SYLLABUS IT-305-F

COMPUTER NETWORKS

Sessional : 50 Marks
Theory : 100 Marks
Total : 150 Marks
Duration of Exam. : 3 Hrs.

Section-A

OSI Reference Model and Network Architecture : Introduction to Computer Networks, Example networks ARPANET, Internet, Private Networks, Network Topologies: Bus-, Star-, Ring-, Hybrid -, Tree -, Complete -, Irregular –Topology; Types of Networks : Local Area Networks, Metropolitan Area Networks, Wide Area Networks; Layering architecture of networks, OSI model, Functions of each layer, Services and Protocols of each layer.

Section-B

TCP/IP: Introduction, History of TCP/IP, Layers of TCP/IP, Protocols, Internet Protocol, Transmission Control Protocol, User Datagram Protocol, IP Addressing, IP address classes, Subnet Addressing, Internet Control Protocols, ARP, RARP, ICMP, Application Layer, Domain Name System, Email – SMTP, POP,IMAP; FTP, NNTP, HTTP, Overview of IP version 6.

Section-C

Local Area Networks: Introduction to LANs, Features of LANs, Components of LANs, Usage of LANs, LAN Standards, IEEE 802 standards, Channel Access Methods, Aloha, CSMA, CSMA/CD, Token Passing, Ethernet, Layer 2 & 3 switching, Fast Ethernet and Gigabit Ethernet, Token Ring, LAN interconnecting devices: Hubs, Switches, Bridges, Routers, Gateways.

Wide Area Networks: Introduction of WANs, Routing, Congestion Control, WAN Technologies, Distributed Queue Dual Bus (DQDB).

Section-D

Synchronous Digital Hierarchy (SDH)/ Synchronous Optical Network (SONET), Asynchronous Transfer Mode (ATM), Frame Relay., Wireless Links.

Introduction to Network Management: Remote Monitoring Techniques: Polling, Traps, Performance Management, Class of Service, Quality of Service, Security management, Firewalls, VLANs, Proxy Servers.

Introduction to Network Operating Systems: Client-Server infrastructure, Windows NT/2000.

NOTE : Examiner will set 9 questions in total, with two questions from each section and one question covering all sections which will be Q.1. This Q.1 is compulsary and of short answer type. Each question carries equal mark (20marks). Students have to attempt 5 questions in total at least one question from each section.

COMPUTER NETWORKS

Dec - 2016

Paper Code:- IT-305-F

Note : *Question No. 1 is compulsory. Attempt any four questions from the rest of paper choosing one from each Section*

Q.1.(a) What is ARPANET ? Explain.

Ans. ARPANET : It is basically a WAN. It was developed by the ARPA (Advanced Research Project Agency). ARPANET was designed to service even a nuclear attack. ARPANET used the concept of packet switching network consisting of subnet and host computers. The subnet was a datagram subnet and each subnet consist of minicomputers called IMPs (Interface Message Processors). Each node of the network used to have an IMP and a host connected by a short wire. The host could send messages of upto 8063 bits to its IMP which would break them into packets and forward them independently toward the destination. The subnet was the first electronic store-and-forward type packet switched network. So each packet was stopped before it was forwarded. The original ARPANET design is as shown in fig.

The software for ARPANET was split into two parts, namely, subnet and host. The TCP/IP model and protocol were invented specifically to handle communication over internet works because more and more networks were getting connected to ARPANET.

The TCP/IP made the connection of LANs to ARPANET easy. So, DNS (Domain Naming System) was created for organizing machines into domains and map host names onto IP address.

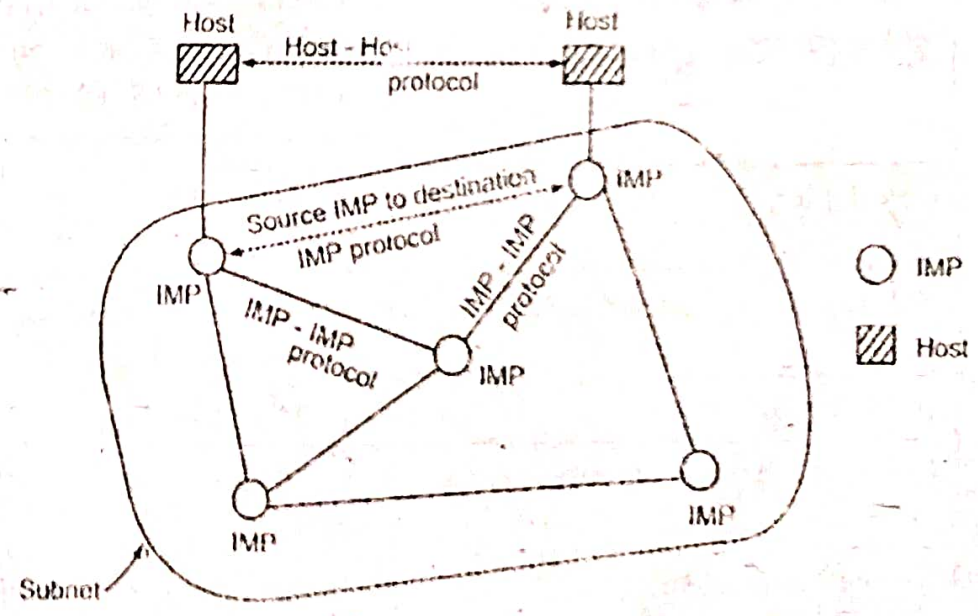


Fig. : APRANET

Q.1.(b) What is the difference between Hub and Switch ?
Ans.

	Hub	Switch
Definition	An electronic device that connects many network device together so that devices can exchange data.	A network switch is a computer networking device that is used to connect many devices together on a computer network. A switch is considered more advanced than a hub because a switch will on send msg to device that needs or request it.
Layer	Physical layer. Hubs are classified as layer 1 devices per the OSI model.	Data Link layer. Network switches operate at layer 2 of the OSI model.
Function	To connect a network of personal computers together, they can be joined through a central hub.	Allow to connect multiple device and port can be manage. Vlan can create security also can apply.
Data Transmission form	Electrical signal or bits	Frame (L2 Switch) Frame & packet (L3 switch)
Ports	4/12 ports	Switch is multi port Bridge. 24/48 ports
Transmission Type	Hubs always perform frame flooding: may be unicast multicast or broadcast	First broadcast: then unicast & multicast as needed.
Device Type	Passive Device (Without software)	Active Device (with software) & Networking device
Used in (LAN, MAN, WAN)	LAN	LAN
Table	A network hub cannot learn or store MAC address.	Switches use content accessible memory CAM table which is typically accessed by ASIC (Application Specific integrated chips).
Transmission Mode	Half duplex	Half/Full duplex
Broadcast Domain	Hub has one Broadcast Domain.	Switch has one broadcast domain [unless VLAN implemented]
Speed	10 Mbps	10/100 Mbps, 1 Gbps
Collisions	Collisions occur commonly in setups using hubs.	No collisions occur in a full-duplex switch.
Spanning-Tree	No spanning-Tree	Many spanning-tree possible
Manufacturers	Sun systems, oracle and cisco	Cisco and D-link juniper

Q.1.(c) What do you mean by IP addressing ? Explain.

Ans. IP Addressing : An IP address is a unique address used to locate and identify a device over a network. That device can be an electronic device, a computer, a server, a router or even an IP phone. It is the addressing used for the transmission of data packets over a network working with the IP protocol.

It is classified as :

(i) Class A address format : The network field is 7 bit long as shown in fig.(a) and the host field is of 24 bit length. So the network field can have numbers between 1 to 127. But the host numbers will range from 0.0.0.0 to 127.255.255.255. Thus in class A, there can be 126 types of network and 17 million hosts. The "0" in the first field identifies that it is a class A network address.

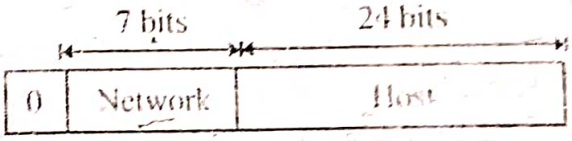


Fig. (a) : Class A IP Address formats

(ii) Class B address Format : The Class B address format is show in fig.(b).

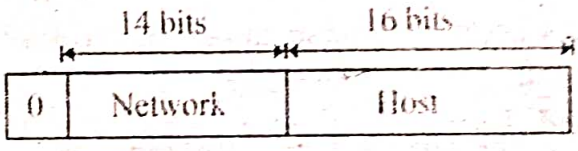


Fig. (b) : Class B Format

The first two fields identify the network, and the number in the first field must be in the range 128-191. Class B networks are large. Host numbers 0.0 and 255.255 are reserved. So there can be upto 65.234 (216-2) host in a class B network. Most of the 16.382 class B address have been allocated. The first block covers address from 128.0.0.0.0 in 128.255.255.255.255 and the last block covers from 191.255.0.0 to 191.255.255.255.

(iii) Class C address format : Class C address format is shown in fig.(c).

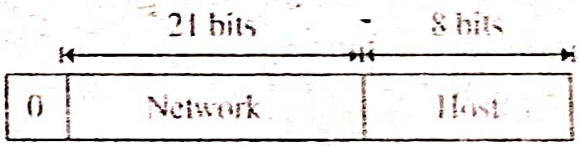


Fig. (c) : Class C Format

The first block in class covers addresses from 192.0.0.0 to 192.0.0.253 and the last block covers address from 223.255.255.0 to 223.255.255.255

(iv) Class D format : The class D address format is show in fig.(d).

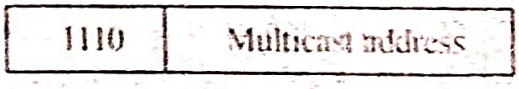


Fig. (d) : Class D Format

The class format allows for upto 2 million networks with upto 254 hosts each and class D format allows the multicast in which a datagram is directed to multiple hosts.

(v) Class E address format : Fig.(e) shows the address format for a class E address. This address begins with 1110 which shows that it is reserved for the future use.

1110	Reserved for future use

Fig. (e) : IP address for class E Network

The 32 bit (4 byte) network address are usually written in dotted decimal notation. In this notation each of the 4 bytes is written in decimal from 0 to 255. So the lowest IP address 0.0.0.0 i.e. all the 32 bites are zero and highest IP address is 255.255.255.255

Q.1.(d) What is VLAN ? Explain.

Ans. Virtual LAN is software that is employed to provide multiple networks in single hub by grouping terminals connected to switching hubs. It is a LANs that is grouped together by logical addresses into a virtual LAN instead of a physical LAN through a switch. The switch can support many virtual LANs that operate with having different network addresses or as subnets. Users within a virtual LAN are grouped either by IP address or by port address, with each node attached to the switch via a dedicated circuit. Users also can be assigned to more than one virtual LAN.

The VLAN can be defined as a broadcast domain in which the broadcast address reaches all stations belonging to the VLAN. Communications within the VLAN can be secured and between those two controlled separate VLANs.

Characteristics of VLAN :

(1) Individual VLAN acts as a separate LAN, thus sharing the traffic among VLANs and reducing the congestion

(2) Workstations can be provided with full bandwidth at each port

(3) Relocation of terminals becomes easy

VLAN Benefits : As we have seen, there are several benefits to using VLANs. To summarize, VLAN benefits include:

(1) Increased performance

(2) Improved manageability

(3) Simplification of software configurations

(4) Increased security options

Increased performance : Switched networks by nature will increase performance over shared devices in use today by reducing collisions. Grouping users into logical networks will also increase performance by limiting broadcast traffic to users performing similar functions within workgroups. Additionally, less traffic will need to be routed, and the latency added to routers will be reduced.

Improved manageability : VLANs provide an easy, flexible, less costly way to modify logical groups in changing environments. VLANs make large networks more manageable by allowing centralized configuration of devices located in assorted locations.

Simplification of software configurations : VLANs will allow LAN administrators to "fine tune" their networks by grouping users. Software configurations can be made the same across machines with the consolidation of a department's resources into a single subnet. IP

addresses and subnet masks will be more consistent across the entire VLAN. These services can be more effectively deployed when they can span buildings within a VLAN.

Increased security options : VLANs have the ability to provide additional security not available in a shared network environment. A switched network delivers packets only to the intended recipients and packets only to other members of the VLAN. This allows the network administrator to segment users requiring access to sensitive information into separate VLANs from the rest of the general users regardless of physical location.

VLAN Limitations : There are a few limitations to using VLANs:

(1) Device limitations

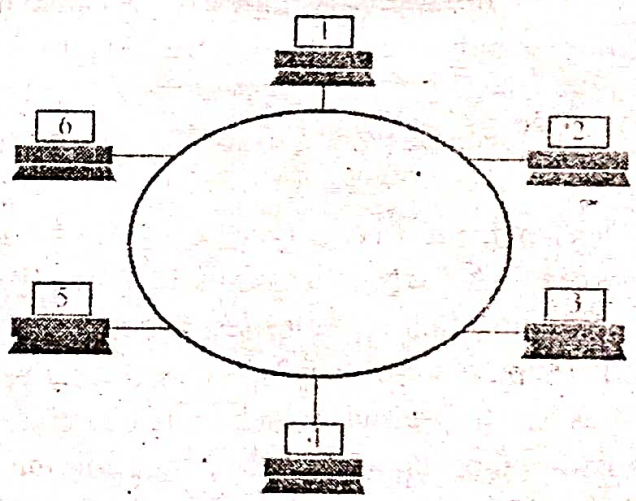
(2) Port constraints

Device limitations : The number of Ethernet addresses than can be supported by each device is 500. This is a distribution of about 20 devices per port on a 25 port switch. In an ideal network situation, there is one device per port, for example, a printer, a workstation, and voice IP phone will require 3 ports. If you wanted to have one VLAN assignment for each port, then the maximum VLANs will equal 25.

Port Constraints : If a hub or switch is connected to one port, every port on that hub must belong to the same VLAN. Hubs do not have the capability to provide VLANs to individual ports, and VLANs can not be extended beyond the device port even if a switch capable of supporting VLANs is attached.

Q.1.(e) What is token Ring ? Explain.

Ans. Token ring : Token ring or is a network where all computers are connected in a circular fashion. The term token is used to describe a segnient of information that is sent through that circle; when a computer on the network can decode that token, it receives data.



The data transmission process goes as follows:

– Empty information frames are continuously circulated on the ring.

– When a computer has a message to send, it seizes the token. the computer will then be able to send the frame.

– The frame is then examined by each successive workstation. The workstation that identifies itself to be the destination for the message copies it from the frame and changes the token back to 0.

– When the frame gets back to the originator, it sees that the token has been changed to 1 and that the message has been copied and received. It removes the message from the frame.

– The frame continues to circulate as an "empty" frame, ready to be taken by a workstation when it has a message to send.

SECTION – A

Q.2. What is a computer network ? Discuss different type of network. Discuss in detail the advantages and disadvantages of a computer network.

Ans. Computer Network: Computer network is a system which allows communication amoung the computers connected in the network. A network must be able to meet certain criteria. The most important of them are:

1. Performance
2. Relaibility
3. Security

1. *Performance* : Performance can be measured in many ways. We can measure it in terms of transit time and response time.

(a) Transit time is defined as the amount of time required for a message to travel from one device to the other.

(b) Response time: It is the time elapsed between enquiry and response.

The other factors deciding the performance are as follows:

(i) Number of users

(ii) Type of transmission medium

(iii) Capability of connected hardware

(iv) Efficiency of software.

2. *Reliability* : The network reliability is important because it decides the frequency at which network failure takes place. It also decides the time taken by the network to recover and its robustness in the catastrophe.

3. *Security* : The network secutiry refers to protection of data from the unauthorized user or access.

Different types of Network : Different types of Network are as follows :

(i) Local Area Network : A LAN is a computer network that covers only a small geographical area (usually within a square mile or less) such as an office, home or building (Fig.a). In a LAN, connected computers have a network operating system installed onto them. One computer is designated as the file server, which stores all the software that controls the network. It also stores the software that can be shared by the computers attached to the network. Other computers connected to the file server are called workstations. The workstations can be less powerful than the file server and they may have additional software on their hard drive. On most LANs, cables are used to connect the computer. Generally, LAN offers a bandwidth of 10-100Mbps.

(ii) Metropolitan Area Network : A MAN is a network of computers spread over a "metropolitan" area such as city and its suburbs (fig.b). As the name suggests, this sort of network is usually reserved for metropolitan areas where the city bridges its LANs with a series of backbones, making one large network for the entire city. It may be a single network such as a cable television network or it may be a means of connecting as number of LANs. Note that

MAN may be operated by one organization (a corporate with several offices in one city) or be shared and used by several organization in the same city.

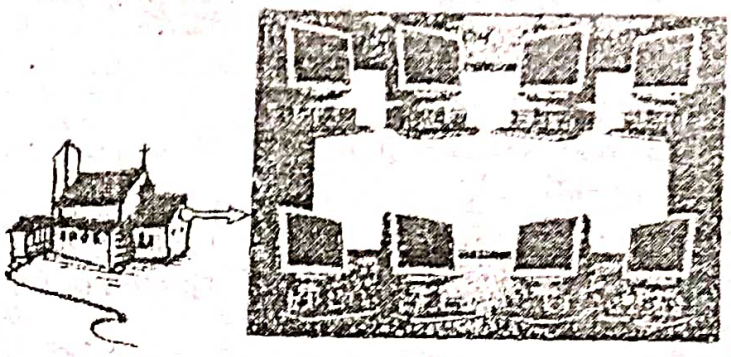


Fig.(a) : Local area network

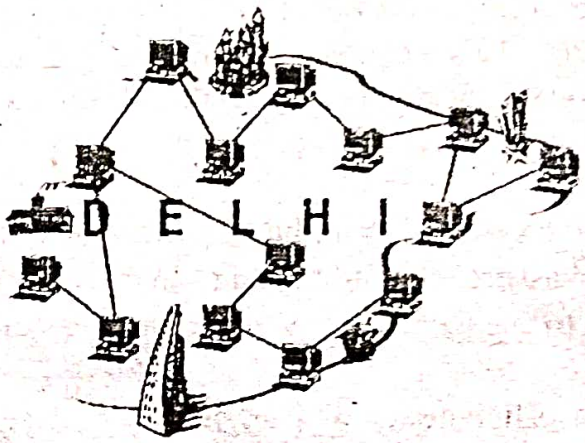


Fig.(b) : Metropolitan area network

(iii) WAN : It stands for wide area network. This is the largest network and can interconnect networks throughout the world and is not restricted to a geographical location. The Internet is an example of a worldwide public WAN. Most WANs exist to connect LANs that are not in the same geographical area. This technology is high speed and very expensive to setup. It is shown in fig.(c).

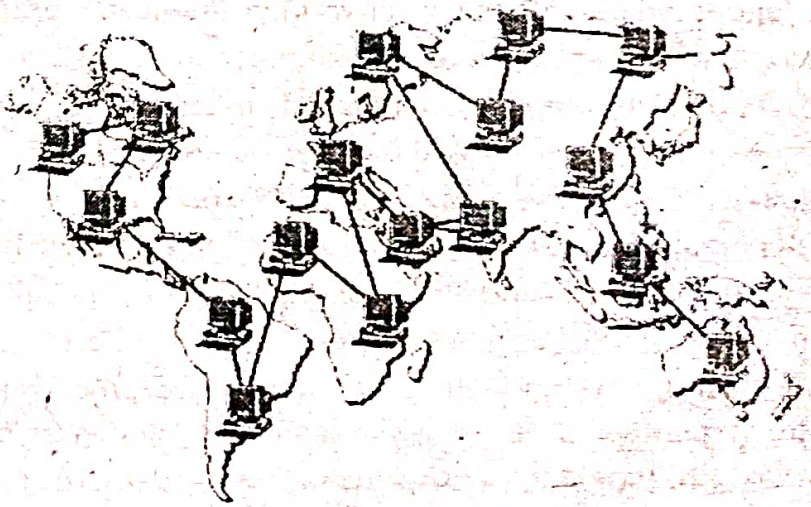


Fig.(c) : Wide area network

Advantages of Computer Networking :

1. It enhances communication and availability of information : Networking, especially with full access to the web, allows ways of communication that would simply be impossible before it was developed. Instant messaging can now allow users to talk in real time and send files to other people wherever they are in the world, which is a huge boon for businesses. Also, it allows access to a vast amount of useful information, including traditional reference materials and timely facts, such as news and current events.

2. It allows for more convenient resource sharing : This benefit is very important, particularly for larger companies that really need to produce huge numbers of resources to be shared to all the people. Since the technology involves computer-based work, it is assured that the resources they wanted to get across would be completely shared by connecting to a computer network which their audience is also using.

3. It makes file sharing easier : Computer networking allows easier accessibility for people to share their files, which greatly helps them with saving more time and effort, since they could do file sharing more accordingly and effectively.

4. It is highly flexible : This technology is known to be very flexible, as it gives users the opportunity to explore everything about essential things, such as software without affecting their functionality. Plus, people will have the accessibility to all information they need to get and share.

5. It is an inexpensive system : Installing networking software on your device would not cost too much, as you are assured that it lasts and can effectively share information to your peers. Also, there is no need to change the software regularly, as mostly it is not required to do so.

6. It increases cost efficiency : With computer networking, you can use a lot of software products available on the market which can just be stored or installed in your system or server, and can then be used by various workstations.

7. It boosts storage capacity : Since you are going to share information, files and resources to other people, you have to ensure all data and content are properly stored in the system. With this networking technology, you can do all of this without any hassle, while having all the space you need for storage.

Disadvantages of Computer Networking :

1. It lacks independence : Computer networking involves a process that is operated using computers, so people will be relying more of computer work, instead of exerting an effort for their tasks at hand. Aside from this, they will be dependent on the main file server, which means that, if it breaks down, the system would become useless, making users idle.

2. It poses security difficulties : Because there would be a huge number of people who would be using a computer network to get and share some of their files and resources, a certain user's security would be always at risk. There might even be illegal activities that would occur, which you need to be careful about and aware of.

3. It lacks robustness : As previously stated, if a computer network's main server breaks down, the entire system would become useless. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill. To deal with these problems, huge networks should have a powerful computer to serve as file server to make setting up and maintaining the network easier.

4. It allows for more presence of computer viruses and malware : There would be instances that stored files are corrupt due to computer viruses. Thus, network administrators should conduct regular check-ups on the system, and the stored files at the same time.

5. Its light policing usage promotes negative acts : It has been observed that providing users with internet connectivity has fostered undesirable behavior among them. Considering that the web is a minefield of distractions—online games, humor sites and even porn sites—workers could be tempted during their work hours. The huge network of machines could also encourage them to engage in illicit practices, such as instant messaging and file sharing, instead of working on work-related matters. While many organizations draw up certain policies on this, they have proven difficult to enforce and even engendered resentment from employees.

6. It requires an efficient handler : For a computer network to work efficiently and optimally, it requires high technical skills and know-how of its operations and administration. A person just having basic skills cannot do this job. Take note that the responsibility to handle such a system is high, as allotting permissions and passwords can be daunting. Similarly, network configuration and connection is very tedious and cannot be done by an average technician who does not have advanced knowledge.

7. It requires an expensive set-up : Though computer networks are said to be an inexpensive system when it is already running, its initial set up cost can still be high depending on the number of computers to be connected. Expensive devices, such as routers, switches, hubs, etc., can add up to the cost. Aside from these, it would also need network interface cards (NICs) for workstations in case they are not built in.

Q.3. Describe in details ISO-OSI reference model with the help of a diagram and explain its layers.

Ans. Refer Q.2(a) of paper May 2019.

SECTION – B

Q.4.(a) Explain the protocols which are essential for Email.

Ans. Refer Q.4.(a) of paper May 2017.

Q.4.(b) What is IPv6 ? Explain the frame structure of IPv6 ?

Ans. Refer Q.1.(c) of paper May 2019.

Q.5. What is TCP/IP Model ? Explain function and protocols of each layer.

Ans. TCP/IP reference model : The Internet Protocols (IP) and Transmission Control Protocol (TCP) are together known as TCP / IP protocol. TCP /IP are two protocols : Transmission control protocol and Internet prolocol. These two protocols describe the movements of data between the host computers or Internet.

TCP /IP offers simple naming and addressing scheme whereby different resources on Internet can be easily located. Information on Internet is carried in Packets. The IP protocol is used to put a message into a packet. Each packet has the address of the sender and the recipient's address. These addresses are known as the IP addresses. Using the TCP protocol, a single large message is divided into a sequence of packets and each is put an IP packet.

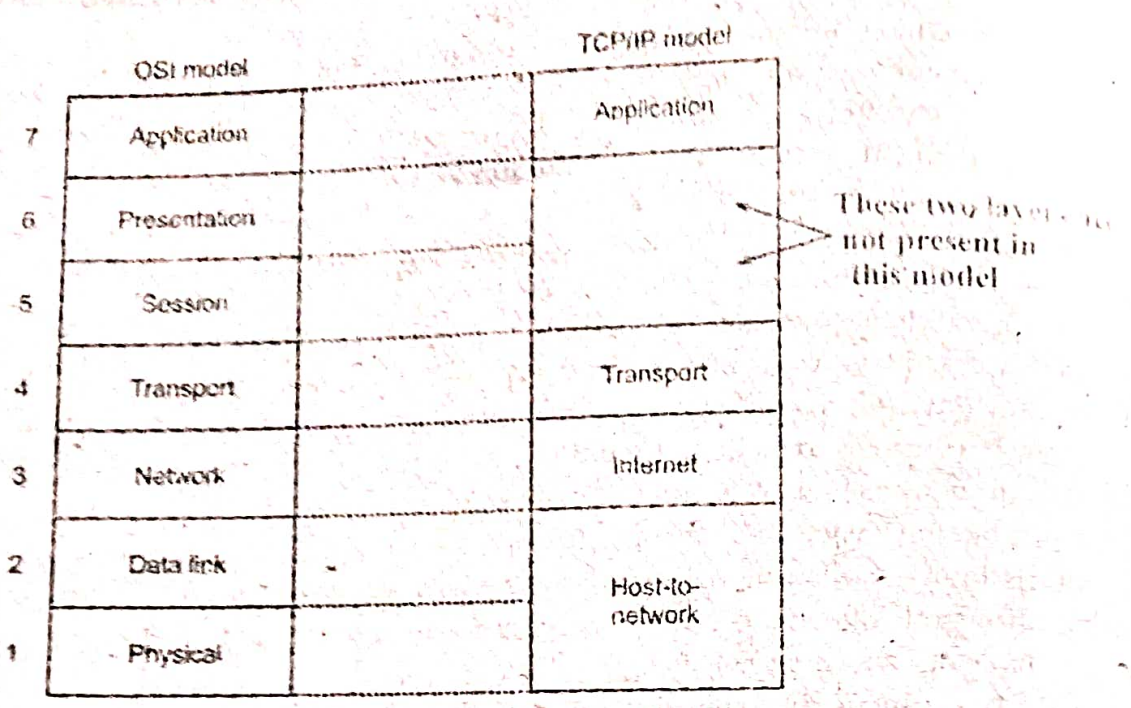


Fig.(a) : TCP/IP reference model

The packets are passed from one network to another until they reach their destination. At the destination, the TCP software reassembles the packets into a complete message. It is not necessary for all the packets in a single message to take the same route each time it is sent.

As shown in fig.(a), the TCP/IP model has only four layers.

1. Internet Layer : The goals requirements lead to the selection of a packet switching network which is based on a connectionless internetwork layer. This layer is called as the internet layer and it holds the whole architecture together. The task of this layer is to allow the host ot insert packets into any network and then make them travel independently to the destination. The order in which the packets are received can be different from the sequence in which they were sent. Then the higher layers are supposed to arrange them in the proper order. The internet layer defines (specifies) a packet format and a protocol called internet protocol (IP). The internet layer is supposed to deliver IP packets to their destinations. So routing of packets and congestion control are important issues related to this layer.

2. Transport Layer : This is the layer above the internet layer. Its functions are same as those of a transport layer in OSI layer. This layer allows the per entities of the source and destination machines to converse with each other. The end to end protocols used here are TCP and UDP. TCP is a reliable connection oriented protocol. It allows a byte stream transmitted from one machine to be delivered to the other machine without introducing any errors. TCP also handles the flow control. UDP (user datagram protocol) is the protocol used in the transport layer. It is an unreliable, connectionless protocol and used for the applications which do not want the TCP's sequencing or flow control. UDP is also preferred over TCP in those applications in which prompt delivery is more important than accurate delivery. It is used in transmitting a video.

