1: A) Explain TCP/IP Architecture in detail.

:-TCP/IP Protocol Architecture

TCP/IP protocols map to a four-layer conceptual model known as the *DARPA model* , named after the U.S. government agency that initially developed TCP/IP. The four layers of the DARPA model are: Application, Transport, Internet, and Network Interface. Each layer in the DARPA model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) model.
Figure 1.1 shows the TCP/IP protocol architecture.

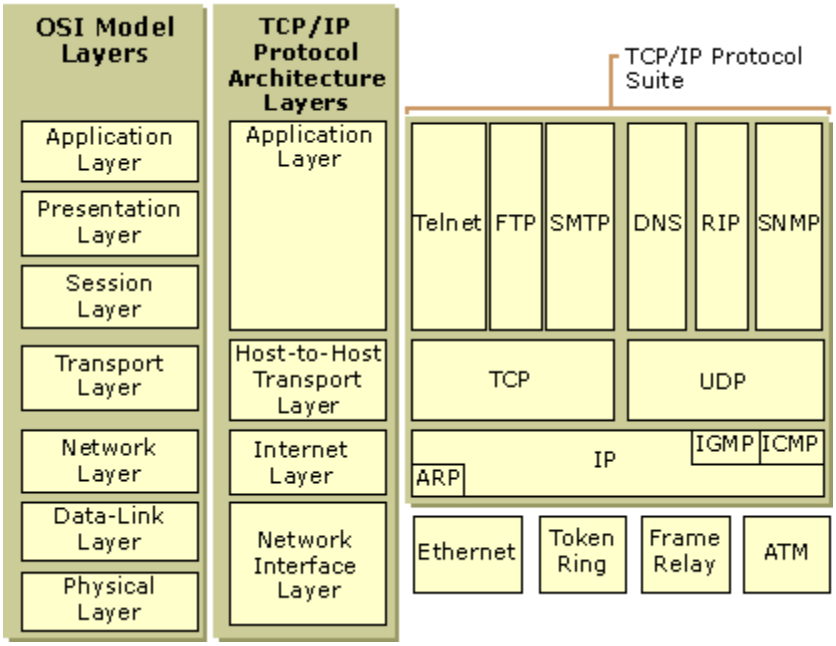


Figure 1.1 TCP/IP Protocol Architecture

Network Interface Layer

The *Network Interface layer* (also called the Network Access layer) is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect differing network types. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).

The Network Interface layer encompasses the Data Link and Physical layers of the OSI model. Note that the Internet layer does not take advantage of sequencing and acknowledgment services that might be present in the Data-Link layer. An unreliable Network Interface layer is assumed, and reliable communications through session establishment and the sequencing and acknowledgment of packets is the responsibility of the Transport layer.

Internet Layer

The *Internet layer* is responsible for addressing, packaging, and routing functions. The core protocols of the Internet layer are IP, ARP, ICMP, and IGMP.

- The *Internet Protocol* (IP) is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.
- The *Address Resolution Protocol* (ARP) is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.
- The *Internet Control Message Protocol* (ICMP) is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.
- The *Internet Group Management Protocol* (IGMP) is responsible for the management of IP multicast groups.

The Internet layer is analogous to the Network layer of the OSI model.

Transport Layer

The *Transport layer* (also known as the Host-to-Host Transport layer) is responsible for providing the Application layer with session and datagram communication services. The core protocols of the Transport layer are *Transmission Control Protocol* (TCP) and the *User Datagram Protocol* (UDP).

- TCP provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.
- UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet), when the overhead of establishing a TCP connection is not desired or when the applications or upper layer protocols provide reliable delivery.

The Transport layer encompasses the responsibilities of the OSI Transport layer and some of the responsibilities of the OSI Session layer.

Application Layer

The *Application layer* provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data. There are many Application layer protocols and new protocols are always being developed.

The most widely-known Application layer protocols are those used for the exchange of user information:

- The Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages of the World Wide Web.
- The File Transfer Protocol (FTP) is used for interactive file transfer.
- The Simple Mail Transfer Protocol (SMTP) is used for the transfer of mail messages and attachments.
- Telnet, a terminal emulation protocol, is used for logging on remotely to network hosts.

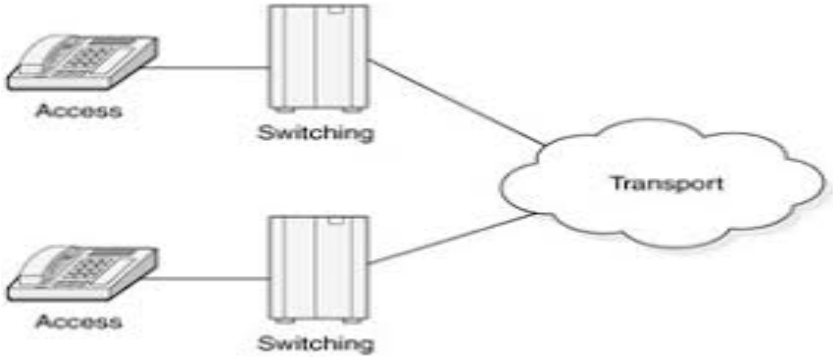
Additionally, the following Application layer protocols help facilitate the use and management of TCP/IP networks:

- The Domain Name System (DNS) is used to resolve a host name to an IP address.

- The Routing Information Protocol (RIP) is a routing protocol that routers use to exchange routing information on an IP internetwork.
- The Simple Network Management Protocol (SNMP) is used between a network management console and network devices (routers, bridges, intelligent hubs) to collect and exchange network management information.

Examples of Application layer interfaces for TCP/IP applications are Windows Sockets and NetBIOS. Windows Sockets provides a standard application programming interface (API) under Windows 2000. NetBIOS is an industry standard interface for accessing protocol services such as sessions, datagrams, and name resolution. More information on Windows Sockets and NetBIOS is provided later in this chapter.

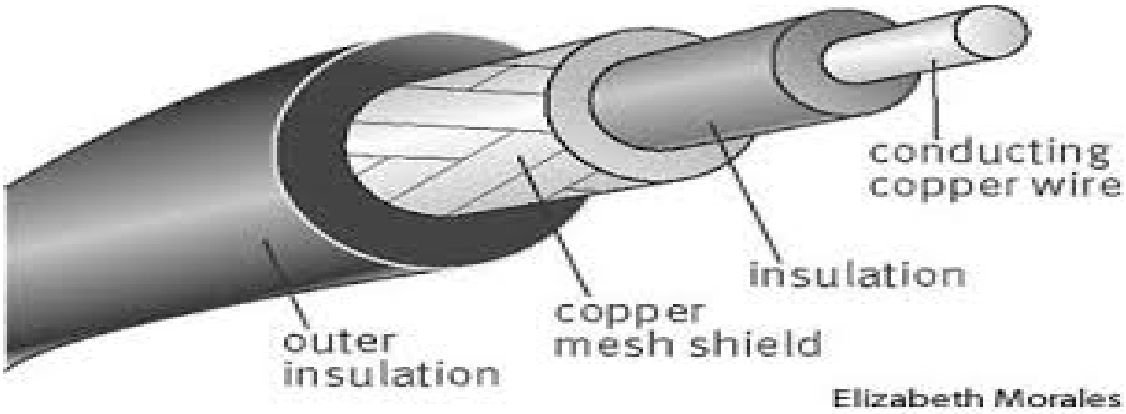
b) Write a note on telephone Network.



:- The earliest electronic network is the telephone system. This telephone network commonly uses analog technology that was quite different from digital technology used in the computer-based networks. The advantages of digital technology over the analog technology in terms of economics and services forced the telephone industry to move rapidly to install fiber and digital networks.

