to admit or deny the service.

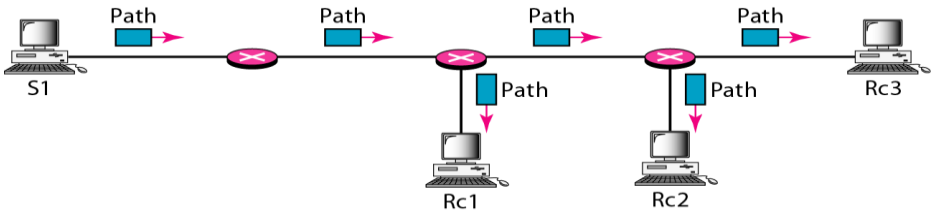
**iv) Service Classes:**

Two classes of service have been defined for integrated service: guaranteed service and controlled load service.

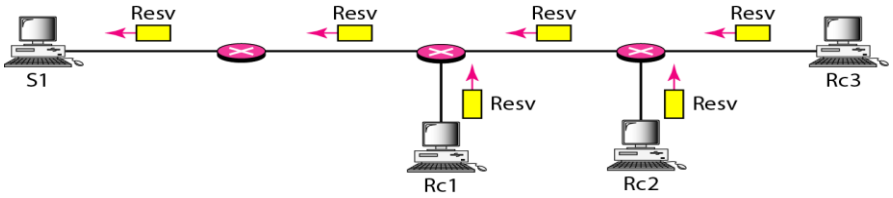
**v) RSVP:**

The Resource Reservation Protocol is a signaling protocol to help IP create a flow and consequently make a resource reservation.

Path messages




Resv messages




## Q).Write a short notes on Differentiated Services.

Differentiated Services (DS or Diffserv) was introduced by the IETF (Internet Engineering Task Force) to handle the shortcomings of Integrated Services. Differentiated Services is a class-based QoS model designed for IP

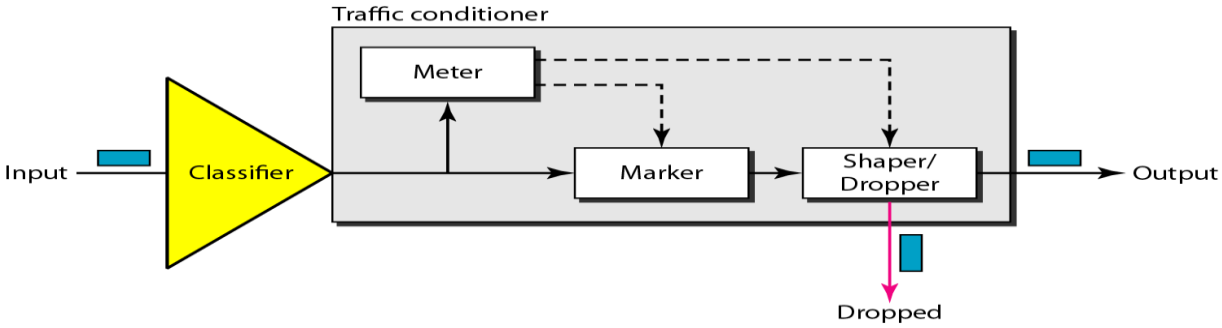
**i) DS Field**

In Diffserv, each packet contains a field called the DS field. The value of this field is set at the boundary of the network by the host or the first router designated as a boundary router.


The DS field contains two subfields: DSCP and CU. The DSCP defines the per-hop behaviour(PHB) and CU subfield is not currently used.

**ii) Traffic conditioner:**

To implement Diffserv, the DS node uses traffic conditioners such as meters, markers , sharpers and droppers.




## Q).Explain IPV4 Addresses in Network Layer.

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.

IPV4 address are unique. They are unique in the sense that each address defines one and one and only one connection to the internet. The IPV4 addresses are universal in the sense that the addressing system must be accepted by any hst that wants to be communicated to the Internet.

**I ) Address space:**

A Protocol such as IPV4 that defined addresses has an Address Space. An Address Space is the total number of addresses used by the protocol. IPV4 uses 32-bit addresses, which means that the address space is $2^{32}$ or 4,24967296.

**II) Notations:**

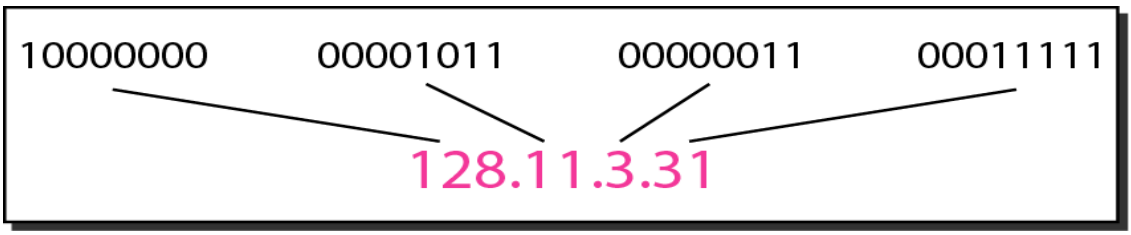
There are **two** notations to show an IPV4 address: binary notation and dotted-decimal notation.

*Binary notation:*

In binary notation , IPV4 addresses is displayed as 32 bits.

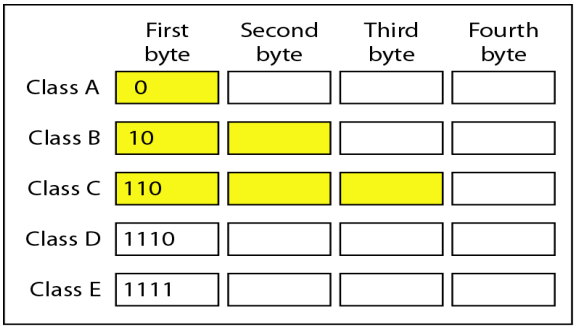
*Dotted –decimal notation:*

To make IPV4 address more compact and easier to read, internet addresses are usually written in decimal form with a decimal point(dot) separating the bytes

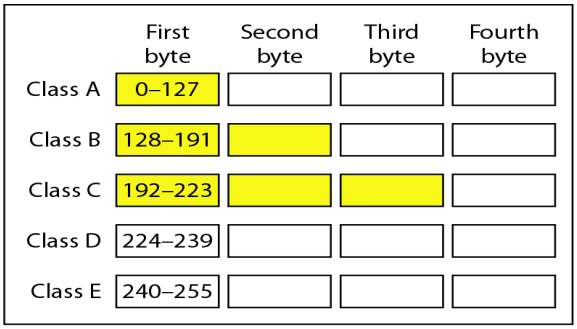



**III) classful Addressing:**

Ipv4 addressing used the concept of classes. This architecture is called classful addressing.In classful addressing, the address space is divided into five classes A,B,C,D,E. We can find the class of an address when given the address in binary notation or dotted-decimal notation.




a. Binary notation




b. Dotted-decimal notation

*a) Classes and Blocks*

One problem with classful addressing is that each class is divided into a fixed number of Blocks with each block having fixed size.**Class A addresses** were designed for large organizations with a large number of attached host or routers.

**Class B addresses** were designed for midsize organizations with tens of thousands of attached host or routers.**Class C addresses** were designed for small Organizations with a small number of attached host or routers.**Class D** were designed for multicasting and **Class E** were reserved for future use.

| *Class* | *Number of Blocks* | *Block Size* | *Application* |
|---|---|---|---|
| A | 128 | 16,777,216 | Unicast |
| B | 16,384 | 65,536 | Unicast |
| C | 2,097,152 | 256 | Unicast |
| D | 1 | 268,435,456 | Multicast |
| E | 1 | 268,435,456 | Reserved |

*b) netid and hostid*

In classful addressing , an IP address in class A,B and C is divided into netid and hostid. In classA ,one-byte defines netid and three bytes defines hosted. In classB two bytes defines netid and 2 bytes defines hosted. In class C, three bytes define the netid and one byte define the hostid.

*c) Mask :*

We can use a mask called default mask , a 32-bit number made of contiguous 1s followed by contiguous 0s.

| *Class* | *Binary* | *Dotted-Decimal* | *CIDR* |
|---|---|---|---|
| A | **11111111** 00000000 00000000 00000000 | **255**.0.0.0 | /8 |
| B | **11111111 11111111** 00000000 00000000 | **255.255**.0.0 | /16 |
| C | **11111111 11111111 11111111** 00000000 | **255.255.255**.0 | /24 |

*d) Subnetting:*

If an organization was granted a large block in class A or B , it could divide the addresses into several contiguous groups and assign each group to smaller network (subnets)

*e) Supernetting:*

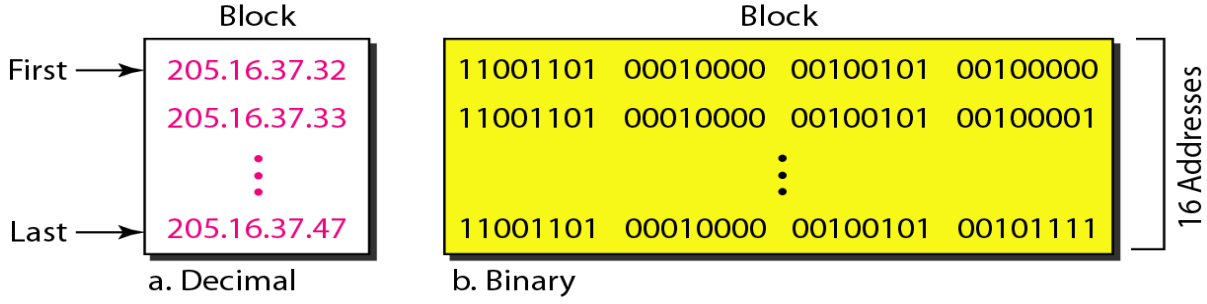
an organization can combine several class C blocks to create a super network. Or a supernet.

iv) **classless addressing:**

In classless address there in no concept of classes.In classless addressing ,when an entity, small,large, it is granted a block of addresses. The size of he block varies based on nature and size of the entity.