3. Application Layer : TCP / IP model does not have session or presentation layers, because they are of little importance in most applications. The layer on top of transport layer is called as application layer.

4. Host network layer : This is the lowest layer in TCP /IP reference model. The host has to connect to the network using some protocol, so that it can send the IP packets over it. This protocol varies from host to host and network to network.

Application Layer	TELENT, FTP, DMTP, DM, HTTP, NNTP
Transport	TCT-UDP
Internet (Network)	IP
Host-to-network	ARPANET, SATNET LAN, packet radio

SECTION – C

Q.6.(a) What do you mean by Ethernet ? Explain.

Ans. Ethernet : The Ethernet is most successful local area networking technology. It is working example of the more general carrier sense multiple access with collision detect (CSMA CD). The Ethernet is a multi-access network, meaning that a set of nodes send and receive frames over a shared link you can, therefore, think of an Ethernet or being like a bus that has multiple stations plugged into it.

Three generations of Ethernet are as follows :

(i) Traditional Ethernet (10 Mbps)

(ii) Fast Ethernet (100 Mbps)

(iii) Gigabit Ethernet (1000 Mbps)

(i) Traditional Ethernet : The traditional Ethernet is the oldest version of Ethernet created in 1976 which is designed to operate at 10 Mbps.

The access to the network by a device is through the CDMA/CD and the media are shared between all the stations.

(ii) Fast Ethernet : Fast Ethernet is the protocol designed to work upto 100 Mbps. The traditional Ethernet can operate only upto 10 Mbps. Hence for higher data rates fast Ethernet has been developed.

Autonegotiation : This is the new feature of the fast Ethernet. The autonegotiation will make the negotiation on the mode or data rare of operation between devices possible.

(iii) Gigabit Ethernet : The gigabit Ethernet protocol has been designed in order to support the data rates upto 1000 Mbps. The MAC layer was supposed to remain unchanged throughout the evolution of the Ethernet but it does not remain so when the rate of 1 Gbps is to be supported. The Gigabit Ethernet is capable of operating in either half duplex or full duplex modes. If it operates in the half duplex mode, then the access method used in CSMA/CD. But if the full duplex mode is used then CSMA/CD is not required. Almost all the implementations in Gigabit Ethernet use the full duplex mode.

Q.6.(b) Explain briefly ALOHA.

Ans.ALOHA : Aloha is a system for co-ordinating and arbitrating access to a shared communication networds channel. The basic idea of Aloha system is applicable to any system in which uncoordinated users are competing for the use of a single shared channel.

In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost.

Pure Aloha : It works on a very simple principle. Essentially, it allows for any station to broadcast at any time. If two signals collide, each station simply waits a random time and tries again. Collisions are easily detected. As shown in the fig.(1), when the central station receives a frame it sends an acknowledgment on a different frequency.

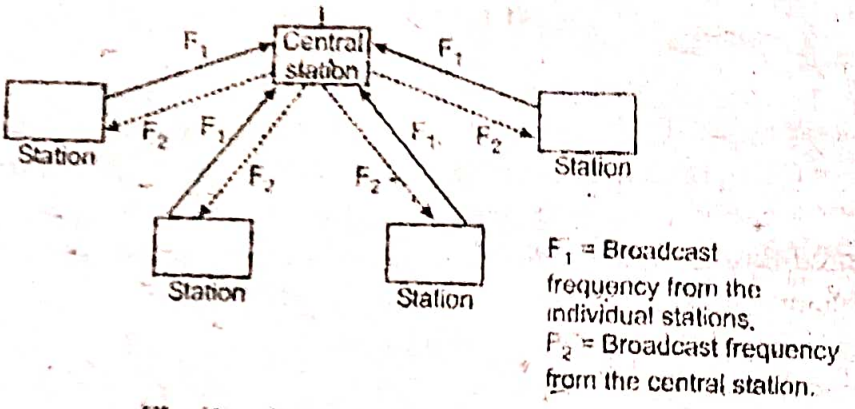


Fig.(1) : Pure Aloha system

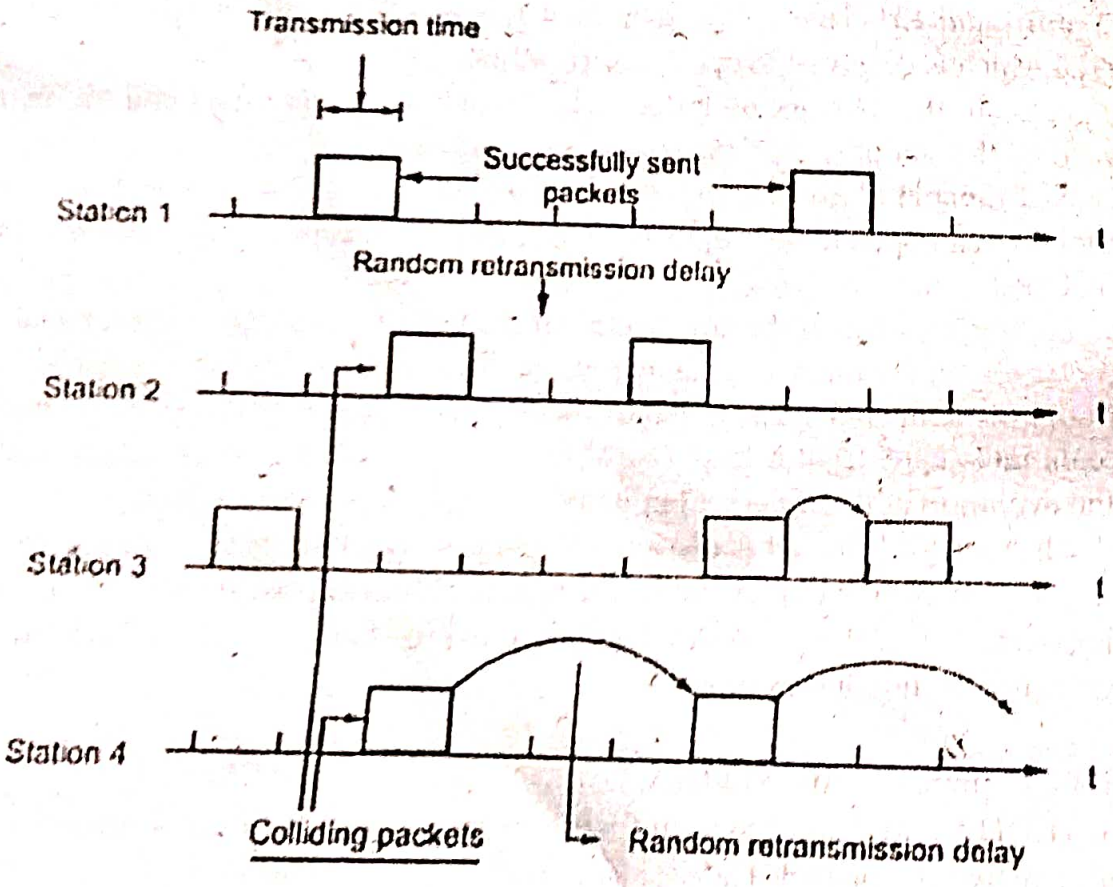


Fig.(2) : Slotted Aloha system

If a user station receives an acknowledgment it assumes that the transmitted frame was successfully received and if it does not get an acknowledgment it assumes that collision had occurred and is ready to retransmit.

The advantage of pure aloha is its simplicity in implementation but its performance becomes worse as the data traffic on the channel increases.

Slotted Aloha : In slotted Aloha, the channel time is divided into time slots and the stations are allowed to transmit at specific instance of time. These time slots are exactly equal to the packet transmission time. All users are then synchronized to these time slots. so that whenever a user generates a packet it must synchronize exactly with the next possible channel slot. Consequently the wasted time due to collisions can be reduced to one packet time or vulnerable period is reduced to half.

Transmission attempts for four network user and random retransmission delays for colliding packets in slotted Aloha is shown in fig.(2).

Q.7.(a) What do you mean by routing? Explain Distance vector Routing approach.

Ans. Routing : Routing is the act of moving information across an inter-network from a source to a destination. Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement; such as path bandwidth, reliability, delay, current load on that path etc. that is used by routing algorithms to determine the optimal path to a destination.

Distance vector routing, Algorithm : In this algorithm, each router maintains a table called vector; such a table gives the best known distance to each destination and the information about which line to be used to reach there. This algorithm is sometimes called by other names such as,

(*i*) Distributed Bellman-Ford routing algorithm.

(*ii*) Ford-Fulkerson algorithm.

In distance vector routing, each router maintains a routing table. It contains one entry for each router in the subnet.

The entry has two parts :

(*i*) The first port shows the preferred outgoing line to be used to reach the destination, and

(*ii*) Second part gives an estimate of the time or distance to the destination.

The first means used can be one of the following :

(*i*) Number of hops

(*ii*) Time delay

(*iii*) Number of packets in a queue etc.

The example of a subnet is shown in fig.1(a) and the routing tables are shown in fig.1(b).

The entries in router tables of fig.1(b) are the delay vectors. For example, let us consider the shaded boxes of fig.1(b). The entry in the first shaded box shows that the delay from A to B is 10 msec, whereas the entry in the other shaded box indicates that the delay from A to D is 38 msec.

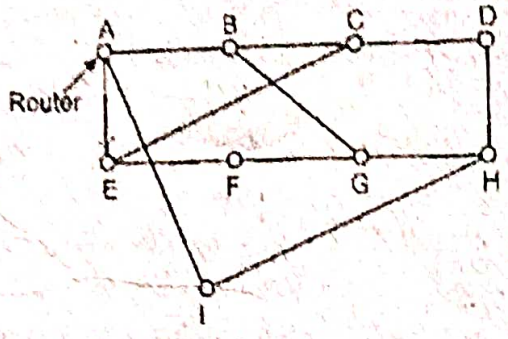


Fig.1(a) : A subnet

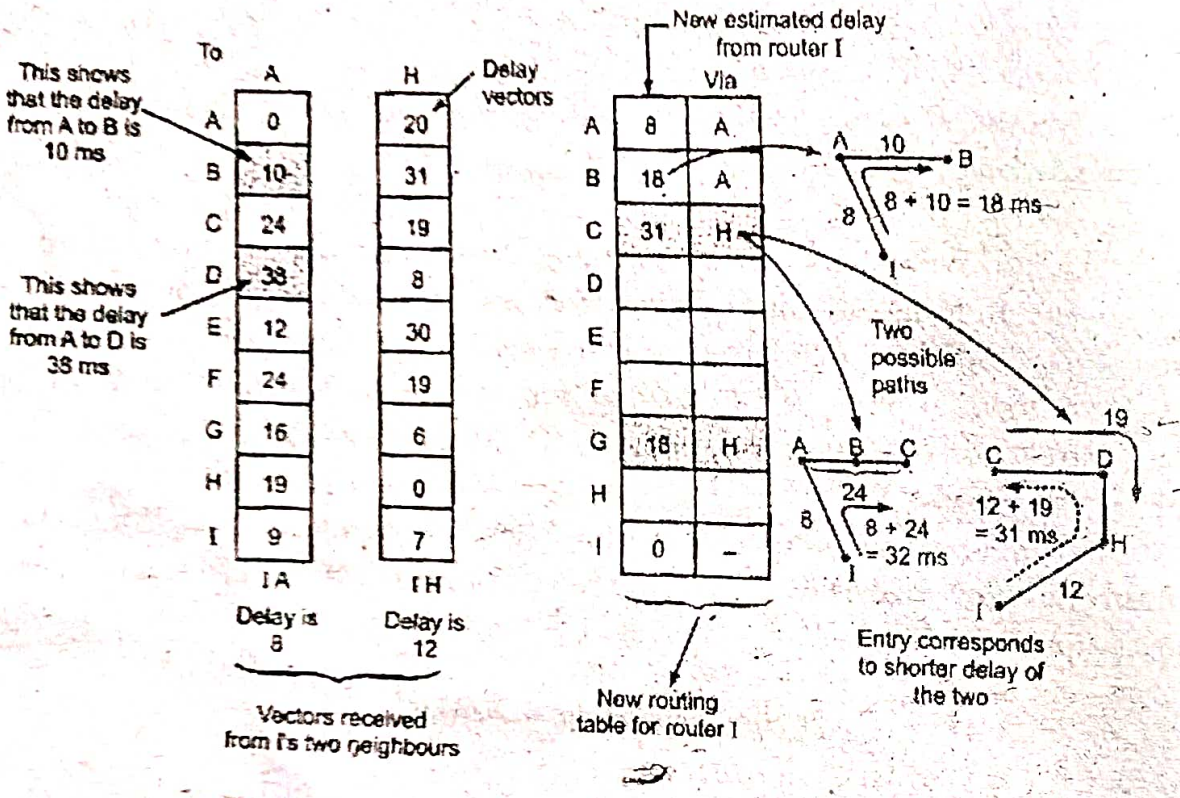


Fig.1(b) : Routing Tables

Let us consider how router I computers its new route to router G. Fig.(2) shows the two possible routes between I and G.

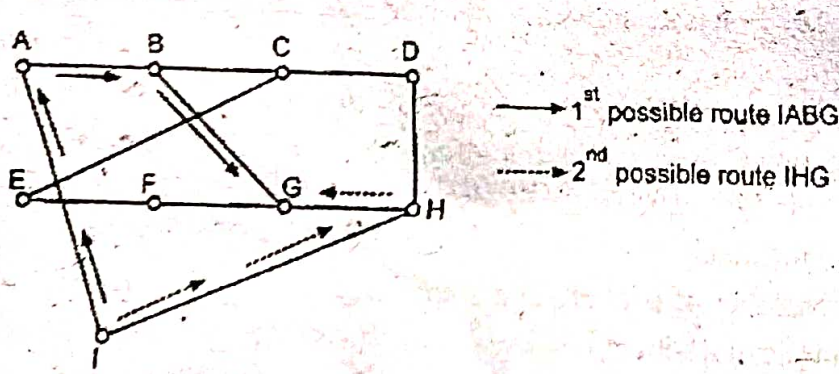


Fig. : (2)

I knows that the reach G via A, the delay required is :

I to A Delay = 8 ms

A to G. Delay = 16 ms

∴ I to G Delay = 8 + 16 = 24 msec.

Whereas the delay between I and G via H (route IHG) is :

I to H Delay = 12 ms ∴ I to G Delay = 12 + 6 = 18 msec.

H to G Delay = 6 ms

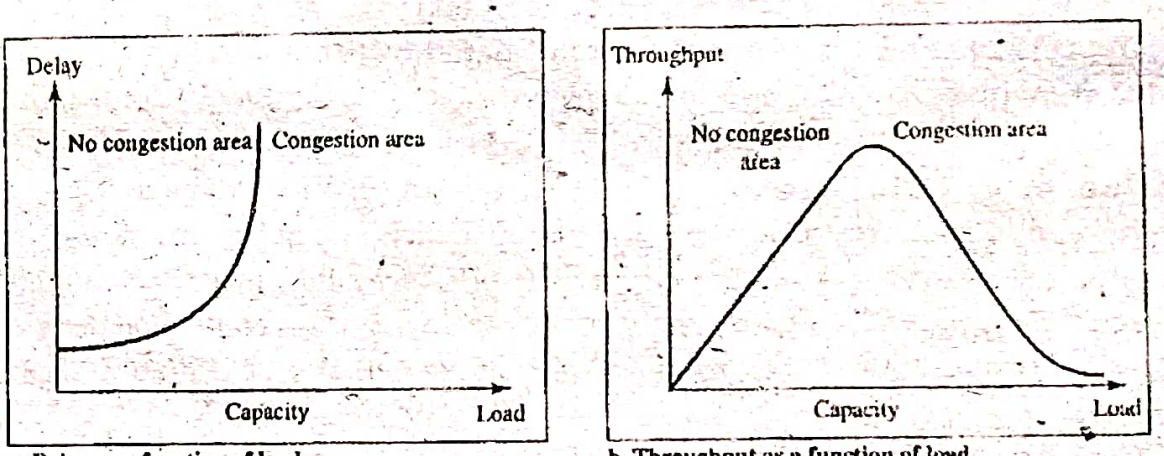
The best of these values is 18 msec corresponding to the path IHG. Hence, it makes an entry in its routing table (I's table) that the delay to G is 18 msec and that the route to use it is via H. The new routing table for router I is shown in fig.1(b). Similarly, we can calculate the delays, from I to different destinations from A to I and enter the minimum possible delay into the I's router table.

Q.7.(b) What is congestion in a computer network ? How it is controlled ? Explain.

Ans. Congestion in a network may occur if the load on the load on the network – the number of packets sent to the network – is greater than the capacity of the network –the number of packets a network can handle. Congestion happens in any system that involves waiting. For example, congestion happens on a freeway because any abnormality in the flow, such as an accident during rush hour, creates blockage.

Congestion in a network or internet work occurs because routers and switches have queues–buffers that hold the packets before and after processing. A router, for example, has an input queue and an output queue for each interface.

Congestion control involves two factors that measure the performance of a network: delay and throughput. Fig.(a) shows these two performance measures as function of load.



a. Delay as a function of load

b. Throughput as a function of load

Fig (a) : Packet delay and throughput as functions of load

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

Open-Loop Congestion Control: In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination. Following are the policies that can prevent congestion :

(i) *Retransmission Policy* :Retransmission is sometimes unavoidable . If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted.

Re-transmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion.

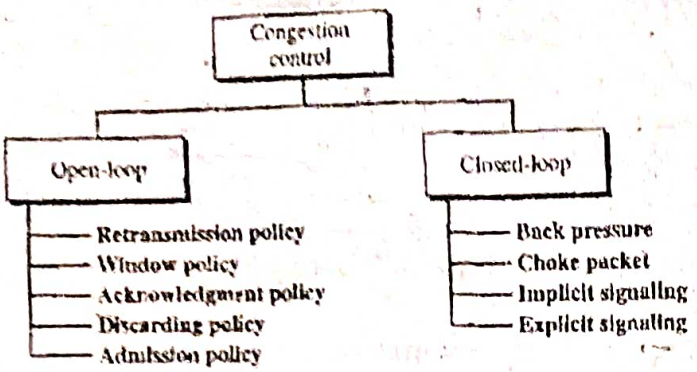


Fig (b) : Congestion control categories

(ii) *Window Policy* : The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control. In the Go-Back-N window, when the timer for a packet times out, several packets may be resent, although some may have arrived safe and sound at the receiver. This duplication may make the congestion worse. The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted.

(iii) *Acknowledgment policy* : The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.

(iv) *Discarding policy* : A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission. For example, in audio transmission, if the policy is to discard less sensitive packets when congestion is likely to happen, the quality of sound is still preserved and congestion is prevented or alleviated.

(v) *Admission policy* : An admission policy, which is a quality-of-service machanism, can also prevent congestion in virtual-circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny establishing a virtual-circuit connection if there is congestion in the network or if there is a possibility of future congestion.

Closed-Loop Congestion Control : Closed-loop congestion control mechanisms try to alleviate congestion after it happens. Several mechanisms have been used by different protocols. We describe a few of them here.

(i) *Backpressure* : Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source. The backpressure technique can be applied only to virtual circuit networks, in which each node knows the upstream node from which a flow of data is coming. Fig.(c) shows the idea of backpressure.

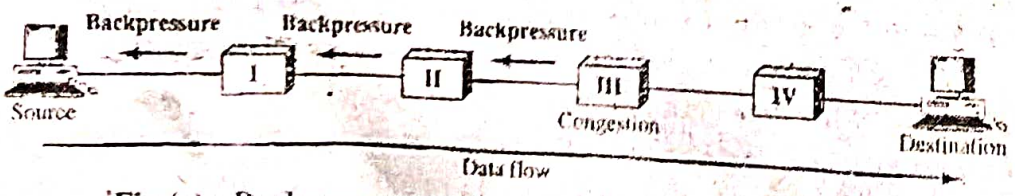


Fig (c) : Backpressure method for alleviating congestion

(ii)*Choke packet :* A choke packet is packet sent by a node to the souce to inform it of congestion. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes through which the packet has traveled are not warped.

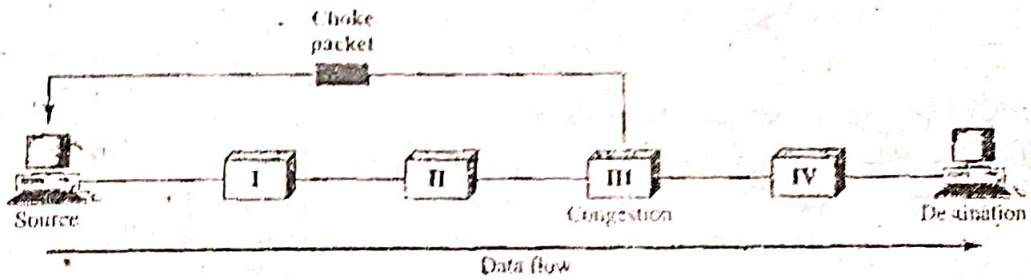


Fig (d) : Choke packet

(iii) *Implicit Signaling :* In implicit signaling there is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network from other symptoms. For example, when source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested. The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down.

(iv) *Explicit Signaling :* The node that experiences congestion can explicitly send a signal to the source or destination. In the explicit signaling method, the signal is included in the packets that carry data. Explicit signaling, can occur in either the forward or the backward direction.

(v) *Backward Signaling :* A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.

(vi) *Forward Signaling :* A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the congestion.

SECTION – D

Q.8. Explain the following :

(i) Proxy Server

(ii) Security Management

(iii) Firewalls

(iv) Client-server infrastructure

Ans.(i) Proxy Server : 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 checks its cache. If the response is not stored in the cache, the proxy server sends the request to the corresponding server. Incoming response are sent to the proxy server and stored for future requests from other clients.

The proxy server reduces the load on the original server, decrease traffic and improves latency. However, to use the proxy server, the client must be configured to access the proxy instead of the target server.

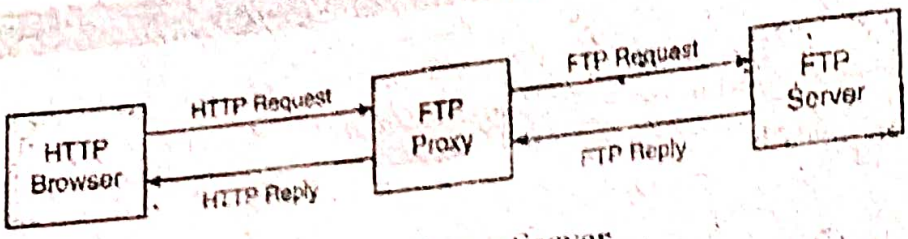


Fig. : Proxy Server

Types of proxy server are as follows :

(i) *Open proxy server* : An open proxy is a forwarding proxy server that is accessible by any Internet user. Gordon Lyon estimates there are "hundreds of thousands" of open proxies on the Internet. An anonymous open proxy allows users to conceal their IP address while browsing the Web or using other Internet services. There are varying degrees of anonymity however, as well as a number of methods of 'tricking' the client into revealing itself regardless of the proxy being used.

(ii) *Reverse proxy server* : A reverse proxy (or surrogate) is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or mo. : proxy servers which handle the request. The response from the proxy server is returned as if it come directly from the origin server, leaving the client no knowledge of the origin servers. Reverse proxies are installed in the neighborhood of one or more web servers. All traffic coming from the Internet and with a destination of one of the neighborhood's web servers goes through the proxy server. The use of "reverse" originates in its counterpart "forward proxy" since the reverse proxy sits closer to the web server and serves only a restricted set of websites.

Ans.(ii)Security Management : Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

Homes & Small Businesses :

– A basic firewall or a unified threat management system.

– For Windows users, basic Antivirus software. An anti-spyware program would also be a good idea. There are many other types of antivirus or anti-spyware programs out there to be considered.

– When using a wireless connection, use a robust password. Also try to use the strongest security supported by your wireless devices, such as WPA2 with AES encryption.

– If using Wireless: Change the default SSID network name, also disable SSID Broadcast; as this function is unnecessary for home use. (However, many security experts consider this to be relatively useless).

– Enable MAC Address filtering to keep track of all home network MAC devices connecting to your router.

– Assign STATIC IP addresses to network devices.

– Disable ICMP ping on router.

Medium businesses :

– A fairly strong firewall or Unified Threat Management System

– Strong Antivirus software and Internet Security Software.

– For authentication, use strong passwords and change it on a bi-weekly/monthly basis.

– When using a wireless connection, use a robust password.
– Raise awareness about physical security to employees.

Large businesses :

– A strong firewall and proxy to keep unwanted people out.
– A strong Antivirus software package and Internet Security Software package.
– For authentication, use strong passwords and change it on a weekly/bi-weekly basis.
– When using a wireless connection, use a robust password.
– Exercise physical security precautions to employees.
– Prepare a network analyzer or network monitor and use it when needed.
– Implement physical security management like closed circuit television for entry areas and restricted zones.

School :

– An adjustable firewall and proxy to allow authorized users access from the outside and inside.
– Strong Antivirus software and Internet Security Software packages.
– Wireless connections that lead to firewalls.
– Children's Internet Protection Act compliance. (Only schools in the USA)
– Supervision of network to guarantee updates and changes based on popular site usage.

Large government :

– A strong firewall and proxy to keep unwanted people out.
– Strong antivirus software and Internet Security Software suites.
– Strong encryption.
– Whitelist authorized wireless connection, block all else.
– All network hardware is in secure zones.

Ans.(iii)Firewalls : A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (bit forward) others. Fig.(a) shows a firewall.

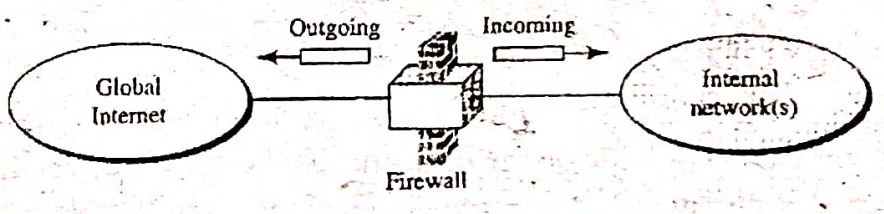


Fig. (a) : Firewall

For example, a firewall may filter all incoming packets destined for a specific host or specific server such as HTTP. A firewall can be used to deny access to a specific host or a specific service in the organization.

The firewall consists of two components, namely:

(i) Two routers for packet filtering.

(ii) An application gateway.

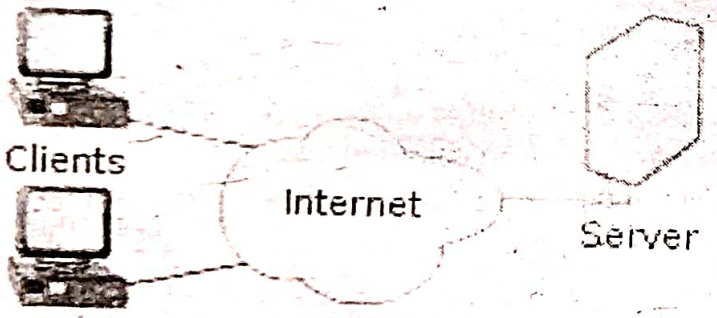
So, every packet has to travel through two packet filtering routers and an application gateway while going in or coming out because there is no additional route existing.

[i] *Packet Filter :* A packet filter is basically a standard router with some additional

facilities. The additional facilities make it possible to inspect each incoming and outgoing packet. The packet satisfying certain criteria only are allowed to pass through. Those who fail to satisfy these conditions are dropped. The packet filter on the input side(inside LAN) checks the outgoing packets and that on the output side (outside LAN) checks the incoming packets. The application gateway makes further examination of the packets which have reached it through the router. Thus, every packet going in or coming out has to pass through the application gateway.

(ii) *Application Gateway:* Application gateway is the second half of the firewall mechanism. The application gateway does not just look at the raw packets but it operates at the application level. It is possible to set up a mail gateway to examine each message going in or coming out.

Ans.(iv)Client-server infrastructure : In this architecture, each computer is either a client or a server. To complete a particular task, there exists a centralized powerful host computer known as server and a user's individual workstation known as client (fig.). The client requests for services (file sharing, resource sharing etc.) from the server and the server responds by service. The servers provide access to resouces, while the clients have access to the resource available only on the servers. In addition, no clients can communicate directly with each other in this architecture. A typical example of client/server architecture is accessing a website (server) from home with the help of a browser(client). When a client makes a request for an object to the server, then the server responds by sending the object to the client. In addition, it must be noticed that two browsers accessing the same website, never communicate with each other.



