B.Tech.

Fifth Semester Examination

Computer Networks (IT-305F)

Q. 1. (a) Which OSI layer performs the following functions :

(i) Converting digital baits into electrical signals and to define voltages and data rates for transmission.

(ii) Providing remote login to network users.

(iii) Routing

(iv) Compression and decompression of data.

Ans. (i) Physical layer converts digital bits into the electrical signals. It also decides the voltage to be assigned to various data levels.

(ii) Application layer provides remote login via TELNET.

(iii) Network layer performs routing.

(iv) Presentation layer deals with compression and decompression.

Q. 1. (b) What is the number of cable links required for *n* devices connected in Mesh, Ring, Star and Bus topologies?

Ans. In mesh topology each device is connected to every other device in the network using dedicated links. Thus, for *n* devices in **Mesh Topology** we require $n(n-1)/2$connections/cable links. For **Bus Topology, Ring Topology** and **Star Topology** we require only **n cables** to connect *n* devices. Because here all devices are not connected to every other device instead has point-to-point dedicated link to some other device.

Q. 1. (c) What is the baud rate of a 5Mbps IEEE 802.3 CSMA/CD LAN?

Ans. Baud rate $= 2^*$ Bit rate

Here, Bit rate $= 5$ Mbps

$= 5 \times 10^6$ bps

$\therefore$ Baud rate $= 2^* 5^* 10^6$ bps

$= 10 \times 10^6 = 10^7$ **bauds per seconds**

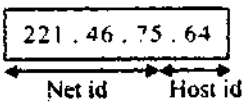
Q. 1. (d) If the address of a system is 221.46.75.64. Find network id, host id and class of network and network address.

Ans. IP Address is 221.46.75.64 : This is a **class C** address. Range of class C is 192 to 223 in first byte (left hand side). In class C the leftmost three bytes are reserved for net id and rightmost one byte is host id.

$\therefore$ Net id is : 221.46.75

Host id is : 64

Network address : 221.46.75.0



Q. 1. (e) Identify the protocols used for following :

(i) Connection oriented communication

(ii) Global Addressing

(iii) File transfer in connection oriented methodology

(iv) Mapping logical address to physical address

Ans. (i) Connection Oriented Communication—TCP (Transmission Control Protocol)

(ii) Global Addressing—IP (Internet Protocol)

(iii) File Transfer in Communication Oriented Methodology—FTP (File Transfer Protocol)

(iv) Mapping Logical Address to Physical Address—ARP (Address Resolution Protocol).

Q. 1. (f) What are the advantages of IMAP4 over POP3 mail access protocol?

Ans. Advantages of IMAP4 over POP3 are as follows :

(i) A user can check email header prior to downloading.

(ii) A user can search the contents of the email for a specific string of characters priors to downloading.

(iii) A user can partially download email. This is especially useful if bandwidth is limited and the email contains multimedia with high bandwidth requirements.

(iv) A user can create, delete, or rename mailboxes on the mail server.

(v) A user can create a hierarchy of mailboxes in a folder for email storage.

Q. 1. (g) Write a short note on CSMA channel access technique.

Ans. CSMA stands for carrier sense multiple access which is a random channel method. CSMA requires that each station first listen to the medium (to check whether the channel is free or idle) before sending. CSMA can reduce the possibility of collision, but it cannot eliminate it. CSMA can be divided into three sub categories :

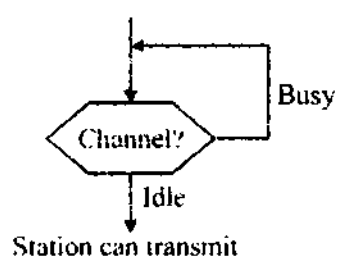


Fig. 1-Persistent

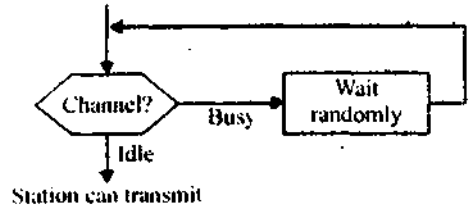


Fig. Non-persistent

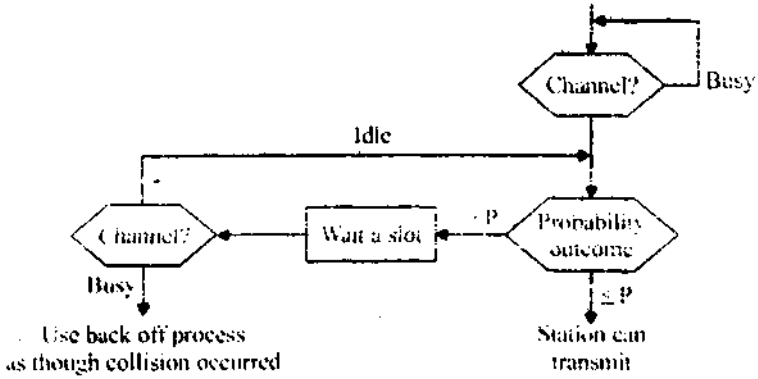
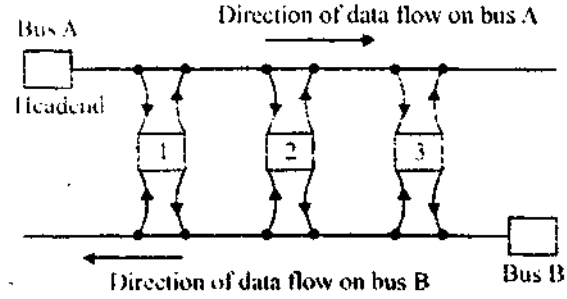


Fig. p-persistent

Q. 1. (h) Explain in short about DQDB.

Ans. DQDB stands for Distributed Queue Dual Bus. It consist of two unidirectional cables (buses) to which all computers are connected. Each bus has a device which initiates the transmission (policy) activity called as head-end. Traffic that is destined for a computer to the right of the sender uses the upper bus and to the left uses lower bus.