*a) Restriction:*

3. Addresses in a bock must be contiguous , one after another.
4. The number of addresses in a blocks must be power of 2(1,2,4,8,---)
5. The first address must be evenly divisible by the number of addresses.



*b) Mask :*

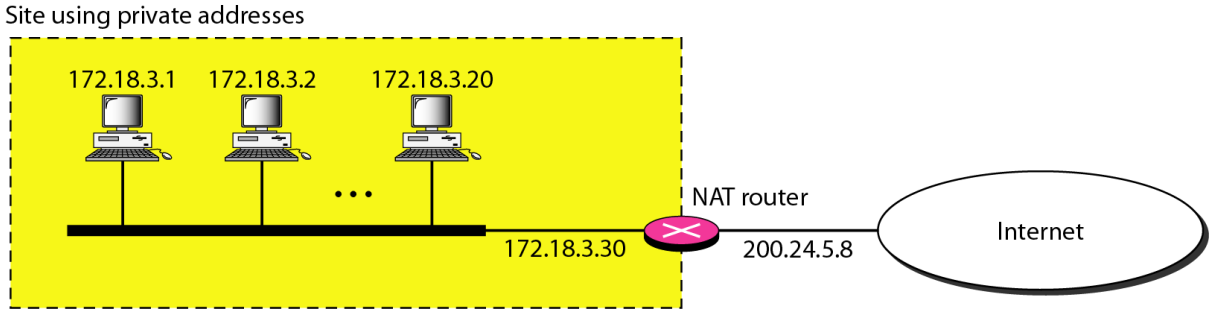
In IPv4 addressing, a block of addresses can be defined as x.y.z.t /*n*in which x.y.z.t defines one of the addresses and the /*n* defines the mask.

v) **Network Address Translation:**

NAT enables a user to have large set of addresses internally and one address or a small set of addresses, externally. To separate the addresses used inside the home or business and he one used for the internet. The internet authorities have reserved three set of address s private addresses.

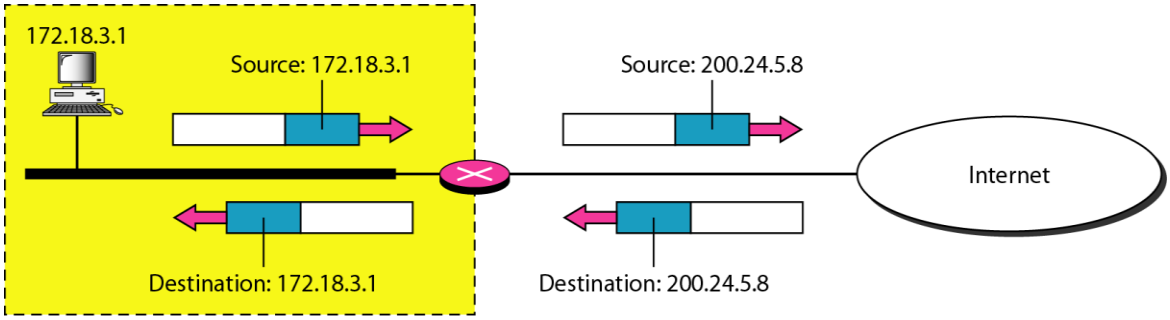
| Range | | | Total |
|---|---|---|---|
| 10.0.0.0 | to | 10.255.255.255 | $2^{24}$ |
| 172.16.0.0 | to | 172.31.255.255 | $2^{20}$ |
| 192.168.0.0 | to | 192.168.255.255 | $2^{16}$ |

Below figure shows , the private network uses private addresses. The router that connects the network to the global address and one global address. The private network is transparent to the rest of the internet ; the rest of the Internet sees only the NAT router with the address 200.24.5.8




*a) Address Translation:*

All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address. All the incoming packets also pass through the NAT router, which replaces the destination address in the packet.




**Q) Explain IPV6 Addressing in Network layer.**

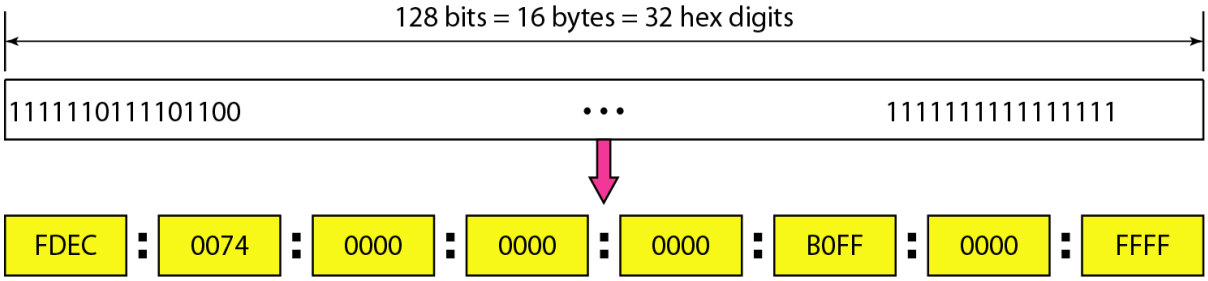
Despite all short-term solutions, address depletion is still a long-term problem for the Internet. This and other problems in the IP protocol itself have been the motivation for IPv6

i) **Structure:**

An IPV6 address consists of 16 bytes (octets); An IPv6 address is 128 bits long.

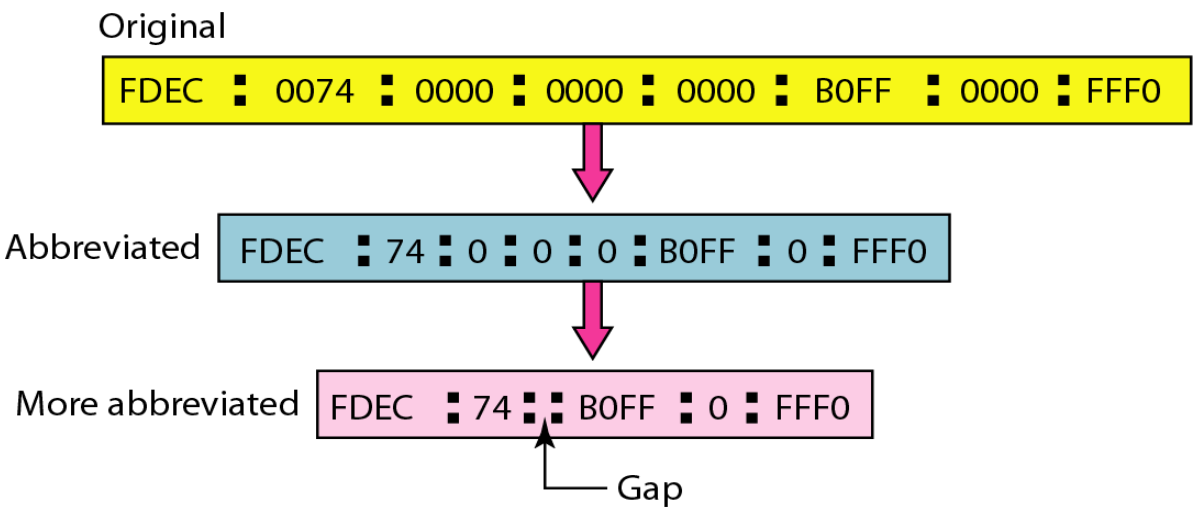
*a) Hexa decimal colon notation:*

In this notation , 128 bits is divided into eight sections, each 2 bytes in length. two bytes in hexa decimal notation requires 4 hexadecimal digits.so the address consist of 32 hexadecimal digits,with every 4 digits separted by colon.




b) **Abbreviation:**

The IP address is very long, many of the digits are zeros. In this case, we can abbreviate the address. the leading zeros can be omitted.