An advantage of client/server architecture is that the IP address of the server is always fixed and the server is always available on the network for clients. However, the disadvantage of this architecture is that with time as the number of client starts to increase, the number of requests to the server also increases rapidly. In this scenario, we might need more than one server to serve larger number of requests.

Q.9. Explain ATM reference model with proper diagram.

Ans. ATM Protocol Architecture (ATM Reference Model) : Fig. shows the ATM protocol architecture. ATM is a streamlined protocol. It has minimal error and flow control capabilities. Hence, the number of overhead bits required with each cell is reduced which enables ATM to operate at high data rates. Also, due to the ATM cells of fixed size, the processing required at each node is simplified. This also supports the use of ATM at high data rates. Fig. shows the ATM protocol architecture for an interface between user and network. The standards issued for ATM by ITU-T are based on this protocol architecture.

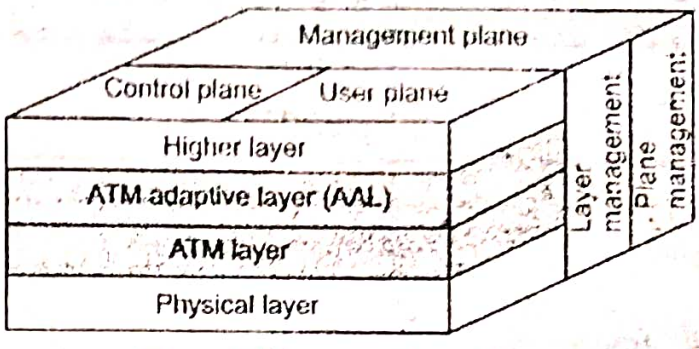


Fig. : ATM protocol architecture

Physical Layer : The physical layer of the protocol involves the specifications of a transmission medium and signal encoding scheme. The data rates specified at this layer are between 25.6 Mbps and 622.08 Mbps, but data rates higher and lower than these are possible.

Layers Related to ATM Functions : The two shaded layers in fig. correspond to the ATM functions. The two layers are :

1. ATM layer
2. ATM adaption layer (AAL).

1. *ATM Layer* : This layer is common to all the services that provide the packet transfer capabilities. This layer defines the transmission of data in fixed size cells and it also defines the use of logical connections.

2. *ATM Adaption Layer (AAL)* : This layer is a service dependent layer. It is used for supporting the information transfer protocol not based on ATM.

The AAL maps the higher layer information into the ATM cells and cell is transported over the ATM network.

Various Planes in the ATM Protocol Model : The ATM protocol architecture of fig. consists of three separate planes :

1. User plane
2. Control plane
3. Management plane.

1. *User Plane* : It is used for transferring user information alongwith associated controls such as flow control, error control etc.

2. *Control Plane* : It is supposed to perform the call control and connection control functions.

3. *Management Plane* : It includes the plane management. The management plane performs management functions related to a system. They include :

(i) Provision of coordination between all planes

(ii) Layer management

(iii) Management functions relating to resources and parameters residing in its protocol entities.

COMPUTER NETWORK

May - 2017

Paper Code:-IT-305-F

Note : *Attempt five questions in all, selecting one question from each Section. Question No. 1 is compulsory. All questions carry equal marks.*

Q.1. Explain the following : (20)

(a) Private Network

(b) POP

(c) Fast Ethernet

(d) VLAN

Ans. (a) Private Network : A private network is designed for use inside an organization. It allows access to shared resources and, at the sametime, provides privacy.

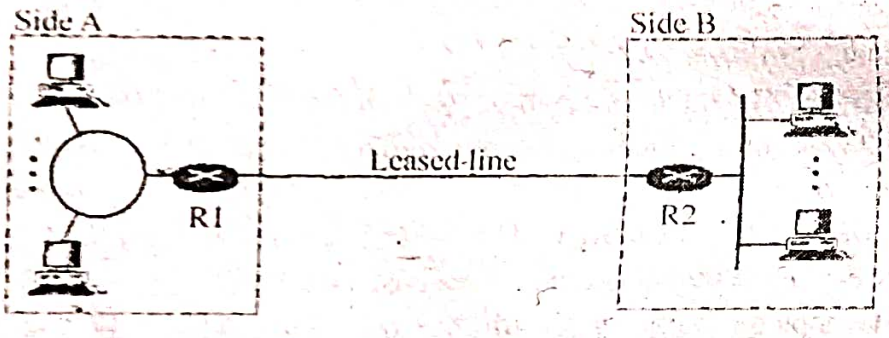


Fig. : Private network

An orgnization that needs privacy when routing information inside the organization can use a private network. A small organization with one single site can use an isolated LAN. People inside the organization can send data to one another that totally remain inside the organization, secure from outsiders. A larger organization with several sites can create a private internet. The LANs at different sited can be connected to each other by using routers and leased lines. In other words, an internet can be made out of private LANs and private WANs. Fig. shows such a situation for an organization with two sites. The LANs are connected to each other by routers and one leased line.

In this situation, the organization has created a private internet that is totally isolated from the global Internet. For end-to-end communication between stations at different sites, the organization can use the Internet model. However, there is no need for the organization to apply for IP address with the Internet authorities. It can use private IP addresses. The organization can use any IP class and assign network and host addresses internally. Because the intenet is private,duplication of addresses by another organization in the global Internet is not a problem.

Ans.(b) POP : POP is short for Post Office Protocol, a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP protocol.

POP3 version is moslty used. The POP3 consists of client POP3 software and server POP3 software. Out of these, the client POP3 software is installed on the receiving computer

whereas the server POP3 software is installed on the mail server. When the user wants to download e-mail from the mailbox on the email server, the events take place in the following sequence :

(i) The client (user) opens a connection with the server on TCP port 110.
(ii) It sends it user name and password to the server so as to access the mailbox.
(iii) The user is then allowed to list and get the mail messages one by one.

POP3 has following *two modes* :

– *Delete Mode* : In this mode, the mail is deleted from the mailbox after each retrieval. This mode is used when the user is working at his permanent computer.

– *Keep Mode* : If operated in this mode, the mail remains in the mailbox after retrieval. This mode is used whin the user accesses mail away from the primary computer.

Disadvantages of POP3 :

(i) POP3 does not allow organization of e-mail on the server.
(ii) The user can not have different folders on the server.
(iii) The user can not partially check the contents of E mail before downloading.

Ans.(c) Fast Ethernet : The IEEE 802.3 commitee developed a set of specifications referred to as the fast Ethernet to provide low-cost data transfer at the rate of 100 Mbps. It was designed to compete with LAN protocols such as fibre distributed data interface(FDDI) and it was also compatible with the standard Ethernet. The fast Ethernet uses a new feature called autonegotiation, which enables two devices to negotiate on certain features such as data rate or mode of transmission. It also allows a station to determine the capability of hub and two incomptible devices can also be connected to one another using this feature. Like the standard Ethernet, various physical-layer implementations of the fast Ethernet have also been specified. Some of them are as follows:

– *100Base-TX* : It either uses two pairs of either cat5 UTP cable or STP cable. The maximum length of the cable should not exceed 100m. This implementation uses MLT-3 line coding scheme due to its high bandwidth. However, since MLT-3 coding scheme is not self-synchronized, the 4B/5B block coding scheme is used to pervent long sequences of 0s and 1s. The block coding increases the data rate from 100Mbps to 125 Mbps.

– *100 Base-FX* : It uses two wires of fibre optic cable that can easily satisfy the high bandwidth requirements. The implementation uses NRZ-I coding scheme. As NRZ-I scheme suffers from synchronization problem in case of long sequence of 0s and 1s, 4B/5B block coding is used with NRZ-I to overcome this problem. The block coding results in increased data rate of 125 Mbps. The maximum cable length in 100 Base-FX must not exceed 100 m.

– *100 Base-T4* : It is the new standard that uses four pairs of cat3 or higher UTP cables. For this implementation, 8B/6T line coding scheme is used. The maximum length of cable must not exceed 100 m.

Ans.(d) VLAN : Virtual LAN is software that is employed to provide multiple networks in single hub by grouping terminals connected to switching hubs. It is a LANs that is grouped together by logical addresses into a virtual LAN instead of a physical LAN through a switch. The switch can support many virtual LANs that operate with having different network addresses or as subnets. Users within a virtual LAN are grouped either by IP address or by port address,

with each node attached to the switch via a dedicated circuit. Users also can be assigned to more than one virtual LAN.

The VLAN can be defined as a broadcast domain in which the broadcast address reaches all stations belonging to the VLAN. Communications within the VLAN can be secured and between those two controlled separate VLANs.

Characteristics of VLAN :

(1) Individual VLAN acts as a separate LAN, thus sharing the traffic among VLANs and reducing the congestion

(2) Workstations can be provided with full bandwidth at each port

(3) Relocation of terminals becomes easy

VLAN Benefits : As we have seen, there are several benefits to using VLANs. To summarize, VLAN benefits include:

(1) Increased performance

(2) Improved manageability

(3) Simplification of software configurations

(4) Increased security options

Increased performance : Switched networks by nature will increase performance over shared devices in use today by reducing collisions. Grouping users into logical networks will also increase performance by limiting broadcast traffic to users performing similar functions within workgroups. Additionally, less traffic will need to be routed, and the latency added to routers will be reduced.

Improved manageability : VLANs provide an easy, flexible, less costly way to modify logical groups in changing environments. VLANs make large networks more manageable by allowing centralized configuration of devices located in assorted locations.

Simplification of software configurations : VLANs will allow LAN administrators to "fine tune" their networks by grouping users. Software configurations can be made the same across machines with the consolidation of a department's resources into a single subnet. IP addresses and subnet masks will be more consistent across the entire VLAN. These services can be more effectively deployed when they can span buildings within a VLAN.

Increased security options : VLANs have the ability to provide additional security not available in a shared network environment. A switched network delivers packets only to the intended recipients and packets only to other members of the VLAN. This allows the network administrator to segment users requiring access to sensitive information into separate VLANs from the rest of the general users regardless of physical location.

VLAN Limitations : There are a few limitations to using VLANs:

(1) Device limitations

(2) Port constraints

Device limitations : The number of Ethernet addresses than can be supported by each device is 500. This is a distribution of about 20 devices per port on a 25 port switch. In an ideal network situation, there is one device per port, for example, a printer, a workstation, and voice IP phone will require 3 ports. If you wanted to have one VLAN assignment for each port, then the maximum VLANs will equal 25.

Port Constraints : If a hub or switch is connected to one port, every port on that hub must belong to the same VLAN. Hubs do not have the capability to provide VLANs to individual

ports, and VLANs can not be extended beyond the device port even if a switch capable of supporting VLANs is attached.

Section - A

Q.2. Given a complete description about ISO-OSI reference model. (20)

Ans. The ISO-OSI Reference Model : This reference model is proposed by International standard organization (ISO) as a a first step towards standardization of the protocols used in various layers in 1983 by Day and Zimmermann. This model is called Open system Interconnection (OSI) reference model. It is referred OSI as it deals with connection open systems. That is the systems are open for communication with other systems. It consists of seven layers.

Fig. shows the seven layer architecture of ISO-OSI reference model.

– The Physical Layer (Layer 1) : Functions of the physical layer are as follows:

(i) To activate, maintain and deactivate the physical connection.

(ii) To define voltages and data rates needed for transmission.

(iii) To convert the digital bits into electrical signal.

(iv) To decide whether the transmission is simplex, half duplex or full duplex.

– Data Link Layer (Layer 2) : Functions of the data link layer are as follows :

(i) Functions of the data link layer are synchronization and error control for the information which is to be transmitted over the physical link.

(ii) To enable the error detection, it adds error detection bits to the data which are to be transmitted.

(iii) The encoded data are then passed to the physical layer.

(iv) These error detection bits are used by the data link on layer on the other side to detect and correct the errors.

(v) At this level, the outgoing messages are assembled into frames, and the system waits for the acknowledgments to be received after every frame transmitted.

(vi) Correct operation of the data link layer ensures reliable transmission of each message. Examples of data link layer protocols are HDLC, SDLC and X.25 protocols.

– The Network Layer (Layer 3) : The functions of network layer are as follows :

(i) To route the signals through various channels to the other end.

(ii) To act as the network controller by deciding which route data should take.

(iii) To divide the outgoing messages into packets and to assemble incoming packets into messages for the higher levels.

– Transport Layer (Layer 4) : The functions of the transport layer are as listed below :

(i) It decides if the data transmission should take place on parallel paths or single path.

(ii) It does the functions such as multiplexing, splitting or segmenting on the data.

(iii) Transport layer guarantees transmission of data from one end to the other.

(iv) It breaks the data groups into smaller units so that they are handled more efficiently by the network layer.

– The Session Layer (Layer 5) : The functions of the session layer are as listed below :

(i) This layer manages and synchronizes conversations between two different

applications. This is the level at which the user will establish system to system connection

(ii) It controls logging on and off, user identification, billing and session management

(iii) In the transmission of data from one system to the other, at session layer streams of data are marked and resynchronized properly so that the ends of messages are not cut prematurely and data loss is avoided.

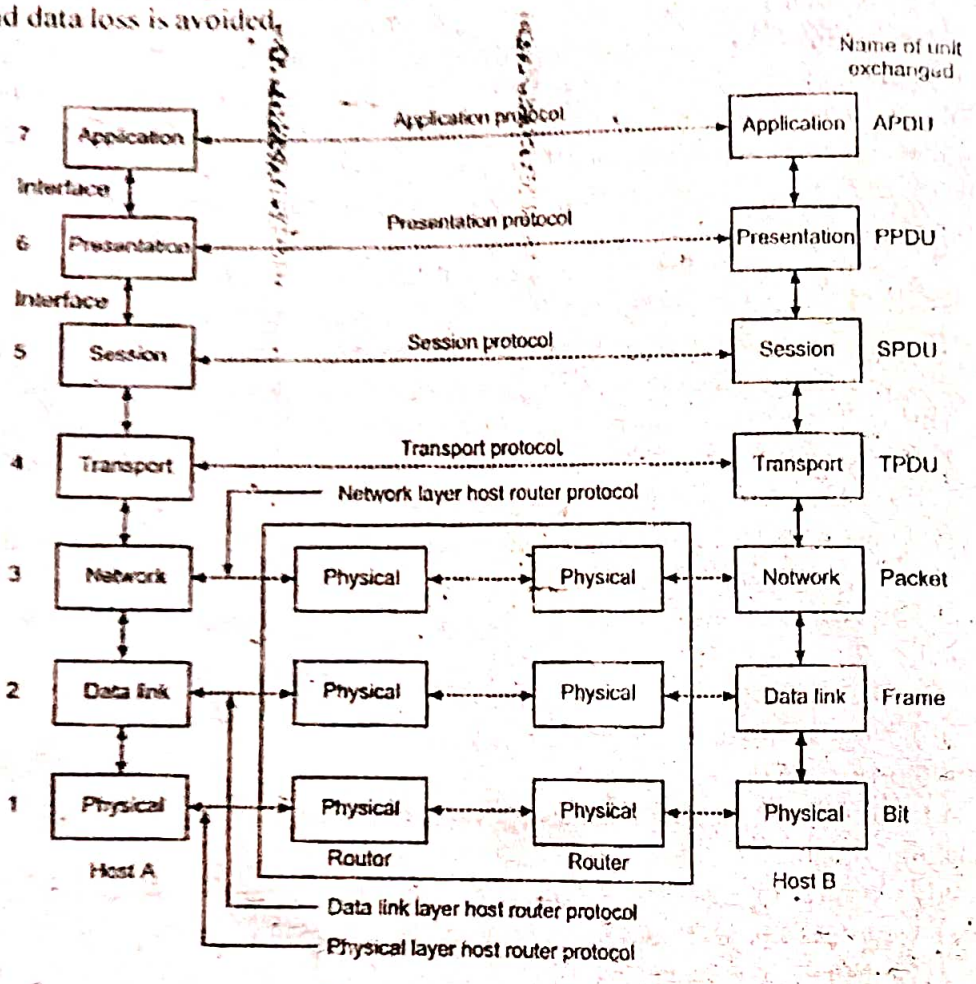


Fig. : The ISO-OSI reference model

– The Presentation Layer (Layer 6) : The functions of the presentation layer are as listed below :

(i) The presentation layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it.

(ii) The form and syntax (language) of the two communicating systems can be different e.g. one system is using the ASCII code for file transfer and the other one use IBM's EBCDIC.

(iii) Under such conditions, the presentation layer provides the translation from ASCII to EBCDIC and vice versa.

– Application Layer (Layer 7) : The functions of the application layer are as listed below :

(i) Application layer is at the top of all as shown in fig. It provides different services such as manipulation of information in various ways, retransferring the files of information, distribut-

ing the results etc. to the user who is sitting above this layer.

(ii) The functions such as LOGIN, or password checking are also performed by the application layer.

Q.3. Define Network Topology. Explain different types of Network Topologies in detail. (20)

Ans. Network topology : The topology of a network is the geometric representation of the relationship of all the links connecting the devices (or nodes). The five basic network topology are as shown in fig.(a).

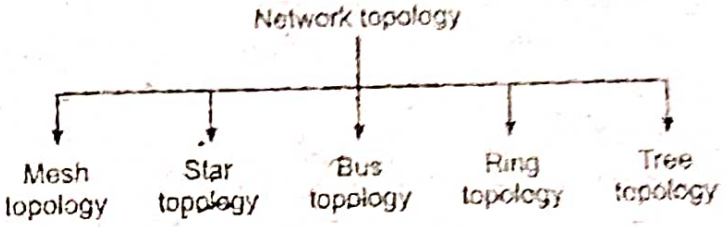


Fig.(a) : Classification of network topology

1. Bus Topology : The bus topology is usually used when a network installation is small, simple or temporary as shown in fig.(b).

When one computer sends a signal up to the cable, all the computers on the network receive the information, but the one with the address that matches the one encoded in the message accepts the information while all the others reject the message.

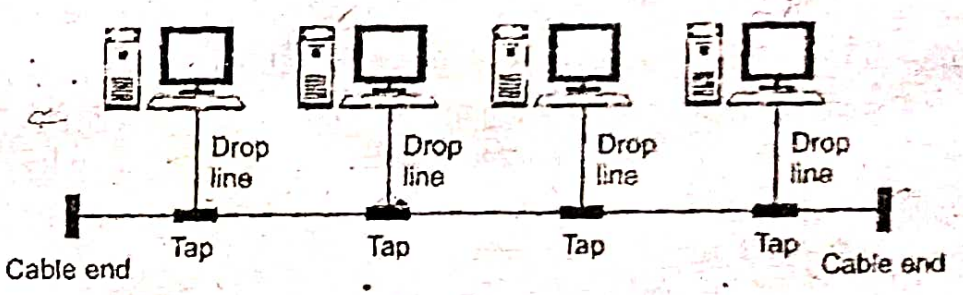


Fig.(b) : Bus topology

Advantage of Bus Topology :

(i) The bus topology is easy to understand, install, and use for small networks.

(ii) The cabling cost is less as the bus topology requires the least amount of cable to connect the computers.

(iii) The bus topology is easy to expand by joining two cables with a BNC barrel connector.

(iv) In the expansion of a bus topology, repeaters can be used to boost the signal and increase the distance.

Disadvantages of Bus Topology :

(i) Heavy network traffic slows down the bus speed. In bus topology, only one computer can transmit and others have to wait till their turn comes and there is no co-ordination between computers for reservation of transmitting time slot.

(ii) The BNC connectors used for expansion of the bus attenuates the signal considerably.

(iii) A cable break or loose BNC connector causes reflection and brings down the whole network causing all network activity to stop.

2. Ring Topology : In a ring topology, each computer is connected to the next computer, with the last one connected to the first as shown in fig.(c). Rings are used in high-performance networks where large bandwidth is necessary, e.g. time attractive features such as video and audio.

The messages flow around the ring in one direction. There is no termination because there is no end to the ring. Some ring networks do token passing. A short message called a token, is passed around the ring until a computer wishes to send information to another computer. That computer modifies the token, adds an electronic address and data and sends it around the ring. Each computer in sequence receives the token and the information and passes them to the next computer until either the electronic address matches the address of a computer or the token returns to its origin. The receiving computer returns a message to the originator indicating that the message has been received. The sending computer then creates another token and places it on the network, allowing another station to capture the token and begin transmitting. The token circulates until a station is ready to send and capture the token. Faster network circulate several tokens at once.

Advantages of Ring Topology :

(i) No one computer can monopolise the network because every computer in given equal access to the token.

(ii) The fair sharing of the network allows the network to continue function in a useful, if slower, manner rather than fail once capacity is exceeded as more users are added.

Disadvantages of Ring Topology :

(i) Failure of one computer on the ring can affect the whole network.

(ii) It is difficult to trouble short the ring.

(iii) Adding or removing the computers disturbs the network activity.

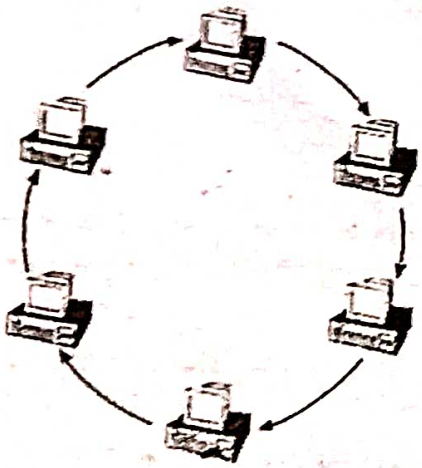


Fig.(c) : Ring topology

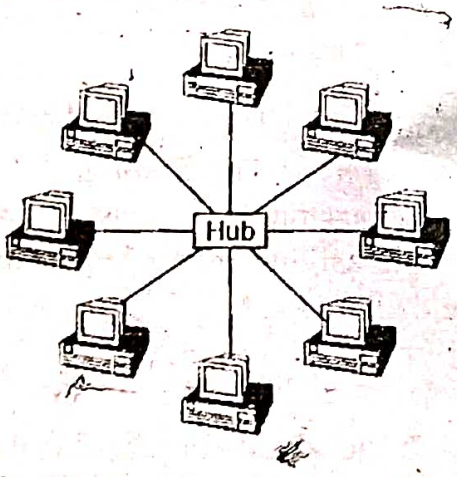


Fig.(d) : Illustration of star topology

3. Star Topology : In a star topology, all the cables run from the computers to a central location where they are all connected by a device called a hub as shown in fig.(d).

Each computer on a star network communicates with a central hub that re-sends the message either to all the computers in a broadcast star network or only to the destination computer in a switched star network. The hub in a broadcast star network can be active or passive.

Advantages of Star Topology :

(i) Star topology has minimal line cost because only n–1 lines are required for connecting *n* nodes.

(ii) Transmission delays between the two nodes do not increase by adding two nodes to network, because any two nodes are connected via two links only.

Disadvantages of Star Topology :

(i) If the central hub fails, the whole network fails to operate.

(ii) Many star networks require a device at the central point to rebroadcast or switch the network traffic.

(iii) The cabling cost is more since cables must be pulled from all computers to the central hub.

4. Mesh Topology : In a mesh topology. every device has a dedicated point-to-point link to every other device as shown in fig.(e).

A fully connected mesh network therefore has $n(n-1)/2$ physical channels to link h devices. To accommodate those links, every device on the network must have $n-1$ input / output ports.

Advantages :

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

(ii) A mesh topology is robust because the failure of single computer does not bring down the entire network.

(iii) It provides security and privacy because every message sent travels along a dedicated line.

(iv) Point to point links make fault diagnose easy.

Disadvantages :

(i) Since every computer must be connected to every other computer installation and reconfiguration is difficult.

(ii) Cabling cost is more.

(iii) The hardware required to connect each link input / output and cable is expensive.

5. Tree Topology : A tree topology is the variation of a star. As in a star. nodes in a tree are linked to a central hub that controls the traffic to the network.

However, not every computer plugs into the central hub, majority of them are connected to a secondary hub which , in turn, is connected to the central hub as shown in fig.(f). The central hub in the tree is an active hub which contains repeater. The repeater amplifies the signal and increases the distance a signal can travel. The secondary hubs may be active or passive. A passive hub provides a simple physical connection between the attached devices.

Advantages :

(i) It allows more devices to be attached to a single hub and can therefore increase the distance of a single can travel between devices.

(ii) It allows the network to isolate and priorities communications from different computers.

Disadvantages :

(i) If the central hub fails, the system breaks down.

(ii) The cabling cost is more.

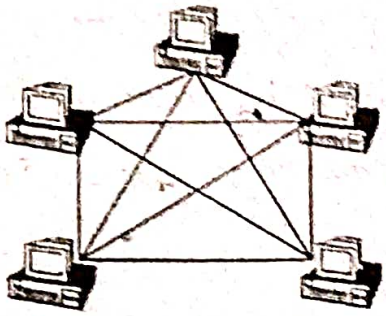


Fig.(e) : Illustration of Mesh topology

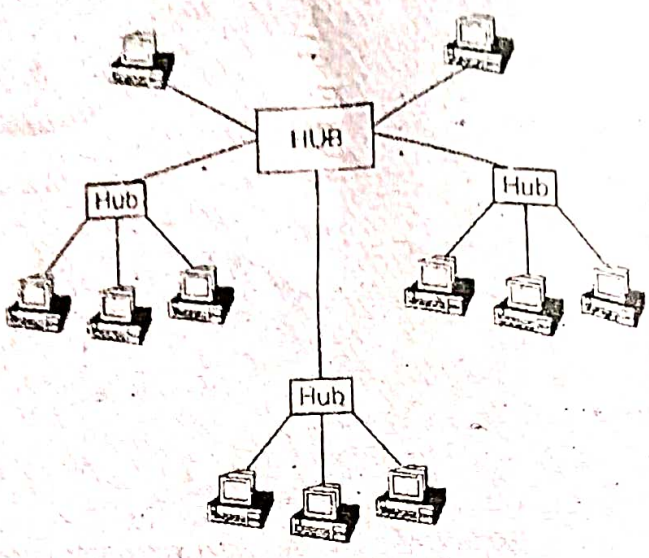


Fig.(f) : Illustration of tree topology

Section - B

Q.4. Explain the following : (20)

(a) Internet Protocol

(b) Transmission control protocol

Ans. (a) Internet Protocol : In addition to IP, which is used for data transfer, the Internet has several control protocols used in the network layer, including ICMP, ARP, RARP, BOOTP, and DHCP.

– ARP : ARP is used for associating an IP address to its MAC address. For a LAN, each device has its own physical or station address as its identification. This address is imprinted on the NIC (Network Interface Card).

– Reverse Address Resolution Protocol (RARP): RARP (Reverse Address Resolution Protocol) is part of the TCP/IP protocol suit. It allows a computer, particularly a diskless workstation, to obtain an IP address from a server. When a diskless TCP/IP work station is booted on a network, it broadcasts a RARP request packet on the local network. This address packet is broadcast on the network for all to receive because the workstation does not know the IP address of the server that can supply it with an address. It includes its own physical network address (the MCA adddress) in the request so the server could know where to return a reply. The server that receives the request looks in a table and matches the MAC address with an IP address, and then returns the IP address workstation.

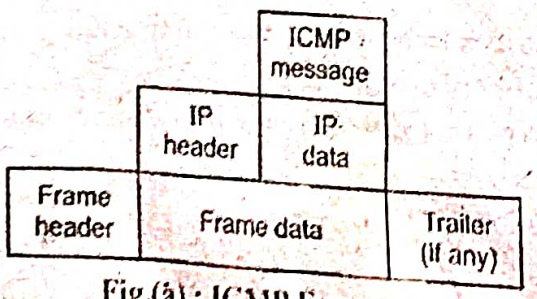


Fig.(a) : ICMP Encapsulation

– **ICMP(Internet Control Message Protocol) :** The Internet Control Message Protocol(ICMP) reports errors and sends control messages on behalf of IP. ICMP does not attempt to make IP a reliable protocol. It simply attempts to report errors and provide feedback on specific conditons. ICMP Messages are carried as IP a reliable protocol. It simply attempts to report errors and provide feedback on specific conditions. ICMP message are carried as IP packets and are therefore unreliable. IP also lacks a mechanism for host and management queries. A host sometimes needs to determine if a router or another host is alive. And sometimes a network manager needs information from another host or router. The Internet Control Message Protocol (ICMP) has been designed to compensated for the above two deficiencies. It is a companion to the IP, ICMP itself is a network layer protocol. However, its messages are not passed directly to the data link layer as would be expected. Instead, the messages are first encapsulated inside IP datagrams before going to the lower layer. This has been shown in fig.(a).