Q. 1. (i) What is VLAN?

Ans. A virtual LAN can be defined as a local area network designed/configured by a software and not by physical wiring. VLAN divides a LAN into logical, instead of physical segments. VLANs create broadcast domains. The stations in a VLAN communicate with one another as though they belonged to a physical segment. In VLANs stations can be grouped using port number MAC addresses, IP addresses, IP multicast addresses.

Q. 1. (j) Define Proxy Servers.

Ans. HTTP supports proxy servers. A proxy server is a computer that keeps copies of responses to recent requests. The HTTP client sends a request to the proxy server. The proxy server then checks its cache. If the response is not stored in the cache, the proxy server sends the request to the corresponding server. In coming responses are send to the proxy server and stored for future requests from other clients.

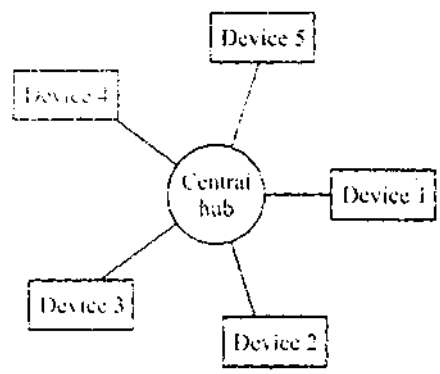
Section—(A)

Q. 2. (a) Explain the following topologies with their advantages and disadvantages :

(i) Star Topology

(ii) Mesh Topology

Ans. (i) Star Topology : In star topology, each device has a dedicated point-to-point link only to a central controller, usually called as hub. The devices here are not directly linked to one another. Thus, to connect n devices in star topology, it requires n cables. The controller acts as an exchange: if one device wants to send data to another, it sends the data to the controller, which then relays the data to other connected devices.



Advantages : (i) Less expensive than mesh topology as it requires less cabling. Thus, easy to install and reconfigure. Addition and deletions of devices is easy so, becomes more scalable.

(ii) It is robust network. If one link fails only that link is affected, other links remain active. Fault identification and isolation is easy.

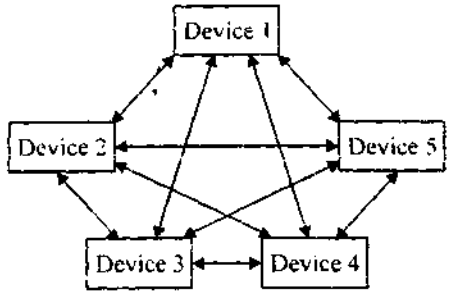
Disadvantages : (i) Biggest disadvantage is dependence of whole network on central controller hub. If the hub goes down, whole network goes down.

(ii) Mesh Topology : In mesh topology, every device has a dedicated (path) point-to-point link to every other device. Thus, if there are n devices to be connected in mesh topology, it requires $n(n-1)$ cables. In mesh topology duplex mode links are used. Practical application can be seen in connection of telephone regional offices.

Advantages : (i) The use of dedicated links guarantees that each connection can carry its own data, thus eliminating traffic problems.

(ii) Mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

(iii) Mesh topology guarantees privacy and security.

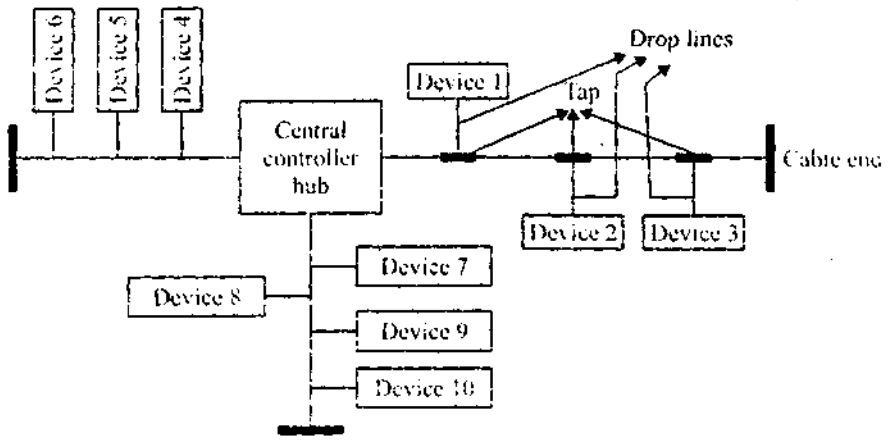


Disadvantages : (i) Major disadvantage of mesh topology is related to vast amount of cabling required and number of I/O ports.

(ii) Also, the hardware required to connect each link I/O ports and cables can be prohibitively expensive.

Q. 2. (b) Draw hybrid topology with a Star backbone and three bus networks.

Ans. Hybrid topology is nothing but a combination of two or more topologies. Here the hybrid topology consist of Star as main topology with each branch consisting on several station connected in bus topology.



