14EI705C

Hall Ticket Number:

IV/IV B.Tech (Regular/Supplementary) DEGREE EXAMINATION

Jan/Feb, 2021 **Electronics & Instrumentation Engineering**

Seventh Semester **Computer Networks**

Time: Three Hours **Maximum :** 60 Marks

*Answer **All** Questions from Part - A.* (1X12 = 12 Marks)

Answer Any FOUR Questions from Part - B. (4X12=48 Marks)

Part - A

1 Answer all questions (1X12=12 Marks)

a) Define computer network.
b) What is the purpose of layer?
c) Uses of twisted pair.
d) Write various error detection methods.
e) A bit string 0111101111101111110, needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing.
f) What is meant by piggybacking?
g) State optimality principle.
h) List Network layer design Issues.
i) What is subnet? Give Example.
j) Write primitives for simple transport service.
k) Uses of POP-3 and NNTP protocols.
l) What is meant by upward multiplexing?

Part - B

2 a) Find out what networks are used at your college or place of work. Describe network types, topologies and switching methods used there. 6M
b) Explain TCP/IP Reference Model in detail. 6M

3 a) Explain Coaxial cable with figure. 6M
b) Explain about wireless transmission media. 6M

4 Illustrate error correcting codes with relevant example. 12M

5 a) Explain about stop-and-wait protocol in detail. 6M
b) Describe dynamic channel allocation in LAN's and MAN's. 6M

6 a) Describe general principles of Congestion control. 6M
b) Explain Hierarchical Routing algorithm in detail. 6M

7 a) Explain various Techniques for Achieving Good Quality of Service. 6M
b) Describe IP Protocol in detail. 6M

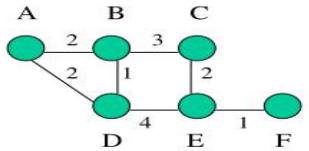
8 a) Explain about TCP protocol in detail. 6M
b) Explain leaky bucket algorithm. 6M

9 a) Explain Domain Name System with relevant figures. 6M
b) Explain about E-Mail. 6M

IV/IV B.Tech (Regular/Supplementary) DEGREE EXAMINATION
Jan/Feb, 2021 Electronics & Instrumentation Engineering
Seventh Semester
Computer Networks(14EI705)
SCHEME AND SOLUTION

Part - A

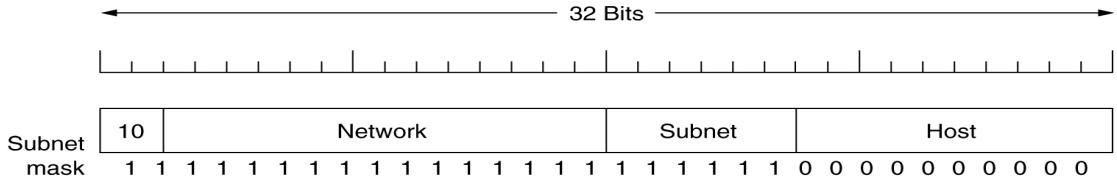
1.a.What is the purpose of layer?
A: The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.
b. Uses of twisted pair.
A:
1. better-quality signal reception over longer distances
2.suitable for high-speed computer communication.
c. Write various error detection methods.
1.single parity bit
2. Two-dimensional Parity check.
3.Checksum.
4.Cyclic redundancy check.
d. A bit string 0111101111101111110, needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing.
A: Same string: 0111101111101111110
e. What is meant by piggybacking?
A: In two-way communication, whenever a frame is received, the receiver waits and does not send the control frame (acknowledgement or ACK) back to the sender immediately. This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as piggybacking.
f. State optimality principle.
A: Assume that "optimal" path is the shortest one OP indicates that any portion of any optimal path is also optimal Set of optimal paths from all sources to a given destination forms a tree that is routed at the destination.



➔ Optimal path between A and F is A-B-C-E-F
➔ Then, the optimal path between B and F is B-C-E-F

g. List Network layer design Issues.
- Store-and-Forward Packet Switching
- Services Provided to the Transport Layer
- Implementation of Connectionless Service
- Implementation of Connection-Oriented Service

h. What is subnet? Give Example.
A: A subnet is a single small network created from a large network. In Subnetting we break a single large network in multiple small networks. These networks are known as subnets.
ex: A class B network can be subnetted into 64 subnets.



i. Write primitives for simple transport service.
A:

Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	This side wants to release the connection

j. Uses of POP-3 and NNTP protocols.

A: **POP3** is the most commonly **used** Internet mail **protocols** for retrieving emails assumes that your email is being accessed only from one **application.**

(NNTP) is an application protocol used for transporting Usenet news articles (netnews) between news servers and for reading and posting articles by end user client applications.

k. What is meant by upward multiplexing?

A: In upward multiplexing, the different transport connections are multiplexed in to one network connection.

- These transport connections are grouped by the transport layer as per their destinations.
- It then maps the groups with the minimum number of network connections possible.
- The upward multiplexing is quite useful where the network connections come very expensive.

Part - B

2 a) Find out what networks are used at your college or place of work. Describe network types, topologies and switching methods used there. 6M

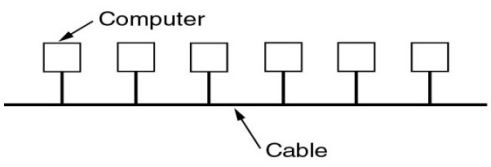
A:Types of networks(2),Toplogies(2),switching methods(2)marks

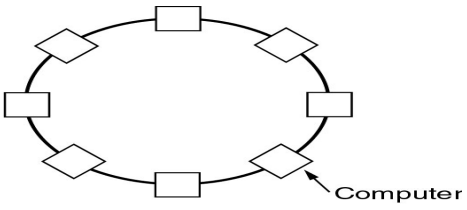
Classification of interconnected processors by scale

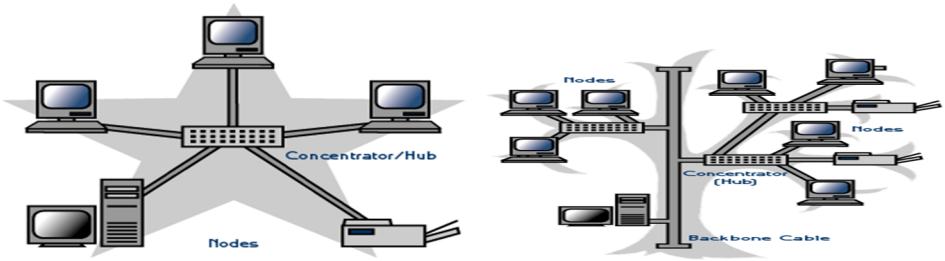
Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Local Area Networks:Topologies