Ans. (b) Transmission control protocol : Fig.(1). shows the layout of a TCP segement. Every segment begins with a 20 byte fixed formed header. The fixed header may be followed by header options. After the options, if any upto 65535 – 20 – 20 = 65495 data bytes may follow.

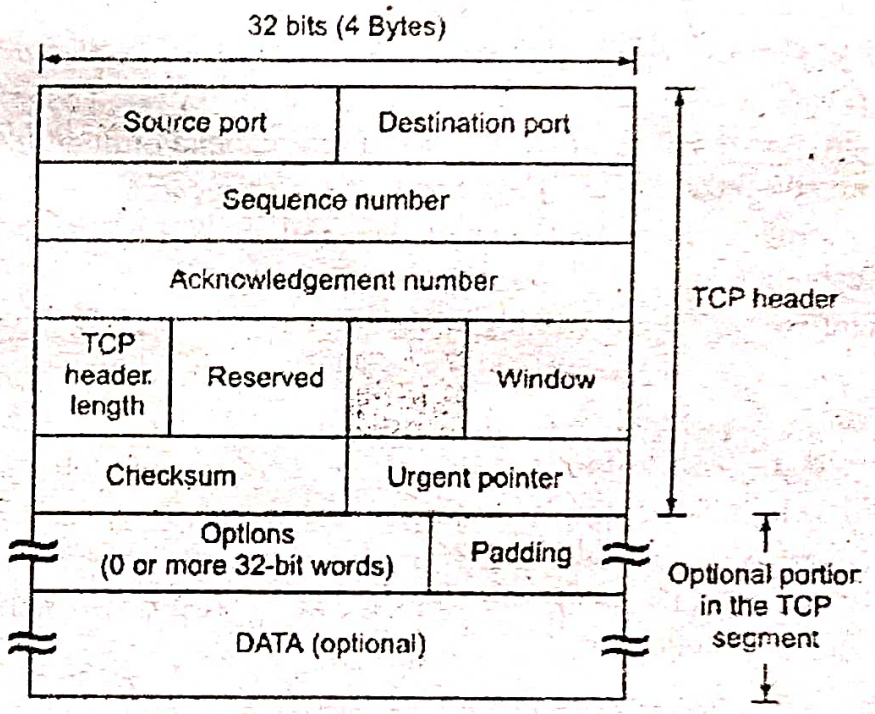


Fig.(1) : Illustration of TCP header format

Note that the first bytes correspond to the IP header and the next 20 correspond to the tCP header. The TCP segment without data are used for sending the acknowledgments and control messages.

Source Port : A 16 bit number identifying the application the TCP segement originated from within the sending host. The port numbers are divided into three ranges, well known ports (0 through 1023) registered ports (1024 through 49151) and private ports (49152 through 65535) Port assignments are used by TCP as an interface to the application layer.

Destination port : A 16 bit number identifying the application th TCP segement is destined for on a receiving host Destination port use the same port number assignment as those set aside for source ports.

Sequence number : A 32 bit number identifying the current position of the first data byte in the segment within entire byte stream for the TCP connection. After reaching $2^{32} - 1$, this number will warp around to 0.

Acknowledgments number : A 32 bit number identifying the next data byte the sender expects from the receiver. Therefore, the number will be one greater than the most recently received data type. This field is only used when the ACK control bit is turned on.

Header length or offset : A 4-bit field that specifies the total TCP header length in 32 bits words (or in multiplies of 4 bytes if you prefer). Without options, a TCP header a always 20 bytes in length. The largest, a TCP header, may be of 60 bytes. This field is required becuase the size of the options field (s) cannot be determined in advance. Note that this field is called "Data Offset" in the official TCP standard, but header length is more commonly used.

Reserved : A 6 bit field currently unused and reserved for future are.

Control Bits or Flags :

(i) Urgent pointer (URG) : If this bits field is set, receciving TCP should interpret the urgent pointer field.

(ii) Acknowledgment (ACK) : If this bit field is set, the acknowledgment field described eariler is valid.

(iii) Push Function (PSH) : If this bit field is set, the receiver, should deliver this segment to he receiving application as soon as possible. An example of its use may be to send a Control BREAK request to an application, which can jump ahead of queuded data.

(iv) Reset the connection (RST) : If this bit is present, it signals the receiver that the sender is aborbing the connection and all quened data and allocated buffers for the connection can be freely relinquished.

(v) Synchronize (SYZ) : When present this bit field signifies that sender is attempting to "synchronize" sequence numbers. This bit is used during the initial stages of connection establishment between a sender and receiver.

(vi) No more Data from Sender (FIN) : If set, this bit filed tells the receiver that the sender has reached the end of its byte stream for the current TCP connection.

Window : A 16 bit integer used by TCP for flow control in the form of a data transmission window size. This number tells the sender how much data the receiver is willing to accept. The maximum value for this field would limit be window size to 65,535 bytes, however a "window scale" option can be used to make use of even large windows.

Checksum : A TCP sender computes a value based on the contents of the TCP header and data fields. This 16 bit value be compared with the value the receiver generates using the same computation. If the values match, the receiver can be very confident that the segment arrived intact.

Urgent Pointer : In certain circumstances, it may be necessary for a TCP sender to notify the receiver urgent data that should be processed by the receiving application as soon as possible. This 16-bit field tells the receiver when the last byte of urgent data in the segment ends.

Options : In order to provide additional functionality, several optional parameters may be used between a TCP sender and receiver. Depending on the option (s) used, the length of this field will vary in size, but it cannot be larger than 40 bytes due to the size of the header length field (4 bits). The most common option is the maximum segment size (MASS) option . A TCP

receiver tells the TCP sender the maximum segment size it is willing to accept through the use of this option. Other options are often used for various flow control and congestion control techniques.

Padding : Because options may very in size, it may be necessary to "pad" the TCP header with zeros so that the segment ends on a 32 bit word boundary as defined by the standard.

Data : Although not used in some circumstances (e.g acknowledgment segments with no data in the reverse direction), this variable length field carries the application data from TCP sender to receiver. This field coupled with the TCP header field constitutes a TCP segment.

Q.5. Describe the following : **(20)**

(a) DNS

(b) IMAP

(c) MNTP

(d) HTTP

Ans. (a) DNS : The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.

Working of DNS : To map a name into an IP address, an application program calls a library procedure called the resolver. The name is passed on to the resolver as a parameter. The resolver sends a UDP packet to a local DNS server which looks up the name and returns the corresponding IP address to the resolver. The resolver then sends this address to the caller. Then the program can establish a tcp connection with the destination or send in the UDP packets.

The top level domains are of two types, namely. generic and countries.

DNS example : The DNS systemis a database. and no other databse on the planet gets this many requests. No other database on the planet millions of people changing it everyday. either. That is what makes the DNS system so unique.

For example :

(i) www.yahoo,com – the world's best known name.

(ii) www.mit.edu – a popular EDU name.

(iii) encarta.mas.com – a Web server that does not start with www.

(iv) www.bbc.co.uk – a name using four parts rather than three.

(v) ftp.microsoft.com – an FTP server rather than a Web server.

(vi) www.spce.ac.in – Server in India 'in' domain.

Ans.(b) IMAP : IMAP4 is similar to POP3, but it has more features: IMAP4 is more powerful and more complex.

IMPA4 provides the following extra functions:

(i) A user can check the e-mail header prior to downloading.

(ii) A user can search the onctents of the e-mail for a specific string of characters prior to downloading.

(iii) A user can partially donwload e-mail. This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.

(iv) A user can create a hierarchy of mailboxes in a folder for e-mail storage.

Ans.(c) MNTP : NNTP stands for Network News Transfer Protocol, Which is defined in RFC 997. NNTP has same as SMTP, with a client issuing commands in ASCII and a server

issuing responses as decimal numbers coded in ASCII. Mostg USENET machines now use NNTP.

NNTP was designed for two purposes. The first goal was to allow users whose desktop computers can't recive news to reade news remotely. Both are widely used. In the first one, news pull, the clients calls one of its news feeds and asks for new news. In the second one, news push, the news feed calls the client and announces that it has news. The NNTP commands support both of these approaches, as well as having people read news remotely.

Ans.(d) HTTP : HTTP stands for Hyper Text Transfer Protocol. HTTP is used mainly to acces data on WWW. This is protocol transfers data in the form of plaintext, hypertext, autio, video etc. The function of HTTP is like a combination of FTP and SMTP. It uses services of TCP. It uses only one TCP connection (port 80). There is no separate control connection. Only the data transfer take place between the client and server. The data transfer in HTTP is similar to SMTP. The format of the message is controlled by MIME like headers.

Principle of HTTP Operation : The principle of HTTP is simple. A client sends a request. The server sends a response. The request and response messages carry data in the form of a letter with a MIME like format. Fig.(1) shows the HTTP transactions between client and sever. The client initializes the transaction by sending a request message and the server replies it by sending a response.

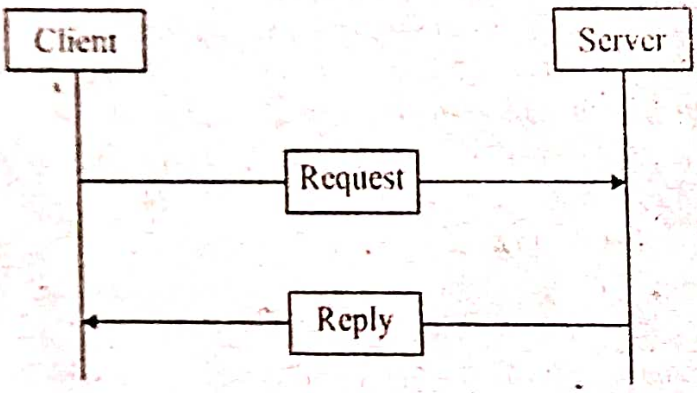


Fig.(1) : HTTP transaction

Types of HTTP Connection : There are following two types of connections in HTTP:

(i) Nonpersistent connections

(ii) Persistent connections

HTTP use persistent connections in its default mode. But it is possible to configure HTTP clients and servers to use nonpersistent connections.

The nonpersistent connection have some problems. First is that everytime a new connection requires to be established and maintained. Second problem is that each object suffers a delivery delay of two RTTs (Round Trip Time) – One RTT corresponding to TCP connection establishment and the other is request and receive an object.

If the persistent types of connection is used, then the server will leave the TCP connection open after sending a response. Hence, the same connection can be utilized sending request and response between a pair of client and server.

Further, the persistent connections can be of folllowing two version :

(i) Without pipelining

(ii) With pipelining

The default mode of HTTP uses persistant connections with pipelining.

Section - C

Q.6.(a) Define LAN. Explain in detail about features components of LAN. (10)

Ans. LAN(Local Area Network) : A LAN is a computer network that covers only a small geographical area (usually within a square mile or less) such as an office, home or building (Fig.a). In a LAN, connected computers have a network operating system installed onto them. One computer is designated as the file server, which stores all the software that controls the network. It also stores the software that can be shared by the computers attached to the network.

Different features of LAN are as follows :

(i) Limited Geographic Limits: A LAN is designed for a small area. Generally it spans a single office, work group floor in a building, or in a campus etc. LAN uses different protocols or rules lor information transmission.

(ii) Limited No. of Users: Most LAN supports I number of users usually around five or ten. More users can be supported by connecting different LANs together, which gives better results than making one: by network of the nature of MAN.

(iii) Reliability & Stability: LANS tend to be very reliable failures on a LAN are mostly due to wrong or improper installation and monitoring. Software that comes along with a LAN provides a number of useful programs like error-detection, prevention of transmission loss and excellent security features.

(iv) Flexibility: Major development in LANs today is flexibility they offer. Earlier versions would support only one type of desktop computers. Today's advanced LANs however can support different types of computers. The flexibility also extends to operating systems & storage media.

(v) Expandable: Most LANs can be expanded easily. More nodes (Terminal) can be added. Although, this depends on design of cabling plan (Topology) also. Also LANs can have more servers oil same network and a user at a terminal can connect to one or many servers and work comfortably.

Component of LAN :

(i) Basic Concept : Fig.(1) shows the components of LANs. A number of computers and network devices, such as printers, are interconnected by a shared transmission medium, typically a cabling system, which is arranged in a bus, ring, or star topology. The cabling system may use twisted-pair cable, coaxial cable, or optical fiber transmission media. In some cases, the cabling system is replaced by wireless transmission based on radio or infrared signals. The Ethernet bus topoloty using co-axial cable is shown in fig.1.(a). LAN standards define physical layer protocols that specify the physical properties of the cabling or wireless system for example, connectors and maximum cable lengths, as well as the digital transmission system, for example, modulation, line code, and transmission speed.

(ii) Network Interface Card(NIC) : The computers and network devices are connected to the cabling system through a network interface card (NIC) or LAN adapter card as shown in fig.1.(b). For desktop computers, the NIC is inserted into an expansion slot or built into the system. Laptop computers typically use the smaller PCMCIA card, which is inserted into a slot that can also be used by a modern or other device.

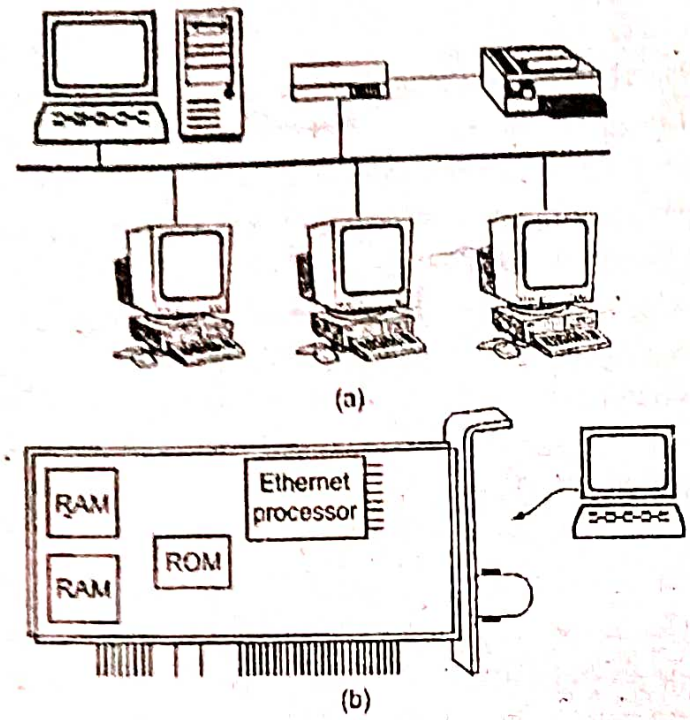


Fig.(1) : (a) Typical LAN Structure (b) Network interface card

Q.6.(b) What do you understand about layer 2 and 3 Switching. Explain. (10)

Ans. Layer 2 and Layer 3 Switching : A Layer 2 LAN switch performs switching and filtering based only on the OSI data link layer (Layer 2) MAC address. A Layer 2 switch is completely transparent to network protocols and uses applications. Recall that a Layer 2 switch builds a MAC address table that it uses to make forwarding decisions.

A Layer 3 switch, such as a Catalyst 3560 with an IP Servies image, functions similarly to a layer 2 switch, such as a Catalyst 2960, but instead of using only the Layer 2 MAC address information for forwarding decisions, a Layer 3 switch can also use IP address information. Fig.(1) illustrates the icons reserved for layer 2 and 3 switches. Instead of learing only which MAC addresses are associated with each of its ports, a Layer 3 switch can also learn which IP addresses are associated with its interfaces. This allows the Layer 3 switch to direct traffic throughout the network based on IP address information.

Layer 3 switches are also capable of performing Layer 3 routing functions, reducing the need for dedicated routers on a LAN. Because Layer 3 switches have specialized hardware, they can typically route data as quickly as they can switch data.

It should be emphasized that layer 2 switches do not completely replace the need for routers on a network. Routes perform additional Layer 3 services that Layer 3 switches are not capable of performing. Routers are also capable of performing packet-forwarding tasks not found on Layer 3 switches, such as establishing remote access connections to remote networks and devices. Dedicated routers are more flexible in their support of WAN interfece cards (WIC) making them the preferred, and somtimes only, choice the connecting to a WAN. Layer 3 switches can provide basic routing fucntions in a LAN and reduce the need for dedicated routers.

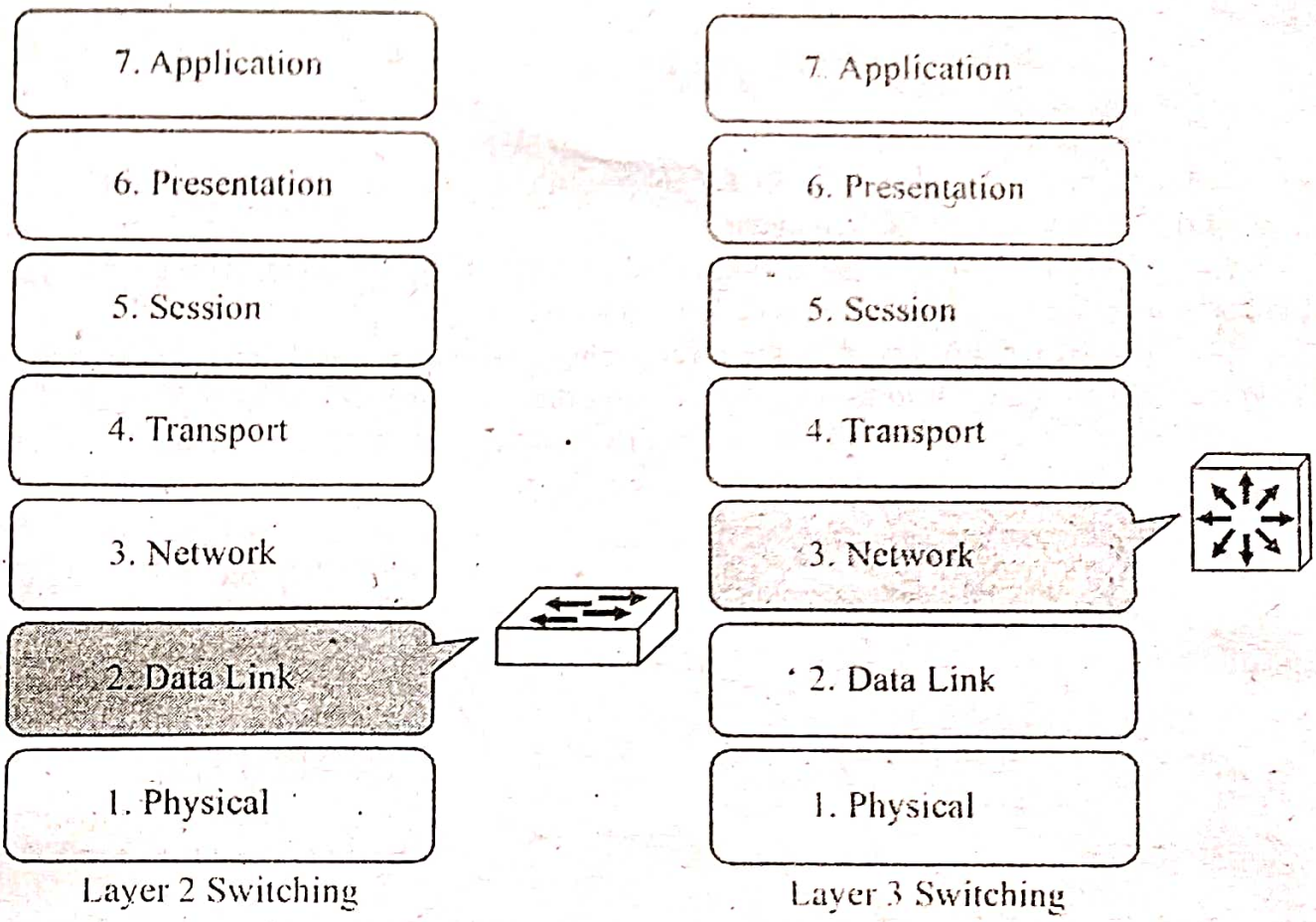


Fig.(1) : Layer 2 and Layer 3 Switching

Q.7. Explain the following : **(20)**

(a) Routing

(b) DQDB

Ans. (a) Routing : Routing is the act of moving information across an inter-network from a source to a destination. Routing protocols use metrics to evaluate what path will be the best for a packet to travel. A metric is a standard of measurement; such as path bandwidth, reliability, delay, current load on that path etc. that is used by routing algorithms to determine the optimal path to a destination.

Various **routing techniques** are as follows :

(a) *Mobile Routing* : A large number of people have portable computers and they want to work on them wherever they are in the world. Such computers are called *mobile hosts*. To route a packet to a mobile host, the network has first to find it. Let us consider fig. which shows a network model suitable for mobile communication. The network of fig. consists of a WAN which has routers and hosts. MANs, LANs and wireless cells are connected to this WAN.

The world is divided into areas. Each area has one or more foreign agents. A foreign agent is supposed to keep track of all the mobile users visiting his area. In addition to the foreign agents, each area has a home agent which keeps track of users whose home in the area but who are currently visiting some other area. When a new users enters an area, his computer has to register itself to the foreign agent of that area and when the user leaves that area, the deregistration should be carried out. The routing of packets to a mobile host takes place by following the routing

procedure given below :

(i) When a packet is to be sent to a mobile user, it is first routed to the user's home LAN.

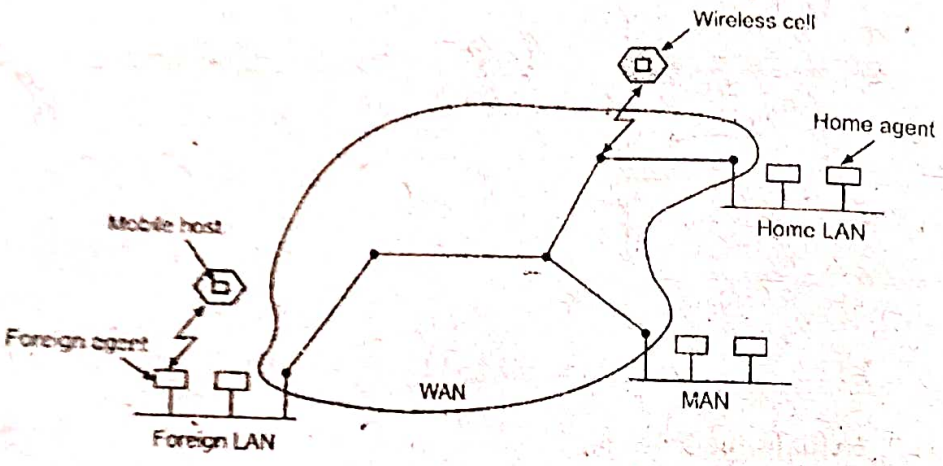
(ii) This packet is intercepted by the home agent.

(iii) This home agent then looks for the mobile user's current location and finds the address of the corresponding foreign agent.

(iv) The home agent then encapsulates the packet in the payload field of an outer packet and sends it to the foreign agent. This is called tunneling.

(v) This packet is received by the foreign agent, who removes the original packet from the payload field and sends it to the mobile user as a data link frame.

(vi) The home agent then tells the sender to send the packets directly to the mobile user. The packets are then routed directly to the user via the foreign agent.



(b) *Hierarchical Routing* : The hierarchical routing, such as the one used in telephone networks should be adopted. In this type of routing the total number of routers are divided into different regions. A router knows everything about the other routers in its own region only. It does not know anything about the internal structure of other regions. This reduces the size of the router table. When various networks are connected together, each network is treated as a separate region. For very large networks, the hierarchy is prepared as follows :

Level 1 : Regions

Level 2 : Clusters : it is a group of regions

Level 3 : Zones : zone is a group of clusters.

Level 4 : Groups : group contains many zones.

Two Level Hierarchical Routing : For networks of smaller size, a two-level hierarchical routing is sufficient. Fig.(a) shows network containing 3 regions. Fig.(b) shows the full routing table of router 1A which has 9 entries. Now, with a two-level hierarchical routing, the routing table of the same router reduces to a much smaller size as shown in fig.(c). This table has only 5 entries.

In the hierarchical table of fig.(c), there are entries for all local routers (1A, 1B and 1C) as before. But there are not detailed entries for the other regions. Instead all other regions have

been condensed into s single router per region. For example, traffic from 1A to any router in region-2 is via 1B-2A line as shown by the shaded entry in fig.(c). Similarly, all the traffic from 1A to region 3 is routed through the line 1C-3B. Comparison of fig.(b) and fig.(c) shows how hierarchical routing reduces the size of routing tables.

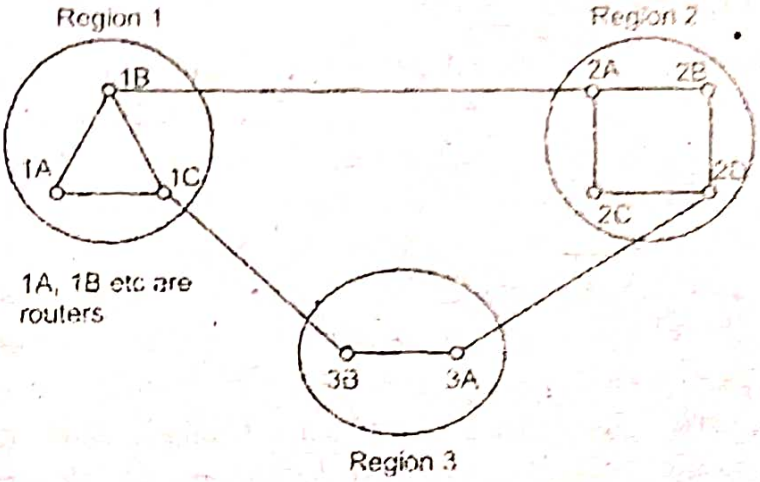


Fig.(a)

Full routing table for 1 A

Destination	Line	Hops
1 A	--	-
1 B	1 B	1
1 C	1 C	1
2 A	1 B	2
2 B	1 B	3
2 C	1 B	3
2 D	1 B	4
3 A	1 C	3
3 B	1 C	2

Fig.(b)

Hierarchical routing table For 1 A

	Destination	Line	Helps
Region 1	1 A	-	-
	1 B	1B	1
	1 C	1C	1
Region 2	2	1B	2
Region 3	3	1C	2

Fig.(c)

(c) *Flooding* : Flooding is the form of static algorithm. In this algorithm, every incoming packet is sent out on every outgoing line except the line on which it has arrived. One disadvantage of flooding is that it generates a large number of duplicate packets. Infact, it produces infinite number of duplicate packets unless we somehow damp the process. There are various damping techniques such as,

(i) Using a hop counter.

(ii) To keep a track of packets which have been flooded.

(iii) Selective flooding.

To prevent endless copies of packets circulating indefinitely through the network, a hop count may be used suppress onwards transmission of packets after a number of hops exceeding the network diameter. The destination must be prepared to receive multiple copies of an incoming

packet. Flooding has two interesting characteristics that arise from the fact that all possible routes are tried :

(i) As long as there is a route from souree to destination, the delivery of the packet is guaranteed.

(ii) One copy of the packet will arrive by the quickest possible route.

Ans.(b) DQDB : Distributed queue dual bus (DQDB) is a data-link layer communication protocol for Metropolitan Area Networks (MANs), specified in the IEEE 802.6 standard, designed for use in MANs. DQDB is designed for data as well as voice and video transmission based on cell switching technology. DQDB, which permits multiple systems to interconnect using two unidirectional logical buses, is an open standard that is designed for compatibility with carrier transmission standards such as SMDS, which is based on the DQDB standards.

For a MAN to be effective it requires a system that can function across long, city-wide *i.e* distances of several miles, have a low susceptibility to error, adapt to the number of nodes attached and have variable bandwidth distribution. Using DQDB, networks can be thirty miles long and function in the range of 34 Mbps to 155 Mbps. The data rate fluctuates due to many hosts sharing a dual bus as well as the location of a single host in relation to the frame generator, but there are schemes to compensate for this problem making DQDB function reliably and fairly for all hosts.

DQDB concept includes following things :

(i) A dual bus, with stations attached to both buses.

(ii) A frame generator at the end of each bus, creating frames of empty slots.

(iii) Stations can read from a bus, and can OR in data to a bus.

(iv) Station failure must leave the bus operating (isolation).