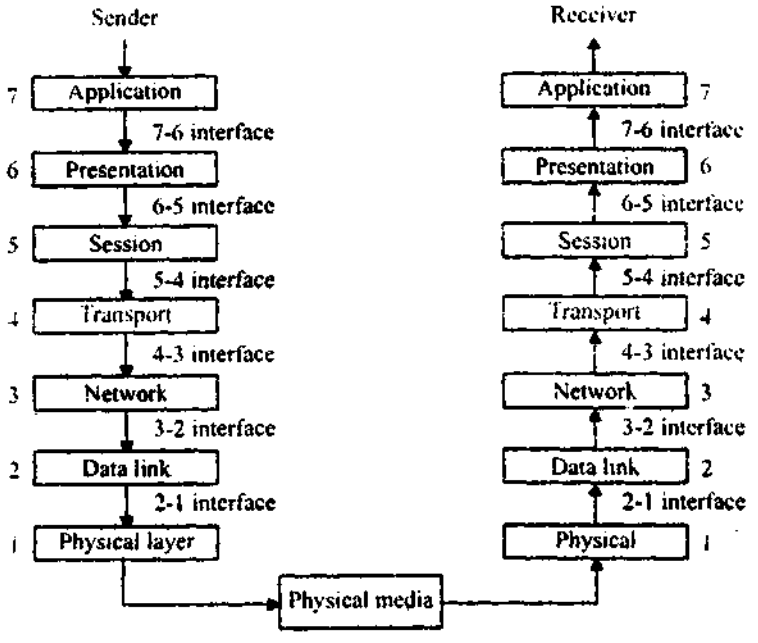
Q. 2. (c) If the frequency spectrum of a signal has a bandwidth of 1000 Hz with the highest frequency of 800Hz. Then, according to Nyquist theorem what should be the sampling rate?

Ans. According to Nyquist theorem, sampling rate is twice the highest frequency.

$\therefore$ Sampling rate $= 2 * \text{Freq.} = 2 * 800 = 1600$

Q. 3. Draw OSI Reference Model and explain the functions of different layers. Also mention the protocols required at layers. Give similarities and differences to TCP/IP Model.

Ans. OSI Reference Model :



(i) Physical Layer : (i) Physical layer is concerned with various characteristics of the transmission medium or physical medium used.

(ii) It defines the encoding of how bits (0's and 1's) are changed to electrical or optical signals.

(iii) Physical layer decides what topology should be used. Decides on whether connection should be point to point or multipoint. It also decides what should be the communication mode—simplex, half duplex or full duplex.

(ii) Data Link Layer : (i) Data link layer performs framing-dividing continuous bit stream into data chunks called frames.

(ii) It performs physical addressing—MAC addresses.

(iii) Data link layer takes care of error control and error detection and correction.

(iv) It performs flow control and checks sender should send the data at which receiver is ready to accept at.

(v) Data link layer performs access control. When two or more devices want to send data at same time, data link layer should decide on which device should the channel be given access to.

Protocols Used : CSMA, Aloha, CSMA/CD, CSMA/CA.

(iii) Network Layer : (i) Network layer performs logical, global addressing–IP addressing.

(ii) It performs routing which decides on which route/path data packets should follow inorder to reach the destination.

Protocol Used : IP (Internet Protocol), ICMP.

Service Access Points : ARP, RARP.

(iv) Transport Layer : (i) Transport layer is responsible for end to end process delivery. This means data should reach a particular host and that too a particular process.

(ii) It performs segmentation and reassembly of messages.

(iii) It decides whether connection established should be connection oriented or connectionless.

(iv) It performs congestion control, multiplexing and demultiplexing.

Protocol Used : TCP (Transmission Control Protocol)

(v) Session Layer : (i) Session layer performs dialog control, allows two system to enter into dialog.

(ii) It allows a process to add checkpoints, or synchronization points, to a stream of data.

Protocol Used : RPC (Remote Procedure Call)

(vi) Presentation Layer : (i) It performs compression and decompression.

(ii) It also deals with encoding and decoding of data.

Protocols Used : MPEG, JPEG, Kerberos, MAC.

(vii) Application Layer :

(i) Application layer provides a network virtual terminal, which allows a user to log on to a remote host.

(ii) File transfer, access and management.

(iii) Mailing services

(iv) Directory services

Protocols Used : FTP (File Transfer Protocol), TELNET (Terminal Network), DNS (Domain Name System), HTTP (Hyper Text Transfer Protocol), POP3 (Post Office Protocol), DHCP (Dynamic Host Configuration Protocol), BOOTP.

Similarities Between OSI and TCP/IP :

(i) In both the models layers have roughly same functionality.

(ii) Both models use same concept of layered architecture.

(iii) The transport layers and layer below it provide transport services independent of networks.

(iv) In both the models, the layers above transport layer are application oriented

Differences Between OSI and TCP/IP Model :

(i) TCP/IP model didnot originally distinguish clearly between services, interface and protocols, but OSI model makes a clear distinguistion between the three.

(ii) OSI reference model was devised before the corresponding protocols were devised, whereas TCP/IP protocols were in place first and then came the layers.

(iii) OSI model supports both connection oriented and connectionless communication in network layer, but only connection oriented in transport layer. Whereas, TCP/IP supports connectionless in network layer and both the modes at transport layer.

(iv) OSI model has seven layers—Physical, Data Link, Network, Transport, Session, Presentation and Application TCP/IP has four layers—Host-to-network, Internet, Transport and Application layer.