**ii) Address Space:**

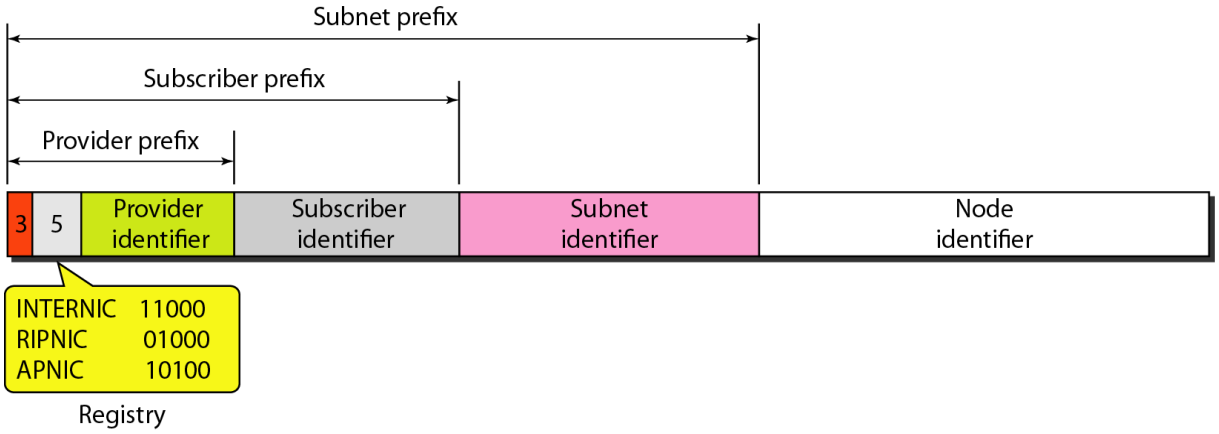
IPv6 has large address space;$2^{128}$ addresses are available. IPv6 addresses are divided into several categories. A few left most bits, called the *Type prefix*, in each address defines its category. The *Type prefix* is a variable length, but it is designed such that no code is identical to the first part of any other code.the third column shows *Fraction of each type of* address relative to the whole address space.

| *Type Prefix* | *Type* | *Fraction* |
|---|---|---|
| 0000 0000 | Reserved | 1/256 |
| 0000 0001 | Unassigned | 1/256 |
| 0000 001 | ISO network addresses | 1/128 |
| 0000 010 | IPX (Novell) network addresses | 1/128 |
| 0000 011 | Unassigned | 1/128 |
| 0000 1 | Unassigned | 1/32 |
| 0001 | Reserved | 1/16 |
| 001 | Reserved | 1/8 |
| **010** | **Provider-based unicast addresses** | **1/8** |

**a) Unicast address:**

Unicast address defines a single computer. IPV6 defines two types of unicast addresses: geographically based and provider- based. The First type is left for future definition. The provider based address is generally used by normal host

as a unicast address.




Fields

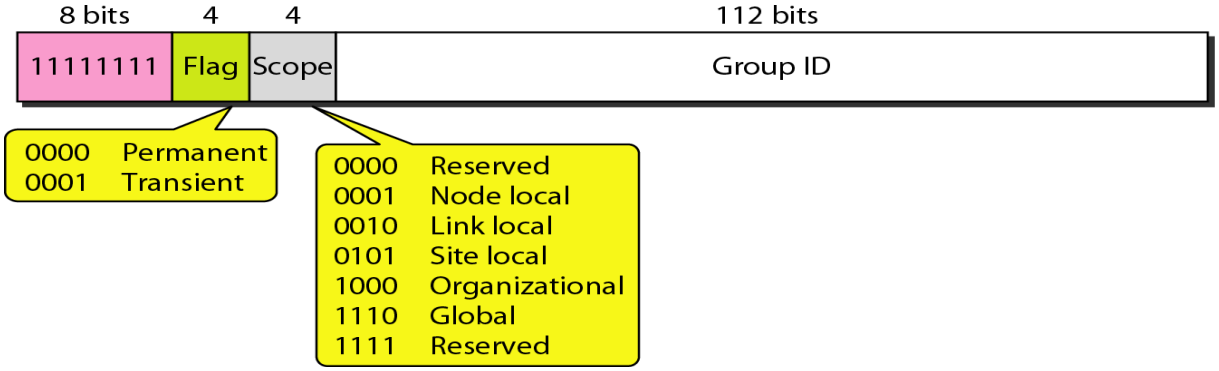
- Type identifier: this is a 3 bit field defines address as provider based address.
- Registry identifier: this is 5-bit field indicated the agency that has registered as address.
- Provider identifier: this variable length field identifies the provider for the internet

access

- Subscriber identifier: when an organization subscribes to the Internet through a provider, it is assigned a subscriber identifier
- Node identifier: defines the identity of the node connected to the subnet.

**b) Multicast addresses:**

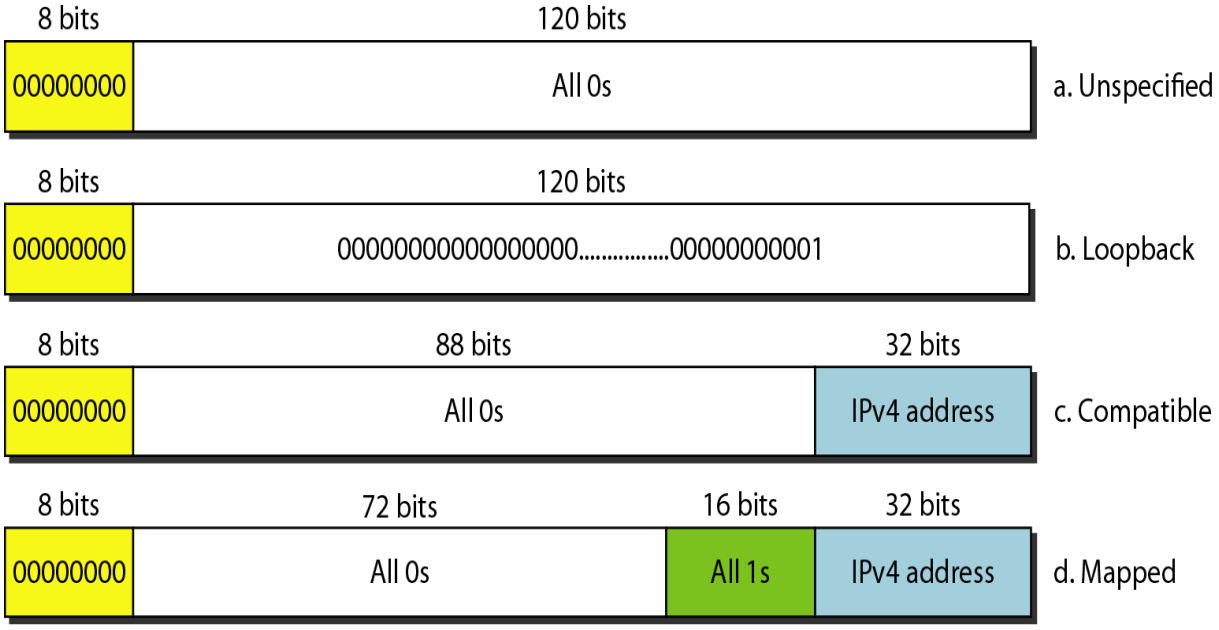
Multicast addresses are used to define a group of hosts instead of just one.A packet sent to a multicast address must be delivered to each member of the group.




The second field is a flag that defined the group address as either permanent or transient A **permanent group** address is defined by the internet authorities and can be accessed at all times. A **transient** is used only temporarily .The third field defines the scope of the group address

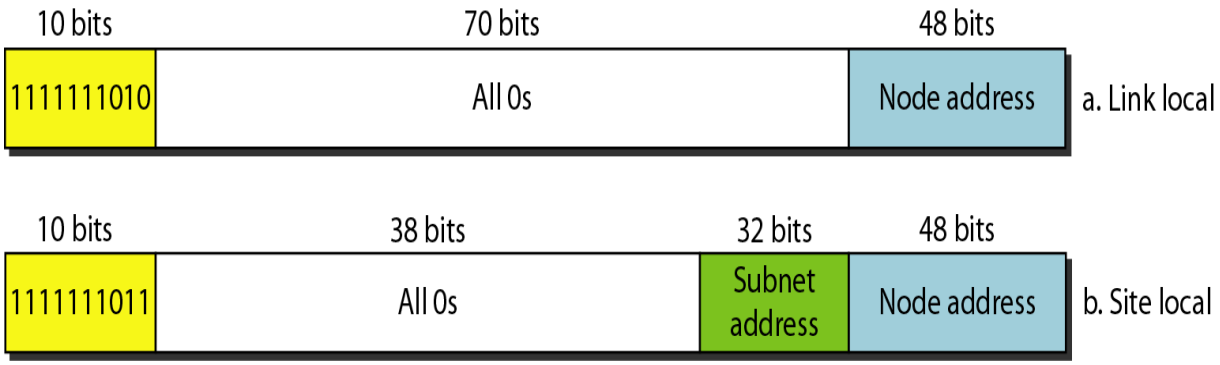
**c) Reserved Addresses:**

These addresses start with eight 0s




**d) Local Addresses:**

These addresses are used when an organiation wants to use IPV6 protocol without Being connected to the global internet.




A link local address is used in an isolated subnet; a site local address is used in an Isolated site wit several subnets.

**Q).Explain Address Mapping in Network Layer.**

The delivery of a packet to a host or a router requires two levels of addressing: logical and physical. We need to be able to map a logical address to its corresponding physical address and vice versa. This can be done by using either static or dynamic mapping.