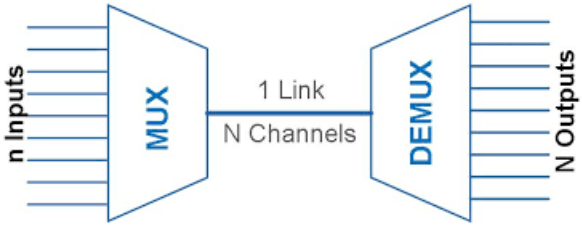
The telephone network transmits analogsignalsand hence a modem is required whenever a computer or terminal is connected to the telephone line. The modem then converts digital data from a computer to an analog signal that can be transmitted via a telecommunication line and converts the analog signal received to computer data.

c) Explain Coaxial Cable



Coaxial cable is a type of copper **cable** specially built with a metal shield and other components engineered to block signal interference. It is primarily used by **cable** TV companies to connect their satellite antenna facilities to customer homes and businesses.

2:A) What is multiplexing? Explain



I) FDM (Frequency Division Multiplexing)

II) TDM (Time Division Multiplexing)

:- In telecommunications and computer networks, **multiplexing** (sometimes contracted to **muxing**) is a method by which multiple analog or digital signals are combined into one signal over a shared medium. The aim is to share a scarce resource. For example, in telecommunications, several telephone calls may be carried using one wire

FDM (Frequency Division Multiplexing)

Figure 6.4 *FDM multiplexing process*

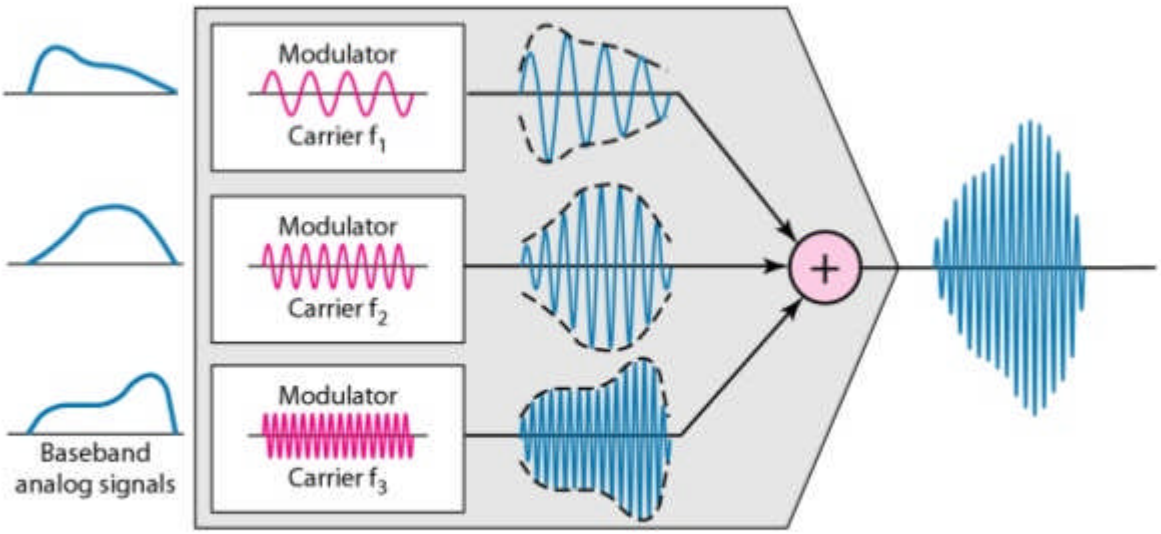
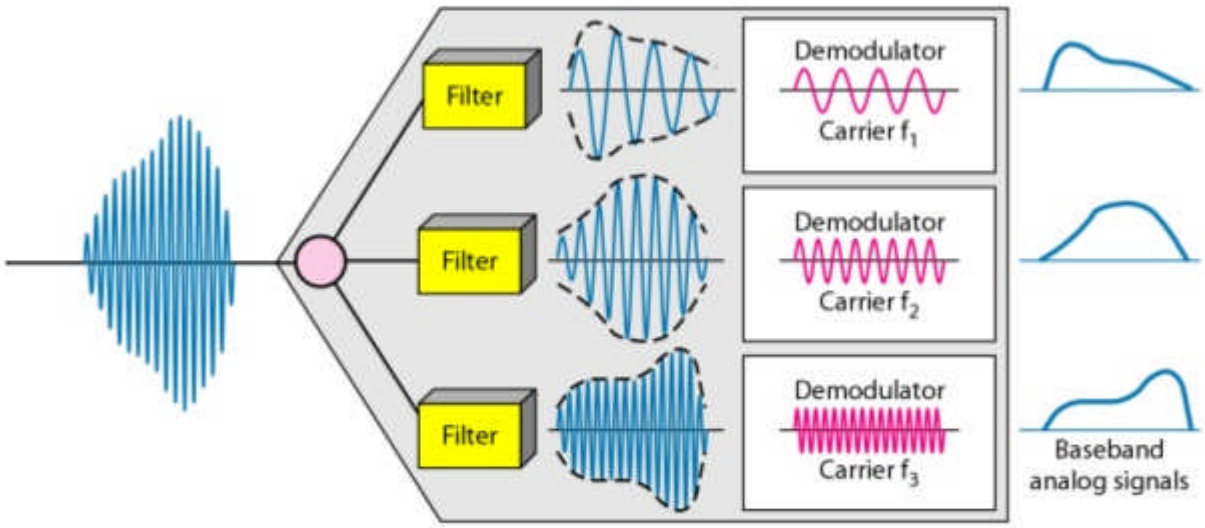
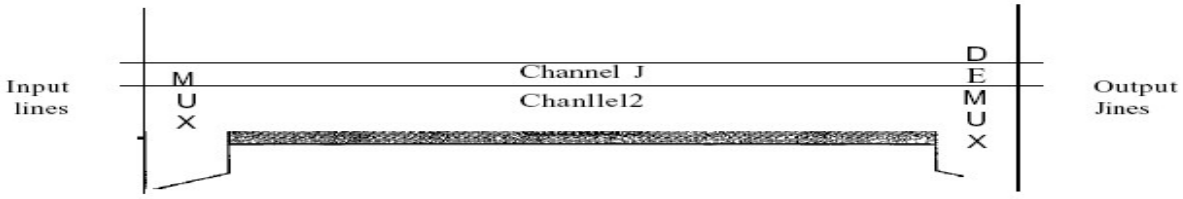


Figure 6.5 *FDM demultiplexing example*



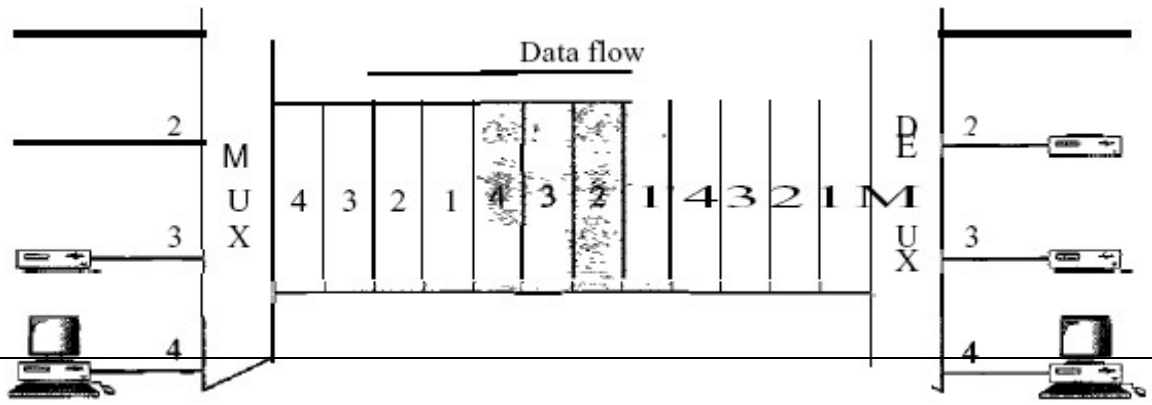
:- Frequency Division Multiplexing (FDM) is a networking technique in which multiple data signals are combined for simultaneous transmission via a shared communication medium. FDM uses a carrier signal at a discrete frequency for each data stream and then combines many modulated signals.