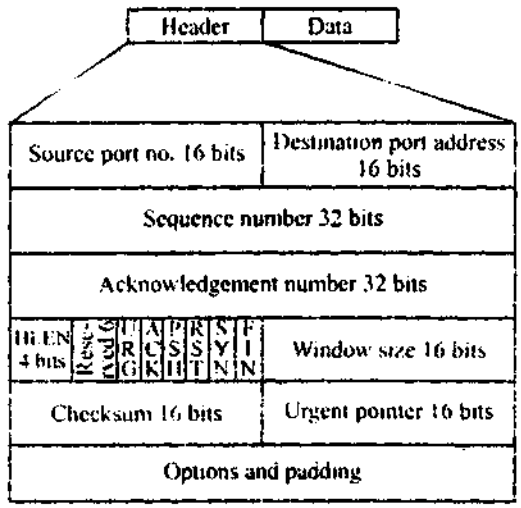
Section—(B)

Q. 4. (a) Compare and contrast TCP and UDP. Also draw headers of both.

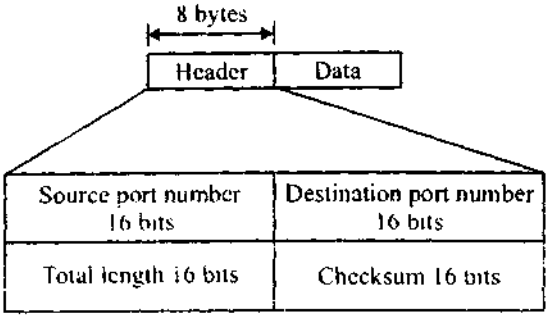
Ans.

	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
(i)	Transmission control protocol is a connection oriented methodology. Here, a connection is established via three way handshake before the data is exchanged.	User datagram protocol is a connectionless approach. The data is exchanged without setting up a prior connection establishment.
(ii)	TCP is a reliable protocol as it consist of flow control error control, acknowledgement and sequence number mechanism.	UDP is an unreliable protocol. Though UDP performs the error control using checksum but it has limited functionality having no flow control, no acknowledgements and no sequence number mechanism.
(iii)	TCP is a protocol where data is sent in form of a stream of bytes.	UDP sends data in small packets or datagram.
(iv)	TCP is slower than UDP as it waits for acknowledgement before sending data.	UDP is simple protocol with minimum overhead and is very fast as it doesnot wait for acknowledgement and sends data in form of small messages called datagrams.
(v)	**Applications :** FTP (File Transfer Protocol), DNS (Domain Name System).	**Applications :** TFTP (Trival File Transfer Protocol) SNMP, RIP.

TCP Header :



UDP Header :



Q. 4. (b) Define the functions of following protocols in a single line :

(i) ARP **(ii) RARP** **(iii) SMTP**

(iv) FTP **(v) ICMP**

Ans. (i) ARP (Address Resolution Protocol) : ARP is used for mapping logical address to physical address. Thus, if a system knows IP address and wants to find physical MAC address ARP is used.

(ii) RARP (Reverse Address Resolution Protocol) : RARP is used to map physical address to logical address. Thus, RARP helps to find IP address if MAC address imprinted on NIC (Network Interface Card) is known.

(iii) SMTP (Simple Main Transfer Protocol) : SMTP is a push protocol which is used to send a mail through internet. It is used two times, once between sender and sender's mail server and then between sender and receiver's main server.

(iv) FTP (File Transfer Protocol) : FTP is a standard mechanism provided by TCP/IP for copying a file from one system/host to another. It uses services of TCP and requires two connections one through port 21-control connection and other through port 20-data connection.

(v) ICMP (Internet Control Message Protocol) : IP protocol lacks a mechanism for host and management queries. IP also has no error reporting and correcting mechanisms. Thus, ICMP has been designed to accompany IP and avoid these two problems.

ICMP has : (i) Error reporting messages

(ii) Query messages

Q. 4. (c) A class C network has IP address of a host as 198.123.46.237. Four subnetworks are allowed for this network. What is the subnet mask, number of host per subnet and subnet address?

Ans. Class C network has default subnet mask

255 . 255 . 255 . 0

Net id Host id

If we need to form 4 subnets, we need to borrow 2 bits from host id (moving from left to right)

$2^2 = 4$ ∴ 2 bits for subnet

Subnet mask 11111111.11111111.11111111.11000000

↔ 2 bits borrowed for subnet

255.255.255.192 **Ans.**

No. of host per subnet $= 2^n - 2$

Where n is no of host bits

$= 2^6 - 2 = 64 - 2 = 62$ **Ans.**

Subnet Address = Destination address*Subnet mask

198 . 123 . 46 . 237

Destination address = 11000110 . 01111011 . 00101110 . 11101001

Subnet mask = 11111111 . 11111111 . 11111111 . 11000000

↓ Anding

Subnet address = 11000110 . 01111011 . 00101110 . 11000000

ANDING

198 . 123 . 46 . 192 **Ans.**

Q. 5. (a) Perform the subnetting of the following IP address 160.111.X.X.

Original subnet mask : 255.255.0.0

Number of subnets six (6)

Ans. IP address 160.111.X.X is of class B

∴ Original subnet mask : 255.255.0.0

We require 6 subnets $2^3 > 6 \Rightarrow 876$ This indicates we need to borrow 3 bits from host id to design subnets

Subnet Mask : 11111111 · 11111111 · 11100000 · 00000000

255 · 255 · 224 · 0

← Net id → ← Host id →

6 subnets will be from 000 to 001.

1st Subnet : "000"

Identification Address : 160 · 111 · 0 · 0

(All host id bits are 0) 160 · 111 · 10001 00000 · 00000000

← Net id → ← Subnet → ← Host id →

First host address : 160 · 111 · 0 · 1

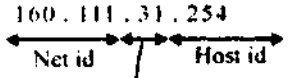
(Set last bit of host id as 1) 160 . 111 . 1000100000 . 00000001

← Net id → ← Subnet →

Last host address 160 · 111 · 31 · 254

Set all bits "1" leaving

rightmost bits "1" in host id .