A Physical address is a local address, it is unique locally. An example of physical address is 48-bit MAC address in the Ethernet protocol. The physical address and logical address are two different identifiers. We need to able to map a logical address to its corresponding physical address and vice versa.This can be done either static or dynamic mapping

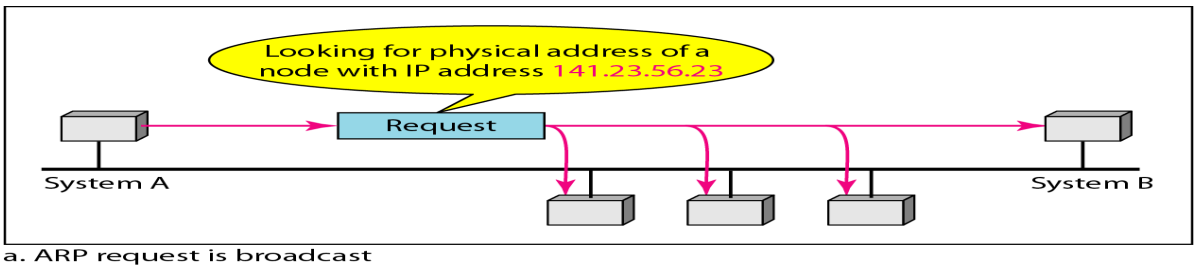
*Static mapping* involves in the creation of a table that associates a logical address with a physical address. This table is stored in each machine on the network.If changes are there, then static table must be updated periodically

In *Dynamic mapping* each time a machine knows one of the two addresses , it can use a protocol to find the other one.

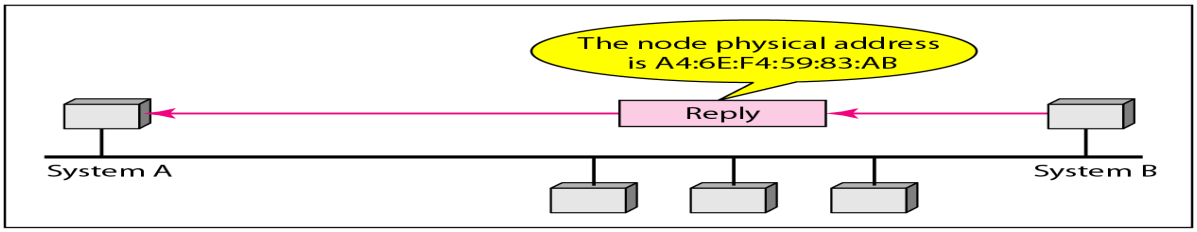
**i) Mapping logical to physical addresses: ARP**

When sender needs to send a packet , he has to know the physical address of the receiver. The host or router sends an ARP query packet. The packet includes the physical and IP address of the sender and the IP of the receiver, the query is broadcast.

- Every host or router receives and process the ARP query packet, but the intended recipient recognizes its IP address and send back an ARP response ,which is unicast.



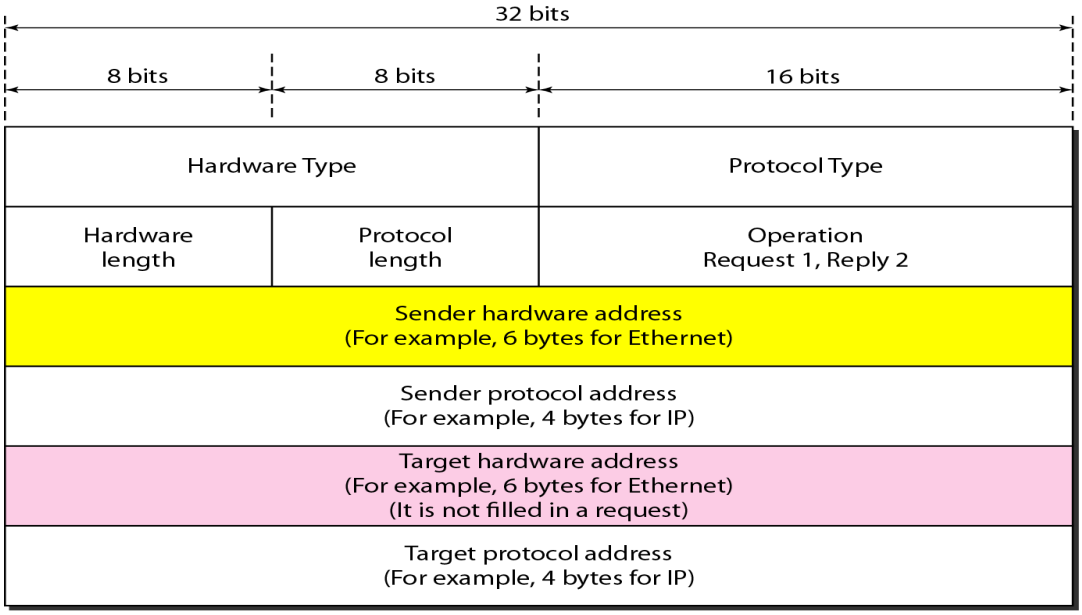

a. ARP request is broadcast




b. ARP reply is unicast

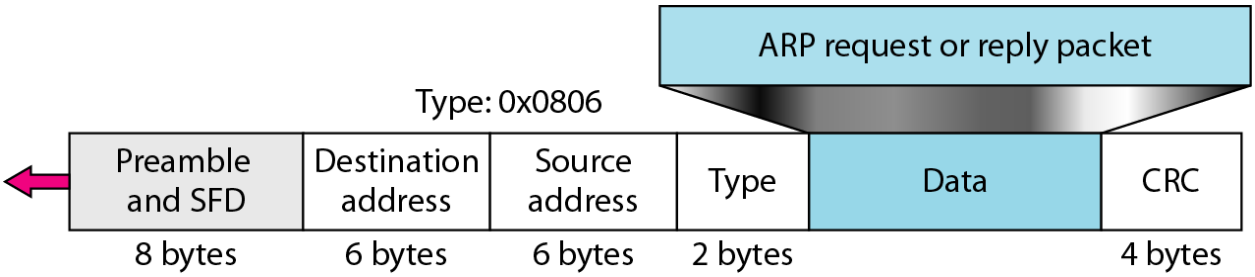
*Packet Format :* the fields are as follows:

- Hardware type: this is a 16 bit field defining type of network on which ARP is running.
- Protocol type: this is a 16 bit field defining the protocol.
- Hardware length: this is an 8 bit field defining the length of the physical address in bytes.
- Protocol length: this is 8 bit field defining the logical address in byte.
- Operation: this is a 16 bit field defining the type of packet , either request or reply
- Sender hardware address : defining the physical address of the sender
- Sender protocol address : defining the logical address of the sender
- Target hardware address: defining the physical address of the target.
- Target protocol address: defining the logical address of the target.



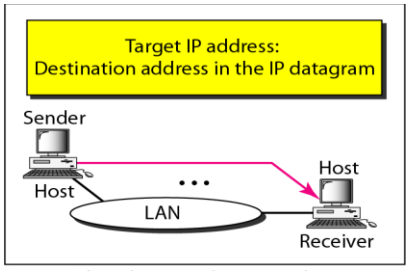
***Encapsulation:***

An ARP packet is encapsulated directly into a data link frame.

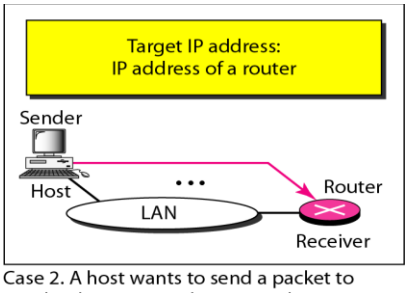



**Four different cases:**

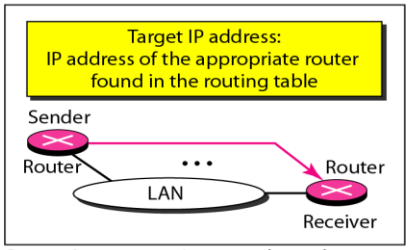
- Case 1: the logical address that must be mapped to a physical address is the destination IP address in the datagram header.
- Case 2: the host looks at its routing table and finds the IP address of the next hop for this destination.
- Case 3: the sender is a router and the receiver is also router
- Case 4: the sender is a router and the receiver is a host



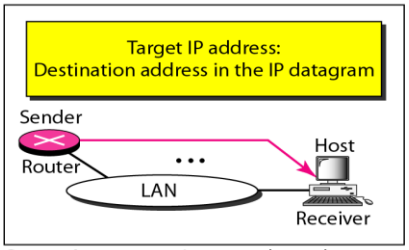

Case 1. A host has a packet to send to another host on the same network.




Case 2. A host wants to send a packet to another host on another network. It must first be delivered to a router.




Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.



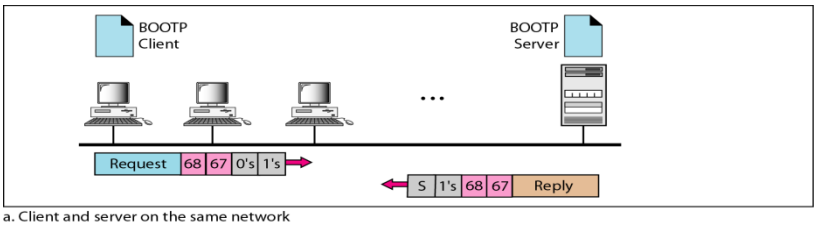

Case 4. A router receives a packet to be sent to a host on the same network.