When FDM is used to allow multiple users to share a single physical communications medium (i.e. not broadcast through the air), the technology is called frequency-division



multiple access (FDM.

TDM (Time Division Multiplexing)



Time-division multiplexing (**TDM**) is a method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line so that each signal appears on the line only a fraction of time in an alternating pattern. It is used when the bit rate of the transmission medium exceeds that of the signal to be transmitted. This form of signal multiplexing was developed in telecommunications for telegraphy systems in the late 19th century, but found its most common application in digital telephony in the second half of the 20th century.

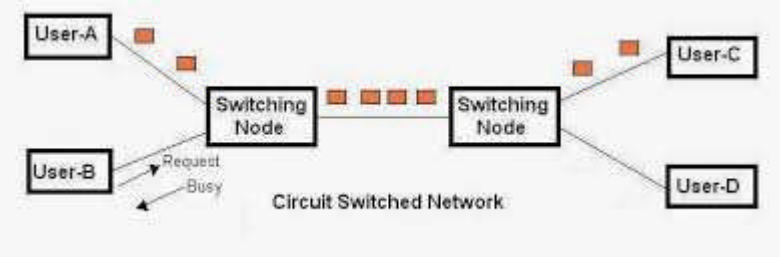
b) Define switching. Explain The Fallowing

i) Circuit switching.

ii) Packet Switching.

:- A **network switch** (also called **switching** hub, bridging hub, officially MAC bridge) is a **computer networking** device that connects devices together on a **computer network** by using packet **switching** to receive, process, and forward data to the destination device.

i) Circuit switching.

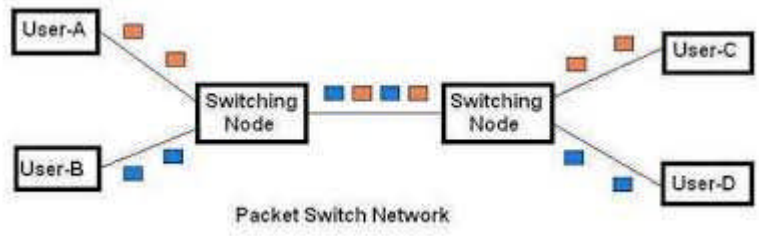


A type of communications in which a dedicated channel (or *circuit*) is established for the duration of a transmission. The most ubiquitous circuit-switching network is the telephone system, which links together wire segments to create a single unbroken line for each telephone call.

The other common communications method is packet switching, which divides messages into packets and sends each packet individually. The Internet is based on a packet-switching protocol, TCP/IP.

Circuit-switching systems are ideal for communications that require data to be transmitted in real-time. Packet-switching networks are more efficient if some amount of delay is acceptable**.**

ii) Packet Switching.



Packet switching is a method of grouping data which is transmitted over a digital network into packets which are made of a header and a payload. Data in the header is used by networking hardware to direct the packet to its destination where the payload is extracted and used by application software. Packet switching is the primary basis for data communications in computer networks worldwide.

Packet switching features delivery of variable bit rate data streams, realized as sequences of packets, over a computer network which allocates transmission resources as needed using statistical multiplexing or dynamic bandwidth allocation techniques. As they traverse network nodes, such as switches and routers, packets are received, buffered, queued, and transmitted (stored and forwarded), resulting in variable latency and throughput depending on the link capacity and the traffic load on the network.

3: A) What is Polynomial code? Explain CRC With Example.

> a **polynomial code** is a type of linear **code** whose set of valid **code** words consists of those **polynomials** (usually of some fixed length) that are divisible by a given fixed **polynomial** (of shorter length, called the generator **polynomial**).

:- A **cyclic redundancy check** (**CRC**) is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Blocks of data entering these systems get a short *check value* attached, based on the remainder of a polynomial division of their contents. On retrieval, the calculation is repeated and, in the event the check values do not match, corrective action can be taken against data corruption. CRCs can be used for error correction .

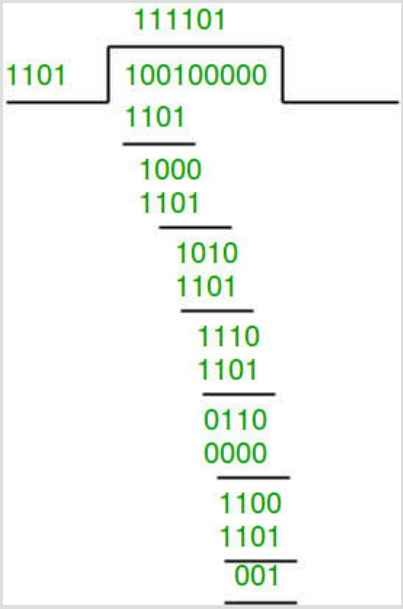
CRCs are so called because the *check* (data verification) value is a *redundancy* (it expands the message without adding information) and the algorithm is based on *cyclic* codes. CRCs are popular because they are simple to implement in binary hardware, easy to analyzemathematically, and particularly good at detecting common errors caused by noise in transmission channels. Because the check value has a fixed length, the function that generates it is occasionally used as a hash function.

Example 1 (No error in transmission):

Data word to be sent - 100100

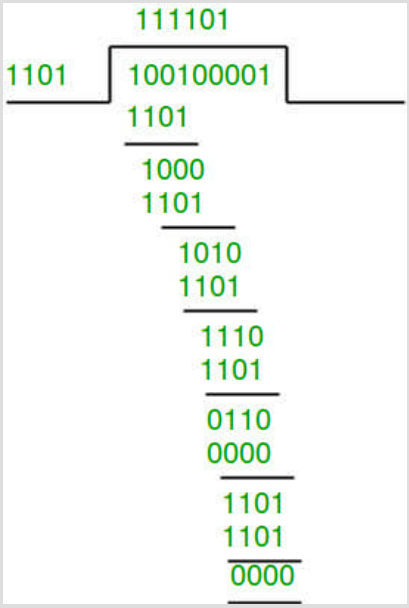
Key - 1101 [Or generator polynomial $x^3 + x + 1$]

Sender Side:



Therefore, the remainder is 001 and hence the encoded data sent is 100100001.

Receiver Side:
Code word received at the receiver side 100100001



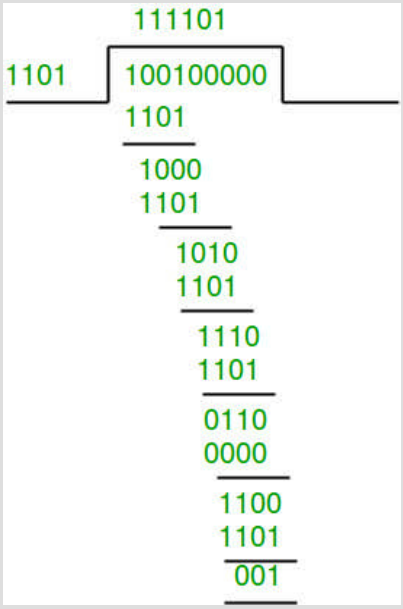
Therefore, the remainder is all zeros. Hence, the data received has no error.

Example 2: (Error in transmission)

Data word to be sent - 100100

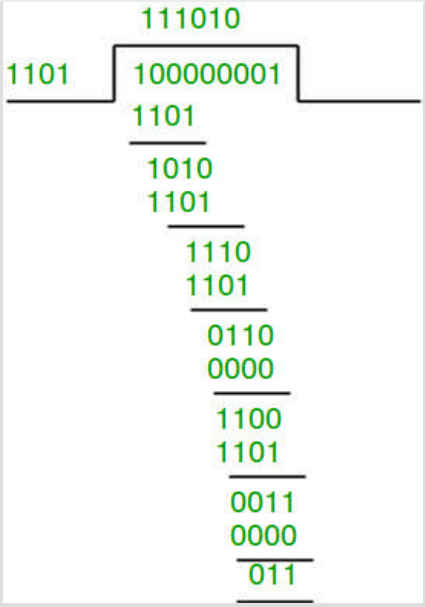
Key - 1101

Sender Side:



Therefore, the remainder is 001 and hence the code word sent is 100100001.