160 . 111 . 000| 1111 . 1111110

Broadcasting 160 · 111 · 31 · 255

Set all host id bits as 1

2nd Subnet : "001"

Identification Address · 160 · 111 · 32 · 0

Host Address : 160 · 111 · 32 · 1 to 160 · 111 · 63 · 254

Broadcasting Address : 160 · 111 · 63 · 255

3rd Subnet : "010"

Identification Address : 160 · 111 · 64 · 0

Host Addresses : 160 · 111 · 64 · 1 to 160 · 111 · 95 · 254

Broadcasting Address : 160 · 111 · 95 · 255

4th Subnet : "011"

Subnet Identification Address : 160 · 111 · 96 · 0

Host Addresses : 160 · 111 · 96 · 1 to 160 · 111 · 254

Broadcasting Address · 160 · 111 · 127 · 255

5th Subnet : "100"

Subnet Identification : 160 · 111 · 128 · 0

Host Addresses : 160 · 111 · 128 · 1 to 160 · 111 · 159 · 254

Broadcasting Address : 160 · 111 · 159 · 255

6th Subnet : "101"

Subnet Identification : 160 · 111 · 160 · 0

Host Addresses : 160 · 111 · 160 · 1 to 160 · 111 · 191 · 254

Broadcasting Address : 160 · 111 · 192 · 255

Q. 5. (b) Differentiate between IPv4 and IPv6. Also draw the header of IPv4.

Ans. Following are the comparisons between IPv4 and IPv6 :

(i) The header length field is eliminated in IPv6 because the length of the header is fixed in this version.

(ii) The service type field is eliminated in IPv6. The priority and label fields together take over the function of the service type field.

(iii) Total length field is eliminated in IPv6 and replaced by the payload length field.

(iv) The identification, flag, and offset fields are eliminated from base header in IPv6. They are included in the fragmentation extension header.

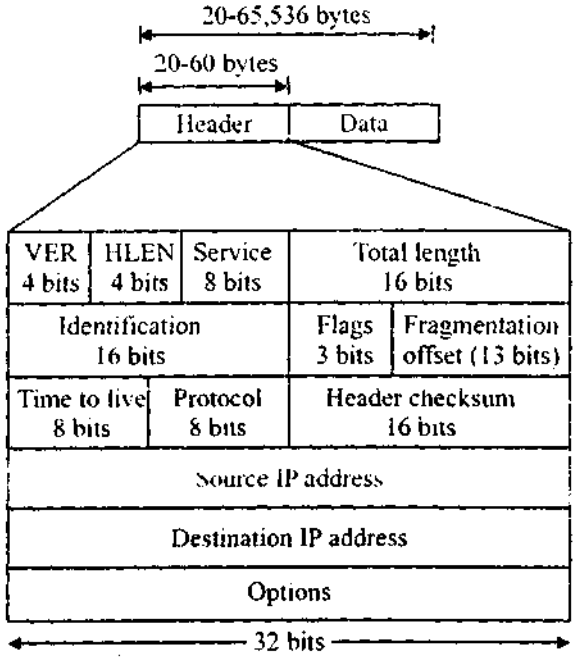
(v) The TTL field is called hop limit in IPv6.

(vi) The protocol field is replaced by the next header field

(vii) The header checksum is eliminated because the checksum is provided by upper layer protocols, it is therefore not needed at this level.

(viii) The options field in IPv4 are implemented as extension headers in IPv6.

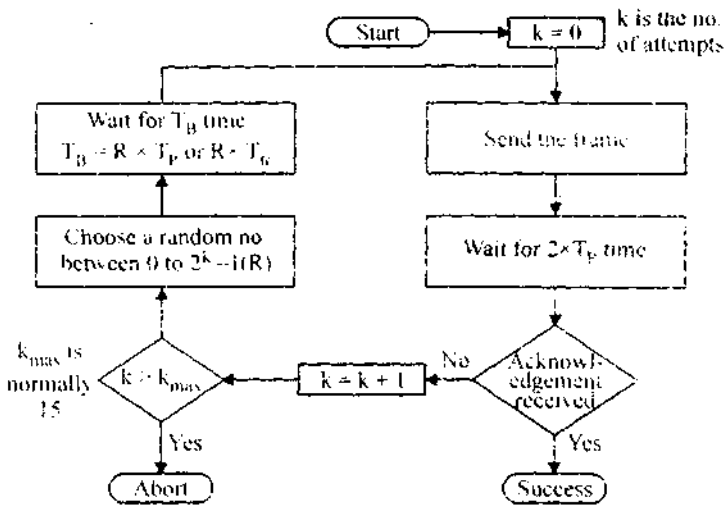
IPv4 Header :



Section—(C)

Q. 6. (a) Discuss and state the differences between pure and slotted Aloha. Also derive the efficiency of both pure and slotted Aloha. State the Binary Exponential Algorithm used here.

Ans. Pure Aloha : Pure aloha is random channel access protocol. Here the simple idea works, where a station sends a frame whenever it has a frame to send. But as all the devices access same channel, there are high chances of collision. All the devices are accessing same station and has no priority on basis of which channel could be allocated to them.