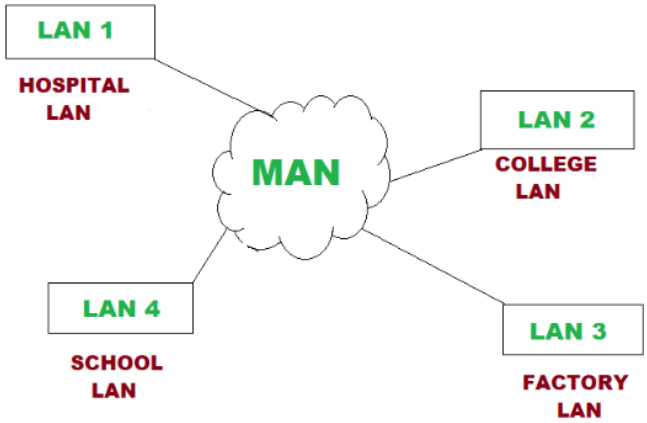
- Bus
- Ring
- Star
- Tree
- Mesh



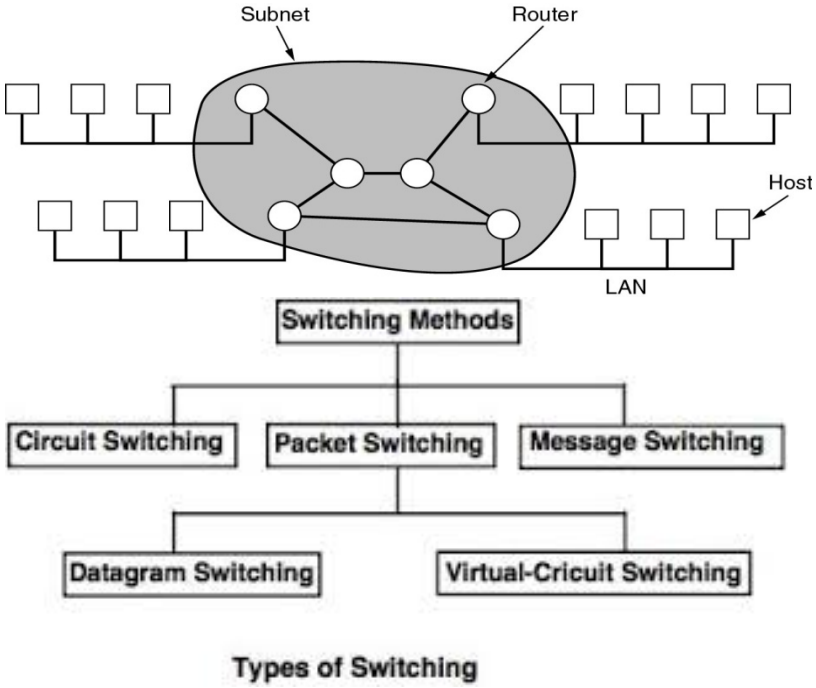




A metropolitan area **network** (**MAN**) is a **network** that interconnects users with **computer** resources in a geographic area or region larger than that covered by even a large local area **network** (**LAN**) but smaller than the area covered by a wide area **network** (WAN)



Wide Area Networks



Types of Switching

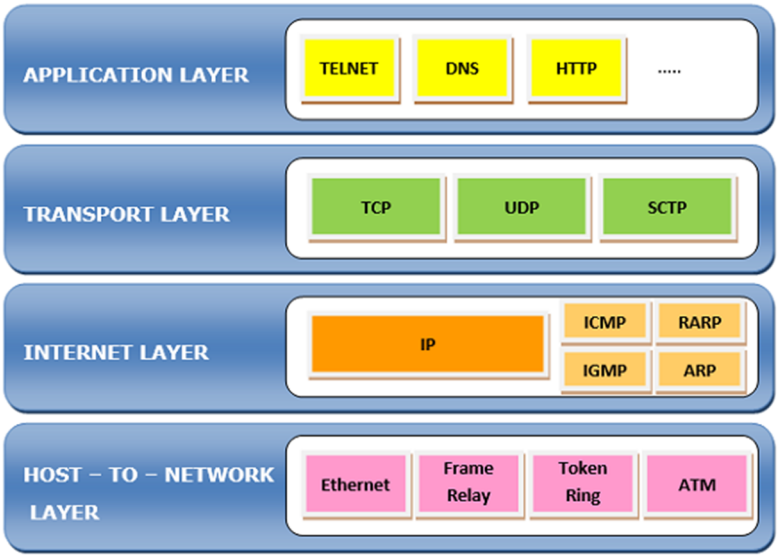
b) Explain TCP/IP Reference Model in detail. 6M

A: TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

The four layers in the TCP/IP protocol suite are –

Host-to- Network Layer –It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.
Internet Layer –It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.

Transport Layer – It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
Application Layer – This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.
The following diagram shows the layers and the protocols in each of the layers –

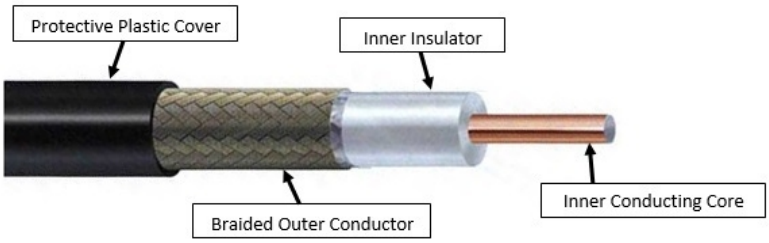


3 a) Explain Coaxial cable with figure. 6M

A: Coaxial cables, commonly called coax, are copper cables with metal shielding designed to provide immunity against noise and greater bandwidth. Coax can transmit signals over larger distances at a higher speed as compared to twisted pair cables.

Structure of Coaxial Cables

Coax has a central core of stiff copper conductor for transmitting signals. This is covered by an insulating material. The insulator is encased by a closely woven braided metal outer conductor that acts as a shield against noise. The outer conductor is again enclosed by a plastic insulating cover. The structure is shown in the following figure –



Categories of Coaxial Cables

Coaxial cables are categorized into three types as per radio government (RG) ratings –

- RG – 59: Has impedance of 75W and used in cable TV
- RG – 58: Has impedance of 50W and used in thin Ethernet
- RG – 11: Has impedance of 50W and used in thick Ethernet

Applications of Coaxial Cables

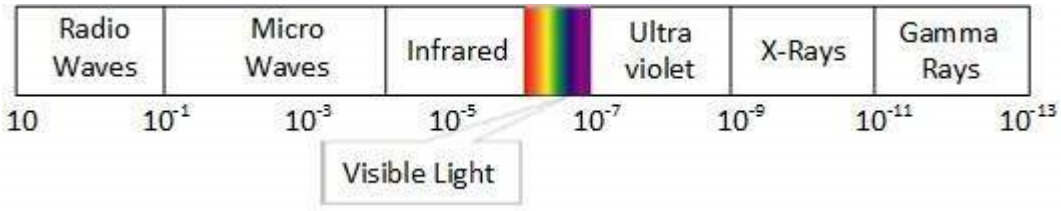
- In analog telephone networks: A single coaxial network can carry about 10,000 voice signals.
- In digital telephone networks: A coax has a data rate of 600 Mbps.
- In cable TV networks
- In traditional Ethernet LANs
- In MANs

b) Explain about wireless transmission media. 6M

A: Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

A little part of electromagnetic spectrum can be used for wireless transmission.