Receiver Side
Let there be error in transmission media
Code word received at the receiver side - 100000001



Since the remainder is not all zeroes, the error is detected at the receiver side.

b) Discuss The Concept of CSMA Protocols.

Ans: CSMA (Carrier Sense Multiple Access)

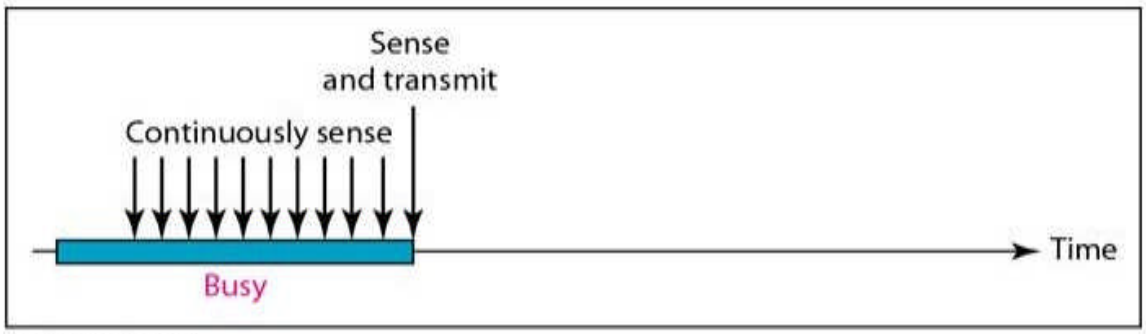
CSMA requires that each station first listen to the medium or check a state of a medium before sending. In other words CSMA is based on the principle sense before transmit or listen before talk.

CSMA can reduce possibility of collision but it can not eliminate it there are various ways in which carrier is sense (persistent method).

The 3 persistence methods are

1) I-persistence:

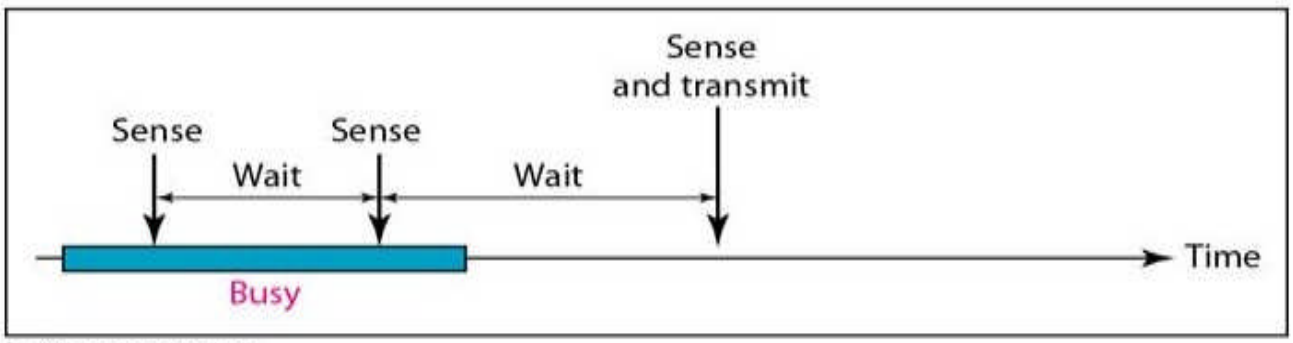
This method is simple and straight forward. In this method after the station finds line idle it sends his frame immediately this method has the highest chances of collision because two or more stations may find the line idle & send the frame immediately.



a. 1-persistent

2) Non-persistence:

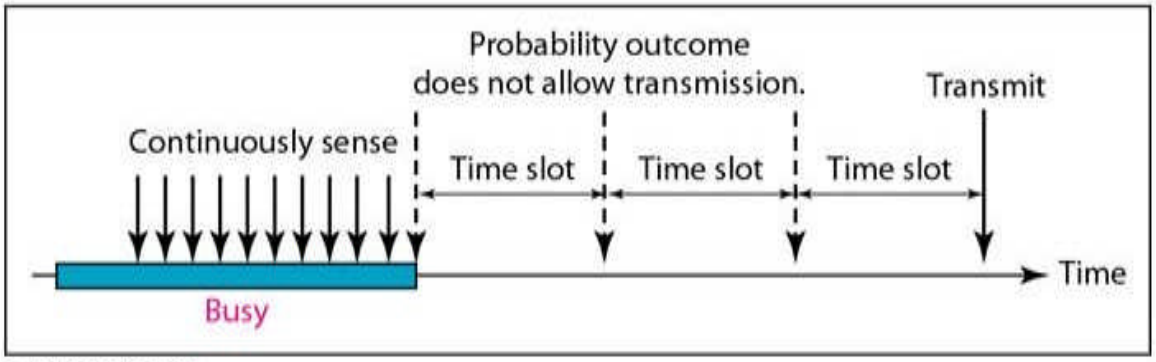
In non-persistence method station that has a form to send sense the line. If the line is idle it sends immediately if the line is not idle it waits random amount of time & then sense line again. The non persistence approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time & retry to send simultaneously



b. Nonpersistent

however this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

3) P-persistence:



c. p-persistent

This method is used if the channel has time slot with the slot duration equal ro or greater than a maximum propagation time the p-persistence approach combine the advantages of two strategy produces chances of collision and improves efficiency.

4: a) What is Line Coding? Explain Line Coding Methods in detail.

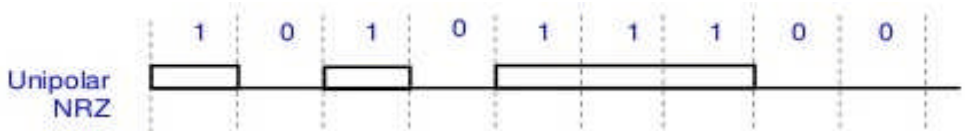
Digital **Line Coding** is a special **coding** system chosen to allow transmission to take place in a communications system. The chosen code or pattern of voltage used to represent binary digits on a transmission medium is called **line encoding**.

Ans: Line coding:

Line coding is the method of conversation of digital data digital signals is called as line coding.

There are 2 types of line coding methods :

1) Unipolar
   - NRZ (non return zero)

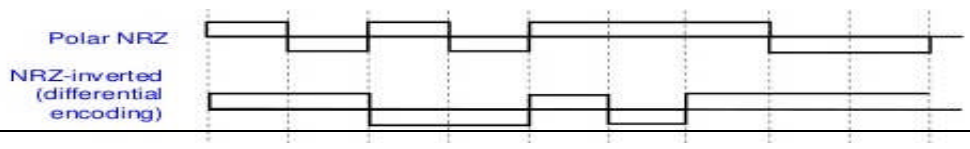


Unipolar NRZ is simply a square wave with +AV being a binary 1, and 0V being a binary 0. NRZ is convenient because computer circuits use unipolar NRZ internally, and it requires little effort to expand this system outside the computer. Unipolar NRZ has a DC term, but a relatively narrow bandwidth.

1-High level

0-Low level (On the Base Line)

2) Polar
   - Level & Invert (NRZ)



-

Non-return to zero level. This is the standard positive logic signal format used in digital circuits.

1-forces a High level

0-forces a Low level

Non-return to zero invert. This is the standard positive logic signal format used in digital circuits.