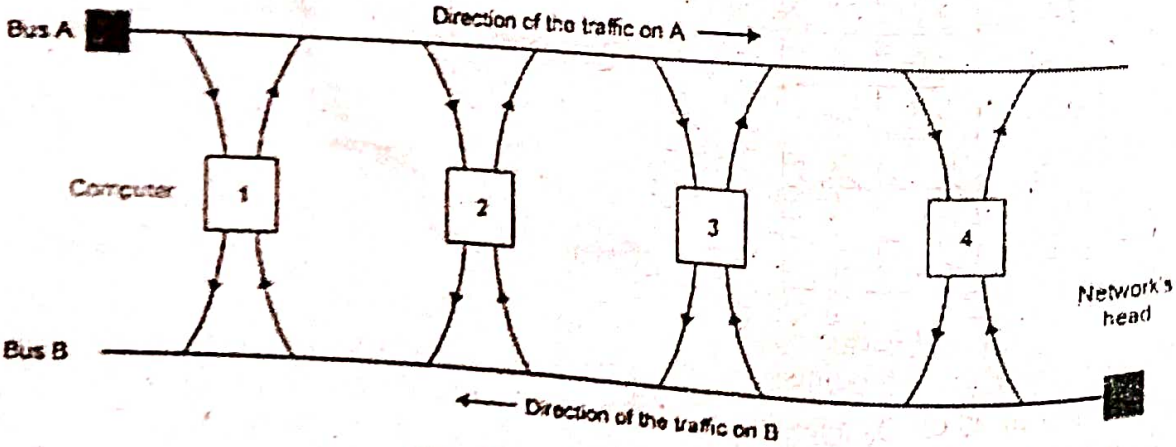


Fig. : DQDB Architecture

Section - D

Q.8. Given a complete decription about Synchronous Optical Network. (20)

Ans. SONET/SDH is a synchronous network using synchronous TDM multiplexing. All clocks in the system are locked to a master clock. The ANSI standard is called the Synchronous Optical Network (SONET). The ITU-T standard is called the Synchronous Digital Hierarchy (SDH).

The **architecture of a SONET system** include following :

(i) Signals

(ii) Devices

(iii) Connections.

(i) Signals : SONET defines a hierarchy of electrical signaling levels called synchronous transport signals (STSs). Each STS level (STS-1 to STS-192) supports a certain data rate, specified in megabits per second. The corresponding optical signals are called optical carriers (OCs). SDH specifies a similar system called a synchronous transport module (STM). STM is intended to be compatible with existing European hierarchies, such as E-lines, and with STS levels.

(ii) SONET Devices : Fig. shows a simple link using SONET devices. SONET transmission relies on three basic devices : STS multiplexers/demultiplexers, regenerators, add/drop multiplexers and terminals.

– *STS Multiplexer/Demultiplexer :* STS multiplexers/demultiplexers mark the beginning points and endpoints of a SONET link. They provide the interface between an electrical tributary network and the optical network. An STS multiplexer multiplexes signals from multiple electrical sources and creates the corresponding OC signal. An STS demultiplexer demultiplexes an optical OC signal into correspondig electric signals.

– *Regenerator :* Regenerators extend the length of the links. A regenerator is a repeater that takes a received optical signal (OC-*n*), demodulates it into the corresponding electric signal (STS-*n*), regenerates the electric signal, and finally modulates the electric signal into its correspondent OC-n signal. A SONET regenerator replaces soem of the existing overhead information (header information) with new information.

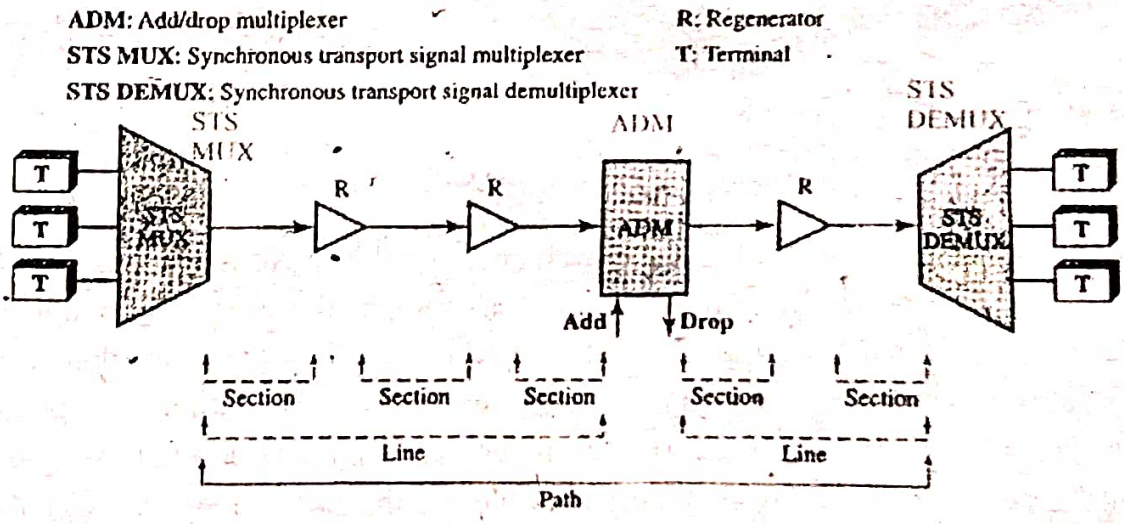


Fig : A simple network using SONET equipment

– *Add/drop Multiplexer :* Add/drop multiplexers allow insertion and extraction of signals. An add/drop multiplexer (ADM) can add STSs coming from different sources into a given path or can remove a desired signal from a path and redirect it without demultiplexing the entire signal.

– *Terminals :* A terminal is a device that uses the sevices of a SONET network. For example, in the Internet, a terminal can be a router that needs to send packets to another router

at the other side of a SONET network.

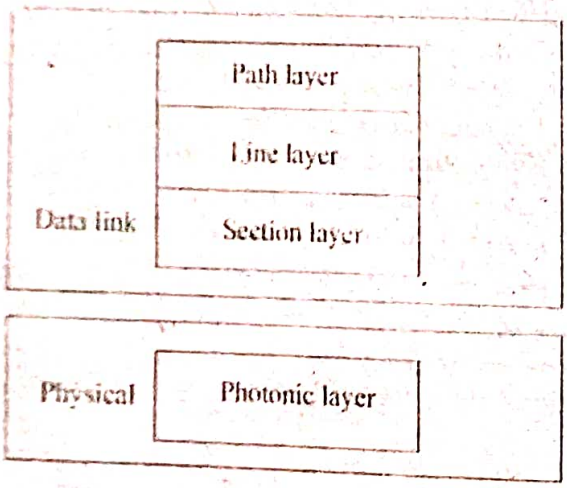
(iii) Connections : The devices in the previous section are connected using sections, lines, and paths.

– *Sections :* A section is the optical link connecting two neighbor devices: multiplexer to multiplexer, multiplexer to regenerator, or regenerator to regenerator.

– *Lines :* A line is the portion of the network between two multiplexers: STS multiplexer to add/drop multiplexer, two add/drop multiplexers, or two STS multiplexers.

– *Paths :* A path is the end-to-end portion of the network between two STS multiplexers. In a simple SONET of two STS multiplexers linked directly to each other, the section, line, and path are the same.

SONET Layers : The SONET standard includes four functional layers: the photonic, the section, the line, and the path layer. The correspond to both the physical and the data link layers (see Fig.).



– *Path Layer :* The Path Layer is responsible for the movement of a signal from its optical source to its optical destination. At the optical source, the signal is changed from an electronic form into an optical form, multiplexed with other signals, and encapsulated in a frame. At the optical destination, the received frame is demultiplexed, and the individual optical signals are changed back into their electronic form. Path layer overhead is added at this layer.

– *Line Layer :* The Line Layer is responsible for the movement of a signal across a physical line. Line layer overhead is added to the frame at this layer.

– *Section Layer :* The Section Layer is responsible for the movement of a signal across a physical section. It handles framing, scrambling, and error control. Section layer overhead is added to the frame at this layer.

– *Photonic Layer :* The Photonic Layer corresponds to the physical layer of the OSI model. It includes physical specifications for the optical fiber channel, the sensitivity of the receiver, multiplexing functions, and so on. SONET uses NRZ encoding with the presence of light representing 1 and the absence of light representing 0.

Q.9. Describe the following : (20)

(i) Proxy Server

(ii) Firewall

(iii) Windows NT/2000

Ans. (i) Proxy Server : 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 checks its cache. If the response is not stored in the cache, the proxy server sends the request to the corresponding server. Incoming response are sent to the proxy server and stored for future requests from other clients.

The proxy server reduces the load on the original server, decrease traffic, and improves latency. However, to use the proxy server, the client must be configured to access the proxy instead of the target server.

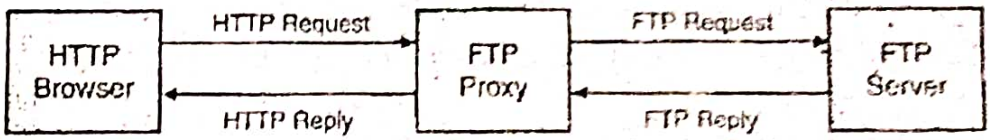


Fig. : Proxy Server

Types of **proxy server** are as follows :

(i) *Open proxy server* : An open proxy is a forwarding proxy server that is accessible by any Internet user. Gordon Lyon estimates there are "hundreds of thousands" of open proxies on the Internet. An anonymous open proxy allows users to conceal their IP address while browsing the Web or using other Internet services. There are varying degrees of anonymity however, as well as a number of methods of 'tricking' the client into revealing itself regardless of the proxy being used.

(ii) *Reverse proxy server* : A reverse proxy (or surrogate) is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more proxy servers which handle the request. The response from the proxy server is returned as if it came directly from the origin server, leaving the client no knowledge of the origin servers. Reverse proxies are installed in the neighborhood of one or more web servers. All traffic coming from the Internet and with a destination of one of the neighborhood's web servers goes through the proxy server. The use of "reverse" originates in its counterpart "forward proxy" since the reverse proxy sits closer to the web server and serves only a restricted set of websites.

Ans. (ii) Firewall : A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (bit forward) others. Fig.(a) shows a firewall.

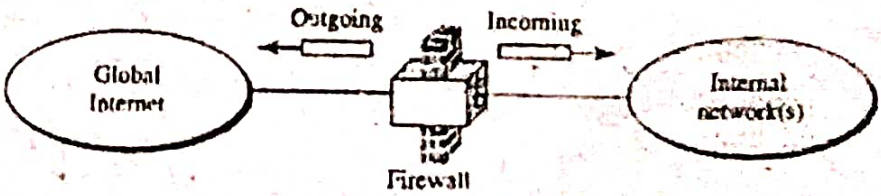


Fig. (a) : Firewall

For example, a firewall may filter all incoming packets destined for a specific host or specific server such as HTTP. A firewall can be used to deny access to a specific host or a specific service in the organization.

The firewall consists of two components, namely:

(i) Two routers for packet filtering.

(ii) An application gateway.

So, every packet has to travel through two packet filtering routers and an application gateway while going in or coming out because there is no additional route existing.

(i) *Packet Filter* : A packet filter is basically a standard router with some additional facilities. The additional facilities make it possible to inspect each incoming and outgoing packet. The packet satisfying certain criteria only are allowed to pass through. Those who fail to satisfy these conditions are dropped. The packet filter on the input side(inside LAN) checks the outgoing packets and that on the output side (outside LAN) checks the incoming packets. The application gateway makes further examination of the packets which have reached it through the router. Thus, every packet going in or coming out has to pass through the application gateway.

(ii) *Application Gateway*: Application gateway is the second half of the firewall mechanism. The application gateway does not just look at the raw packets but it operates at the application level. It is possible to set up a mail gateway to examine each message going in or coming out.

Ans. (iii) Refer Q9(iv) of paper May 2018.

COMPUTER NETWORK

May - 2018

Paper Code:-IT-305-F

Note : *Attempt five questions in all, selecting one question from each Section. Question No. 1 is compulsory. All questions carry equal marks.*

Q.1. Explain the following : (20)

(i) ARPANET

(ii) IMAP

(iii) Gigabit Ethernet

(iv) Frame Relay

Ans.(i) ARPANET : It is basically a WAN. It was developed by the ARPA (Advanced Research Project Agency). ARPANET was designed to service even a nuclear attack. ARPANET used the concept of packet switching network consisting of subnet and host computers. The subnet was a datagram subnet and each subnet consist of minicomputers called IMPs (Interface Message Processors). Each node of the network used to have an IMP and a host connected by a short wire. The host could send messages of upto 8063 bits to its IMP which would break them into packets and forward them independently toward the destination. The subnet was the first electronic store-and-forward type packet switched network. So each packet was stopped before it was forwarded. The original ARPANET design is as shown in fig.

The software for ARPANET was split into two parts, namely, subnet and host. The TCP/IP model and protocol were invented specifically to handle communication over internetworks because more and more networks were getting connected to ARPANET.

The TCP/IP made the connection of LANs to ARPANET easy. So, DNS (Domain Naming System) was created for organizing machines into domains and map host names onto IP address.

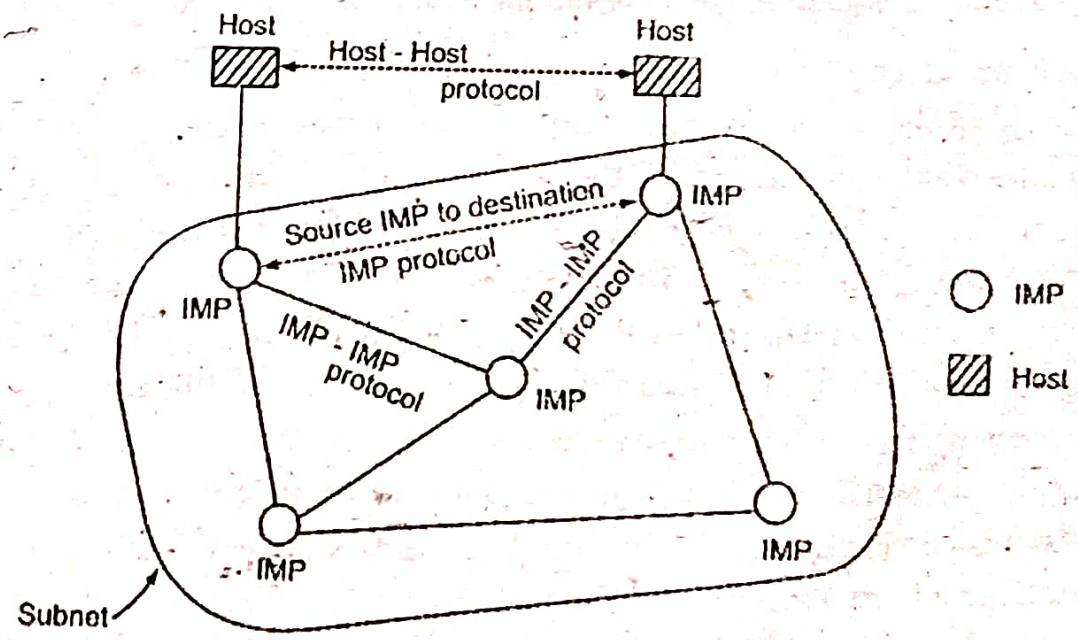


Fig. : APRANET

Ans.(ii)IMAP : IMAP4 is similar to POP3, but it has more features; IMAP4 is more powerful and more complex.

IMPA4 provides the following extra functions:

(i) A user can check the e-mail header prior to downloading.

(ii) A user can search the onctents of the e-mail for a specific string of characters prior to downloading.

(iii) A user can partially donwload e-mail. This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.

(iv) A user can create a hierarchy of mailboxes in a folder for e-mail storage.

Ans.(iii)Gigabit Ethernet : Gigabit Ethernet was developed by the IEEE 802.3 committee to meet the higher data rate requirements. This standard provides a data rate of 1000 Mbps(1 Gbps). It is backward compatible with traditional and fast Ethernet and also supports autonegotiation feature. Various physical layer implementation of gigabit Ethernet are as follows:

– *1000 Base-SX :* It is a two-wire implementation that use short wave fibres. One wire is used for sending the data and other is used for receiving the data. The NRZ line coding scheme and 8B/10B block coding scheme is used for this implementation. The length of the cable should not exceed 550 m in the 1000 Base-SX specifications.

–*1000 Base-LX :* It is also a two-wire implementation that use long wave fibres. One wire is used for sending the data and other is used for receiving. It is implemented by the NRZ line coding scheme and the 8B/10B block coding scheme. The length of the cable should not exceed 5000 m in the 1000 Base-LX specifications.

– *1000 Base-CX :* It uses two STP wires where one wire is used for sending the data and other is used for receiving the data. It is implemented by the NRZ line coding scheme and 8B/10B bolck-coding scheme. The length of the cable should not exceed 25 m in the 1000 Base-CX specifications.

– *1000 Base-T :* It uses four cat5 UTP wires. It is implemented by the 4D-PAMS line coding scheme. In this specification, the length of the cable should not exceed 100 m.

Ans.(iv)Frame Relay : Frame relay is a connection oriented service. It can be imagined to be equivalent to a virtual leased line. On a virtual line, data bursts can be sent at full speed. Frame relay provides a service to determine the start and end of each frame. It also detects the transmission errors. But, the frame relay does not have error control or flow control. If a frame contains errors then the frame relay service discards it. Unlike X.25, frame relay does not provide acknowledgements or normal flow control. Packet switching was developed when the long distance digital communication showed a large error rate. To reduce the error rate, additional coding bits were introduced in each packet in order to introduce redundancy to detect and recover errors. However, in the modern high speed telecommunication systems, this overhead is unnecessary and infact counter productive. Frame relay was developed for taking the advantage of the high data rates and low error rates in the modern communication system. The original m packet switching networks were designed with a data rate at the user end of about 64 kbps.

Section – I

Q.2. What do you understand by Layering architecture of Networks. Draw and explain the five layering architecture. **(20)**

Ans. Layering architecture of Network : Most networks are organized as a series of layers or levels. To reduce the design complexity, networks are organised as a series of layer or levels, one above the other as shown in Fig.(a). The number of layers, the name of each layer, the contents of each layer and the function of each layer differ from network to network.

The purpose of each layer is to offer certain service to the higher layers. Layer *n* on one machine (source) carries on a conversation with layer *n* on another machine (destination).

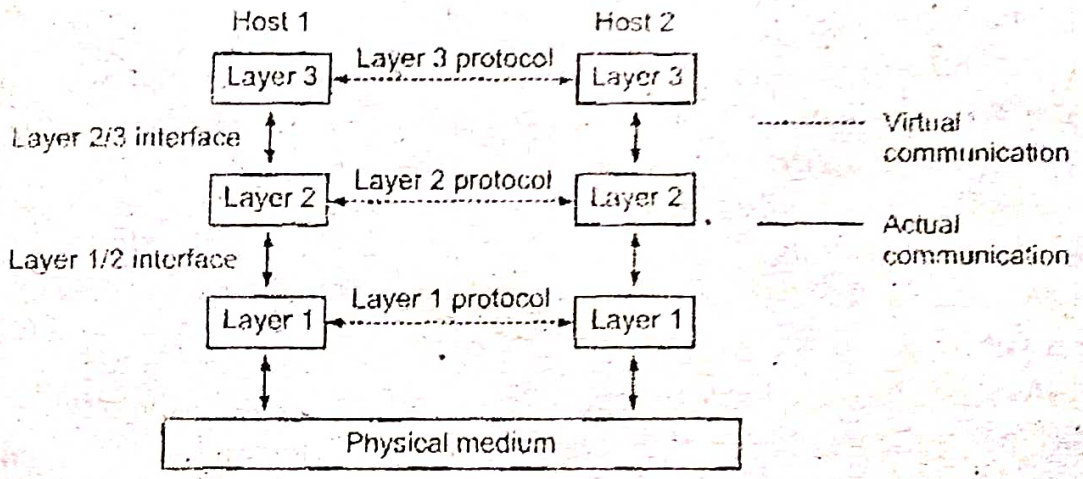


Fig.(a) : Layers, protocols and interfaces

The rules and conventions used in this conversation are collectively known as the layer *n* protocol. Basically, a protocol is an agreement between the two machine as how communication link should be established, maintained and released. Violation of the protocol will make the communication difficult.

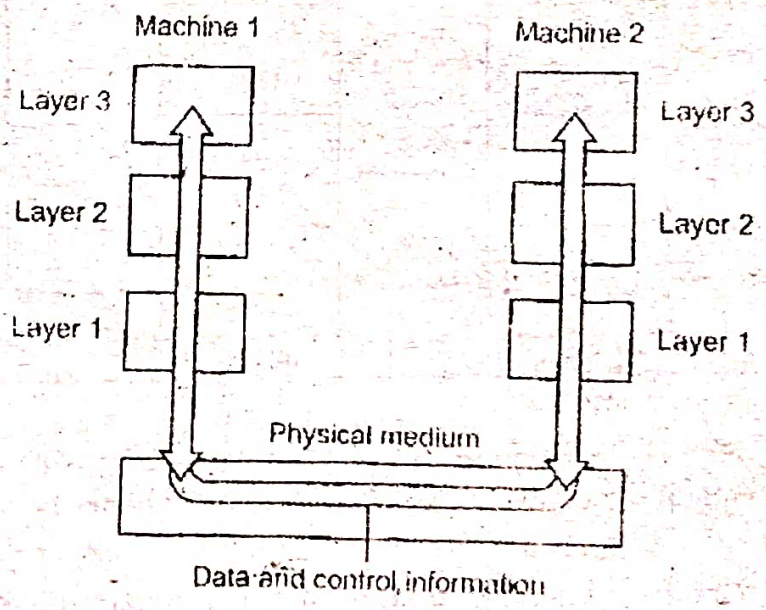


Fig.(b) : Illustration of data transfer

Data do not get transferred directly form layer *n* of one machine to layer *n* of the other machine. Instead the data transfer takes place as explained below.

The data and control information are passed on to the lower layers until the lowest layer (layer 1) is reached. Below layer 1 lies the physical medium such as coaxial cable, through which the actual communication takes place. Thus is shown in fig.(b).

An *interface* defines the operations and services offered by lower layer to the upper layer. There is an interface between each pair of adjacent layers.

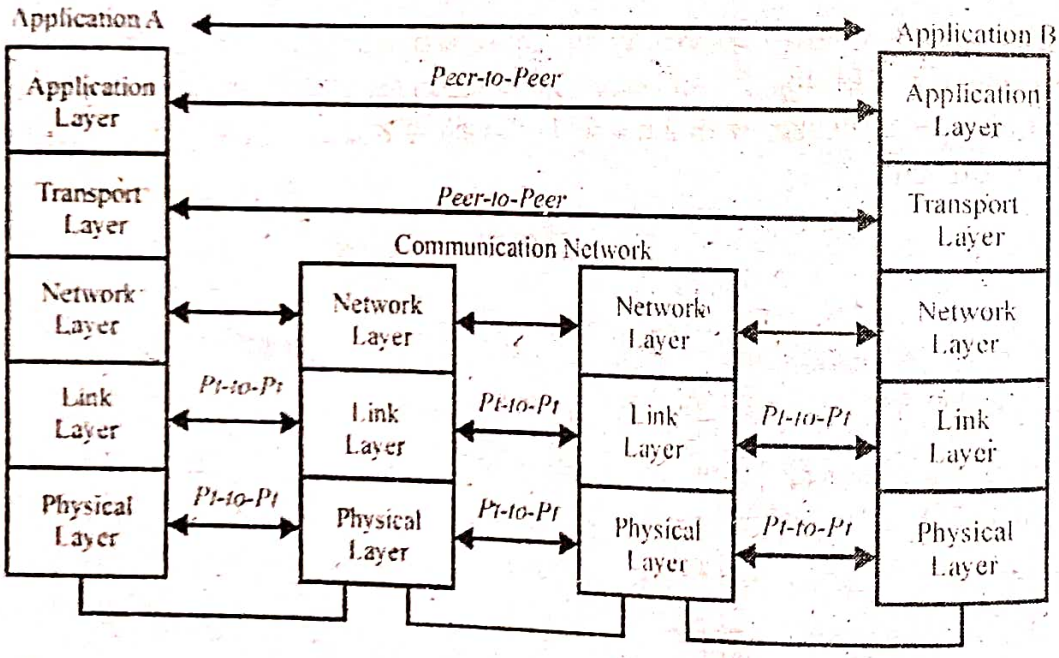
The five layer architecture consists of the following layers:

(i) Application layer
(ii) Transport layer
(iii) Network interface
(iv) Link layer
(v) Physical layer

(1) Applicationlayercontains the higher-level protocols used by most applications for network communication. These contain protocols for specific data communication services on a process to process level. Protocols used are:

- Simple mail transfer protocol
- File transfer protocol
- IMAP
- POP

Interface: It is the layer that provides interface between the applications one uses to communicate and the underlying network over which the messages are transmitted.



(2) Transport Layer: The transport layer establishes a basic data channel that an application uses in its task-specific data exchange. The layer establishes host-to-host connectivity meaning it handles the details of data transmission that are independent of the structure of user data and the logistics of exchanging information for any particular specific purpose. Its responsibility includes end-to-end message transfer independent of the underlying network, along with error control, segmentation, flow control, congestion control, and application addressing (port numbers).

Protocols: The protocols used by transport layer are:
- User datagram protocol
- Transmission control protocol

Interface: The Transport layer Interface or TLI provides an interface to the transport layer based on the use of streams, rather than the file based abstraction of sockets. The basic operations are:
- t_open(), this opens the file that identifies the transport provider
- t_bind() assigns an adress to the transport end point
- t_alloc() allocates storage for the data structures required by the communication
- t_listen() waits for a connection request from a client. This is a server call.
- t_accept() chooses whether or not to accept a request gathered by a t_listen()
- t_rcv() receives data

(3) Network Interface: A Network interface is a systems (software and/or hardware) interface between two pieces of equipment or protocol layers in a network. They usually have some form of network addresses. They may consist of a node Id and a port number or may be a unique node Id in its own right.

Protocol: The protocol used is Internet Protocol

Interface: Network interfaces provide standardised functions such as passing messages, connecting and disconnecting etc. etc.

(4) Link Layer: This layer defines the networking methods within the scope of the local network link on which hosts communicate without intervening routers. This layer describes the protocols used to describe the local network topology and the interfaces needed to effect transmission of Internet layer datagrams to next-neighbour hosts.

Protocol: The protocols used are:
- Address resolution protocol
- Reverse address resolution protocol
- Neighbour discovery protocol

Interface: It contains hardware interface methods such as Ethernet and other IEEE 802 encapsulation schemes.

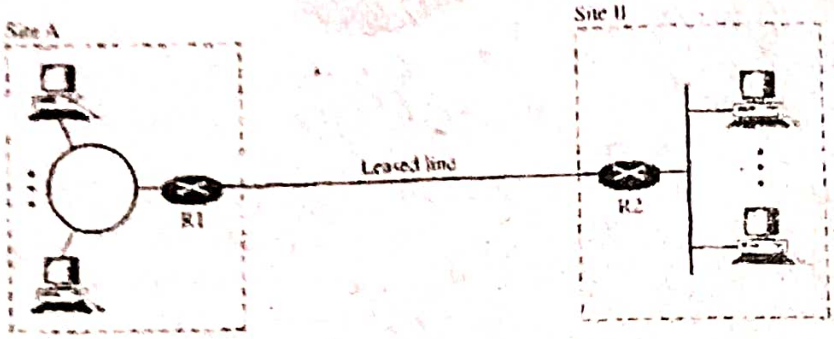
(5) Physical Layer: It is a fundamental layer underlying the logical data structures of he higher level functions in a network. The *physical layer* provides an electrical, mechanical, nd procedural *interface* to the transmission medium.

Q.3.(i) Give a brief description about Private Networks. **(10)**

Ans. Private Network : A private network is designed for use inside an organization. allows access to shared resources and, at the sametime, provides privacy.

An orgnization that needs privacy when routing information inside the organization can se a private network. A small organization with one single site can use an isolated LAN. People nside the organization can send data to one another that totally remain inside the rganization, secure from outsiders. A larger organization with several sites can create a private ternet. The LANs at different sited can be connected to each other by using routers and leased nes. In other words, an internet can be made out of private LANs and private WANs. Fig.

shows such a situation for an organization with two sites. The LANs are connected to each other by routers and one leased line.