Radio Transmission

Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike.Radio waves can have wavelength from 1 mm – 100,000 km and have frequency ranging from 3 Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency). Radio frequencies are sub-divided into six bands.

Radio waves at lower frequencies can travel through walls whereas higher RF can travel in straight line and bounce back.The power of low frequency waves decreases sharply as they cover long distance. High frequency radio waves have more power.

Lower frequencies such as VLF, LF, MF bands can travel on the ground up to 1000 kilometers, over the earth's surface.

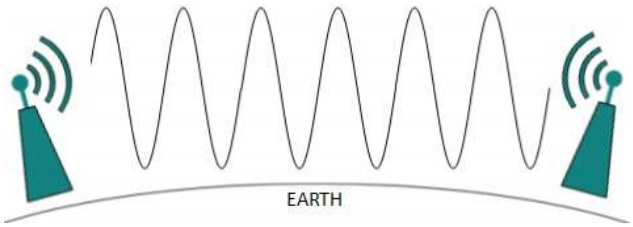


FIG:SPACE WAVE PROPAGATION

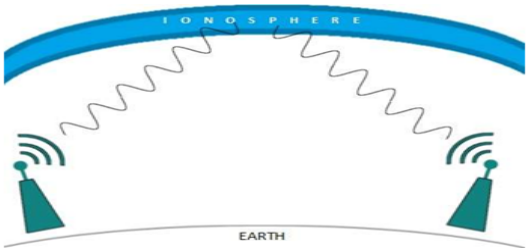


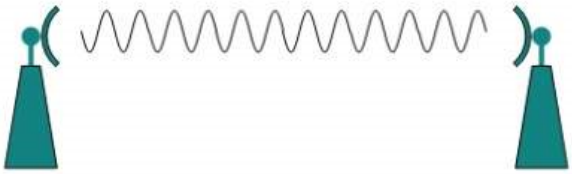
FIG:SKY WAVE PROPAGATION

Radio waves of high frequencies are prone to be absorbed by rain and other obstacles. They use Ionosphere of earth atmosphere. High frequency radio waves such as HF and VHF bands are spread upwards. When they reach Ionosphere, they are refracted back to the earth.

Microwave Transmission

Electromagnetic waves above 100 MHz tend to travel in a straight line and signals over them can be sent by beaming those waves towards one particular station. Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line-of-sight.

Microwaves can have wavelength ranging from 1 mm – 1 meter and frequency ranging from 300 MHz to 300 GHz.



Microwave antennas concentrate the waves making a beam of it. As shown in picture above, multiple antennas can be aligned to reach farther. Microwaves have higher frequencies and do not penetrate wall like obstacles.

Microwave transmission depends highly upon the weather conditions and the frequency it is using.

Infrared Transmission

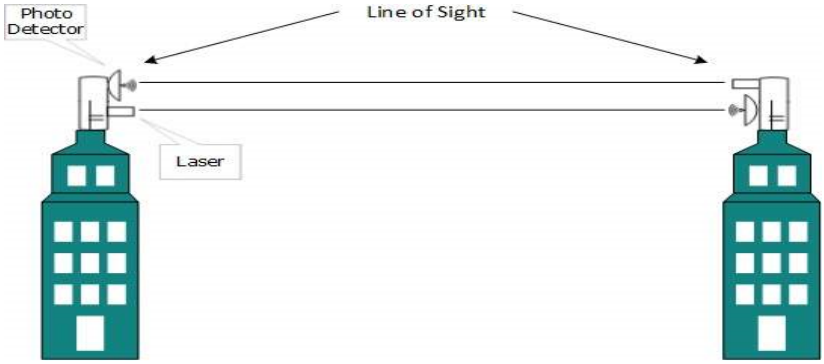
Infrared wave lies in between visible light spectrum and microwaves. It has wavelength of 700-nm to 1-mm and frequency ranges from 300-GHz to 430-THz.

Infrared wave is used for very short range communication purposes such as television and it's remote. Infrared travels in a straight line hence it is directional by nature. Because of high frequency range, Infrared cannot cross wall-like obstacles.

Light Transmission

Highest most electromagnetic spectrum which can be used for data transmission is light or optical signaling. This is achieved by means of LASER.

Because of frequency light uses, it tends to travel strictly in straight line.Hence the sender and receiver must be in the line-of-sight. Because laser transmission is unidirectional, at both ends of communication the laser and the photo-detector needs to be installed. Laser beam is generally 1mm wide hence it is a work of precision to align two far receptors each pointing to lasers source.



Laser works as Tx (transmitter) and photo-detectors works as Rx (receiver).

Lasers cannot penetrate obstacles such as walls, rain, and thick fog. Additionally, laser beam is distorted by wind, atmosphere temperature, or variation in temperature in the path.

Laser is safe for data transmission as it is very difficult to tap 1mm wide laser without interrupting the communication channel.

4 Illustrate error correcting codes with relevant example. 12M

A: The codes which are used for both error detecting and error correction are called as "Error Correction Codes".
The error correction techniques are of two types. They are,
I.Single bit error correction
Burst error correction
The process or method of correcting single bit errors is called "single bit error correction". The method of detecting and correcting burst errors in the data sequence is called "Burst error correction".

II.Hamming Code

Hamming code or Hamming Distance Code is the best error correcting code we use in most of the communication network and digital systems.

This error detecting and correcting code technique is developed by R.W.Hamming .

This code not only identifies the error bit, in the whole data sequence and it also corrects it.

This code uses a number of parity bits located at certain positions in the codeword. The number of parity bits depends upon the number of information bits.

The hamming code uses the relation between redundancy bits and the data bits and this code can be applied to any number of data bits.

Redundancy means "The difference between number of bits of the actual data sequence and the transmitted bits".

These redundancy bits are used in communication system to detect and correct the errors, if any.

How the Hamming code actually corrects the errors?

In Hamming code, the redundancy bits are placed at certain calculated positions in order to eliminate errors. The distance between the two redundancy bits is called "Hamming distance".

Number of parity bits

The number of parity bits to be added to a data string depends upon the number of information bits of the data string which is to be transmitted. Number of parity bits will be calculated by using the data bits. This relation is given below.

$2^P >= n + P + 1$

Here, n represents the number of bits in the data string.

P represents number of parity bits.

For example, if we have 4 bit data string, i.e. n = 4, then the number of parity bits to be added can be found by using trial and error method. Let's take P = 2, then

$2^P = 2^2 = 4$ and $n + P + 1 = 4 + 2 + 1 = 7$

This violates the actual expression.

So let's try P = 3, then

$2^P = 2^3 = 8$ and $n + P + 1 = 4 + 3 + 1 = 8$

So we can say that 3 parity bits are required to transfer the 4 bit data with single bit error correction.

Where to Place these Parity Bits?

After calculating the number of parity bits required, we should know the appropriate positions to place them in the information string, to provide single bit error correction.