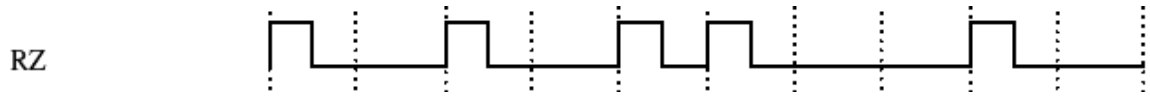
First bit 1-High level

0-low level

Next bit 1-no inversion

0-inversion

- RZ(return zero)

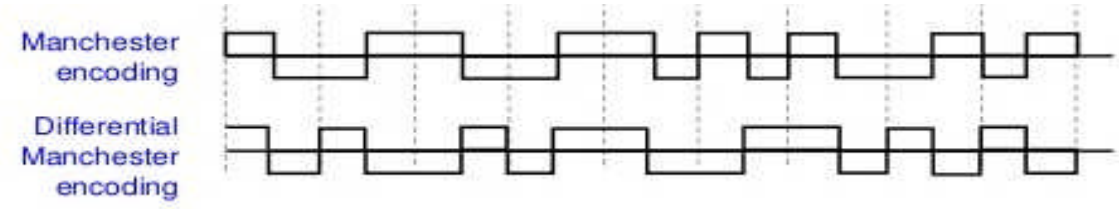


Return to zero. This is the standard positive logic signal format used in digital circuits.

1-Goes high for half the bit period

0-does nothing (low)

- Biphase
  I. Manchester & Differential Manchester



In Manchester encoding, the transition at the middle of the bit is used for both synchronization and bit representation.

1-is represented as

0-is represented as

In differential Manchester encoding , the transition at the middle of the bit is used for both synchronization and bit representation.

First bit 1-represented as

0-represented as

Next bit 1-non inversion

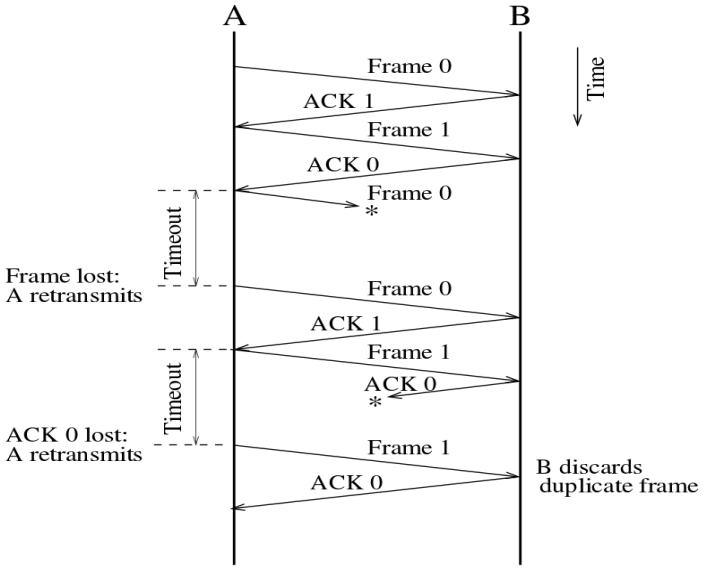
0-inversion

b) Explain stop and wait and go-back N protocols.

Stop-and-wait ARQ, also referred to as alternating bit protocol, is a method in telecommunications to send information between two connected devices. It ensures that information is not lost due to dropped packets and that packets are received in the correct order. It is the simplest automatic repeat-request (ARQ) mechanism. A stop-and-wait ARQ sender sends one frame at a time; it is a special case of the general sliding window protocol with transmit and receive window sizes equal to one and greater than one respectively. After sending each frame, the sender doesn't send any further frames until it receives an acknowledgement (ACK) signal. After receiving a valid frame, the receiver sends an ACK. If the ACK does not reach the sender before a certain time, known as the timeout, the sender sends the same frame again. The timeout countdown is reset after each frame transmission. The above behavior is a basic example of Stop-and-Wait. However, real-life implementations vary to address certain issues of design.

Automatic repeat request (**ARQ**) is a **protocol** for error control in data transmission. When the receiver detects an error in a packet, it automatically requests the transmitter to resend the packet.

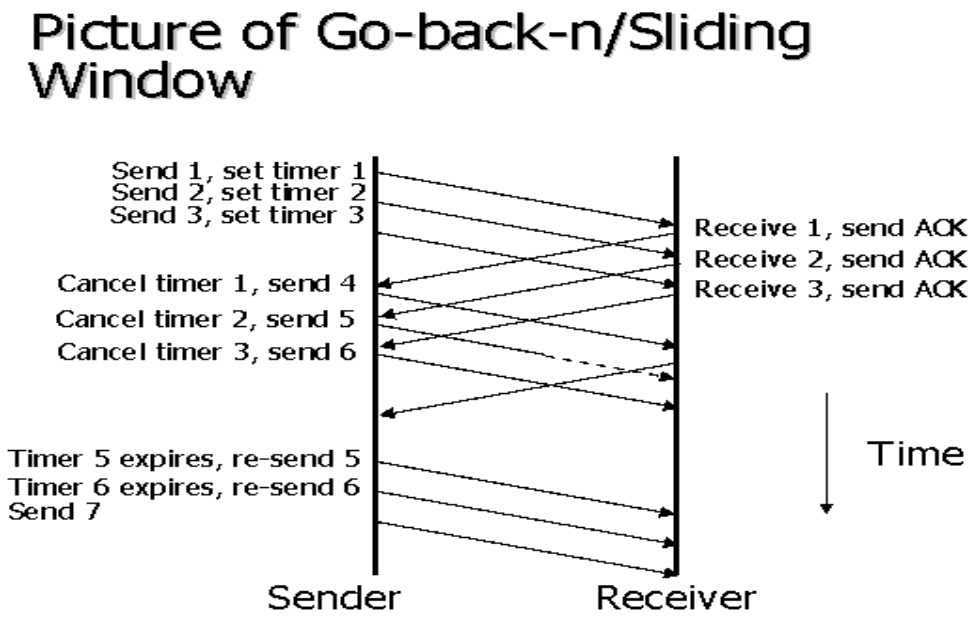
<u>Stop And Wait ARQ:</u>



Stop and Wait transmission is the simplest reliability technique and is adequate for a very simple communications protocol. A

stop and wait protocol transmits a Protocol Data Unit (PDU) of information and then waits for a response. The receiver receives each PDU and sends an Acknowledgement (ACK) PDU if a data PDU is received correctly, and a Negative Acknowledgement (NACK) PDU if the data was not received. In practice, the receiver may not be able to reliably identify whether a PDU has been received, and the transmitter will usually also need to implement a timer to recover from the condition where the receiver does not respond.

Go-Back-N ARQ is a specific instance of the automatic repeat request (ARQ) protocol, in which the sending process continues to send a number of frames specified by a *window size* even without receiving an acknowledgement (ACK) packet from the receiver. It is a special case of the general sliding window protocol with the transmit window size of N and receive window size of 1. It can transmit N frames to the peer before requiring an ACK.



The receiver process keeps track of the sequence number of the next frame it expects to receive, and sends that number with every ACK it sends. The receiver will discard any frame that does not have the exact sequence number it expects (either a duplicate frame it already acknowledged, or an out-of-order frame it expects to receive later) and will resend an ACK for the last correct in-order frame.[1] Once the sender has sent all of the frames in its *window*, it will detect that all of the frames since the first lost frame are *outstanding*, and will go back to the sequence number of the last ACK it received from the receiver process and fill its window starting with that frame and continue the process over again.

Go-Back-N ARQ is a more efficient use of a connection than Stop-and-wait ARQ, since unlike waiting for an acknowledgement for each packet, the connection is still being utilized as packets are being sent. In other words, during the time that would otherwise be spent waiting, more packets are being sent. However, this method also results in sending frames multiple times – if any frame was lost or damaged, or the ACK acknowledging them was lost or damaged, then that frame and all following frames in the window (even if they were received without error) will be re-sent. To avoid this, Selective Repeat ARQ can be used.

5: Differentiate between connection oriented and connectionless service.

Criteria	Connection-Oriented	Connection-Less
Connection	Prior connection needs to be established.	No prior connection is established.
Resource Allocation	Resources need to be allocated.	No prior allocation of resource is required.
Reliability	It ensures reliable transfer of data.	Reliability is not guaranteed as it is a best effort service.
Congestion	Congestion is not at all possible.	Congestion can occur likely.
Transfer mode	It can be implemented either using Circuit Switching or VCs.	It is implemented using Packet Switching.
Retransmission	It is possible to retransmit the lost data bits.	It is not possible.
Suitability	It is suitable for long and steady communication.	It is suitable for bursty transmissions.
Signaling	Connection is established through process of signaling.	There is no concept of signaling.
Packet travel	In this packets travel to their destination node in a sequential manner.	In this packets reach the destination in a random manner.
Delay	There is more delay in transfer of information, but once connection established faster delivery.	There is no delay due absence of connection establishment phase.

b) Define Modulation. Explain ASK, FSK in detail.