T_{fr} → Average transmission time for frame

T_p → Maximum propagation time

Binary Exponential Backoff : It is the process to find T_B time, also called as backoff time. This time T_B is the time device has to wait once the acknowledgement is not received for same data send (means collision has occured)

$$T_B = R \times T_P \text{ or } T_B = R \times T_{fr}$$

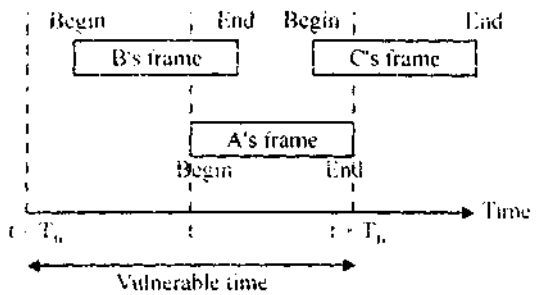
Here, R is any random number between 0 to $2^k - 1$

k is no. of attempts made to send data

T_P is maximum propagation time required

T_{fr} is average frame transmission time.

Vulnerable time in pure aloha is twice the frame transmission time because the collision can occur with previous or upcoming frame. Vulnerable time is the time where chances of collision are high.



All devices has equal sized frame.

Vulnerable time $= t + T_{fr} - t + T_{fr} = 2T_{fr}$

Using Poission distribution :

$$P(K) = \frac{G^K e^{-G}}{K!}$$

$K \rightarrow$ Frame generated during a given frame time

$G \rightarrow$ Mean frames/frame time

$$P(K = 0) = \frac{G^0 e^{-G}}{0!} = e^{-G}$$

Vulnerable period $= 2\times$ Frame transmission time

$\therefore$ $G = 2G$

So, $P_0 = e^{-2G}$

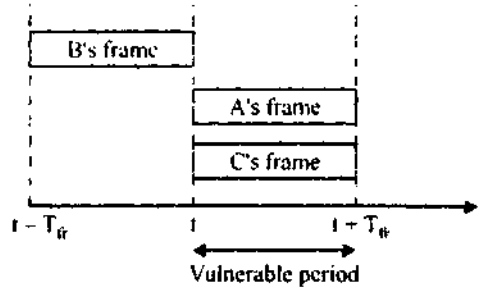
Throughput $= S = GP_0 = Ge^{-2G}$

Maximum throughput $S_{max} = 0.184$ when $G = \frac{1}{2}$

Slotted Aloha : Here, we divide the time into slots of T_{fr} and force the stations to send the data only at beginning of time slot. If a station misses the beginning of a slot at a moment then it must wait for next slot to begin.

Thus, vulnerable time $= T_{fr}$

Vulnerable time $= t + T_{fr} - t = T_{fr}$



$$P(K) = \frac{G^K e^{-G}}{K!}$$ Using Poisson distribution

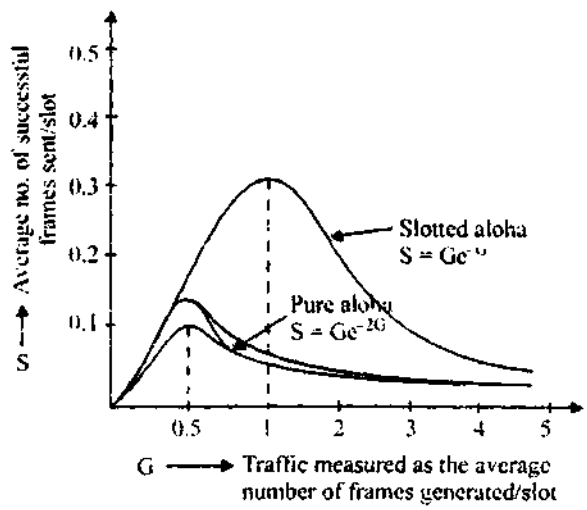
As vulnerable period $= T_{fr}$ $\therefore G$ remains as G

$$P(K = 0) = \frac{G^0 e^{-G}}{0!} = e^{-G}$$

Throughput, $S = GP_0 = Ge^{-G}$

Maximum throughput $S_{max} = 0.368$ Where $G = 1$

	Pure Aloha	Slotted Aloha
(i)	In pure aloha there are no time slots and stations can send the data when these stations wish to send. Thus, chances of collision and time period of collision is more.	In slotted aloha devices or stations can send the data only at beginning of a time slot. Thus, the chances of collision and time period of collision is less.
(ii)	Throughput of pure aloha $S = Ge^{-2G}$	Throughput of slotted aloha $S = Ge^{-G}$
(iii)	Maximum throughput is when $G = 1/2$ $S_{max} = 0.184$	Maximum throughput is when $G = 1$ $S_{max} = 0.368$
(iv)	Pure aloha is less efficient than slotted aloha.	Efficiency of slotted aloha is higher than pure aloha.



Q. 6. (b) Measurements of a slotted aloha channel with an infinite number of user. Show that 10% of the slots are idle :

(i) What is Channel Load?

(ii) What is Throughput?

(iii) Is the channel overloaded or underloaded.

Ans. (i) Channel Load :

For a slotted aloha, $P_0 = e^{-G}$

$P_0 = 10\% = 0.1$

$\therefore \quad 0.1 = e^{-G}$

$-2.3 = -G \quad \Rightarrow G = 2.3$ **Ans.**

(ii) Throughput : $S = Ge^{-G} = 2.3e^{-2.3} = 0.23$ **Ans.**

(iii) Since G is beyond 1, the channel is overloaded.

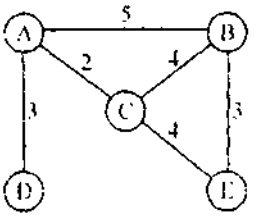
Q. 7. (a) Explain the distance vector routing with the help of an example. Also discuss the major problem encountered in distance vector : Count to infinity problem. What is the protocol using distance vector routing?