In the above considered example, we have 4 data bits and 3 parity bits. So the total codeword to be transmitted is of 7 bits (4 + 3). We generally represent the data sequence from right to left, as shown below.

bit 7, bit 6, bit 5, bit 4, bit 3, bit 2, bit 1, bit 0

The parity bits have to be located at the positions of powers of 2. I.e. at 1, 2, 4, 8 and 16 etc. Therefore the codeword after including the parity bits will be like this

D7, D6, D5, P4, D3, P2, P1

Here P1, P2 and P3 are parity bits. D1 —- D7 are data bits.

Constructing a Bit Location Table

Bit Designation	D7	D6	D5	P4	D3	P2	P1
Bit Location	7	6	5	4	3	2	1
Binary Location Number	111	110	101	100	011	010	001
Data Bits (Dn)				---		---	---
Parity Bits (Pn)	---	---	---		---		

In Hamming code, each parity bit checks and helps in finding the errors in the whole code word. So we must find the value of the parity bits to assign them a bit value.

By calculating and inserting the parity bits in to the data bits, we can achieve error correction through Hamming code.

Let's understand this clearly, by looking into an example.

Ex:

Encode the data 1101 in even parity, by using Hamming code.

Step 1

Calculate the required number of parity bits.

Let P = 2, then

$2^P = 2^2 = 4$ and n + P + 1 = 4 + 2 + 1 = 7.

2 parity bits are not sufficient for 4 bit data.

So let's try P = 3, then

$2^P = 2^3 = 8$ and n + P + 1 = 4 + 3 + 1 = 8

Therefore 3 parity bits are sufficient for 4 bit data.

The total bits in the code word are 4 + 3 = 7

Step 2

Constructing bit location table

Bit Designation	D7	D6	D5	P4	D3	P2	P1
Bit Location	7	6	5	4	3	2	1
Binary Location Number	111	110	101	100	011	010	001
Data Bits (D_n)	1	1	0		1		
Parity Bits (P_n)				0		0	1

Step 3

Determine the parity bits.

For P1 : 3, 5 and 7 bits are having three 1's so for even parity, P1 = 1.

For P2 : 3, 6 and 7 bits are having two 1's so for even parity, P2 = 0.
For P3 : 5, 6 and 7 bits are having two 1's so for even parity, P3 = 0.

By entering / inserting the parity bits at their respective positions, codeword can be formed and is transmitted. It is 1100101.
At the receiving also ,parity bits are calculated and if P1P2P3 represents 000,then there is no error in the received data otherwise P1P2P3 represent the error bit position and it is complemented to make correction.It canot detect double errors.

5 a) Explain about stop-and-wait protocol in detail. 6M

A: 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.

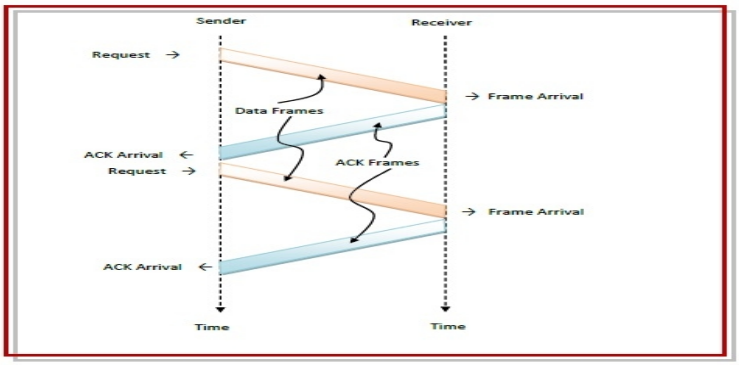
Sender Site Algorithm of Simplex Stop – and – Wait Protocol for Noiseless Channel

```
begin
  canSend = True;       //Allow the first frame to be sent
  while (true)          //check repeatedly
  do
    Wait_For_Event();   //wait for availability of packet
    if ( Event(Request_For_Transfer) AND canSend) then
      Get_Data_From_Network_Layer();
      Make_Frame();
      Send_Frame_To_Physical_Layer();
      canSend = False;
    else if ( Event(Acknowledgement_Arrival)) then
      Receive_ACK();
      canSend = True;
    end if
  end while
end
```

Receiver Site Algorithm of Simplex Stop – and – Wait Protocol for Noiseless Channel

```
begin
  while (true)     //check repeatedly
  do
    Wait_For_Event();    //wait for arrival of frame
    if ( Event(Frame_Arrival) then
      Receive_Frame_From_Physical_Layer();
      Extract_Data();
      Deliver_Data_To_Network_Layer();
      Send_ACK();
    end if
  end while
end
```

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



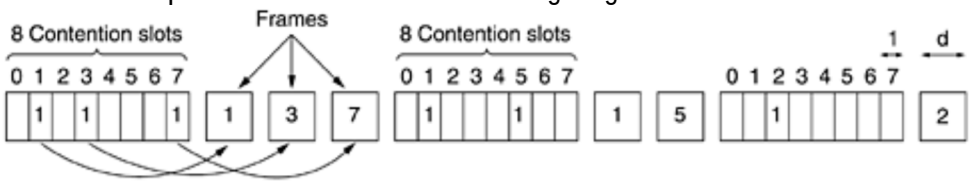
b) Describe dynamic channel allocation in LAN's and MAN's. 6M

A:

In dynamic channel allocation schemes, frequency channels are not permanently allotted to any user.
Channels are assigned to the user as needed depending upon the network environment.
The available channels are kept in a queue or a spool.
The allocation of the channels is temporary.
Distribution of the channels to the contending users is based upon distribution of the users in the network and offered traffic load.
The allocation is done so that transmission interference is minimized.
Reservation protocols are the class of protocols in which the stations wishing to transmit data broadcast themselves before actual transmission. These protocols operate in the medium access control (MAC) layer and transport layer of the OSI model.
Examples of Reservation Protocols
Bit – Map Protocol
Bit – map Protocol that operates in the MAC layer

In this protocol, the contention period is divided into N slots, where N is the total number of stations sharing the channel. If a station has a frame to send, it sets the corresponding bit in the slot.

Suppose that there are 10 stations. So the number of contention slots will be 7. If the stations 1,3 and 7 wish to transmit, they will set the corresponding slots to 1. Generally, the transmission is done in the order of the slot numbers. The process is shown in the following diagram:



CSMA:

(i)1-persistent CSMA: In this case, a node having data to send, start sending, if the channel is sensed free. If the medium is busy, the node continues to monitor until the channel is idle. Then it starts sending data.
(ii)(ii) Non-persistent CSMA: If the channel is sensed free, the node starts sending the packet. Otherwise, the node waits for a random amount of time and then monitors the channel.
(iii) (iii) p-persistent CSMA: If the channel is free, a node starts sending the packet. Otherwise the node continues to monitor until the channel is free and then it sends with probability p.

The efficiency of CSMA scheme depends on the propagation delay, which is represented by a parameter a, as defined below:

a= Propagation delay /Packet transmission time.