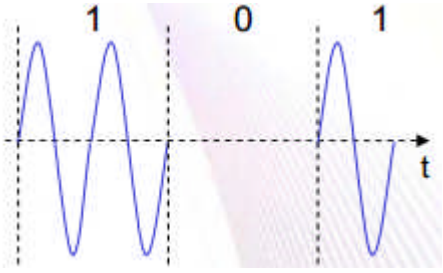
Modulation is a process through which audio, video, image or text information is added to an electrical or optical carrier signal to be transmitted over a telecommunication or electronic medium.

Amplitude Shift Keying (ASK): According to difference signals, it adjusts the amplitude of sine-wave.

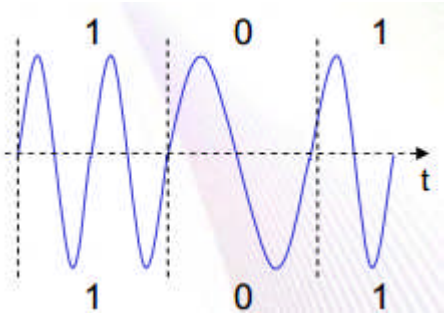
Pros: simple

Cons: susceptible to noise

Example: Many legacy wireless systems, e.g. AMR



Frequency Shift Keying (FSK): It uses digital signal to adjust the frequency of wave carrier.
Pros: less susceptible to noise
Cons: theoretically requires larger bandwidth/bit than ASK
Popular in modern systems



c) Write a note on flooding.

Flooding is a simple routing technique in computer networks where a source or node sends packets through every outgoing link. Flooding, which is similar to broadcasting, occurs when source packets (without routing data) are transmitted to all attached network nodes. Because flooding uses every path in the network, the ...

There are generally two types of flooding available, uncontrolled flooding and controlled flooding.

Uncontrolled flooding is the fatal law of flooding. All nodes have neighbors and route packets indefinitely. More than two neighbours creates a broadcast storm.

Controlled flooding has its own two algorithms to make it reliable, SNCF (Sequence Number Controlled Flooding) and RPF (Reverse Path Forwarding). In SNCF, the node attaches its own address and sequence number to the packet, since every node has a memory of addresses and sequence numbers. If it receives a packet in memory, it drops it immediately while in RPF, the node will only send the packet forward. If it is received from the next node, it sends it back to the sender.

6: a) Differentiate between data gram packet switching and virtual circuit packet switching.

Ans:

Datagram packet switching	Virtual packet switching
• It is connectionless service. There is no need of reservation of resources as there is no dedicated path for a connection session. • All packets are free to go to any path on any intermediate router	• It is connection-oriented simply meaning that there is a reservation of resources like buffers, CPU, bandwidth, etc. for the time in which the newly setup VC is going to be used by a data transfer session. • First packet goes and reserves

which is decided on the go by dynamically changing routing tables on routers. • Since every packet is free to choose any path, all packets must be associated with a header with proper information about source and the upper layer data. • The connectionless property makes data packets reach destination in any order, means they need not reach in the order in which they were sent. • Datagram networks are not reliable as Virtual Circuits. • But it is always easy and cost efficient to implement datagram networks as there is no extra headache of reserving resources and making a dedicated each time an application has to communicate.	resources for the subsequent packets which as a result follow the same path for the whole connection time. • Since all the packets are going to follow the same path, a global header is required only for the first packet of the connection and other packets generally don't require global headers. • Since data follows a particular dedicated path, packets reach in order to the destination. • From above points, it can be concluded that Virtual Circuits are highly reliable means of transfer. • Since each time a new connection has to be setup with reservation of resources and extra information handling at routers, its simply costly to implement Virtual Circuits.

b) Explain Dijkstras algorithm for routing

Dijkstra's algorithm is an algorithm for finding the shortest paths between nodes in a graph, which may represent, for example, road networks.

For a given source node in the graph, the algorithm finds the shortest path between that node and every other.It can also be used for finding the shortest paths from a single node to a single destination node by stopping the algorithm once the shortest path to the destination node has been determined. For example, if the nodes of the graph represent cities and edge path costs represent driving distances between pairs of cities connected by a direct road, Dijkstra's algorithm can be used to find the shortest route between one city and all other cities. As a result, the shortest path algorithm is widely used in network routing protocols, most notably IS-IS (Intermediate System to Intermediate System) and Open Shortest Path First (OSPF). It is also employed as a subroutinein other algorithms such as Johnson's.

Dijkstra's original algorithm does not use a min-priority queue and runs in time

(where is the number of nodes). The idea of this algorithm is also given in Leyzorek et al. 1957. The implementation based on a min-priority queue implemented by a Fibonacci

heap and running in (where is the number of edges) is due to Fredman&Tarjan 1984. This is asymptotically the fastest known single-source shortest-path algorithm for

arbitrary directed graphs with unbounded non-negative weights. However, specialized cases (such as bounded/integer weights, directed acyclic graphs etc.) can indeed be improved further as detailed in § Specialized variants.

c) Write a note on Bridges.

A **network bridge** is a computer networking device that creates a single aggregate network from multiple communication networks or network segments. This function is called **network bridging**. Bridging is distinct from routing

First, many university and corporate departments have their own LANs, primarily to connect their own personal computers, workstations, and servers. Since the goals of the various departments differ, different departments choose different LANs, without regard to what other departments are doing. Sooner or later, there is a need for interaction, so bridges are needed. In this example, multiple LANs came into existence due to the autonomy of their owners.

Second, the organization may be geographically spread over several buildings separated by considerable distances. It may be cheaper to have separate LANs in each building and connect them with bridges and laser links than to run a single cable over the entire site.

Third, it may be necessary to split what is logically a single LAN into separate LANs to accommodate the load. At many universities, for example, thousands of workstations are available for student and faculty computing. Files are normally kept on file server machines and are downloaded to users' machines upon request. The enormous scale of this system precludes putting all the workstations on a single LAN—the total bandwidth needed is far too high. Instead, multiple LANs connected by bridges are used, as shown in Fig.17.1. Each LAN contains a cluster of workstations with its own file server so that most traffic is restricted to a single LAN and does not add load to the backbone.

7: a) Define congestion. Explain Leaky-bucket algorithm for congestion control.

:- **congestion** in data **networking** and queueing theory is the reduced quality of service that occurs when a **network** node or link is carrying more data than it can handle. Typical effects include queueing delay, packet loss or the blocking of new connections.

Leaky bucket algorithm for congestion control:

The leaky bucket algorithm is a method of temporarily storing a variable number of requests and organizing them into a set-rate output of packets in an asynchronous transfer mode (ATM) network.

The leaky bucket is used to implement traffic policing and traffic shaping in Ethernet and cellular data networks. The algorithm can also be used to control metered-

bandwidth Internet connections to prevent going over the allotted bandwidth for a month, thereby avoiding extra charges.

The algorithm works similarly to the way an actual leaky bucket holds water: The leaky bucket takes data and collects it up to a maximum capacity. Data in the bucket is only released from the bucket at a set rate and size of packet. When the bucket runs out of data, the leaking stops. If incoming data would overfill the bucket, then the packet is considered to be non-conformant and is not added to the bucket. Data is added to the bucket as space becomes available for conforming packets.

The leaky bucket algorithm can also detect both gradually increasing and dramatic memory error increases by comparing how the average and peak data rates exceed set acceptable background amounts.