In this situation, the organization has created a private internet that is totally isolated from the global Internet. For end-to-end communication between stations at different sites, the organization can use the Internet model. However, there is no need for the organization to apply for IP address with the Internet authorities. It can use private IP addresses. The organization can use any IP class and assign network and host addresses internally. Because the intenet is private,duplication of addresses by another organization in the global Internet is not a problem.

Q.3.(ii) Define Network. Explain in detail about types of Networks. (10)

Ans. Computer Network : Computer network is a system which allows communication amoung the computers connected in the network. A network must be able to meet certain criteria. The most important of them are:

1. Performance
2. Relaibility
3. Security

1. *Performacnce* : Performance can be measured in many ways. We can measure it in terms of transit time and respnse time.

(a) Transit time is defined as the amount of time required for a message to travel from one device to the other.

(b) Response time: It is the time elapsed between enquiry and response.

The other factors deciding the performance are as follows:

(i) Number of users

(ii) Type of transmission medium

(iii) Capability of connected hardware

(iv) Efficiency of software.

2. *Reliability :* The network reliability is importnat because it decides the frequency at which network failure takes place. It also decides the time taken by the network to recover and its robustness in the catastrophe.

3. *Security :* The network secutiry refers to protection of data from the unauthorized user or access.

Different types of Network : Different types of Network are as follows :

(i) Local Area Network : A LAN is a computer network that covers only a small geographical area (usually within a square mile or less) such as an office, home or building

(Fig.a). In a LAN, connected computers have a network operating system installed onto them. One computer is designated as the file server, which stores all the software that controls the network. It also stores the software that can be shared by the computers attached to the network. Other computers connected to the file server are called workstations. The workstations can be less powerfull than the file server and they may have additional software on their hard drive. On most LANs, cables are used to connect the computer. Generally , LAN offers a bandwidth of 10-100Mbps.

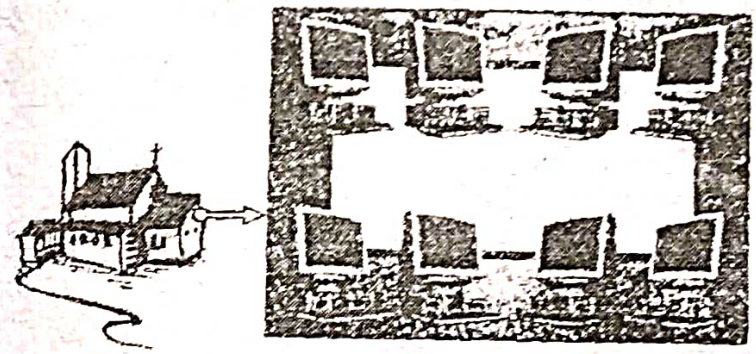


Fig.(a) : Local area network

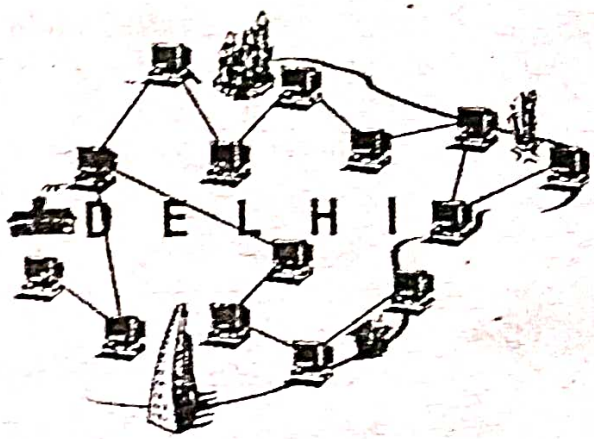


Fig.(b) : Metropoiltian area network

(ii) Metropolitan Area Network : A MAN is a network of computers spread over a "metropolitan" area such as city and its suburbs (fig.b). As the name suggests, this sort of network is usually reserved for metropolitan areas where the city bridges its LANs with a series of backbones, making one large network for the entire city. It may be a single network such as a cable television network or it may be a means of connecting as number of LANs. Note that MAN may be operated by one organization (a corporate with several offices in one city) or be shared and used by serval organization in the same city.

(iii) WAN : It stands for wide area network. This is the largest network and can inter-connect networks throughout the world and is not restricted to a geographical location. The Internet is an example of a worldwide public WAN. Most WANs exist to connect LANs that are not in the same geographical area. This technology is high speed and very expensive to setup. It is shown in fig.(c).

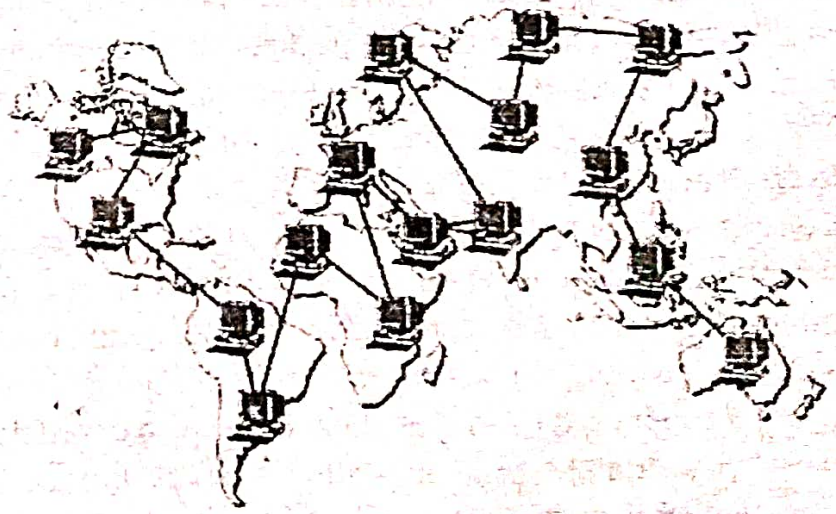


Fig.(c) : Wide area network

Section – II

Q.4. Give a complete description about TCP/IP reference Model. (20)

Ans. TCP/IP reference model : The Internet Protocols (IP) and Transmission Control Protocol (TCP) are together known as TCP / IP protocol. TCP/IP are two protocols : Transmission control protocol and Internet protocol. These two protocols describe the movements of data between the host computers or Internet.

TCP /IP offers simple naming and addressing scheme whereby different resources on Internet can be easily located. Information on Internet is carried in Packets. The IP protocol is used to put a message into a packet. Each packet has the address of the sender and the recipient's address. These addresses are known as the IP addresses. Using the TCP protocol, a single large message is divided into a sequence of packets and each is put an IP packet.

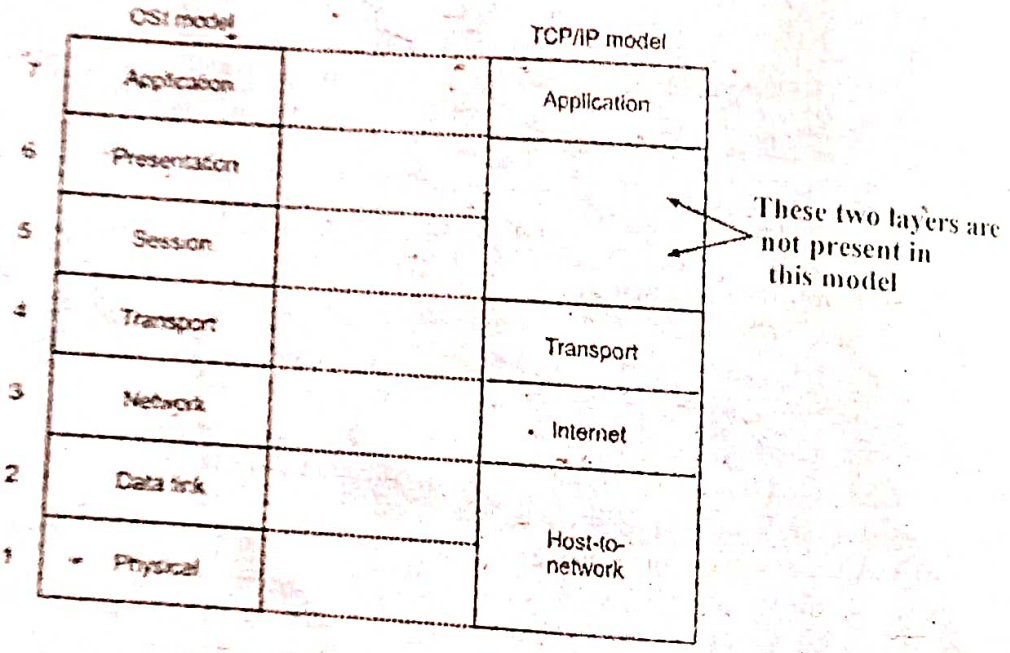


Fig.(a) : TCP/IP reference model

The packets are passed from one network to another until they reach their destination. At the destination, the TCP software reassembles the packets into a complete message. It is not necessary for all the packets in a single message to take the same route each time it is sent.

As shown in fig.(a), the TCP/IP model has only four layers.

1. Internet Layer : The goals requirements lead to the selection of a packet switching network which is based on a connectionless internetwork layer. This layer is called as the internet layer and it holds the whole architecture together. The task of this layer is to allow the host ot insert packets into any network and then make them travel independently to the destination. The order in which the packets are received can be different from the sequence in which they were sent. Then the higher layers are supposed to arrange them in the proper order. The internet layer defines (specifies) a packet format and a protocol called internet protocol (IP). The internet layer is supposed to deliver IP packets to their destinations. So routing of packets and congestion

control are important issues related to this layer.

2. Transport Layer : This is the layer above the internet layer. Its functions are same as those of a transport layer in OSI layer. This layer allows the per entities of the source and destination machines to converse with each other. The end to end protocols used here are TCP and UDP. TCP is a reliable connection oriented protocol. It allows a byte stream transmitted from one machine to be delivered to the other machine without introducing any errors. TCP also handles the flow control. UDP (user datagram protocol) is the protocol used in the transport layer. It is an unreliable, connectionless protocol and used for the applications which do not want the TCP's sequencing or flow control. UDP is also preferred over TCP in those applications in which prompt delivery is more important than accurate delivery. It is used in transmitting a video.

3. Application Layer : TCP / IP model does not have session or presentation layers. because they are of little importance in most applications. The layer on top of transport layer is called as application layer.

4. Host network layer : This is the lowest layer in TCP /IP reference model. The host has to connect to the network using some protocol, so that it can send the IP packets over it. This protocol varies from host to host and network to network.

Application Layer	TELENT, FTP, DMTP, DM, HTTP, NNTP
Transport	TCT UDP
Internet (Network)	IP
Host-to-network	ARPANET, SATNET LAN, packet radio

Q.5.(i) Explain in detail about E-mail System. **(10)**

Ans. Electronic mail is a way of exchanging digital messages. It is sent from the sender to one or more receiver. Email systems are based upon store and forward model. Email address identifies to the email box to which the messages are delivered. The email address can be divided into two parts :

– Local part

– Domain part

Email working takes place in the following steps :

(i) *Message sender :* The sender of the message makes use of mail software to compose the document.

(ii) *Internet Mail address :* It is attached to each message.

(iii) *Mail submission server :* Mail submission server converts the domain name of the recipient's mail address into Internet protocol address.

(iv) *Routers :* Routers read the IP address on a packet and sends it towards its destination.

(v) *Destination mail server :* Destination mail server places the packets in its original order.

Advanced Features of E-mail Systems are as follows :

(i) Forwarding an e-mail to a person away from his computer.

(ii) Creating and destroying mailboxes to store incoming e-mail.

(iii) Inspection contents of mailbox, insert and delete messages from the mailboxes.

(iv) Sending a messsage to a large group of people using the idea of mail list.
(v) To provide registered e-mail.
(vi) Automatic notification of undelivered e-mail.
(vii) Carbon copies.
(viii) High priority e-mail.
(ix) Alternative recipient.

Q.5.(ii) Give a brief description about IP addressing. (10)

Ans. IP Addressing : An IP address is a unique address used to locate and identify a device over a network. That device can be an electronic device, a computer, a server, a router or even an IP phone. It is the addressing used for the transmission of data packets over a network working with the IP protocol.

It is classified as :

(i) Class A address format : The network field is 7 bit long as shown in fig.(a) and the host field is of 24 bit length. So the network field can have numbers between 1 to 127. But the host numbers will range from 0.0.0.0 to 127.255.255.255. Thus in class A, there can be 126 types of network and 17 million hosts. The "0" in the first field identifies that it is a class A network address.

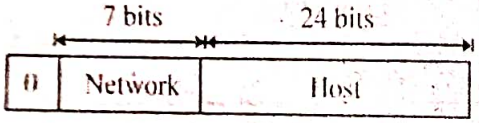


Fig. (a) : Class A IP Address formats

(ii) Class B address Format : The Class B address format is show in fig.(b).

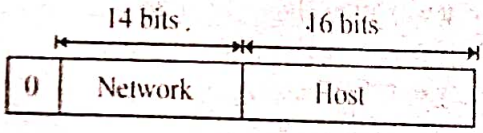


Fig. (b) : Class B Format

The first two fields identify the network, and the number in the first field must be in the range 128-191. Class B networks are large. Host numbers 0.0 and 255.255 are reserved. So there can be upto 65,234 (216-2) host in a class B network. Most of the 16,382 class B address have been allocated. The first block covers address from 128.0.0.0.0 in 128.255.255.255.255 and the last block covers from 191.255.0.0 to 191.255.255.255.

(iii) Class C address format : Class C address format is shown in fig.(c).

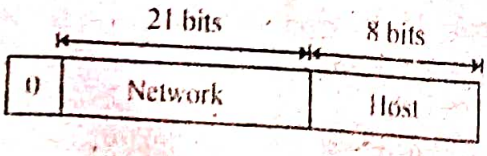


Fig. (c) : Class C Format

The first block in class covers addresses from 192.0.0.0 to 192.0.0.253 and the last block covers address from 223.255.255.0 to 223.255.255.255

(iv) Class D format : The class D address format is show in fig.(d).

1110	Multicast address

Fig. (d) : Class D Format

The class format allows for upto 2 million networks with upto 254 hosts each and class D format allows the multicast in which a datagram is directed to multiple hosts.

(v) Class E address format : Fig.(e) shows the address format for a class E address. This address begins with 1110 which shows that it is reserved for the future use.

1110	Reserved for future use

Fig. (e) : IP address for class E Network

The 32 bit (4 byte) network address are usually written in dotted decimal notation. In this notation each of the 4 bytes is written in decimal from 0 to 255. So the lowest IP address 0.0.0.0 i.e. all the 32 bites are zero and highest IP address is 255.255.255.255

Section – III

Q.6.(i) Define LAN. Explain in brief about LAN standards. **(10)**

Ans. Local Area Network : A LAN is a computer network that covers only a small geographical area (usually within a square mile or less) such as an office, home or building (Fig.a). In a LAN, connected computers have a network operating system installed onto them. One computer is designated as the file server, which stores all the software that controls the network. It also stores the software that can be shared by the computers attached to the network. Other computers connected to the file server are called workstations. The workstations can be less powerful than the file server and they may have additional software on their hard drive. On most LANs, cables are used to connect the computer. Generally , LAN offers a bandwidth of 10-100Mbps.

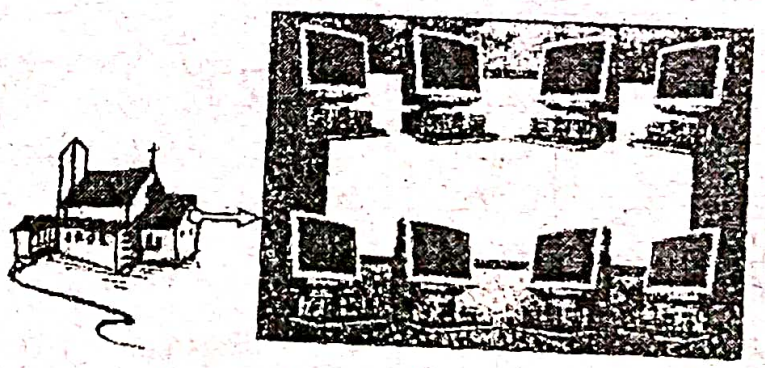


Fig.(a) : Local area network

LAN standards : The Institution of Electrical and Electronics Engineers (IEEE) has developed the layered architecture and other standards of LAN; under their project 802 set up in 1980. The IEEE 802 standards are as follows :

802.1	Architecture, Management and Internetworking
802.2	Logical Link Control (LLC)
802.3	Carrier Sense Multiple Access/Collision Detect (CSMA/CD)
802.4	Token Bus
802.5	Token Ring
802.6	Metropolitan Area Networks (MANs)
802.7	Bandpass Technical Advisory Group
802.8	Fibre Optic Technical Advisory Group
802.9	Integrated Data and Voice Network
802.10	Security Working Group
802.11	Wireless LAN working Group
802.12	Demand Priority Working Group
802.13	Not used
802.14	Cable Modem Working Group
802.15	Wireless Personal Area Networking Group
802.16	Broadband Wireless Access Study Group.

In LAN's all the stations share the common cable (*i.e.*, media). Therefore, IEEE adopted three mechanisms of media access control, namely :

(i) Carrier sense multiple access/collision detection (CSMA/CD)

(ii) Token bus and

(iii) Token ring.

Thus, there are three protocols for the MAC sublayer. The IEEE standards 802.3 (CSMA/CD), 802.4 (Token bus), 802.5 (Token ring) are associated with these protocols as shown in fig.. The physical layer protocols do the job of signal encoding, data rate control and interfacing to the transmission medium. The Logical link control layer (LLC) specifications are given in IEEE 802.2.

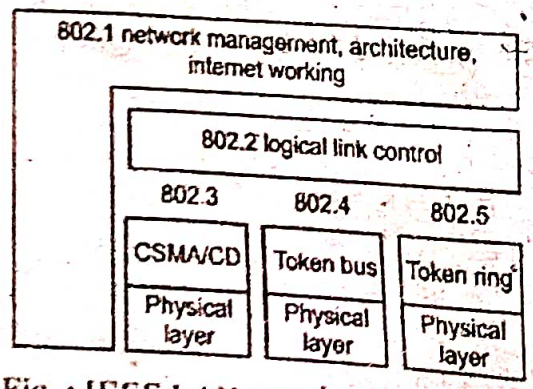


Fig. : IEEE LAN and related standards

Q.6.(ii) What do you understand by channel Access Methods ? Explain. (10)

Ans. Channel access method (CAM) is used in telecommunications and computer networks to allow network terminals to share media capacity through a multipoint transmission medium. CAM examples include bus, hub, wireless and ring networks.

A channel access scheme is based on a multiplexing method, which allows several data streams or signals to share the same communication channel or physical medium. Furthermore,

it is also based on a multiple access protocol and control mechanism known as media access control (MAC).

Channel access method is also know as multiple access method.

CAM is based on the following protocol features :

(i) Physical layer multiplexing

(ii) The media access control layer, which handles addressing and collision prevention

(iii) Token passing

(iv) Polling, a continuous slave/master data querying process

(v) Contention or node network access competition

Channel access schemes generally fall into the following categories.

Frequency-division multiple access (FDMA) : The frequency-division multiple access (FDMA) channel-access scheme is based on the frequency-division multiplexing (FDM) scheme, which provides different frequency bands to different data streams. In the FDMA case, the frequency bands are allocated to different nodes or devices. An example of FDMA systems were the first-generation 1G cell-phone systems, where each phone call was assigned to a specific uplink frequency channel, and another downlink frequency channel. Each message signal (each phone call) is modulatedon a specific carrier frequency.

A related technique is wavelength division multiple access (WDMA), based on wavelength-division multiplexing (WDM), where different data streams get different colors in fiber-optical communications. In the WDMA case, different network nodes in a bus or hub network get a different color.[4]

An advanced form of FDMA is the orthogonal frequency-division multiple access (OFDMA) scheme, for example used in 4G cellular communication systems. In OFDMA, each node may use several sub-carriers, making it possible to provide different quality of service (different data rates) to different users. The assignment of sub-carriers to users may be changed dynamically, based on the current radio channel conditions and traffic load.

Time division multiple access (TDMA) : The time-division multiple access (TDMA) channel access scheme is based on the time-division multiplexing (TDM) scheme. TDMA provides different time slots to different transmitters in a cyclically repetitive frame structure. For example, node 1 may use time slot 1, node 2 time slot 2, etc. until the last transmitter when it starts over. An advanced form is dynamic TDMA (DTDMA), where a assignment of transmitters to time slots vary one each frame.

As an example, 2G cellular systems are based on a combination of TDMA and FDMA. Each frequency channel is divided into eight time slots, of which seven are used for seven phone calls, and one for signalling data.

Statistical time division multiplexing multiple access is typically also based on time-domain multiplexing, but not in a cyclically repetitive frame structure. Due to its random character, it can be categorised as statistical multiplexing methods and capable of dynamic bandwidth allocation. This requires a media access control (MAC) protocol, i.e. a principle for the nodes to take turns on the channel and to avoid collisions. Common examples are CSMA/CD, used in Ethernet bus networks and hub networks, and CSMA/CA, used in wireless networks such as IEEE 802.11.

Code division multiple access (CDMA)/Spread spectrum multiple access (SSMA) : The code division multiple access (CDMA) scheme is based on spread spectrum,

meaning that a wider radio channel bandwidth is used than the data rate of individual bit streams requires, and several message signals are transferred simultaneously over the same carrier frequency, utilizing different spreading codes. Per the Shannon–Hartley theorem, the wide bandwidth makes it possible to send with a signal-to-noise ratio of much less than 1 (less than 0 dB), meaning that the transmission power can be reduced to a level below the level of the noise and co-channel interference from other message signals sharing the same frequency range.

One form is direct sequence spread spectrum (DS-CDMA), used for example in 3G cell phone systems. Each information bit (or each symbol) is represented by a long code sequence of several pulses, called chips. The sequence is the spreading code, and each message signal (for example each phone call) uses a different spreading code.

Another form is frequency-hopping (FH-CDMA), where the channel frequency is changed rapidly according to a sequence that constitutes the spreading code. As an example, the Bluetooth communication system is based on a combination of frequency-hopping and either CSMA/CA statistical time division multiplexing communication (for data communication applications) or TDMA (for audio transmission). All nodes belonging to the same user (to the same virtual private area network or piconet) use the same frequency hopping sequence synchronously, meaning that they send on the same frequency channel, but CDMA/CA or TDMA is used to avoid collisions within the VPAN. Frequency-hopping is used by Bluetooth to reduce the cross-talk and collision probability between nodes in different VPANs.

Space division multiple access (SDMA) : Space-division multiple access (SDMA) transmits different information in different physical areas. Examples include simple cellular radio systems and more advanced cellular systems which use directional antennas and power modulation to refine spatial transmission patterns.

Q.7. Describe the following :

(i) Congestion Control (10)

(ii) WAN Technologies (10)

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

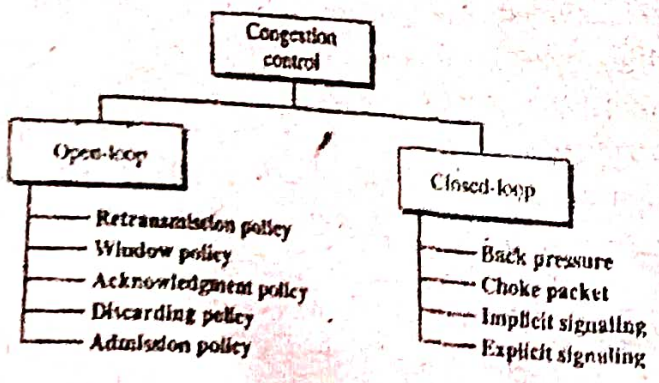


Fig (a) : Congestion control categories

Open-Loop Congestion Control: In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination. Following are the policies that can prevent congestion :

(i) *Retransmission Policy :* Retransmission is sometimes unavoidable . If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion.

(ii) *Window Policy :* The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control. In the Go-Back-N window, when the timer for a packet times out, several packets may be resent, although some may have arrived safe and sound at the receiver. This duplication may make the congestion worse. The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted.

(iii) *Acknowledgment policy :* The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.

(iv) *Discarding policy :* A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission. For example, in audio transmission, if the policy is to discard less sensitive packets when congestion is likely to happen, the quality of sound is still preserved and congestion is prevented or alleviated.

(v) *Admission policy :* An admission policy, which is a quality-of-service machanism, can also prevent congestion in virtual-circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny estgablishing a virtual-circuit connection if there is congestion in the network or if there is a possibility of future congestion.

Closed-Loop Congestion Control : Closed-loop congestion control mechanisms try to alleviate congestion after it happens. Several mechanisms have been used by different protocols. We describe a few of them here.

(i) *Backpressure :* Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source. The backpressure technique can be applied only to virtual-circuit networks, in which each node knows the upstream node from which a flow of data is coming. Fig.(b) shows the idea of backpressure.

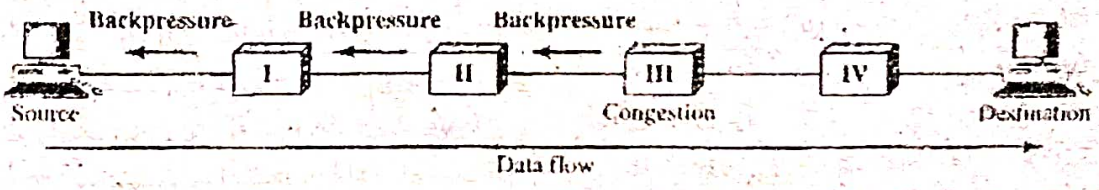


Fig (b) : Backpressure method for alleviating congestion

(ii)*Choke packet :* A choke packet is packet sent by a node to the souce to inform it of congestion. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes through which the packet has traveled are not warned.

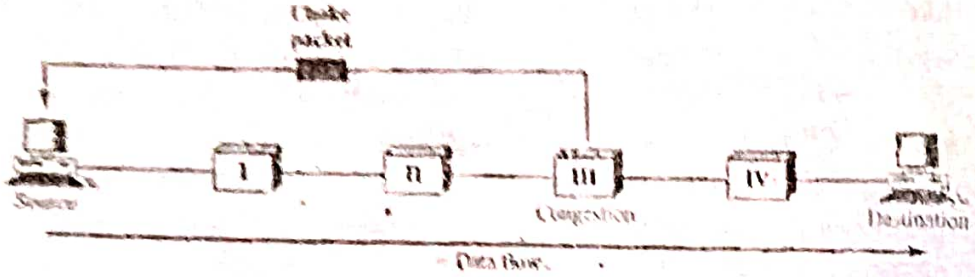


Fig (e) : Choke packet

(iii) *Implicit Signaling* : In implicit singnaline there is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network from other symptoms. For example, when source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested. The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down.

(iv) *Explicit Signaling* : The node that experiences congestion can explicitly send a signal to the source or destination. In the explicit signaling method, the signal is included in the packets that carry data. Explicit signaling, can occur in either the forward or the backward direction.

(v) *Backward Signaling* :A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.

(vi) *Forward Signaling* : A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the congestion.

Ans.(ii)WAN Technologies : A wide area network, or WAN spans a large geographical area, often as country or continent. It contains a collection of machines intended for running user (i.e., application) programs. We will follow traditional usage and call these machines hosts. The hosts are connected by a communication subnet, or just subnet for short. The hosts are owned by the customers (e.g. people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider. The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener. Separation of the pure communication aspects of the network (the subnet) from the application aspects (the hosts), greatly simplifies the complete network design.

In most wide area networks, the subnet consists of two district component ; transmission lines and switching elements. Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links. Switching elements are specialized computer that connect three or more transmission line. When data arrive on an incoming line, These switching element must choose an outgoing line on which to forward them. These swtiching element must choose an outgoing line on which to forward them. These switching computers have been called by various names in the past; the same router is now most commoly used. Unfortunately, some people pronounce it "router" and others have it rhyme with "douber". Determining the correct pronounciation will be left as an exercise for the reader. (Note : the perceived correct answer may depend on where you live).

In this model shown in Fig.(1) each host is frequently connected to a LAN on which a router is present, although in some cases a host can be connected directly to a router. The collection of communication lines and routers (but not the hosts) from the subnet.