### ii) Mapping physical to logical Address: RARP, BOOTP and DHCP

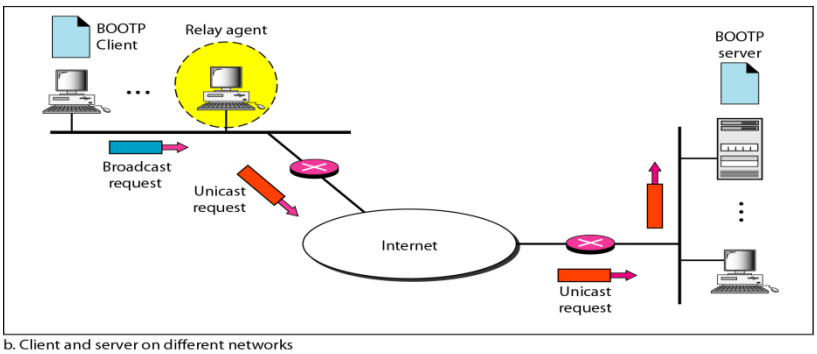
**RARP(Reverse Address Resolution Protocol)** find the logical address for a machine that knows only its physical address.A RARP request is created and broadcast on the local network another machine on the local network knows all the IP addresses will respond with a RARP reply.The requesting machine must be running RARP client program,the responding machine must be running RARP server Program

**Bootstrap Protocol(BOOTP)**

Is a client/server protocol designed to provide physical and logical address mapping. The administrator may put the client and the server on the same network or on different networks. BOOTP messages are encapsulated in a UDP packet and the UDP itself is encapsulated in an IP Packet




a. Client and server on the same network




b. Client and server on different networks

**DHCP**

The Dynamic Host Configuration Protocol (DHCP) provides static and dynamic address allocation that can be manual or automatic.

## Q). Explain ICMP in detail.

The IP protocol has no error-reporting or error-correcting mechanism. The IP protocol also lacks a mechanism for host and management queries. The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol

i) **Types of Messages**

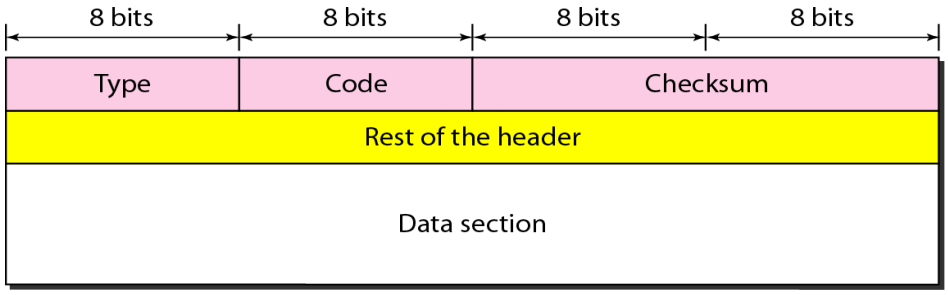
**ICMP** messages are divided into two broad categories: Error –reporting messages and query messages.

The Error Reporting Message report problems that a router or host may encounter when it processes an IP packet.

The Query Message help a host or network manager get specific information from router or another host.

ii) **Message Format**

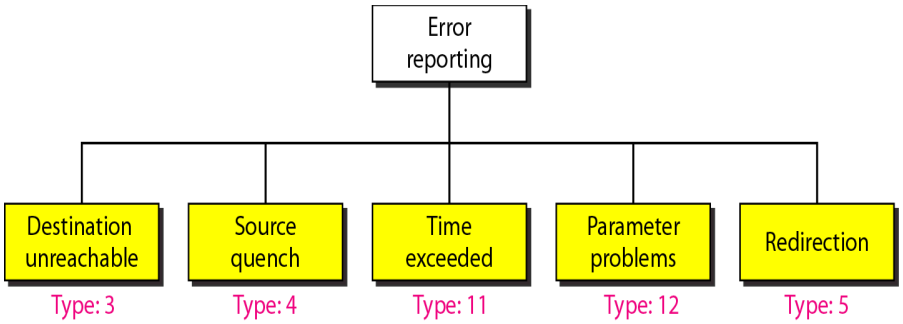
An ICMP message has a 8 byte header and a variable size data section. the first 4 bytes is common to all.




- type: defines the type of message
- code: specifies reason for the particular messages
- checksum for error detection
- Rest of the header: specific for each message
- Data section: carries information for finding the original packet that had the error

iii) **Error Reporting**

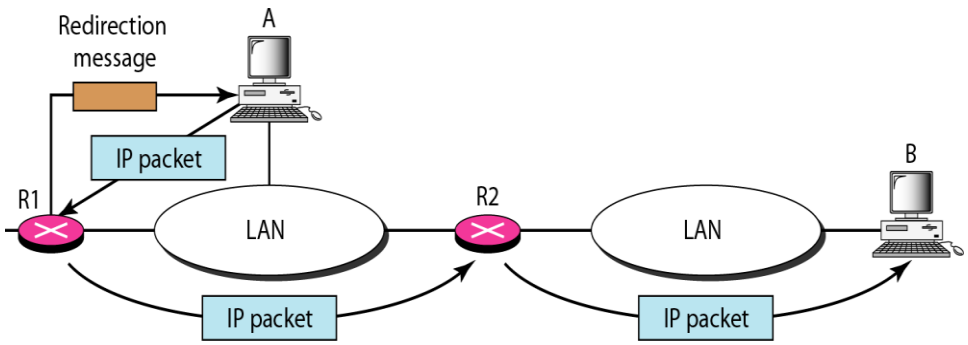
ICMP does not correct errors it simply report them.Error msg are always send to the original source.ICMP uses source IP address to send the error message to the source of the datagram.




- *Destination Unreachable*: sent when a router or host cannot deliver a datagram.
- *Source Quench*: this message was designed to add a kind of flow control to the IP.
- *Time Exceeded*: this message was generated in two cases.

  ->when *time to live* value reaches 0

  ->when not all fragment arrive at the destination host with in a certain time limit.
- *parameter Problem*: if a router or host discovers an ambiguous or missing value .
- *Redirection*: to update the routing table of the host, it sends a redirection msg to host.

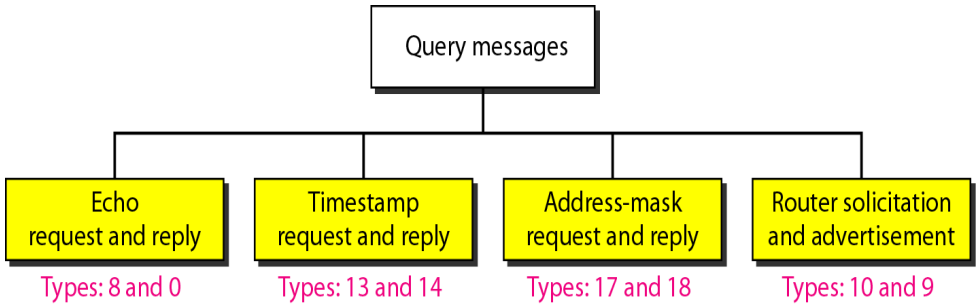



***Important points about ICMP error messages:***

- ❑ No ICMP error message will be generated in response to a datagram carrying an ICMP error message.
- ❑ No ICMP error message will be generated for a fragmented datagram that is not the first fragment.
- ❑ No ICMP error message will be generated for a datagram having a multicast address.
- ❑ No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

iv) **Query**

To diagnose some network problems, ICMP uses Query Messages.ICM uses four different pairs of messages .In this type, a node sends a msg that is answered in a specific format by the destination node.




- *Echo Request and Reply:* the echo request and reply messages can be used to determines whether two systems can communicate with each other
- *Timestamp request and reply:* two machines can use the timestamp request and reply to determine the round trip time needed for an IP datagram to travel between them.
- *Address mask request and reply:* when host or router needs to know mask ,then they use this message

- *Router solicitation and advertisement:* Router solicitation advertisement are used in redirection msg.

A query message is encapsulated in a data link layer frame.


**Q).Explain IGMP protocol in Network layer.**

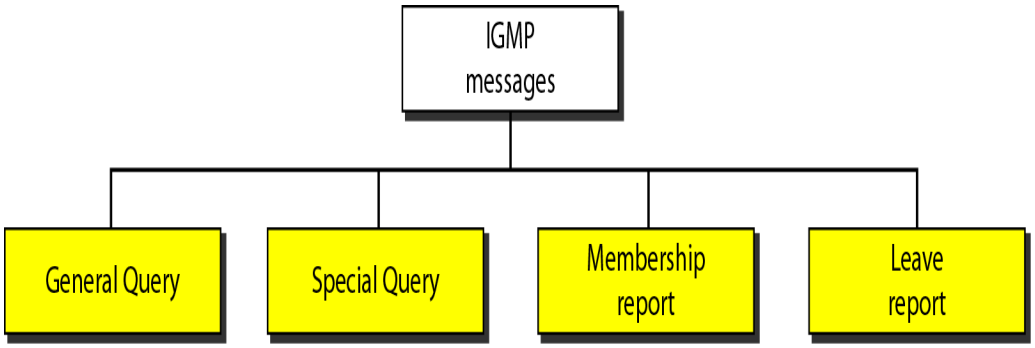
The IP protocol can be involved in two types of communication: unicasting and multicasting. The Internet Group Management Protocol (IGMP) is one of the necessary, but not sufficient, protocols that is involved in multicasting. IGMP is a companion to the IP protocol.

**i) Group Management**

- IGMP is a protocol that manages group management.
- IGMP protocol gives the multicast routers information about the membership status of host.
- A multicast router may receive thousands of multicast packets. If a router has no knowledge about the membership status of host, it broadcast all these packets, which creates traffic. IGMP helps the multicast router create and update this list.