Ans. Distance Vector Routing : Here, the least cost route between any two nodes is the route with minimum distance. Initially, each node knows only the distance between itself and its immediate neighbours, which are directly connected to each other. Nodes prepare initial table using this information only and any entry that is not an immediate neighbour is marked as infinity.

After this each node share its routing table with its own neighbour and update the routing table. The routing table is updated only if the cost of itself and the cost added of neighbour's table is both less than current cost and then the value in next column is also updated, corresponding to the changed row as neighbour's name.

A's table

To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	∞	



B's table

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	∞	—
E	3	—

D's table

To	Cost	Next
A	3	—
B	∞	
C	∞	
D	0	—
E	∞	

C's table

To	Cost	Next
A	2	—
B	4	—
C	0	—
D	∞	—
E	4	—

E's table

To	Cost	Next
A	∞	
B	3	B
C	4	C
D	∞	
E	0	D

Now, C shares its routing table to A. A now creates a new table changing only those rows in the routing table where the cost of A to that neighbour C, then cost of C to corresponding node is less than the current values and put value in the next column of corresponding row as C.

A's new table

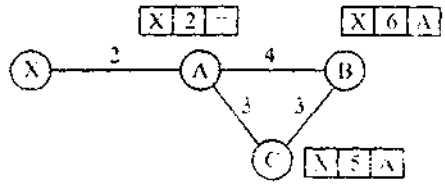
To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

Now A shares this table to D D's new table

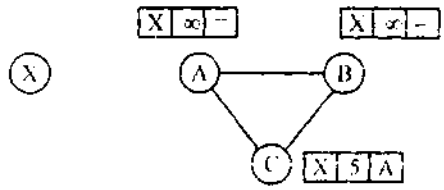
To	Cost	Next
A	5	—
B	8	A
C	5	A
D	0	—
E	9	A

The routing tables are shared periodically every 30sec and also immediately if there is a change in any node's routing table.

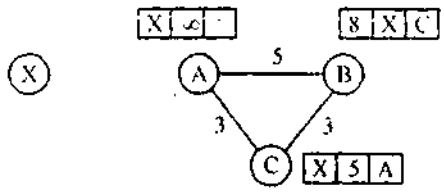
Count to Infinity Problem :



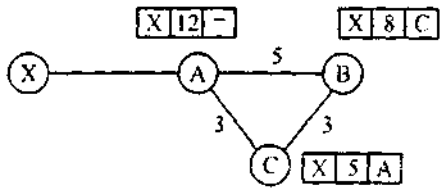
Link from node X to node A fails then A updates its routing table and sends its routing table to B and C. But the table reaches only B and is not able to reach C because it is lost in traffic.



Now, node C sends it routing table to B which is not updated and B is totally fooled. B thinks there is a path to X from C and updates its table accordingly.



B sends it's routing table to A and same A thinks there is a path to X via B.



The process keeps on repeating and the loop starts when the cost in each node reaches infinity.

Q. 7. (b) A computer on a 6-Mbps network is regulated by token bucket. Token bucket filled at a rate of 1 Mbps. It is initially filled to a capacity with 8 megabits. How long can computer transmit at the full 6 Mbps?

Ans. Given : C = Bucket capacity = 8 Mb

m = Maximum output rate = 6 Mbps

ρ = Token arrival rate = 1Mbps

S = Time for which maximum output is obtained

$$S = \frac{C}{m - \rho}$$

$$= \frac{8 \text{ M bits}}{6 \text{ Mbps} - 1 \text{ Mbps}}$$

$$= \frac{8}{5} = 1.6 \text{sec Ans.}$$

So, the computer can transmit at the full 6 Mbps for 1.6 sec. **Ans.**

Section—(D)

Q. 8. Write short note on the following :

(i) Synchronous Optical Network (SONET)

(ii) Asynchronous Transfer Mode (ATM)

(iii) Frame Relay

(iv) Quality of Service

Ans. (i) Synchronous Optical Network (SONET) : SONET is a synchronous network using synchronous TDM multiplexing. All clocks in the system are locked to a master clock. SONET defines a hierarchy of electrical signaling levels called synchronous transport signals (STSs). Each STS level varying from STS-1 to STS-192 support a certain data rate, specified in megabits per second. The corresponding optical signals are called optical carriers.

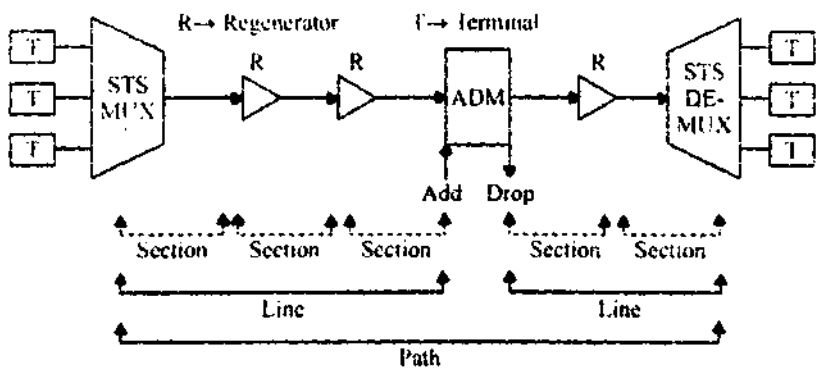
SODENT Devices :

(i) STS Multiplexer/Demultiplexer : These mark beginning and end points of SONET links.