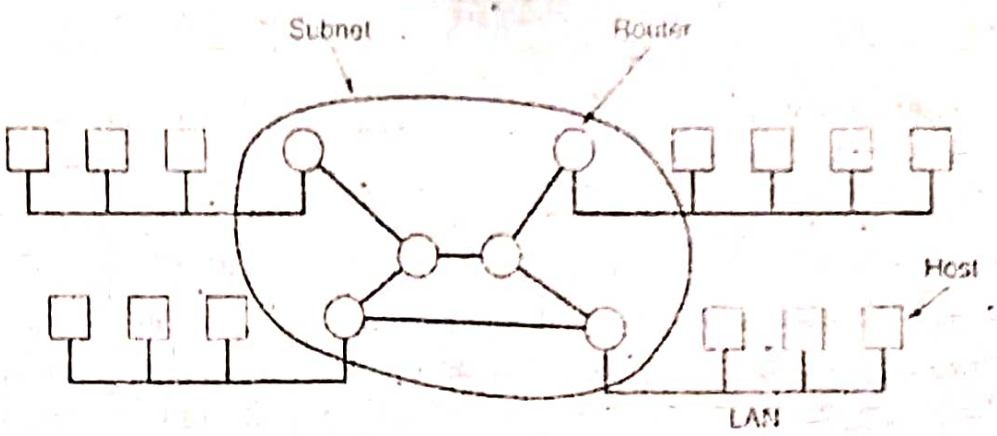


Fig.(1) : Relation betwen hosts on LANs and the subnet

A short comment about the term "subnet" is in order here. Originally, Its only meaning was the collection of routers and communication lines that moved packets from the source host to the destination host. However some years later, it also acquired a second meaning in conjuction with network addressing. Unfortunately, no widely used alternative exists for its initial meaning, so with some hesitation we will use it in both senses. From the context, it will always be clear which is meant.

In most WANs the network contains numerous transmission lines, each one connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers. When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirely, stored there until the required output line is free, and then forwarded. A subset organied according to this principle is called a store and forward or packet switched subnet. Nearly all wide area networks (excets those being satellites) haves store and forward subnets. When the packets are small and all same size, they are often called cells.

The principle of a packet switched WAN is so important that it is worth devoting a few more words to it. Generally, when a process on some host has a message to be sent to a process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence. These packets are then injected into the network one at a time in quick succession. The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process. A stream of packets resulting from some initial message is illustrated in Fig.(2).

In this figure, all the packet follows the route *ACE*, rather than *ABDE* or *ACDE*. In some networks all packets from a given message must follow the same route; in others each packets is routed separately. Of course, if *ACE* is the best route, all packet may be sent along it, even if each packet is individually routed.

Rounting decisions are made locally. When a packet arrives at router *A*, it is up to A to decide if this packet should be sent on the line to *B* or the line to *C*. How *A* makes that decision is called the routing algorithm. Many of them exist.

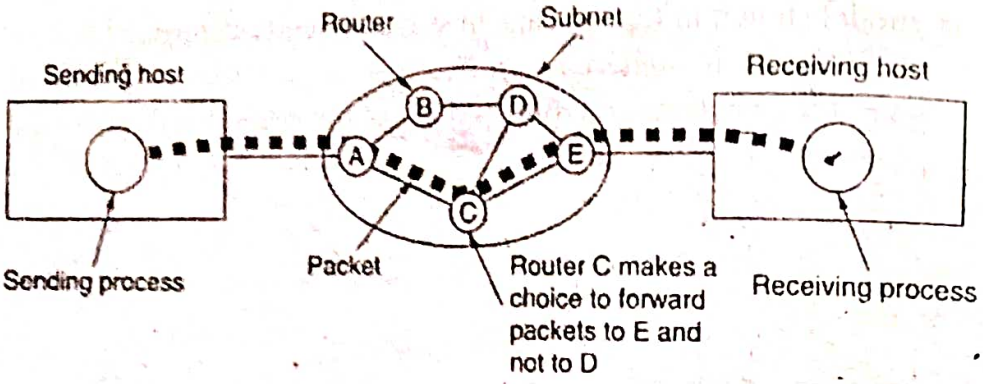


Fig.(1) : A stream of packets from sender to receiver.

Not all WANs are packet switched. A second possibility for WAN is a satellite system. Each router has an antenna through which it can send and receive. All routers can hear the output from the satellite, and in some cases they can also hear the upward transmissions of their fellow routers to the satellite as well. Sometime of outers connected to a substantial point to point subnet, with only some of them having a satellite antenna. Satellite neworks are inherently broadcast and are most useful when the broadcast property is important.

Section – IV

Q.8. Explain the following :

(i) ATM (20)

(ii) Performance Management

Ans. (i) ATM : The ATM stands for asynchronous transfer mode. It is a streamlined packet transfer interface. ATM also is a connection oriented network. ATM uses packets of fixed size for the communication of data. These packets are called as ATM cells. ATM is used for efficient data transfer over high speed data networks. ATM provides real time and non-real time services.

The service provided are

(i) Synchronous TDM streams such as T-1.

(ii) Services using the constant bit rates.

(iii) Compressed voice and video

(iv) Traffic with specific quality requirement using the non real time variable bit rate.

(v) IP-based services using available bit rate(ABR) and unspecified bit rate (BR) services.

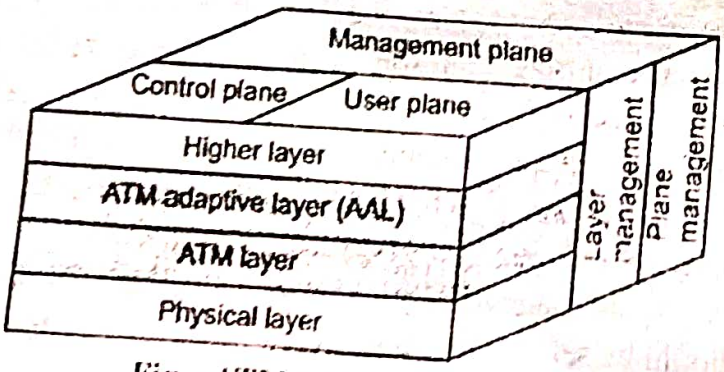


Fig. : ATM protocol architecture

ATM Protocol Architecture : Fig. shows the ATM protocol architecture. ATM is a streamlined protocol. It has minimal error and flow control capabilities. Hence, the number of overhead bits required with each cell is reduced which enables ATM to operate at high data rates. Also, due to the ATM cells of fixed size, the processing required at each node is simplified. This also supports the use of ATM at high data rates. Fig. shows the ATM protocol architecture for an interface between user and network. The standards issued for ATM by ITU-T are based on this protocol architecture.

Physical Layer : The physical layer of the protocol involves the specifications of a transmission medium and signal encoding scheme. The data rates specified at this layer are between 25.6 Mbps and 622.08 Mbps, but data rates higher and lower than these are possible.

The two shaded layers in fig. correspond to the **ATM functions.** The two layers are :

– *ATM Layer* : This layer is common to all the services that provide the packet transfer capabilities. This layer defines the transmission of data in fixed size cells and it also defines the use of logical connections.

– *ATM Adaption Layer* (*AAL*) : This layer is a service dependent layer. It is used for supporting the information transfer protocol not based on ATM.

The AAL maps the higher layer information into the ATM cells and cell is transported over the ATM network.

The ATM protocol architecture of fig. consists of three separate planes :

– *User Plane* : It is used for transferring user information alongwith associated controls such as flow control, error control etc.

– *Control Plane* : It is supposed to perform the call control and connection control functions.

– *Management Plane* : It includes the plane management. The management plane performs management functions related to a system.

Ans.(ii)Performance Management : Performance management is closely related to fault management, It tries to monitor and control the network to ensure that it is running as efficiently as possible. Performance management tries to quantify performance by using some measurable quantity such as capacity, traffic, throughput or response time.

(*i*) *Capacity* : One factor that must be monitored by a performance management system is the capacity of the network. Every network has limited capacity, and the performance management system must ensure that it is not used above this capacity. For example, if a LAN is designed for 100 stations at an average data rate 2 Mbps, it will not operate properly if 200 stations are connected to the network. The data rate will decrease and blocking may occur.

(*ii*) *Traffic* : Traffic can be measured in two ways : *internally* and *externally*. *Internal traffic* is measured by the number of packets (or bytes) traveling inside the network. *External traffic* is measured by the exchange of packets (or bytes) outside the network. During peak hours, when the system is heavily used, blocking may occur if there is excessive traffic.

(*iii*) *Throughput* : We can measure the throughput of an individual device (such as a router) or a part of the network. Performance management monitors the throughput to make sure that it is not reduced to unacceptable levels.

(*iv*) *Response Time* : Response time is normally measured from the time a user requests a service to the time the service is granted. Other factors such as capacity and traffic can affect

the response time. Performance management monitors the average response time and the peak-hour response time. Any increase in response time is a very serious condition as it is an indication that the network is working above its capacity.

Q.9. Describe the following : (20)

(i) Security Management

(ii) Class of Service

(iii) Quality of Service

(iv) Windows NT/2000

Ans. (i) Security Management : Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

Homes & Small Businesses :

– A basic firewall or a unified threat management system.

– For Windows users, basic Antivirus software. An anti-spyware program would also be a good idea. There are many other types of antivirus or anti-spyware programs out there to be considered.

– When using a wireless connection, use a robust password. Also try to use the strongest security supported by your wireless devices, such as WPA2 with AES encryption.

– If using Wireless: Change the default SSID network name, also disable SSID Broadcast; as this function is unnecessary for home use. (However, many security experts consider this to be relatively useless).

– Enable MAC Address filtering to keep track of all home network MAC devices connecting to your router.

– Assign STATIC IP addresses to network devices.

– Disable ICMP ping on router.

Medium businesses :

– A fairly strong firewall or Unified Threat Management System

– Strong Antivirus software and Internet Security Software.

– For authentication, use strong passwords and change it on a bi-weekly/monthly basis.

– When using a wireless connection, use a robust password.

– Raise awareness about physical security to employees.

Large businesses :

– A strong firewall and proxy to keep unwanted people out.

– A strong Antivirus software package and Internet Security Software package.

– For authentication, use strong passwords and change it on a weekly/bi-weekly basis.

– When using a wireless connection, use a robust password.

– Exercise physical security precautions to employees.

– Prepare a network analyzer or network monitor and use it when needed.

– Implement physical security management like closed circuit television for entry areas and restricted zones.

School :

– An adjustable firewall and proxy to allow authorized users access from the outside and inside.

– Strong Antivirus software and Internet Security Software packages.

– Wireless connections that lead to firewalls.

– Children's Internet Protection Act compliance. (Only schools in the USA)

– Supervision of network to guarantee updates and changes based on popular site usage.

Large government :

– A strong firewall and proxy to keep unwanted people out.

– Strong antivirus software and Internet Security Software suites.

– Strong encryption.

– Whitelist authorized wireless connection, block all else.

– All network hardware is in secure zones.

Ans.(ii) Class of Service : The ATM forum defines four service classes : CBR, VBR, ABR and UBR. VBR is divided into two subclasses VBT-RT and VBT-NRT (see fig.(a)).

(*a*) *CBR* : The *constant bit rate* (CBR) class is designed for customers that need realtime audio or video services. The service is similar to that provided by a dedicated line such as a T-line.

(*b*) *VBR* : The *variable bit rate* (VBR) class is divided into two subclasses : *real time* (VBR-RT) and *nonreal time* (VBR-NRT). VBR-RT is designed for those users that need real-time services (such as voice and video transmission) and use compression techniques to create a variable bit rate. VBR-NRT is designed for those users that do not need real-time services but use compression techniques to create a variable bit rate.

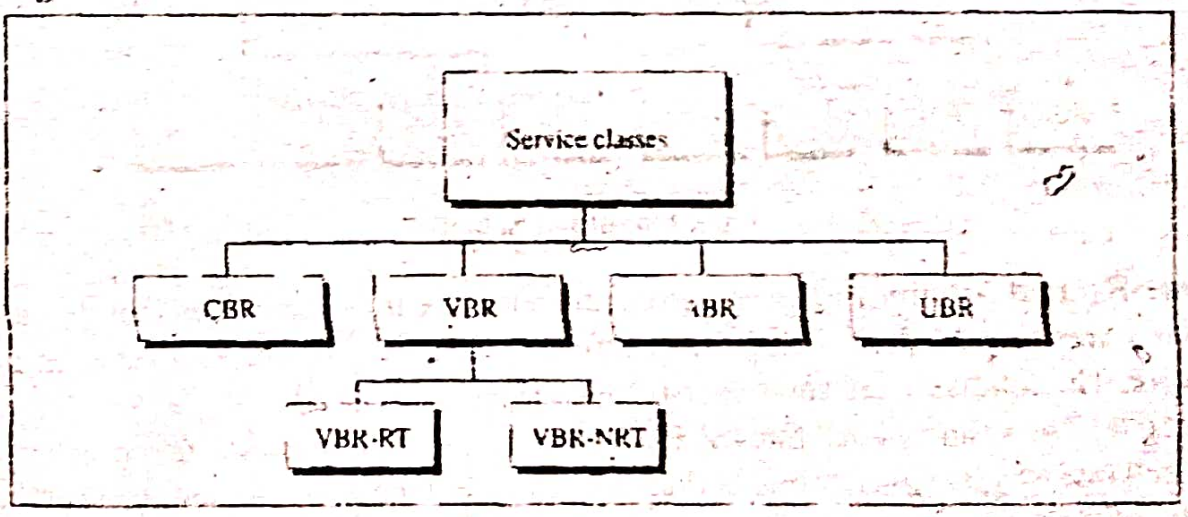


Fig.(a) : Service classes

(*c*) *ABR* : The *available bit rate* (ABR) class delivers cells at a minimum rate. If more network capacity is available, this minimum rate can be exceeded. ABR is particularly suitable for applications that are bursty in nature.

(*d*) *UBR* : The *unspecified bit rate* (UBR) class is a best-effort delivery service that does not guarantee anyuthing.

Fig.(b) shows the relationship of different classes to the total capacity of the network.

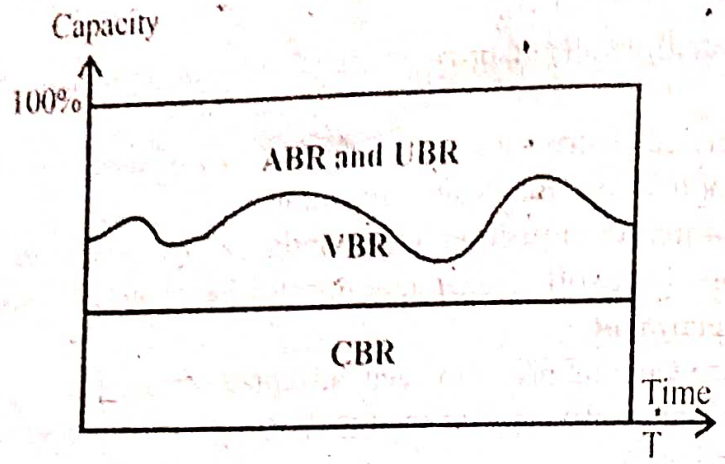


Fig.(b) : Relationship of service classes to the total capacity of the network

Ans.(iii) Quality of service: The quality of service (QoS) defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute. Each service class is associated with a set of the attributes. We can categorize the attributes into those related to the user and those related to the network. Fig. shows the two categories and some important attributes in each category.

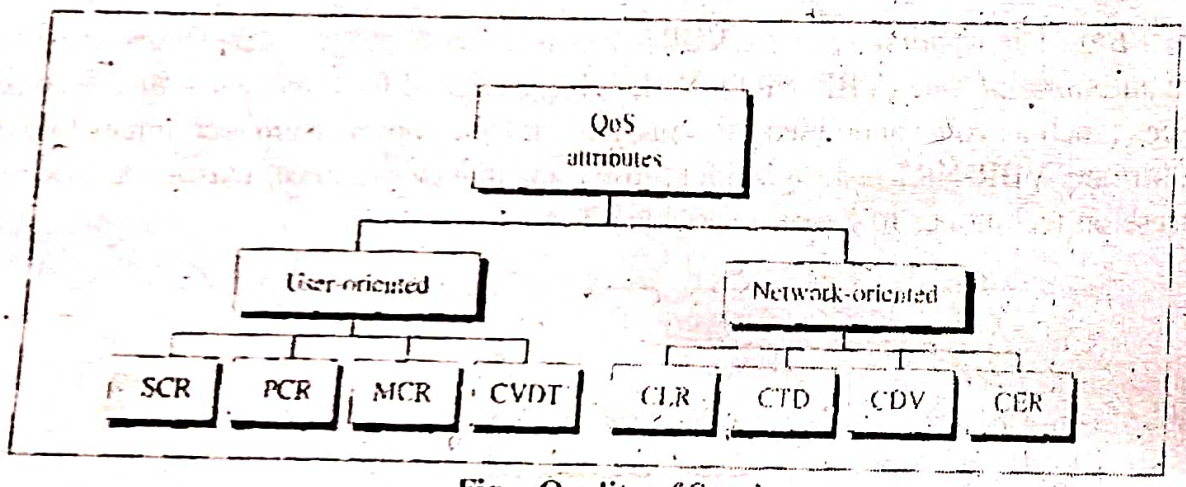


Fig. : Quality of Service

User-Related Attributes : *User-related attributes are those attributes that define how fast the user wants to send data. These are negotiated at the time of contract between a user and a network. The following are some user-related attributes :*

(i) SCR : The sustained cell rate (SCR) is the average cell rate over a long time interval. The actual cell rate may be lower or higher than this value, but the average should be equal to or less than the SCR.

(ii) PCR : The peak cell rate (PCR) defines the sender's maximum cell rate. The user's cell rate can sometimes reach this peak, as long as the SCR is maintained.

(iii) MCR : The minimum cell rate (MCR) defines the minimum cell rate acceptable to the sender. For example, if the MCR is 50,000, the network must guarantee that the sender can send at least 50,000 cells per second.

(iv) CVDT : The cell variation delay tolerance (CVDT) is a measure of the variation in cell transmission times. For example, if the CVDT is 5 ns, this means that the difference

between the minimum and the maximum delays in delivering the cells should not exceed 5 ns.

Network-Related Attributes : The network -related attributes are those that define characteristics of the network. The following are some network-related attributes :

(i) *CLR* : The cell loss ratio (CLR) defines the fraction of cells lost (or delivered so late that they are considered lost) during transmission. For example, if the sender sends 100 cells and one of them is lost, the CLR is

$$CLR = 1/100 = 10^{-2}$$

(ii) *CTD* : The cell transfer delay (CTD) is the average time needed for a cell to travel from source to destination. The maximum CTD and the minimum CTD are also considered attributes.

(iii) *CDV* : The cell delay variation (CDV) is the difference between the CTD maximum and the CTD minimum.

(iv) *CER* : The cell error ratio (CER) defines the fraction of the cells delivered in error.

Ans.(iv) Windows NT : Windows NT is a family of operating systems produced by Microsoft, the first version of which was released in July 1993. It is a processor-independent, multiprocessing, multi-user operating system.

The first version of Windows NT was Windows NT 3.1 and was produced for workstations and server computers. It was intended to complement consumer versions of Windows (including Windows 1.0 through Windows 3.1x) that were based on MS-DOS. Gradually, Windows NT family was expanded into Microsoft's general-purpose operating system family for all personal computers, deprecating Windows 9x family. NT was formerly expanded to "New Technology" but no longer carries any specific meaning. Starting with Windows 2000, "NT" was removed from the product name and is only included in the product version string.

NT was the first purely 32-bit version of Windows, whereas its consumer-oriented counterparts, Windows 3.1x and Windows 9x, were 16-bit/32-bit hybrids. It is a multi-architecture operating system: Initially, it supported several CPU architectures, including IA-32, MIPS, DEC Alpha and PowerPC. The latest versions support, x86 (more specifically IA-32 and x64), and ARM. Major features of Windows NT family include Windows Shell, Windows API, Native API, Active Directory, Group Policy, Hardware Abstraction Layer, NTFS file system, BitLocker, Windows Store, Windows Update, and Hyper-V.

Windows 2000 : Windows 2000 is an operating system for use on both client and server computers. It was produced by Microsoft and released to manufacturing on December 15, 1999 and launched to retail on February 17, 2000. It is the successor to Windows NT 4.0, and is the last version of Microsoft Windows to display the "Windows NT" designation. It is succeeded by Windows XP (released in October 2001) and Windows Server 2003 (released in April 2003). During development, Windows 2000 was known as Windows NT 5.0.

Four editions of Windows 2000 were released: Professional, Server, Advanced Server, and Datacenter Server; the latter was both released to manufacturing and launched months after the other editions. While each edition of Windows 2000 was targeted at a different market, they shared a core set of features, including many system utilities such as the Microsoft Management Console and standard system administration applications.

Support for people with disabilities was improved over Windows NT 4.0 with a number of new

assistive technologies, and Microsoft increased support for different languages and locale information.

All versions of the operating system support NTFS 3.0, Encrypting File System, as well as basic and dynamic disk storage. The Windows 2000 Server family has additional features, including the ability to provide Active Directory services (a hierarchical framework of resources), Distributed File System (a file system that supports sharing of files) and fault-redundant storage volumes. Windows 2000 can be installed through either a manual or unattended installation. Unattended installations rely on the use of answer files to fill in installation information, and can be performed through a bootable CD using Microsoft Systems Management Server, by the System Preparation Tool.

COMPUTER NETWORK

May - 2019

Paper Code:-IT-305-F

Note : ***Attempt five questions in all, selecting one question from each Section. Question No. 1 is compulsory. All questions carry equal marks.***

Q.1. Write a short note on the following :

(a) Computer Network

(b) Transmission control protocol

(c) Overview of IP V6

(d) Fast Ethernet & Gigabit Ethernet

Ans.(a)Computer Network : Computer network is a system which allows communication amoung the computers connected in the network. A network must be able to meet certain criteria. The most important of them are:

1. Performance
2. Relaibility
3. Security

1. *Performacnce* : Performance can be measured in many ways. We can measure it in terms of transit time and respnse time.

(a) Transit time is defined as the amount of time required for a message to travel from one device to the other.

(b) Response time: It is the time elapsed between enquiry and response.

The other factors deciding the performance are as follows:

(i) Number of users

(ii) Type of transmission medium

(iii) Capability of connected hardware

(iv) Efficiency of software.

2. *Reliability* : The network reliability is importnat because it decides the frequency at which network failure takes place. It also decides the time taken by the network to recover and its robustness in the catastrophe.

3. *Security* : The network secutiry refers to protection of data from the unauthorized user or access.

Ans.(b)Transmission control protocol : Fig.(1). shows the layout of a TCP segement. Every segment begins with a 20 byte fixed formed header. The fixed header may be followed by header options. After the options, if any upto 65535 – 20 – 20 = 65495 data bytes may follow.

Note that the first bytes correspond to the IP header and the next 20 correspond to the tCP header. The TCP segment without data are used for sending the acknowledgments and control messages.

Source Port : A 16 bit number identifying the application the TCP segement originated from within the sending host. The port numbers are divided into three ranges, well known ports (0 through 1023) registered ports (1024 through 49151) and private ports (49152 through 65535) Port assigments are used by TCP as an interface to the application layer.

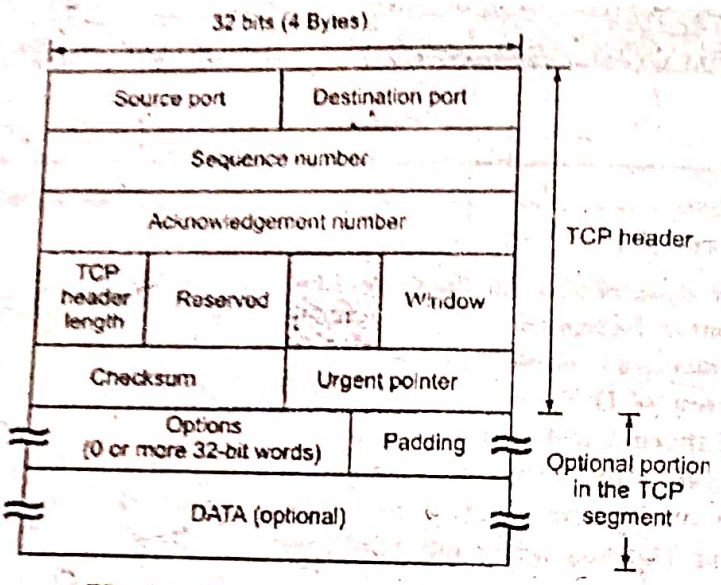


Fig.(1) : Illustration of TCP header format

Destination port : A 16 bit number identifying the application th TCP segement is destined for on a receiving host Destination port use the same port number assignment as those set aside for source ports.

Sequence number : A 32 bit number identifying the current position of the first data byte in the segment within entire byte stream for the TCP connection. After reaching $2^{32}-1$, this number will warp around to 0.

Acknowledgments number : A 32 bit number identifying the next data byte the sender expects from the receiver. Therefore, the number will be one greater than the most recently received data type. This field is only used when the ACK control bit is turned on.

Header length or offset : A 4-bit field that specifies the total TCP header length in 32 bits words (or in multiplies of 4 bytes if you prefer). Without options, a TCP header a always 20 bytes in length. The largest, a TCP header, may be of 60 bytes. This field is required becuase the size of the options field (s) cannot be determined in advance. Note that this field is called "Data Offset" in the official TCP standard, but header length is more commonly used.

Reserved : A 6 bit field currently unused and reserved for future are.

Ans.(c) Overview of IP V6 : *IPv6 is the next generation Internet Protocol designed as a successor to the IP version 4. IPv6 was designed to enable high-performance, scalable Internet. This was achieved by overcoming many of the weaknesses of IPv4 protocol and by adding several new features.*

Frame structure of IPv6 : The IPv6 packet is shown in fig. Each packet consists of a base header which is mandatory followed by the payload. The pay load is made up of two parts.

(i) Optional extension headers and

(ii) Data from an upper layer.

The base header is 40 byte length whereas the extension header and the data from upper layer contain upto 65, 535 bytes of information.

Fig. shows the base header. It has eight fields. These fields are as follows.

(i) *Version (VER) :* It is a 4 bit field which defines the version of IP such as IPv4 or IPv6. For IPv6 the value of this field is 6.

(ii) *Priority :* It is a 4 bit field which defines the priority of the packet which is important in connection with the traffic congestion.

(iii) *Flow label :* It is a 24 bit (3 byte) field which is designed for providing special handling for a particular flow of data.

(iv) *Payload length :* This is a 2 byte length field which is used to define the total length of the IP datagram excluding the base header.

(v) *Next header :* It is an 8 bit field which defines the header which follows the base header in the datagram.

(vi) *Hop limit :* This is an 8 bit field which has the same purpose as TTL, (time to live) in IPv4.

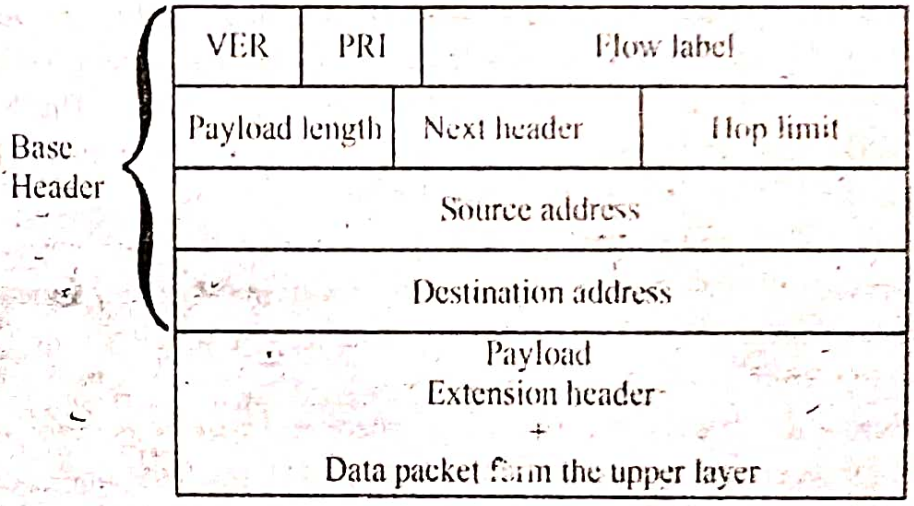


Fig. : Frame structure of Ipv6

(vii) *Source address :* It is a 16 byte (128 bit) Internet address which identifies the original source of datagram.

(viii) *Destination address :* This is a 16 byte (128 bit) internet address which identifies the final destination of datagram. But this field will contain the address of the next router if source routing is being used.