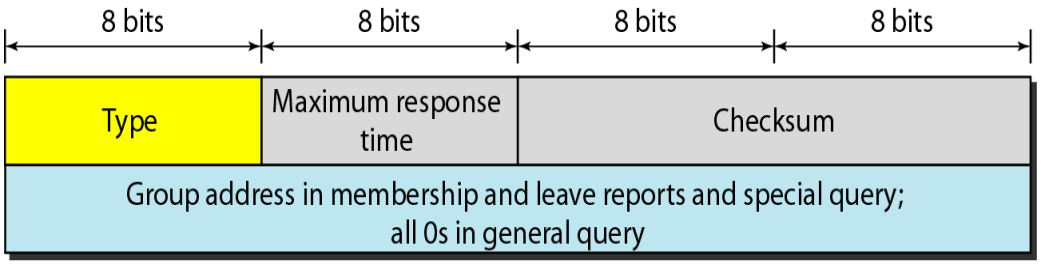
**ii) IGMP Messages**

IGMP has gone through two version. we discuss IGMPv2, the current version. IGMPv2 has three types of messages: the *query*, the *membership report* and *leave report*. There are two types of *query messages: general and special*.




**iii) IGMP Message Format**

Below fig shows the format of an IGMPv2 message




*Type*: this 8-bit field defines the type of message. The value of the type is shown in both hexadecimal and binary notation.

| *Type* | *Value* |
|---|---|
| General or special query | 0x11 or 00010001 |
| Membership report | 0x16 or 00010110 |
| Leave report | 0x17 or 00010111 |

*Maximum response time*: this 8-bit defines the amount of time in which a query must be answered.

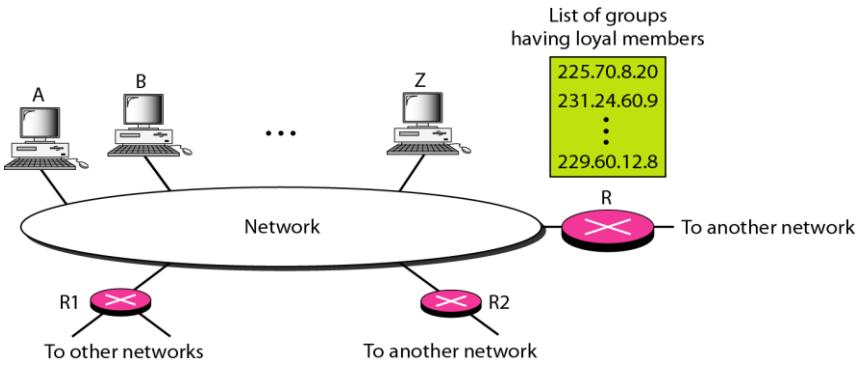
*Checksum*: this is a 16-bit field carrying checksum. The checksum is calculated over the 8-byte message.

*Group address*: the value of this field is 0 for general query messages. The value group id in the special query, membership report and leave report

**iv) IGMP Operation**

IGMP operates locally, a multicast router connected to a network has a list of multicast addresses of the group. When a host has membership, it means that it receives packets from some group.

Eg: in below fig router R is Distributing router. There are two other multicast routersR1 and R2 that depending on the group list maintained by R, could be recipients of router R in this network. Routers R1 and R2 may be distributors for some of these groups in other neworks, but not on this network



*Joining the Group:*

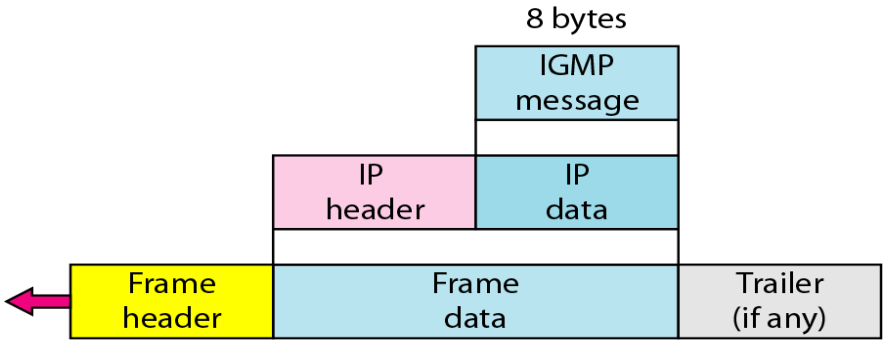
A host or router can join a group. A host maintains a list of processes that have membership in a group. When a process wants to join a new group, it sends its request to the host. The host adds the name of the process and the name of the requested group to its list

*Leaving the group:*

When a host sees that no process is interested in a specific group , it sends a leave report

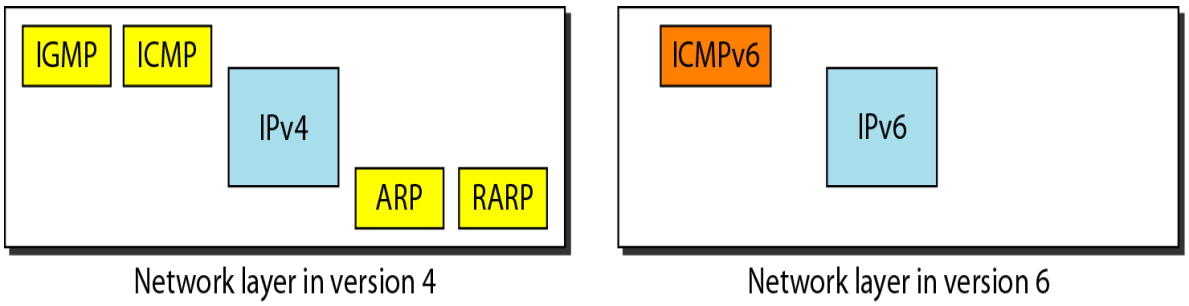
**v) Encapsulation**

IGMP message is encapsulated in an IP datagram, which is itself encapsulated in a frame.




**Q).Write a Short notes on ICMPV6 Protocol .**

Another protocol that has been modified in version 6 of the TCP/IP protocol suite is ICMP (ICMPv6). This new version follows the same strategy and purposes of version 4.




The ARP and IGMP protocols in version4 are combined in IGMPv6. The RARP protocol is dropped from the suite because it was rarely used and BOOTP has the same functionality

**i) Error Reporting**

ICMPV6 forms an error packet, which is then encapsulated in an IP datagram.

| *Type of Message* | *Version 4* | *Version 6* |
|---|---|---|
| Destination unreachable | Yes | Yes |
| Source quench | Yes | No |
| Packet too big | No | Yes |
| Time exceeded | Yes | Yes |
| Parameter problem | Yes | Yes |
| Redirection | Yes | Yes |

- *Destination Unreachable*: sent when a router or host cannot deliver a datagram.
- *Source Quench*: this message was designed to add a kind of flow control to the IP.
- *Packet too big*: if datagram size large than maximum transmission unit(MTU), then this msg was sent.
- *Time Exceeded*: this message was generated in two cases.

  ->when *time to live* value reaches 0

  ->when not all fragment arrive at the destination host with in a certain time limit.
- *parameter Problem*: if a router or host discovers an ambiguous or missing value .
- *Redirection*: to update the routing table of the host, it sends a redirection msg to host.

**ii) Query:**

Two set of query messages are eliminated from ICMPv6: timestamp request and reply and address mask request and reply, remaining are same as ICMP.

***Comparison of query messages in ICMPv4 and ICMPv6***

| *Type of Message* | *Version 4* | *Version 6* |
|---|---|---|
| Echo request and reply | Yes | Yes |
| Timestamp request and reply | Yes | No |
| Address-mask request and reply | Yes | No |
| Router solicitation and advertisement | Yes | Yes |
| Neighbor solicitation and advertisement | ARP | Yes |
| Group membership | IGMP | Yes |

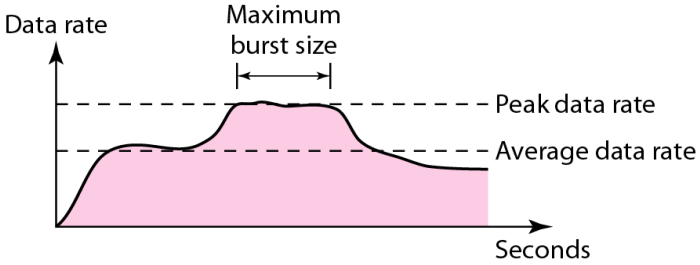
Congestion Control and Quality of Service

## Q).Write a short notes on Data Traffic.

The main focus of congestion control and quality of service is data traffic. In congestion control we try to avoid traffic congestion. In quality of service, we try to create an appropriate environment for the traffic. So, before talking about congestion control and quality of service, we discuss the data traffic itself.

i) **Traffic Descriptor**

Traffic Descriptors are qualitative values that represent a data flow.

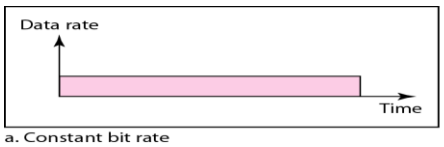



- ➔ Average Data Rate
- ➔ Peak Data Rate
- ➔ Maximum Burst size
- ➔ Effective bandwidth

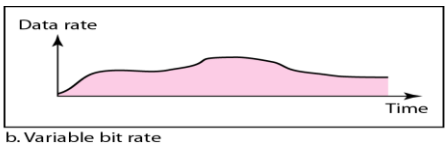
**ii) Traffic Profiles**

A data flow can have one of the following traffic profiles.