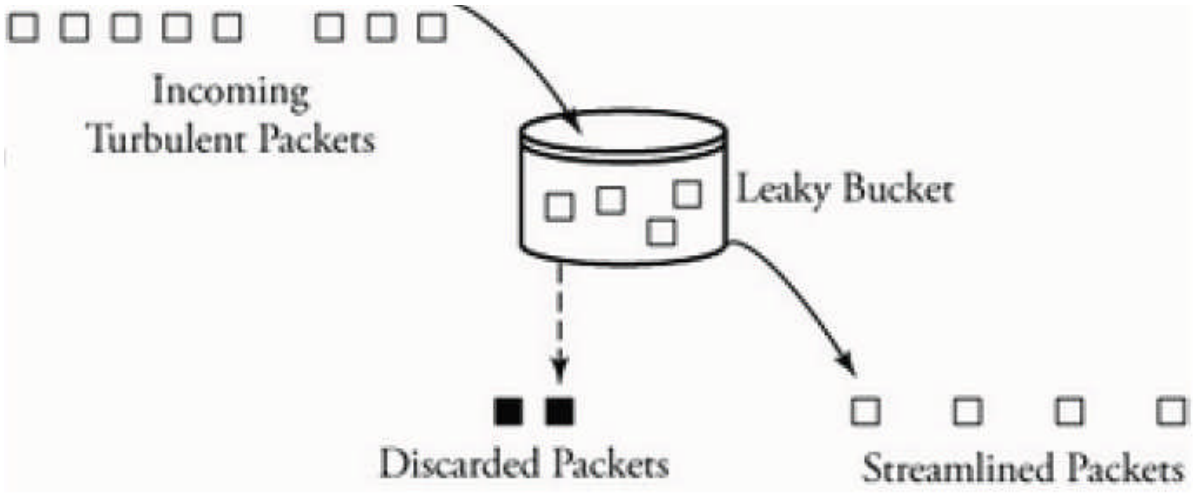


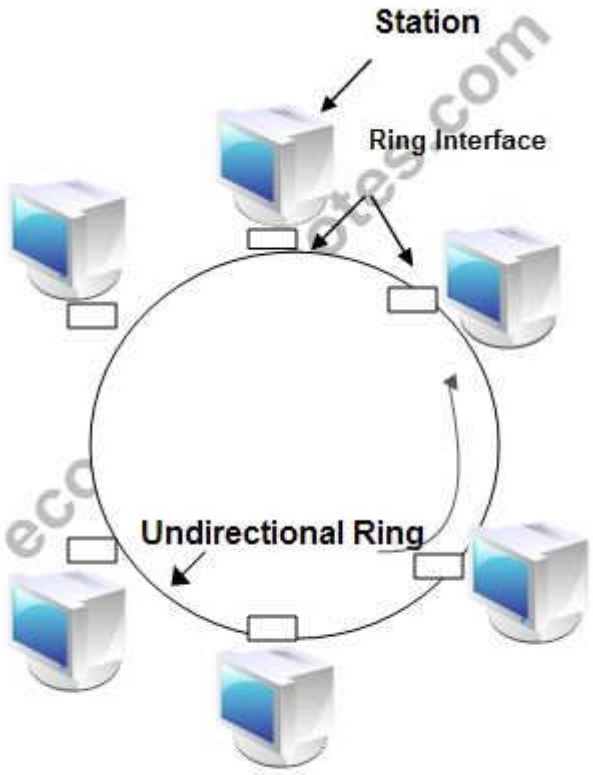
Figure:. The leaky-bucket traffic-shaping algorithm

b)Explain IEEE 802.5 frame structure and its related concepts in detail.

IEEE 802.5 Token Ring: Token ring is the IEEE 802.5 standard for a token-passing ring in Communication networks. A ring consists of a collection of ring interfaces connected by point-to-point lines *i.e.* ring interface of one station is connected to the ring interfaces of its left station as well as right station. Internally, signals travel around the Communication network from one station to the next in a ring.

These point-to-point links can be created with twisted pair, coaxial cable or fiber optics. Each bit arriving at an interface is copied into a 1-bit buffer. In this buffer the bit is checked and may be modified and is then copied out to the ring again. This copying of bit in the buffer introduces a 1-bit delay at each interface.

Token Ring is a LAN protocol defined in the IEEE 802.5 where all stations are connected in a ring and each station can directly hear transmissions only from its immediate neighbor. Permission to transmit is granted by a message (token) that circulates around the ring. A token is a special bit pattern (3 bytes long). There is only one token in the network



A Ring Network

Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token in order to transmit data, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. Since only one station can possess the token and transmit data at any given time, there are no collisions.

There are two operating modes of ring interfaces. There are listen and transmit. In listen mode, the input bits are simply copied to output with a delay of 1- bit time. In transmit mode the connection between input and output is broken by the interface so that is can insert its own data. The station comes in transmit mode when it captures the token.

The frames are acknowledged by the destination in a very simple manner. The sender sends frames to receiver with ACK bit 0. The receiver on receiving frames, copies data into its buffer, verifies the checksum and set the ACK bit to 1. The verified frames come back to sender, where they are removed from the ring.

The information frame circulates the ring until it reaches the intended destination station, which copies the information for further processing. The information frame continues to circle the ring and is finally removed when it reaches the sending station. The sending station can check the returning frame to see whether the frame was seen and subsequently copied by the destination.

A station can hold a token for a specific duration of time. During this time, it has to complete its transmission and regenerates the token in ring. Whenever a station finishes its transmissions, the other station grabs the token and starts its own transmission.

8: Write short notes on any four of the fallowing:

a)LAN

A Local Area Network is a computer network that spans a relatively small area. Most often, a LAN is confined to a single room, building or group of buildings, however, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

A system of LANs connected in this way is called a wide-area network (WAN). The difference between a LAN and WAN is that the wide-area network spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs) and are often connected through public networks.

Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending email or engaging in chat sessions.

LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line; but the distances are limited and there is also a limit on the number of computers that can be attached to a single LAN.

b) Polling

it works with the topologies in which one device is designated as a primary & the other devices are the secondary stations. All data exchange must be made through the primary device even when the ultimate destination is a secondary device. The primary the primary device controls the link; the secondary device follows its instructions. It is up to a primary device to determine which device is allow to use the channel at a given time. The primary device therefore is always the initiator of a session it the primary wants to receive data it ask the secondary if they have anything to send this is called polling function.

It the primary wants to send data it tells the secondary to get ready to receive; this is called select function.