CSMA/CD

In CSMA scheme, when two packets collide the channel remains unutilized for the entire duration of transmission time of both the packets.
If the propagation time is small (which is usually the case) compared to the packet transmission time, wasted channel capacity can be considerable.
This wastage of channel capacity can be reduced if the nodes continue to monitor the channel while transmitting a packet and immediately cease transmission when collision is detected.
This refined scheme is known as Carrier Sensed Multiple Access with Collision Detection (CSMA/CD).
On top of the CSMA, the following rules are added to convert it into CSMA/CD:

(i)If a collision is detected during transmission of a packet, the node immediately ceases transmission and it transmits jamming signal for a brief duration to ensure that all stations know that collision has occurred.
(ii) After transmitting the jamming signal, the node waits for a random amount of time and then transmission is resumed.
The random delay ensures that the nodes, which were involved in the collision are not likely to have a collision at the time of retransmissions. To achieve stability in the back off scheme, a technique known as binary exponential back off is used. A node will attempt to transmit repeatedly in the face of repeated collisions, but after each collision, the mean value of the random delay is doubled. After 15 retries (excluding the original try), the unlucky packet is discarded and the node reports an error. A flowchart representing the binary exponential back off algorithm is given in Fig.

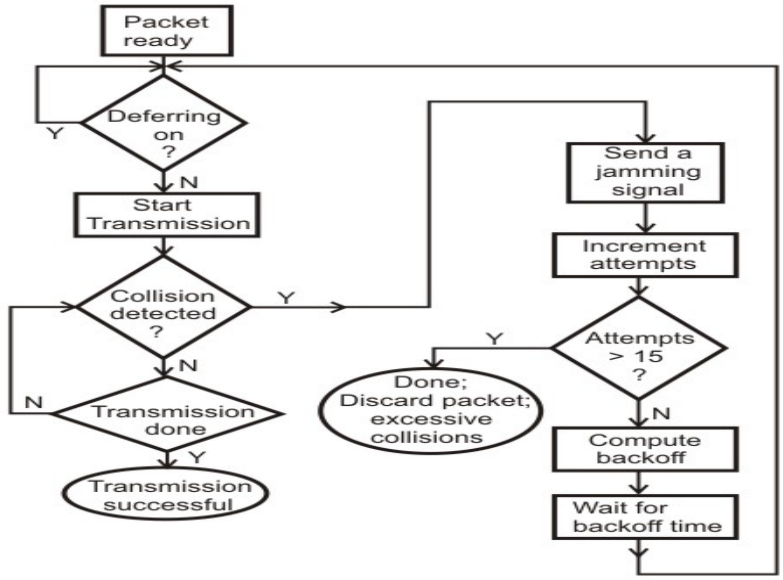


Figure .Binary exponential back off algorithm used in CSMA/CD

6 a) Describe general principles of Congestion control. 6M

A: General Principles of Congestion Control:

There are two types of congestion controls.
1.open loop: Tools for doing open-loop control include deciding when to accept new traffic, deciding when to discard packets and which ones, and making scheduling decisions at various points in the network. All of these have in common the fact that they make decisions without regard to the current state of the network.

2.closed loop:These solutions are based on the concept of a feedback loop.
This approach has three parts when applied to congestion control:

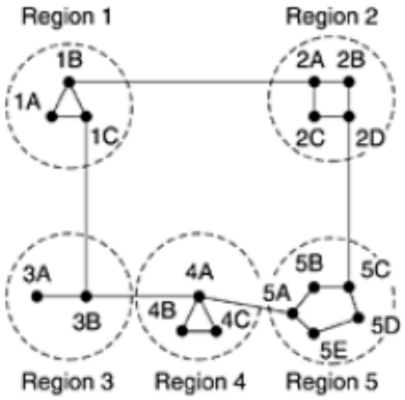
1. Monitor the system .
   - detect when and where congestion occurs.
2. Pass information to where action can be taken.
3. Adjust system operation to correct the problem.

b) Explain Hierarchical Routing algorithm in detail. 6M

A:
This is essentially a 'Divide and Conquer' strategy. The network is divided into different regions and a router for a particular region knows only about its own domain and other routers. Thus, the network is viewed at two levels: The Sub-network level, where each node in a region has information about its peers in the same region and about the region's interface with other regions. Different regions may have different 'local' routing algorithms. Each local algorithm handles the traffic between nodes of the same region and also directs the outgoing packets to the appropriate interface.
The Network Level, where each region is considered as a single node connected to its interface nodes. The routing algorithms at this level handle the routing of packets between two interface nodes, and is isolated from intra-regional transfer.
Networks can be organized in hierarchies of many levels; e.g. local networks of a city at one level, the cities of a country at a level above it, and finally the network of all nations.

In Hierarchical routing, the interfaces need to store information about:

All nodes in its region which are at one level below it.
Its peer interfaces.
At least one interface at a level above it, for outgoing packages.
Advantages of Hierarchical Routing :
Smaller sizes of routing tables.
Substantially lesser calculations and updates of routing tables.
Disadvantage :
Once the hierarchy is imposed on the network, it is followed and possibility of direct paths is ignored. This may lead to sub optimal routing.



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

7 a) Explain various Techniques for Achieving Good Quality of Service. 6M

A: A stream of packets from a source to destination is called flow.

In a connection oriented network,all the packets belong to a flow follow the same route.
The needs of each flow can be characterized by by four parameters.
Reliability,delay,jitter,bandwidth.

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

ATM networks classify flows in four broad categories with respect to their QoS demands as follows:
1. Constant bit rate (e.g., telephony).
2. Real-time variable bit rate (e.g., compressed videoconferencing).
3. Non-real-time variable bit rate (e.g., watching a movie over the Internet).
4. Available bit rate (e.g., file transfer).
Techniques for achieving good quality of service:
1.Over provisioning:
With better router capacity i.e. buffer space and bandwidth, good quality of service can be obtained. It is expensive.
2.Buffering:

Flows can be buffered on the receiving side before delivered.
It does not affect the reliability or bandwidth and increases the delay, but It smooth out the jitter.

Reliability (Packet loss): it happens when the network links become congested and the routers and switches start dropping the packets. When these packets are dropped during real-time communication, such as audio or video, these sessions can experience jitter and gaps in speech.

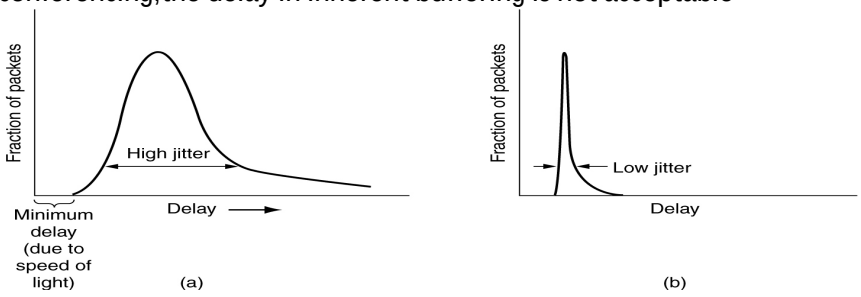
Delay(Latency) is the time delay, which is taken by a packet to travel from its source to its destination. For a Large system, latency should be as low as possible, ideally, it should be close to zero.