(ii) Regenerator : Extends extend the length of links.

(iii) Add/Drop Multiplexer : These can add STSs coming from different sources into a given path or can remove.

(iv) Terminals : It is a device using service of a SONET.



(ii) Asynchronous Transfer Mode (ATM) : ATM is the cell relay protocol designed by ATM forum and adopted by ITU-T. The combination of ATM and SONET will allow high speed interconnection of all the world's network.

ATM is a cell switched network. The user access devices, called the endpoints, are connected through a user to network interface (UNI) to the switches inside the work. The switches are connected through network-to-network interfaces (NNIs).

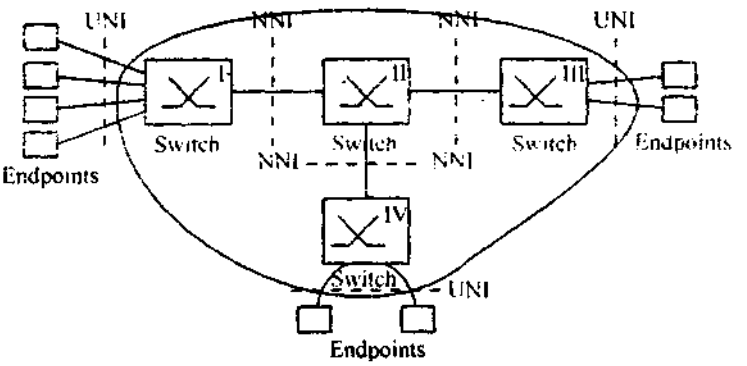


Fig. Architecture of ATM networks

Connection between two endpoints is accomplished through transmission paths (TPs), virtual paths (VPs) and virtual circuits (VCs). A "TP" is the physical connection between an endpoint and a switch or between two switches. A "VP" provides a connection or a set of connections between two switches. A "TP" is divided into several "VP". All cells belonging to a single message follow same virtual circuit and remain in their original order until they reach their destination.

(iii) Frame Relay : Frame relay is a virtual circuit wide-area-network that was designed in response to demands for a new type of WAN in the late 1980s and early 1990s. Frame relay operates at a higher speed 1.544 Mbps. This means that it can be easily used instead of a mesh of T-1 or T-3 lines. It operates in just the physical and data link layers. Frame relay allows bursty data. Frame relay allows a frame size of 9000 bytes, which can accommodate all local area network frame sizes. Frame relay is less

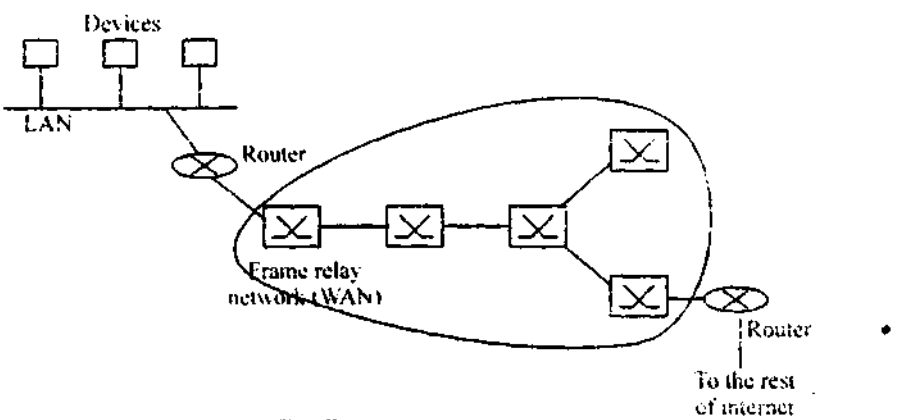


Fig. Frame relay network

expensive than other traditional WANs. It has error detection at data link layer only. There is no flow control or error control. There is not even a retransmission policy if a frame is damaged; it is silently dropped. Frame relay provides permanent virtual circuits and switched virtual circuits.

(iv) Quality of Service : Quality of service is an internetworking issue that has been designed on the basis of flow characteristics. Traditionally, four characteristics are attributed to flow :

(i) Reliability : Reliability is a characteristic that a flow needs. Lack of reliability means losing a packet or acknowledgement, which entails retransmission.

(ii) Delay : Source-to-destination delay is another flow characteristic. Again applications can tolerate delay in different degrees. In case, telephony, audio conferencing, video conferencing and remote log in need minimum delay, while delay in file transfer or e-mails is less important.

(iii) Jitter : Jitter is the variation in delay for packets belonging to the same flow. High jitter means the difference between delays is large, low jitter means the variation is small.

(iv) Bandwidth : Different applications need different bandwidth. In video conferencing we need to send millions of bits per second to refresh a colour screen while the total number of bits in an e-mail may not reach even a million.

Q. 9. (a) What are Firewalls? Why are these used? Explain Packet Filter Firewall and Proxy Firewall?

Ans. A firewall is a device usually a router or a computer installed between the internal network of an organization and the rest of internet. It is designed to forward some packets and filter (not to forward) others. For example, a firewall may filter all incoming packets designed for a specific host or a specific server such as HTTP. A firewall can be used to deny access to a specific host or a specific service in the organization.

Packet Filter Firewall : A firewall can be used as a packet filter. It can forward or block packets based on the information in the network layer and transport layer headers : source and destination IP addresses, source and destination port addresses and type of protocol (TCP or UDP). A packet filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded)

Example :

Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

(i) Incoming packets from 131.34.0.0 are blocked.

(ii) Incoming packets destined for any internal TELNET server (port 23) are blocked.