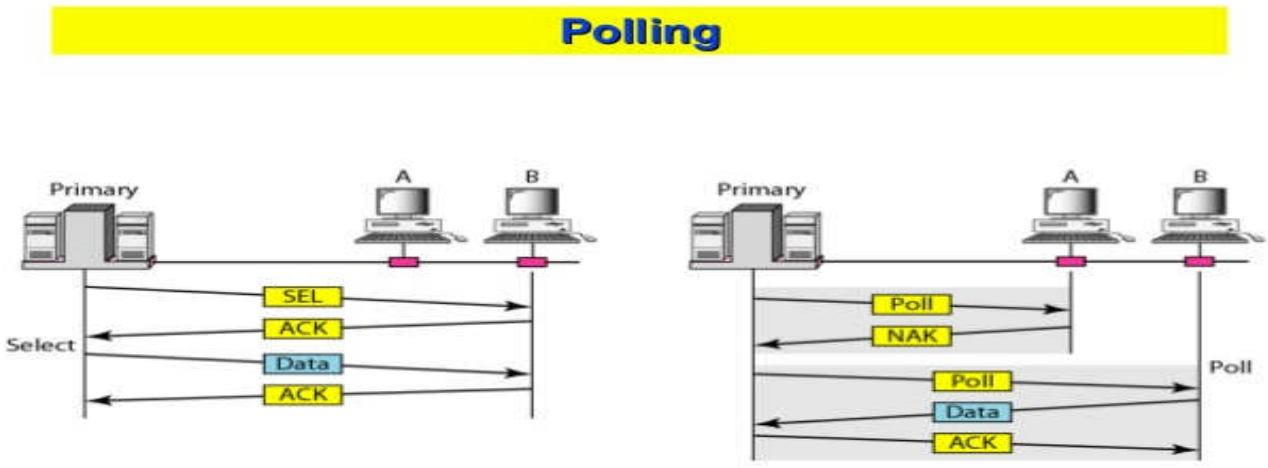


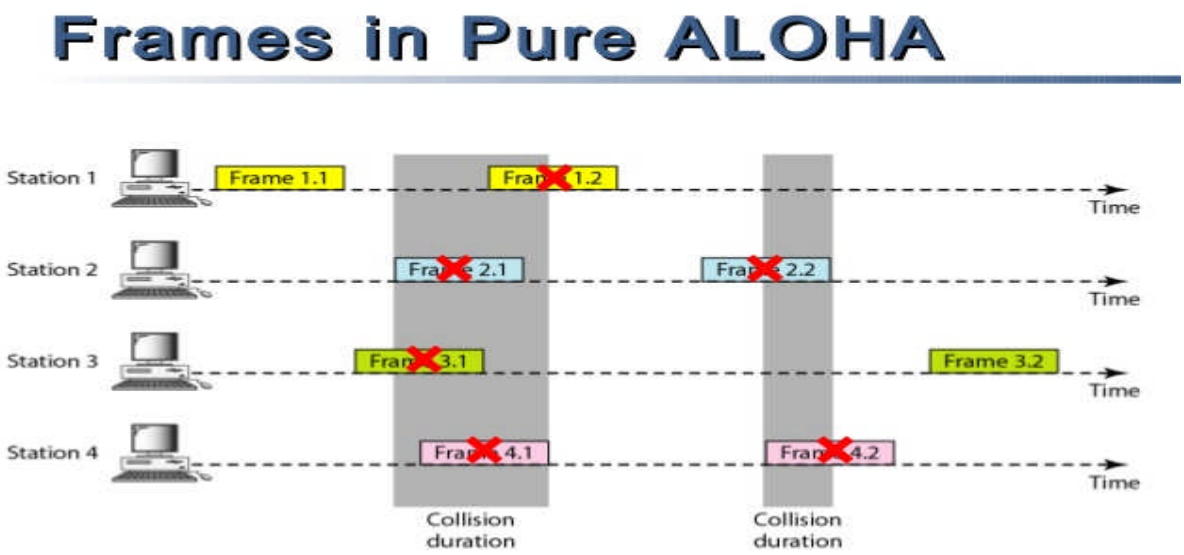
Figure 12.19 *Select and poll functions in polling access method*

c) ALOHA

:-ALOHA system, used ground-based radio broadcasting, the basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel.

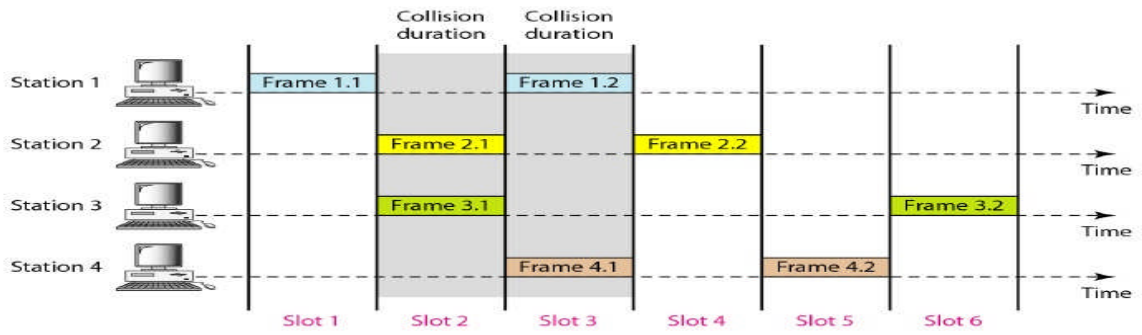
There are two versions of ALOHA

1) Pure ALOHA:
    - If you have a packet just send it.
    - If multiple people try it and so there is collision then try resending it later.
    - Theoretical analysis (based on passion distribution) shows through put of only 18% to reach the destination.



2) Slotted ALOHA:

Figure 12.6 *Frames in a slotted ALOHA network*



- Synchronous that is time is divided into slots
- Slot size is equal to the transmission time of a packet.
- When you are ready to transmit at the start of the time slot.
- Doubles the efficiency of ALOHA (38% through put).
- But requires synchronization.

d) Radio Transmission

Radio Transmission • Radio is the transmission of signals through free space by modulation of electromagnetic waves with frequencies below those of visible light • In telecommunication, transmission is the process of sending and propagating an analogue or digital information signal over a physical p-to-p or p-to-multipoint transmission medium.
Characteristics of Radio Transmission
• Radio frequency (RF) waves are easy to generate.
• It can travel long distances, and can penetrate building easily.
• It is widely used for communication, both indoors and outdoors .
• Radio waves also are omnidirectional, meaning that they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically.

:-Uses
• Audio • Telephony • Video • Navigation • Radar • Data (Digital Radio) • Radio control

:-Advantages
• Simple Circuit • Cheap • No Licenses Needed • High Speed/Bandwidth • Covers Large Areas (Penetrates through walls)

:-Disadvantages

• Limited number of free frequency bands
• Shielding is difficult
• Interference with other electrical devices
• Greater Power Consumption
• Limited Spectrum of Frequency
Examples : FM Channels,Walkie Talkies

e) Channelization

:- The term channelization refers to the sharing of a point-to-point communications medium.1 For example, many telephone conversations (or in our context, computer-to-computer network transactions) can be submitted simultaneously on a single wire, with each conversation being on a separate channel. The notion of a channel is very closely related to the household concept of radio and TV channels. The frequency spectrum for television, for instance, is divided into subranges called channels, and these correspond to our everyday concept of TV channels. Each channel is used to transmit different information, all simultaneously.

There are three main ways of doing this:

• In time-division multiplexing (TDMA),2different sources transmit on the line at different times, each taking (very short) turns. This is used in long-distance phone lines, for example.3

• In frequency-division multiplexing (FDMA), the different sources attached to the line send on different frequencies (e.g. different radio frequencies, or different light frequencies, i.e. different colors). This is used for radio and television transmission, and increasingly for computer-to-computer network transactions.

• In code-division multiplexing (CDMA), all nodes on the network send at the same time, on the same frequency, but using different codes. (Think of one node using a 4B/5B code, another using a second kind of code, and so on.) This is used in some cellular telephone systems.

f)HDLC

High Level Data link control (HDLC) is a bit oriented protocol for communication over point to point and multipoint links. It implements the ARQ mechanism we discussed in this chapter.

In this lesson we shall consider the following aspects of HDLC:

• Stations and Configurations

• Operational Modes

• Non-Operational Modes

• Frame Structure

• Commands and Responses

• HDLC Subsets (SDLC and LAPB)

HDLC Stations and Configurations

HDLC specifies the following three types of stations for data link control:

• Primary Station

With in a network using HDLC as its data link protocol, if a configuration is used in which there is a primary station, it is used as the controlling station on the link. It has the responsibility of controlling all other stations on the link (usually secondary stations). A primary issues commands and secondary issues responses. Despite this important aspect of being on the link, the primary station is also responsible for the organization of data flow on the link. It also takes care of error recovery at the data link level (layer 2 of the OSI model).

• Secondary Station

If the data link protocol being used is HDLC, and a primary station is present, a secondary station must also be present on the data link. The secondary station is under the control of the primary station. It has no ability, or direct responsibility for controlling the link. It is only activated when requested by the primary station. It only responds to the primary station. The secondary station's frames are called responses. It can only send response frames when requested by the primary station. A primary station maintains a separate logical link with each secondary station.

• Combined Station

A combined station is a combination of a primary and secondary station. On the link, all combined stations are able to send and receive commands and responses without any permission from any other stations on the link. Each combined station is in full control of itself, and does not rely on any other stations on the link. No other stations can control any combined station. May issue both commands and responses. HDLC also defines three types of configurations for the three types of stations. The word configuration refers to the relationship between the hardware devices on a link.