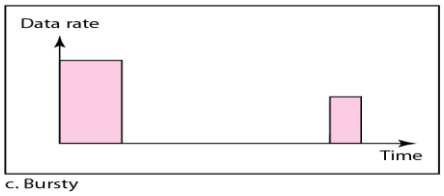
- ➔ Constant bit rate
- ➔ Variable bit rate
- ➔ Burst



a. Constant bit rate



b. Variable bit rate

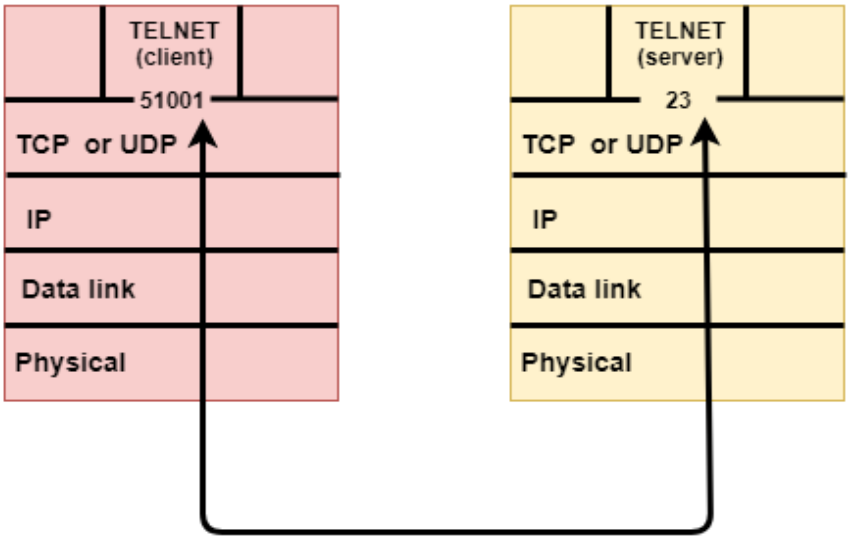


c. Bursty

# UNIT-IV

## Transport Layer protocols

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

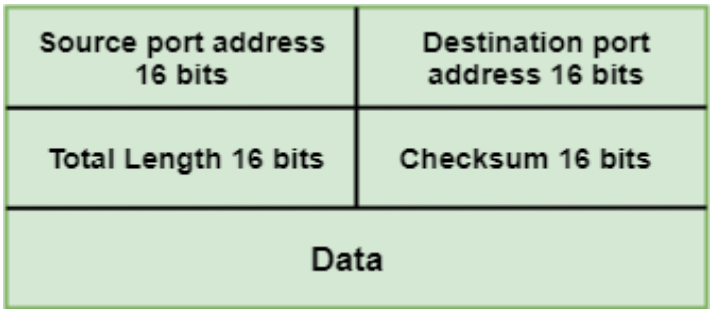



## UDP

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

## User Datagram Format

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




**Where,**

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

## Disadvantages of UDP protocol

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

## TCP

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

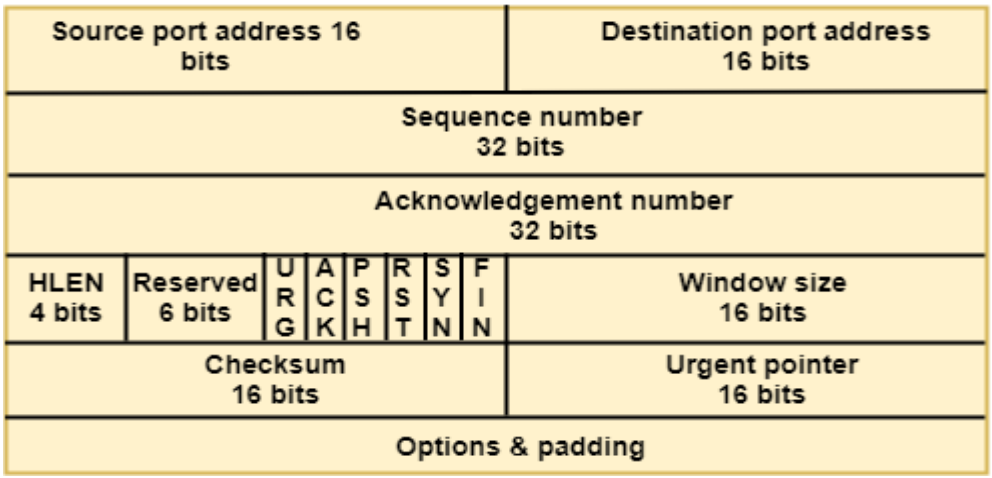
## Features Of TCP protocol

- **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
- **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.

The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.

- **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
- **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
- **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
- **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
  - Establish a connection between two TCPs.
  - Data is exchanged in both the directions.
  - The Connection is terminated.

## TCP Segment Format




**Where,**

- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.

- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.
- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
- **Reserved:** It is a six-bit field which is reserved for future use.
- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

**APPLICATION LAYAR-WORLD WIDE WEB**

## HTTP

- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

## Features of HTTP:

- **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after

which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.

- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages

## Uniform Resource Locator (URL)

- A client that wants to access the document in an internet needs an address and to facilitate the access of documents, the HTTP uses the concept of Uniform Resource Locator (URL).
- The Uniform Resource Locator (URL) is a standard way of specifying any kind of information on the internet.
- The URL defines four parts: method, host computer, port, and path.


- **Method:** The method is the protocol used to retrieve the document from a server. For example, HTTP.
- **Host:** The host is the computer where the information is stored, and the computer is given an alias name. Web pages are mainly stored in the computers and the computers are given an alias name that begins with the characters "www". This field is not mandatory.
- **Port:** The URL can also contain the port number of the server, but it's an optional field. If the port number is included, then it must come between the host and path and it should be separated from the host by a colon.
- **Path:** Path is the pathname of the file where the information is stored. The path itself contain slashes that separate the directories from the subdirectories and files.

## FTP

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

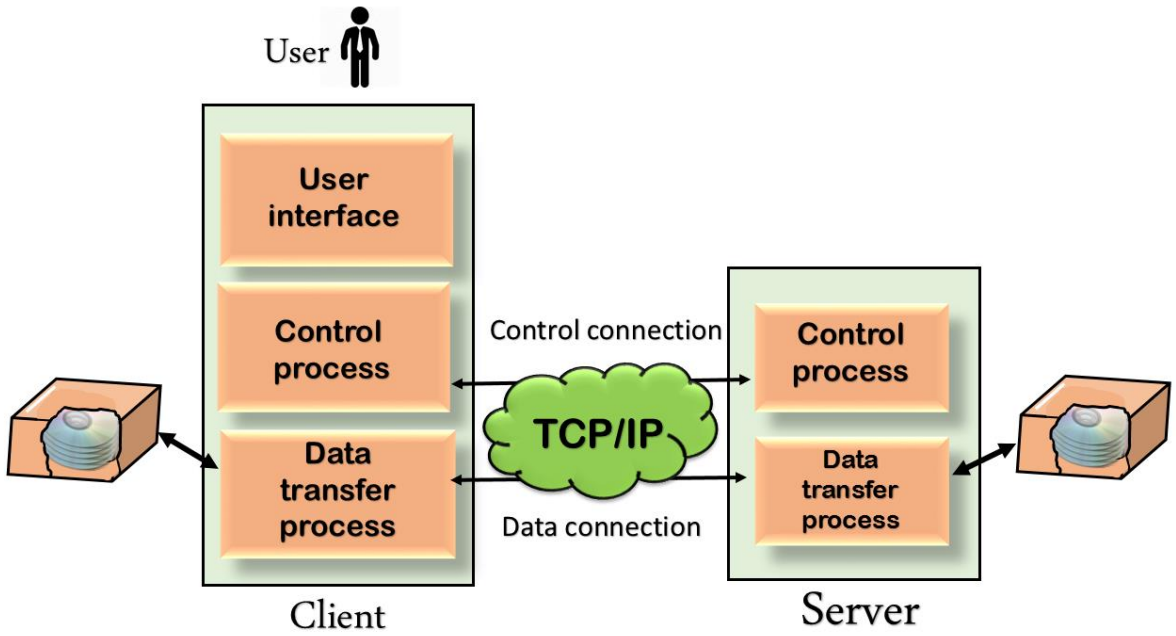
## Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

## Why FTP?

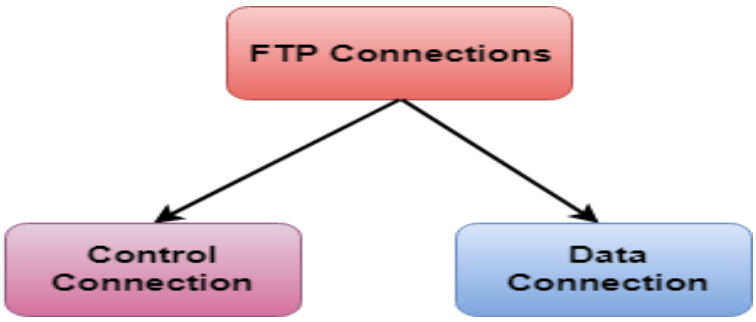
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

## Mechanism of FTP




The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

**There are two types of connections in FTP:**




- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

## FTP Clients

- FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.
- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

## Advantages of FTP:

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

### Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

### Email Architecture and Services

An e-mail system includes two subsystems as under:

- User agents
- Message transfer agents

**User agents**

They allow people to read message transfer agents.