Bandwidth: is the capacity of a network channel to transmit maximum possible data through the channel in a certain amount of time.

Mean opinion score: it is a metric for rating the audio quality which uses a five-point scale, with a five indicating the highest or best quality.

QoS optimizes a network by managing its bandwidth and setting the priorities for those applications which require more resources as compared to other applications.

Jitter control:
For applications such as audios and video streaming ,it does not matter much if packets take 20ms or 30ms to be delivered as long as transit time is constant.The variation in the packet arrival time is called jitter.
EX:99% of the packets delivered with delay in the range of 24.5ms to 25.5ms might be acceptable.
The jitter can be bounded by computing the expected transit time for each hop along the length.
EX: video demand:
jitter can be eliminated by buffering at the receiver and the fetching data for display from buffer instead from the network in real time
For applications,especially that require real time interaction between people such as Internet Telephony and video conferencing,the delay in inherent buffering is not acceptable



b) Describe IP Protocol in detail. **6M**

A:

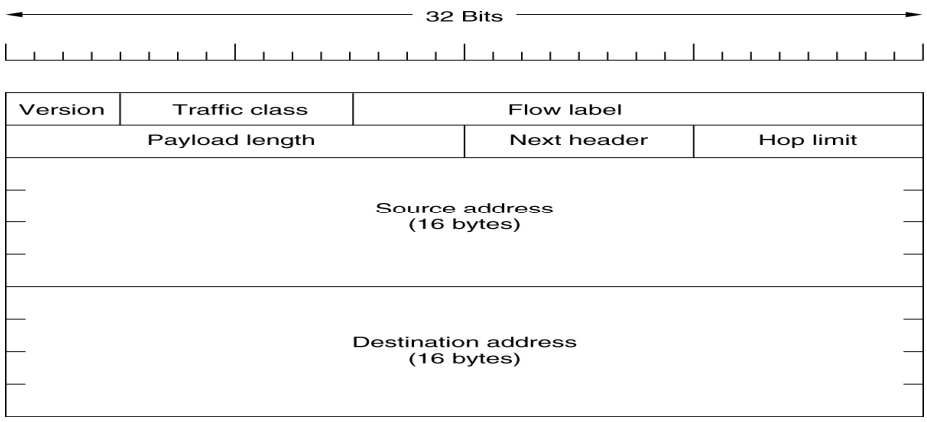


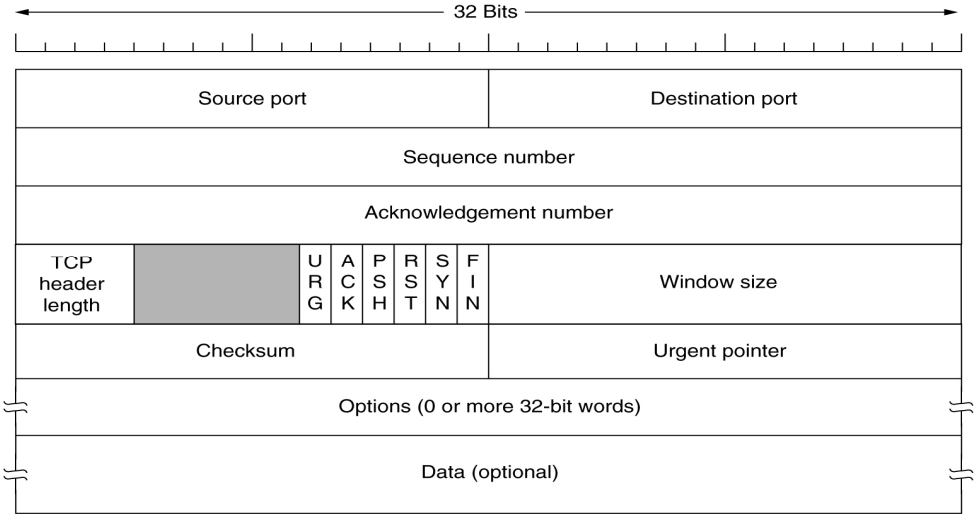
FIG 1

The *Traffic class field is used to distinguish between packets with different real-time delivery requirements.*
The *Flow label field :*
For example, a stream of packets from one process on a certain source host to a certain process on a certain destination host might have stringent delay requirements and thus need reserved bandwidth.
The flow can be set up in advance and given an identifier. When a packet with a nonzero *Flow label shows up, all the routers can look it up in internal tables to see what kind of special treatment it requires.*

In effect, flows are an attempt to have it both ways: the flexibility of a datagram subnet and the guarantees of a virtual-circuit subnet.
Each flow is designated by the source address, destination address, and
The *Payload length field tells how many bytes follow the 40-byte header of Fig.1*
If this header is the last IP header, the *Next header field tells which transport protocol handler (e.g., TCP, UDP) to pass the packet to.*
The *Hop limit field is used to keep packets from living forever. It is, in practice, the same as the Time to live field in IPv4, namely, a field that is decremented on each hop.*
Some of the headers have a fixed format; others contain a variable number of variable-length fields.
For these, each item is encoded as a (Type, Length, Value) tuple.

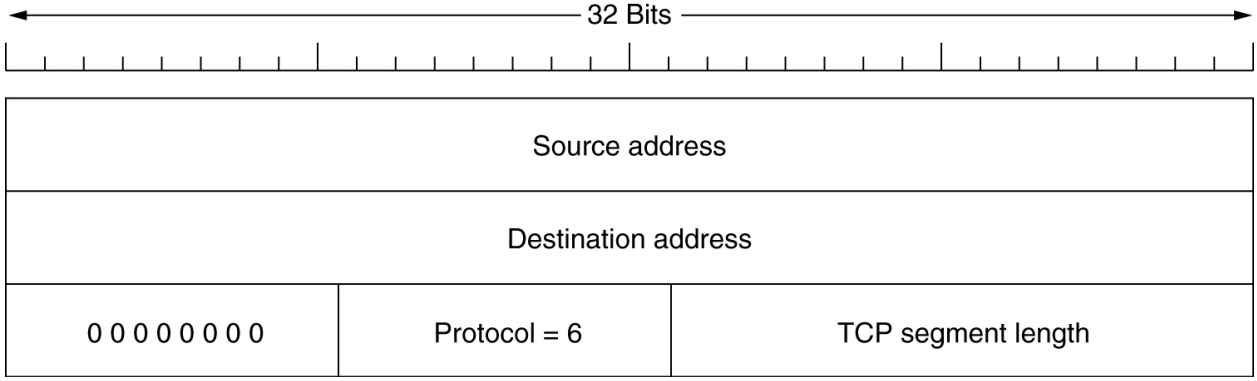
The *Type is a 1-byte field telling which option this is.*
The Type values have been chosen so that the first 2 bits tell routers that do not know how to process the option what to do.
The choices are:
skip the option;
discard the packet;
discard the packet and send back an ICMP packet;
and the same as the previous one, except do not send ICMP packets for multicast addresses (to prevent one bad multicast packet from generating millions of ICMP reports).
The *Length is also a 1-byte field. It tells how long the value is (0 to 255 bytes). The Value is any information required, up to 255 bytes.*
The hop-by-hop header is used for information that all routers along the path must examine.

8 a) Explain about TCP protocol in detail. 6M
A:



The Source port and Destination port fields identify the local end points of the connection.
The well-known ports are defined at www.iana.org but each host can allocate the others as it wishes.
A port plus its host's IP address forms a 48-bit unique end point.
The source and destination end points together identify the connection .
The Sequence number and Acknowledgement number fields perform their usual functions.
Note that the latter specifies the next byte expected, not the last byte correctly received.
Both are 32 bits long because every byte of data is numbered in a TCP stream.
The TCP header length tells how many 32-bit words are contained in the TCP header. This information is needed because the Options field is of variable length, so the header is, too.
URG is set to 1 if the Urgent pointer is in use. The Urgent pointer is used to indicate a byte offset from the current sequence number at which urgent data are to be found.
The ACK bit is set to 1 to indicate that the Acknowledgement number is valid. If ACK is 0, the segment does not contain an acknowledgement so the Acknowledgement number field is ignored.
The PSH bit indicates PUSHed data. The receiver is hereby kindly requested to deliver the data to the application upon arrival and not buffer it until a full buffer has been received (which it might otherwise do for efficiency).
The RST bit is used to reset a connection that has become confused due to a host crash or some other reason.
The SYN bit is used to establish connections.
The connection request has SYN = 1 and ACK = 0 to indicate that the piggyback acknowledgement field is not in use.

The connection reply does bear an acknowledgement, so it has SYN = 1 and ACK = 1.
In essence the SYN bit is used to denote CONNECTION REQUEST and CONNECTION ACCEPTED, with the ACK bit used to distinguish between those two possibilities.
The FIN bit is used to release a connection. It specifies that the sender has no more data to transmit. However, after closing a connection, the closing process may continue to receive data indefinitely. Both SYN and FIN segments have sequence numbers and are thus guaranteed to be processed in the correct order.
Flow control in TCP is handled using a variable-sized sliding window.
The Window size field tells how many bytes may be sent starting at the byte acknowledged.
A Window size field of 0 is legal and says that the bytes up to and including Acknowledgement number - 1 have been received, but that the receiver is currently badly in need of a rest and would like no more data for the moment, thank you.
The receiver can later grant permission to send by transmitting a segment with the same Acknowledgement number and a nonzero Window size field.
A Checksum is also provided for extra reliability. It checksums the header, the data, and the conceptual pseudoheader shown in FIG



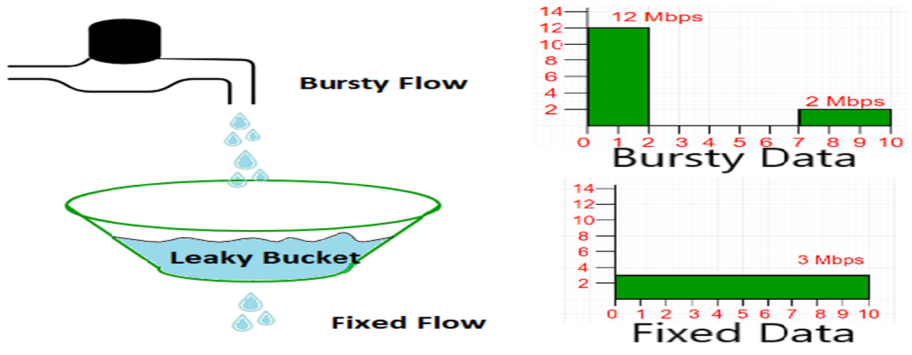
The pseudoheader included in the TCP checksum.

b) Explain leaky bucket algorithm. 6M

A: In the network layer, before the network can make Quality of service guarantees, it must know what traffic is being guaranteed. One of the main causes of congestion is that traffic is often bursty.
To understand this concept first we have to know little about traffic shaping. **Traffic Shaping** is a mechanism to control the amount and the rate of the traffic sent to the network. Approach of congestion management is called Traffic shaping. Traffic shaping helps to regulate rate of data transmission and reduces congestion.
There are 2 types of traffic shaping algorithms:

1. Leaky Bucket
2. Token Bucket

Suppose we have a bucket in which we are pouring water in a random order but we have to get water in a fixed rate, for this we will make a hole at the bottom of the bucket. It will ensure that water coming out is in a some fixed rate, and also if bucket will full we will stop pouring in it.
The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate.



In the figure, we assume that the network has committed a bandwidth of 3 Mbps for a host. The use of the leaky bucket shapes the input traffic to make it conform to this commitment.

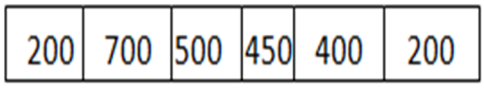
In Figure the host sends a burst of data at a rate of 12 Mbps for 2 s, for a total of 24 Mbits of data.
The host is silent for 5 s and then sends data at a rate of 2 Mbps for 3 s, for a total of 6 Mbits of data.
In all, the host has sent 30 Mbits of data in 10 s. The leaky bucket smooths the traffic by sending out data at a rate of 3 Mbps during the same 10s.
Without the leaky bucket, the beginning burst may have hurt the network by consuming more bandwidth than is set aside for this host. We can also see that the leaky bucket may prevent congestion.

A simple leaky bucket algorithm can be implemented using FIFO queue. A FIFO queue holds the packets. If the traffic consists of fixed-size packets (e.g., cells in ATM networks), the process removes a fixed number of packets from the queue at each tick of the clock. If the traffic consists of variable-length packets, the fixed output rate must be based on the number of bytes or bits.

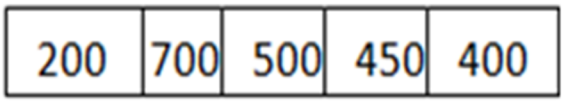
The following is an algorithm for variable-length packets:

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

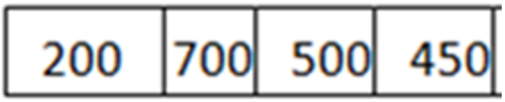
Example – Let n=1000

Packet= 

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



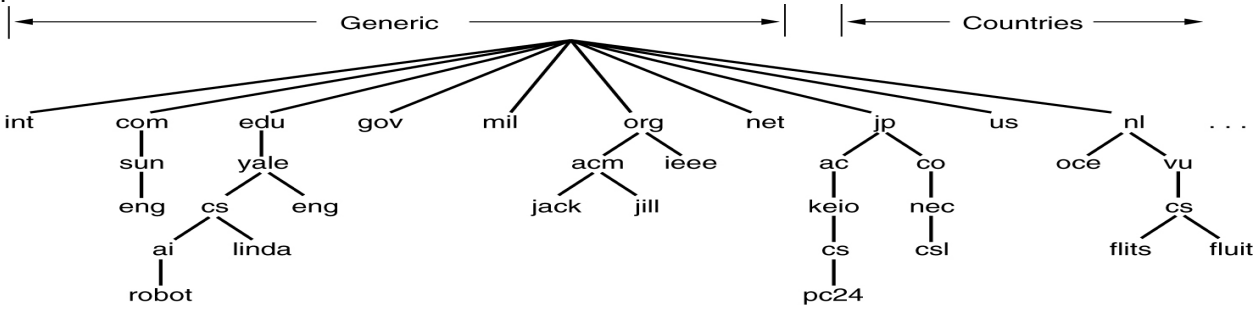
Now Again n>front of the queue i.e. n > 400
Therefore, n=800-400=400
Packet size of 400 is sent to the network.