They transfer the messages from the source to the destination.

**Basic Functions**

The E-mail system supports five basic systems, which are as follows:

**Composition**

The process of generating messages and answering them is called composition. The system can also support assistance with addressing and several header fields attached to each message.

**Transfer**

It is the process of moving messages from the sender to the recipient. This includes establishing a connection from the sender to a destination or some intermediate machine, outputting the message and releasing the connection.

**Reporting**

This is to tell the sender whether the message was delivered or rejected, or lost.

**Displaying**

It is the process of displaying incoming messages. For this purpose, simple conversation and formatting are required to be done.

**Disposition**

This is concerned with what the recipient does with the messages after receiving them. Some of the possibilities are as follows –

- Throw after reading
- Throw before reading
- Save messages
- Forward messages
- Process messages in some other way

**Advanced Features**

Some of the advanced features of Email Systems included in addition to the essential functions are as follows −

- It can be forwarding an email to a person away from his computer.
- It can create and destroy mailboxes to store incoming e-mail.
- It can inspect the contents of the mailbox, insert and delete messages from the mailboxes.
- It can send a message to a vast group of people using the mail list idea.
- It is used to provide a registered email.
- It is used for automatic notification of undelivered email.
- It is used to carbon copies.
- It is used to high priority email.
- It can make an alternative recipient.

**Advantages of Email**

There are various advantages of email, which are as follows:

- It is a cost-effective service to transmit with others as there are various email services available to individuals and organizations for complimentary of cost. Once a customer is online, it does not contain any additional charge for the services.
- Email supports a simple user interface and allows users to categorize and filter their messages. This can help us to identify unwanted emails such as junk and spam mail.
- Emails are beneficial for broadcasting products. As email is a form of transmission, organizations can involve many people and inform them quickly.
- Email exchanges can be saved for future retrieval, which allows users to keep essential conversations or confirmations in their data and can be searched and retrieved when needed quickly.
- Emails are beneficial for advertising products. An email is a form of transmission. Organizations or companies can interact with many people and inform them in a short time.

**Telnet**

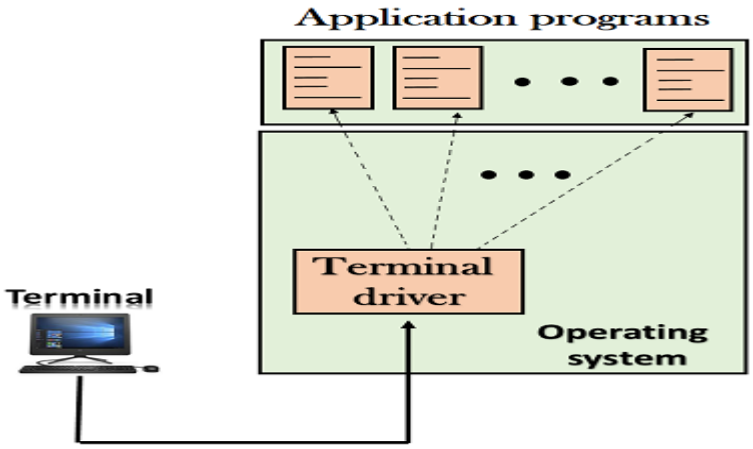
- The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program 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 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.

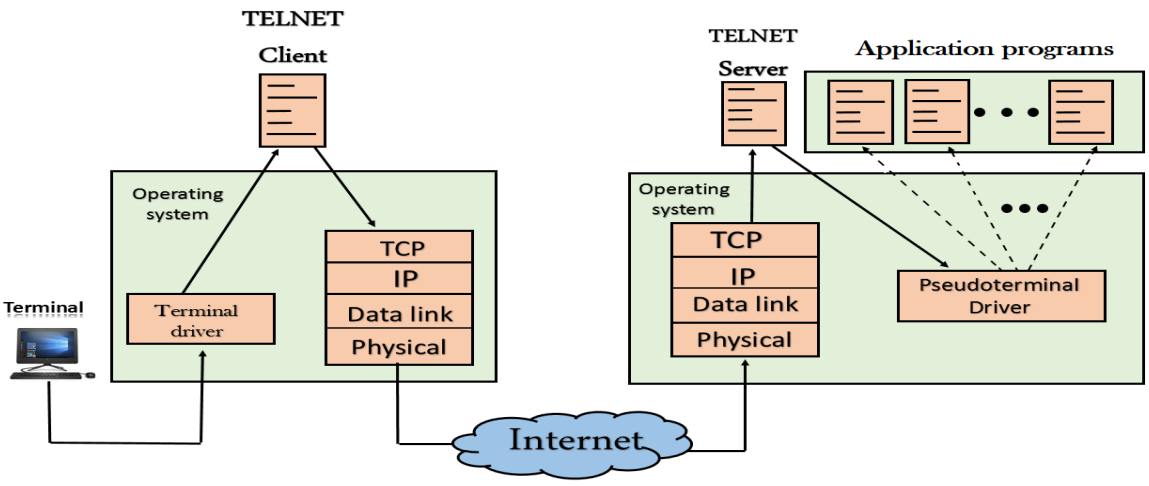
### There are two types of login:

#### 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.

#### Remote login:



### 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.

**Domain Name System**

DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

**Requirement**

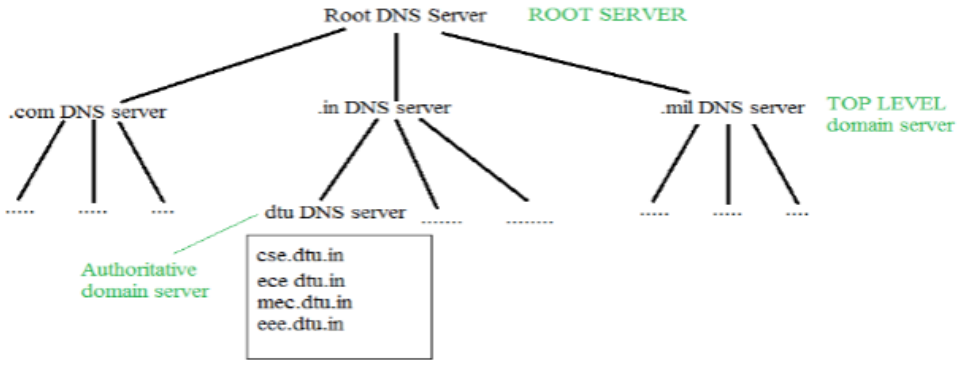
Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

**Domain :**

There are various kinds of DOMAIN :

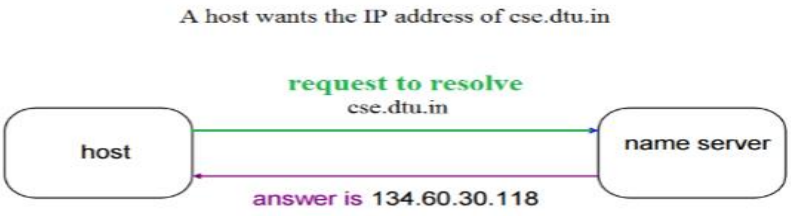
1. Generic domain : .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.
2. Country domain .in (india) .us .uk
3. Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping.So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup www.geeksforgeeks.org.

### Organization of Domain




It is Very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately,
there should not be a lot of delay for that to happen organization of database is very important.
**DNS record** – Domain name, ip address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.
**Namespace** – Set of possible names, flat or hierarchical . Naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value –
**Name server** – It is an implementation of the resolution mechanism.. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.

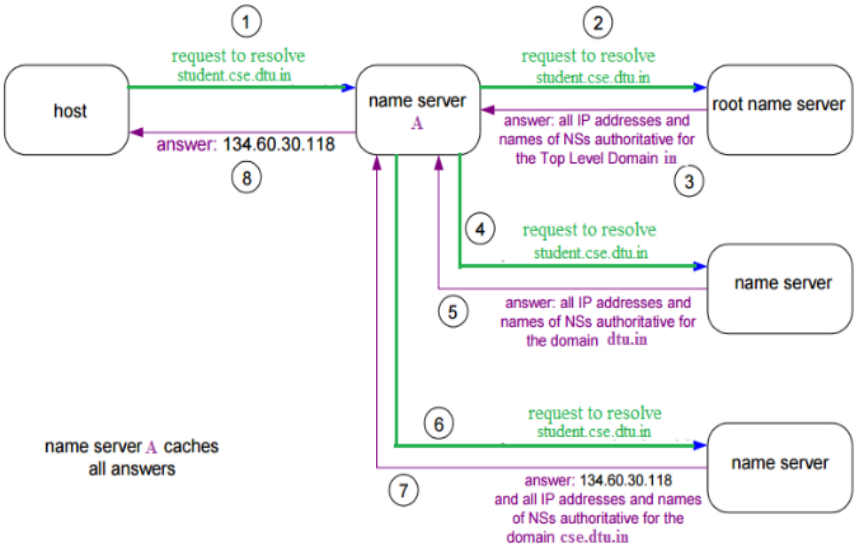
### Name to Address Resolution




The host request the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address

**Hierarchy of Name Servers**
**Root name servers** – It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.
**Top level server** – It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.

**Authoritative name servers** This is organization's DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative ip address.




The client machine sends a request to the local name server, which , if root does not find the address in its database, sends a request to the root name server , which in turn, will route the query to an intermediate or authoritative name server. The root name server can also contain some hostName to IP address mappings . The intermediate name server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.