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

9 a) Explain Domain Name System with relevant figures. 6M

A: It is primarily used for mapping host names and e-mail destinations to IP addresses but can also be used for other purposes.
To map a name onto an IP address, an application program calls a library procedure called the resolver, passing it the name as a parameter.
The resolver sends a UDP packet to a local DNS server, which then looks up the name and returns the IP address to the resolver, which then returns it to the caller.
Armed with the IP address, the program can then establish a TCP connection with the destination or send it UDP packets.



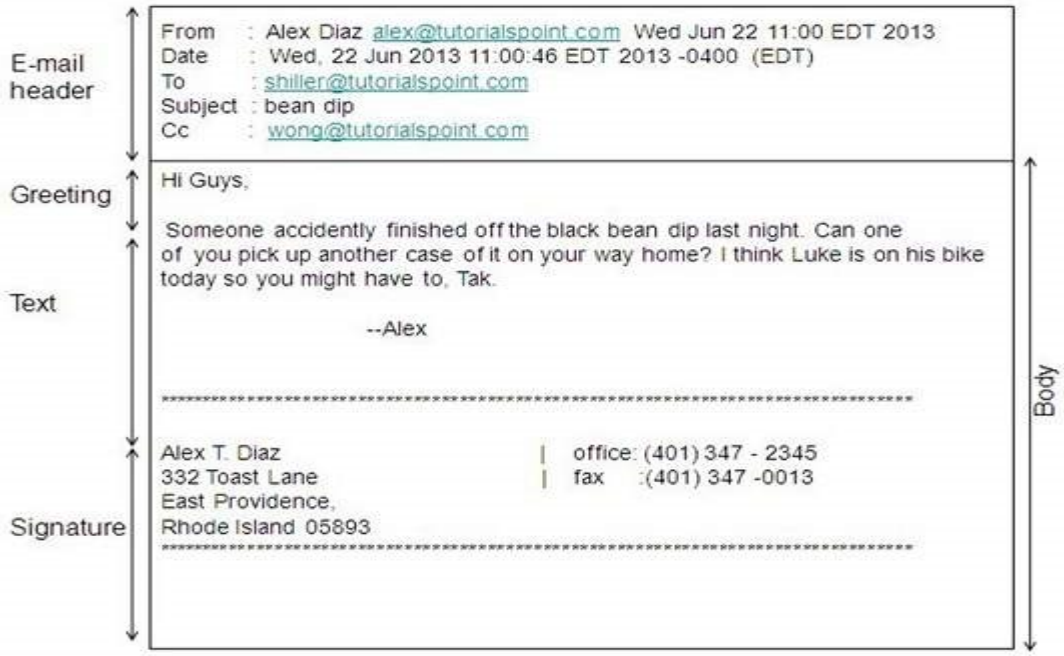
The top-level domains come in two flavors: generic and countries.
The original generic domains were com (commercial), edu (educational institutions), gov (the U.S. Federal Government), int (certain international organizations), mil (the U.S. armed forces), net (network providers), and org (nonprofit organizations).
In November 2000, ICANN approved four new, general-purpose, top-level domains, namely, biz (businesses), info (information), name (people's names), and pro (professions, such as doctors and lawyers).
In addition, three more specialized top-level domains were introduced at the request of certain industries. These are aero (aerospace industry), coop (co-operatives), and museum (museums). Other top-level domains will be added in the future.
Domain names can be either absolute or relative. An absolute domain name always ends with a period (e.g., eng.sun.com.), whereas a relative one does not.
Relative names have to be interpreted in some context to uniquely determine their true meaning. In both cases, a named domain refers to a specific node in the tree and all the nodes under it.
Domain names are case insensitive, so edu, Edu, and EDU mean the same thing.
Component names can be up to 63 characters long, and full path names must not exceed 255 characters.
To create a new domain, permission is required of the domain in which it will be included.
For example, if a VLSI group is started at Yale and wants to be known as vlsi.cs.yale.edu, it has to get permission from whoever manages cs.yale.edu.

b) Explain about E-Mail. 6M

A:Email
Email is a service which allows us to send the message in electronic mode over the internet. It offers an efficient, inexpensive and real time mean of distributing information among people.
E-Mail Address
Each user of email is assigned a unique name for his email account. This name is known as E-mail address. Different users can send and receive messages according to the e-mail address.
E-mail is generally of the form username@domainname. For example, webmaster@tutorialspoint.com is an e-mail address where webmaster is username and tutorialspoint.com is domain name.

- The username and the domain name are separated by **@ (at)** symbol.
- E-mail addresses are not case sensitive.
- Spaces are not allowed in e-mail address.

E-mail Message Components
E-mail message comprises of different components: E-mail Header, Greeting, Text, and Signature. These components are described in the following diagram:



E-mail Header
The first five lines of an E-mail message is called E-mail header. The header part comprises of following fields:

- From
- Date

- To
- Subject
- CC
- BCC

From

The **From** field indicates the sender's address i.e. who sent the e-mail.

Date

The **Date** field indicates the date when the e-mail was sent.

To

The **To** field indicates the recipient's address i.e. to whom the e-mail is sent.

Subject

The **Subject** field indicates the purpose of e-mail. It should be precise and to the point.

CC

CC stands for Carbon copy. It includes those recipient addresses whom we want to keep informed but not exactly the intended recipient.

BCC

BCC stands for Black Carbon Copy. It is used when we do not want one or more of the recipients to know that someone else was copied on the message.

Greeting

Greeting is the opening of the actual message. Eg. Hi Sir or Hi Guys etc.

Text

It represents the actual content of the message.

Signature

This is the final part of an e-mail message. It includes Name of Sender, Address, and Contact Number.

Advantages

E-mail has prooved to be powerful and reliable medium of commmunication. Here are the benefits of **E-mail:**

- Reliable
- Convenience
- Speed
- Inexpensive
- Printable
- Global
- Generality

Reliable

Many of the mail systems notify the sender if e-mail message was undeliverable.

Convenience

There is no requirement of stationary and stamps. One does not have to go to post office. But all these things are not required for sending or receiving an mail.

Speed

E-mail is very fast. However, the speed also depends upon the underlying network.

Inexpensive

The cost of sending e-mail is very low.

Printable

It is easy to obtain a hardcopy of an e-mail. Also an electronic copy of an e-mail can also be saved for records.

Global

E-mail can be sent and received by a person sitting across the globe.

Generality

It is also possible to send graphics, programs and sounds with an e-mail.