Ans.(d)Fast Ethernet : The IEEE 802.3 commitee developed a set of specifications referred to as the fast Ethernet to provide low-cost data transfer at the rate of 100 Mbps. It was designed to compete with LAN protocols such as fibre distributed data interface(FDDI) and it was also compatible with the standard Ethernet. The fast Ethernet uses a new feature called autonegotiation, which enables two devices to negotiate on certain features such as data rate or mode of transmission. It also allows a station to determine the capability of hub and two incomptible devices can also be connected to one another using this feature. Like the standard Ethernet, various physical-layer implementations of the fast Ethernet have also been specified. Some of them are as follows:

- *100Base-TX :* It either uses two pairs of either cat5 UTP cable or STP cable. The maximum length of the cable should not exceed 100m. This implementation uses MLT-3 line coding scheme due to its high bandwidth. However, since MLT-3 coding scheme is not self-

synchronized, the 4B/5B block coding scheme is used to pervent long sequences of 0s and 1s. The block coding increases the data rate from 100Mbps to 125 Mbps.

– *100 Base-FX :* It uses two wires of fibre optic cable that can easily satisfy the high bandwidth requirements. The implementation uses NRZ-I coding scheme. As NRZ-I scheme suffers from synchronization problem in case of long sequence of 0s and 1s, 4B/5B block coding is used with NRZ-I to overcome this problem. The block coding results in increased data rate of 125 Mbps. The maximum cable length in 100 Base-FX must not exceed 100 m.

– *100 Base-T4 :* It is the new standard that uses four pairs of cat3 or higher UTP cables. For this implementation, 8B/6T line coding scheme is used. The maximum length of cable must not exceed 100 m.

Gigabit Ethernet : Gigabit Ethernet was developed by the IEEE 802.3 committee to meet the higher data rate requirements. This standard provides a data rate of 1000 Mbps(1 Gbps). It is backward compatible with traditional and fast Ethernet and also supports autonegotiation feature. Various physical layer implementation of gigabit Ethernet are as follows:

– *1000 Base-SX :* It is a two-wire implementation that use short wave fibres. One wire is used for sending the data and other is used for receiving the data. The NRZ line coding scheme and 8B/10B block coding scheme is used for this implementation. The length of the cable should not exceed 550 m in the 1000 Base-SX specifications.

– *1000 Base-LX :* It is also a two-wire implementation that use long wave fibres. One wire is used for sending the data and other is used for receiving. It is implemented by the NRZ line coding scheme and the 8B/10B block coding scheme. The length of the cable should not exceed 5000 m in the 1000 Base-LX specifications.

– *1000 Base-CX :* It uses two STP wires where one wire is used for sending the data and other is used for receiving the data. It is implemented by the NRZ line coding scheme and 8B/10B bolck-coding scheme. The length of the cable should not exceed 25 m in the 1000 Base-CX specifications.

– *1000 Base-T :* It uses four cat5 UTP wires. It is implemented by the 4D-PAMS line coding scheme. In this specification, the length of the cable should not exceed 100 m.

Section – A

Q.2.(a) What is OSI Reference model ? Explain each layers in detail. (15)

Ans. Refer Q.2 of paper May 2017.

Q.2.(b) Explain various tpes of Networks.

Ans. Different types of Network : Different types of Network are as follows :

(i) Local Area Network : *A LAN is a computer network that covers only a small geographical area (usually within a square mile or less) such as an office, home or building (Fig.a). In a LAN, connected computers have a network operating system installed onto them. One computer is designated as the file server, which stores all the software that controls the network. It also stores the software that can be shared by the computers attached to the network. Other computers connected to the file server are called workstations. The workstations can be less powerfull than the file server and they may have additional software on their hard drive. On most LANs, cables are used to connect the computer. Generally , LAN offers a bandwidth of 10-100Mbps.*

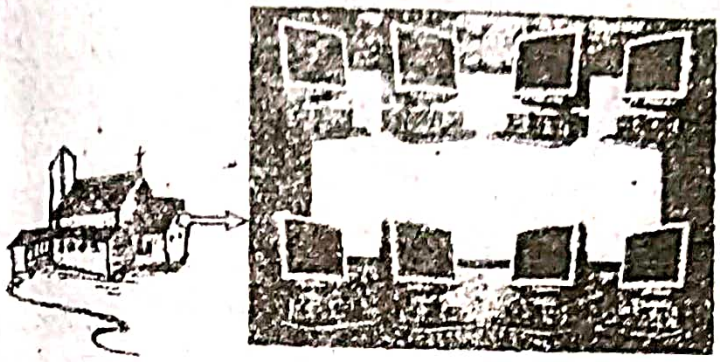


Fig.(a) : Local area network

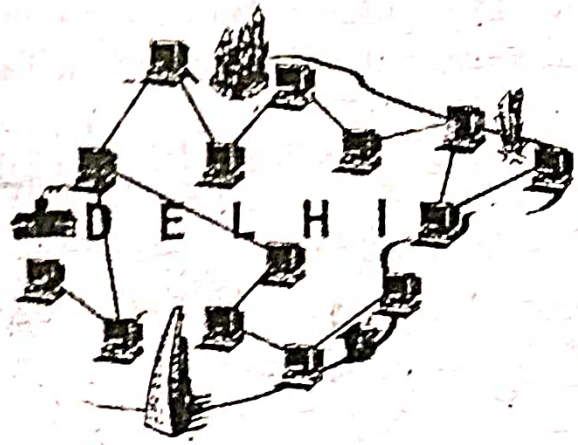


Fig.(b) : Metropoiltian area network

(ii) Metropolitan Area Network : A MAN is a network of computers spread over a "metropolitan" area such as city and its suburbs (fig.b). As the name suggests, this sort of network is usually reserved for metropolitan areas where the city bridges its LANs with a series of backbones, making one large network for the entire city. It may be a single network such as a cable television network or it may be a means of connecting as number of LANs. Note that MAN may be operated by one organization (a corporate with several offices in one city) or be shared and used by serval organization in the same city.

(iii) WAN : It stands for wide area network. This is the largest network and can interconnect networks throughout the world and is not restricted to a geographical location. The Internet is an example of a worldwide public WAN. Most WANs exist to connect LANs that are not in the same geographical area. This technology is high speed and very expensive to setup. It is shown in fig.(c).

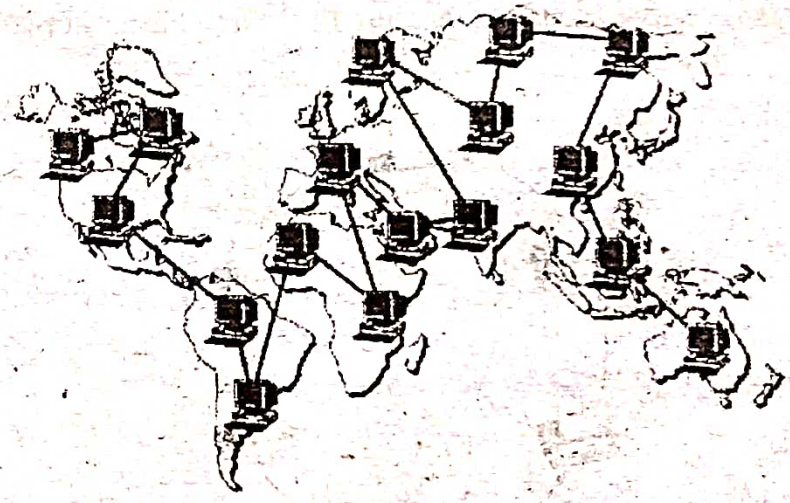


Fig.(c) : Wide area network

Q.3. Write a short note on : **(20)**

(a) Bus & Ring Topology

(b) ARPANET

(c) Private Network

Ans.(a) Bus Topology : The bus topology is usually used when a network installation is small, simple or temporary as shown in fig.(b).

When one computer sends a signal up to the cable, all the computers on the network

receive the information, but the one with the address that matches the one encoded in the message accepts the information while all the others reject the message.

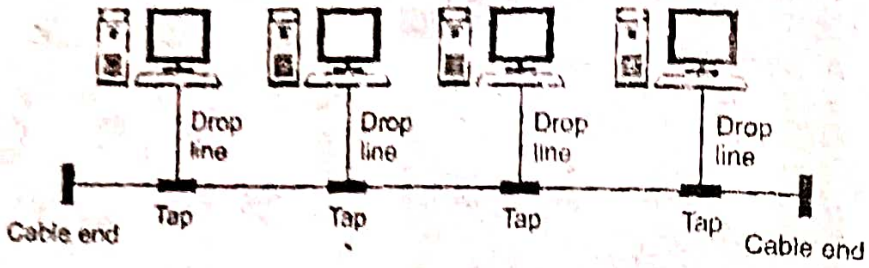


Fig.(b) : Bus topology

2. Ring Topology : In a ring topology, each computer is connected to the next computer, with the last one connected to the first as shown in fig.(c). Rings are used in high-performance networks where large bandwidth is necessary, e.g. time attractive features such as video and audio.

The messages flow around the ring in one direction. There is no termination because there is no end to the ring. Some ring networks do token passing. A short message called a token, is passed around the ring until a computer wishes to send information to another computer. That computer modifies the token, adds an electronic address and data and sends it around the ring. Each computer in sequence receives the token and the information and passes them to the next computer until either the electronic address matches the address of a computer or the token returns to its origin. The receiving computer returns a message to the originator indicating that the message has been received. The sending computer then creates another token and places it on the network, allowing another station to capture the token and begin transmitting. The token circulates until a station is ready to send and capture the token. Faster network circulate several tokens at once.

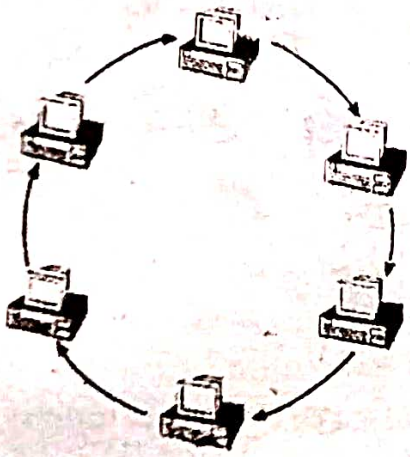


Fig.(c) : Ring topology

Ans.(b) ARPANET : *It is basically a WAN. It was developed by the ARPA (Advanced Research Project Agency). ARPANET was designed to service even a nuclear attack. ARPANET used the concept of packet switching network consisting of subnet and host computers. The subnet was a datagram subnet and each subnet consist of minicomputers called IMPs (Interface Message Processors). Each node of the network used to have an IMP and a*

host connected by a short wire. The host could send messages of upto 8063 bits to its IMP which would break them into packets and forward them independently toward the destination. The subnet was the first electronic store-and-forward type packet switched network. So each packet was stopped before it was forwarded. The original ARPANET design is as shown in fig.

The software for ARPANET was split into two parts, namely, subnet and host. The TCP/IP model and protocol were invented specifically to handle communication over internetworks because more and more networks were getting connected to ARPANET.

The TCP/IP made the connection of LANs to ARPANET easy. So, DNS (Domain Naming System) was created for organizing machines into domains and map host names onto IP address.

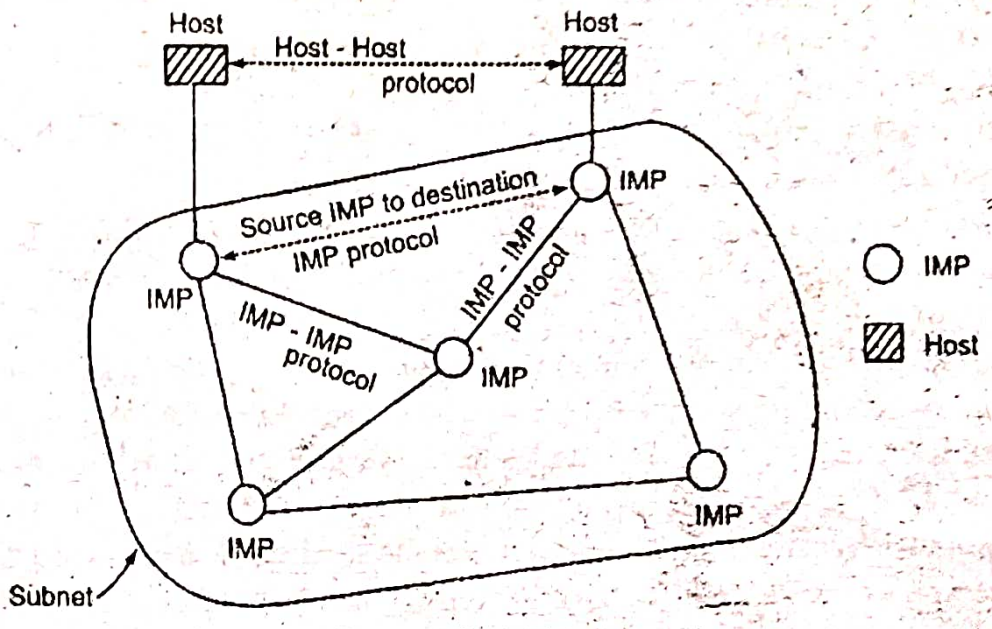
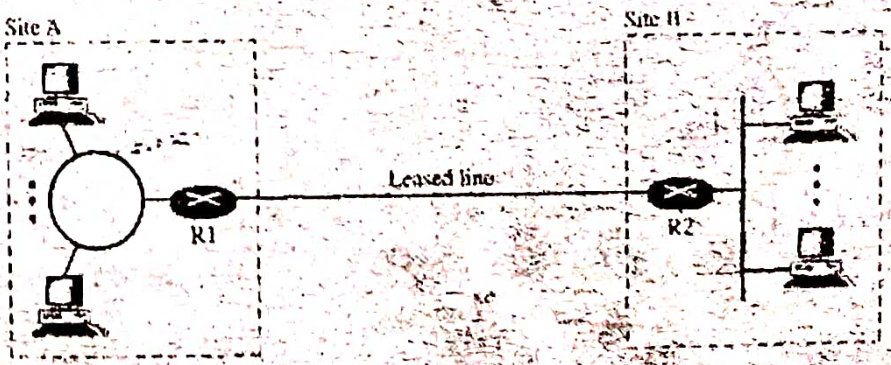


Fig. : APRANET

Ans.(c) Private Network : A private network is designed for use inside an organization. It allows access to shared resources and, at the sametime, provides privacy.

An orgnization that needs privacy when routing information inside the organization can use a private network. A small organization with one single site can use an isolated LAN. People inside the organization can send data to one another that totally remain inside the organization, secure from outsiders. A larger organization with several sites can create a private internet. The LANs at different sited can be connected to each other by using routers and leased lines. In other words, an internet can be made out of private LANs and private WANs. Fig. shows such a situation for an organization with two sites. The LANs are connected to each other by routers and one leased line.



In this situation, the organization has created a private internet that is totally isolated from the global Internet. For end-to-end communication between stations at different sites, the organization can use the Internet model. However, there is no need for the organization to apply for IP address with the Internet authorities. It can use private IP addresses. The organization can use any IP class and assign network and host addresses internally. Because the intenet is private,duplication of addresses by another organization in the global Internet is not a problem.

Section – B

Q.4.(a) Explain TCP/IP Model with its various layers in detail. (10)

Ans. Refer Q.4 of paper May 2018.

Q.4.(b) Briefly explain : (10)

(1) ARP (2) RARP (3) SMTP (4) HTTP

Ans. ARP : ARP is used for associating an IP address to its MAC address. For a LAN, each device has its own physical or station address as its identification. This address is imprinted on the NIC (Network Interface Card).

Fig. shows the ARP protocol operation. Fig.(a) shows host A broadcasts an ARP request containing I_B to all computer on the network and fig.(b) shows host B responds with an ARP reply that contains the pair (I_B, P_B). To reduce communication costs, ARP maintain a cache of recently acquired IP to physical address binding, so they do not have to use ARP repeatedly. Whenever a computer receives an ARP reply, it saves the sender's IP address and corresponding hardware address in its cache for successive lookups. When transmitting a packet, a computer always look in its cache for a binding before sending an ARP request.

If a computer finds the desired binding in its ARP cache, it need not broadcast on the network. When ARP message travel from one computer to another, they must be carried in physical frame.

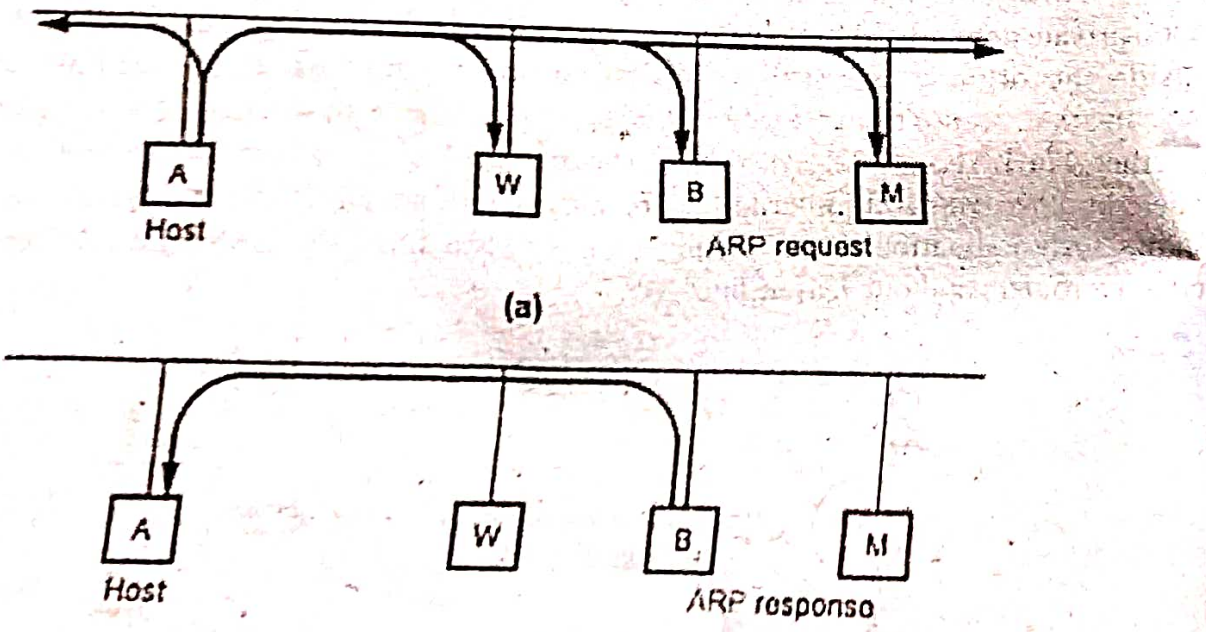


Fig. : ARP protocol operations

Reverse Address Resolution Protocol (RARP) : A diskless machine uses a TCP/IP Internet protocol called RARP to obtain its IP address from a server. RARP uses the same message format like ARP. RARP allows for multiple physical network types. A RARP message is sent from one computer to another encapsulated in the data portion of a network frame. Fig. shows the operation of RARP.

The sender broadcasts a RARP request that specifies itself as both, the sender and target machine and supplies its physical address in the target hardware address field. All the machines on the network receive the request, but only those authorized to supply the RARP service process the request and send a reply, such machines are known as RARP server. For RARP succeed, the network must contain at least one RARP server.

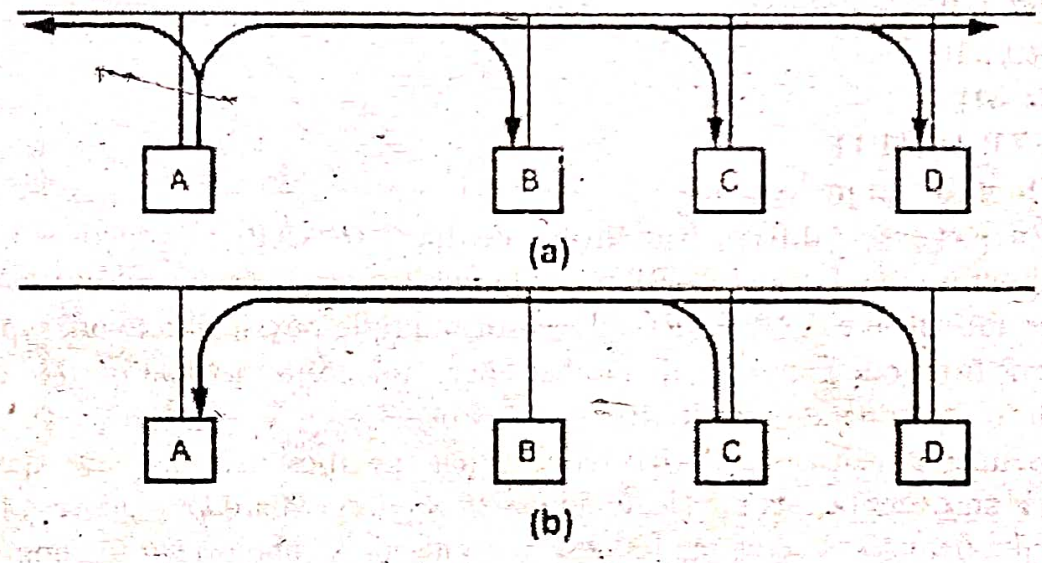


Fig. : RARP protocol

SMTP : The formal protocol that defines the MTA client and server in the Internet is called the Simple Mail Transfer Protocol (SMTP).

SMTP is used two times, between the sender and the sender's mail server and between the two mail servers. SMTP simply defines how commands and responses must be send back and fourth. Each network is free to choose a software package for implementation.

HTTP : HTTP stands for Hyper Text Transfer Protocol. HTTP is used mainly to acces data on WWW. This is protocol transfers data in the form of plaintext, hypertext, autio, video etc. The function of HTTP is like a combination of FTP and SMTP. It uses services of TCP. It uses only one TCP connection (port 80). There is no separate control connection. Only the data transfer take place between the client and server. The data transfer in HTTP is similar to SMTP. The format of the message is controlled by MIME like headers.

Principle of HTTP Operation : The principle of HTTP is simple. A client sends a request. The server sends a response. The request and response messages carry data in the form of a letter with a MIME like format. Fig.(1) shows the HTTP transactions between client and sever. The client initializes the transaction by sending a request message and the server replies it by sending a response.

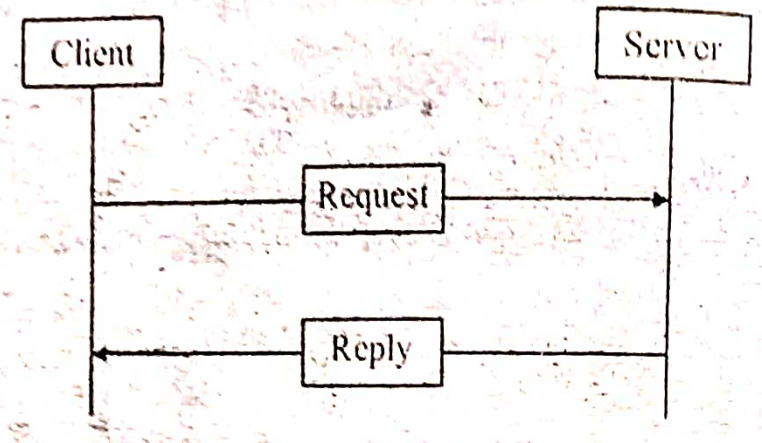


Fig.(1) : HTTP transaction

Q.5. Briefly explain : (20)

(a) RARP

(b) ICMP

(c) FTP & HTTP

(d) Domain name system

Ans.(a)Reverse Address Resolution Protocol (RARP) : A diskless machine uses a TCP/IP Internet protocol called RARP to obtain its IP address from a server. RARP uses the same message format like ARP. RARP allows for multiple physical network types. A RARP message is sent from one computer to another encapsulated in the data portion of a network frame. Fig. shows the operation of RARP.

The sender broadcasts a RARP request that specifies itself as both, the sender and target machine and supplies its physical address in the target hardware address field. All the machines on the network receive the request, but only those authorized to supply the RARP service process the request and send a reply, such machines are known as RARP server. For RARP succeed, the network must contain at least one RARP server.

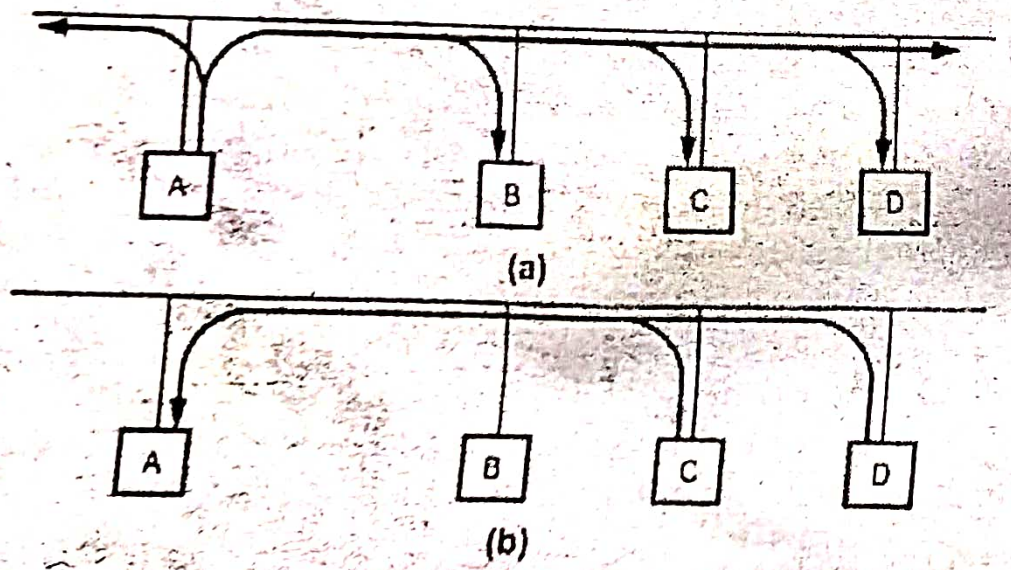


Fig. : RARP protocol

Ans.(b) ICMP(Internet Control Message Protocol) : *The Internet Control Message Protocol(ICMP) reports errors and sends control messages on behalf of IP. ICMP does not*

attempt to make IP a reliable protocol. It simply attempts to report errors and provide feedback on specific conditons. ICMP Messages are carried as IP a reliable protocol. It simply attempts to report errors and provide feedback on specific conditions. ICMP message are carried as IP packets and are therefore unreliable. IP also lacks a mechanism for host and management queries. A host sometimes needs to determine if a router or another host is alive. And sometimes a network manager needs information from another host or router. The Internet Control Message Protocol (ICMP) has been designed to compensated for the above two deficiencies. It is a companion to the IP, ICMP itself is a network layer protocol. However, its messages are not passed directly to the data link layer as would be expected. Instead, the messages are first encapsulated inside IP datagrams before going to the lower layer. This has been shown in fig.(a).

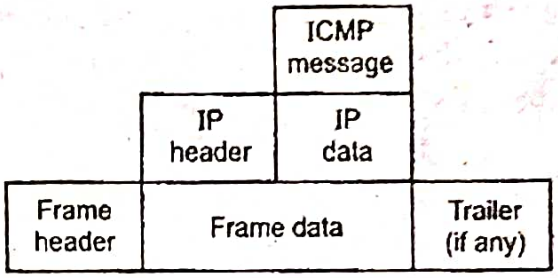


Fig.(a) : ICMP Encapsulation

Ans.(c) FTP : File transfer protocol (FTP) is a TCP/IP client-server application for copying files from one host to another.

FTP establishes two connections between the client and server. One is for data transfer and the other is for the control information. The fact that FTP separates control and data makes it very efficient.

HTTP : HTTP stands for Hyper Text Transfer Protocol. HTTP is used mainly to acces data on WWW. This is protocol transfers data in the form of plaintext, hypertext, autio, video etc. The function of HTTP is like a combination of FTP and SMTP. It uses services of TCP. It uses only one TCP connection (port 80). There is no separate control connection. Only the data transfer take place between the client and server. The data transfer in HTTP is similar to SMTP. The format of the message is controlled by MIME like headers.

Principle of HTTP Operation : The principle of HTTP is simple. A client sends a request. The server sends a response. The request and response messages carry data in the form of a letter with a MIME like format. Fig.(1) shows the HTTP transactions between client and sever. The client initializes the transaction by sending a request message and the server replies it by sending a response.

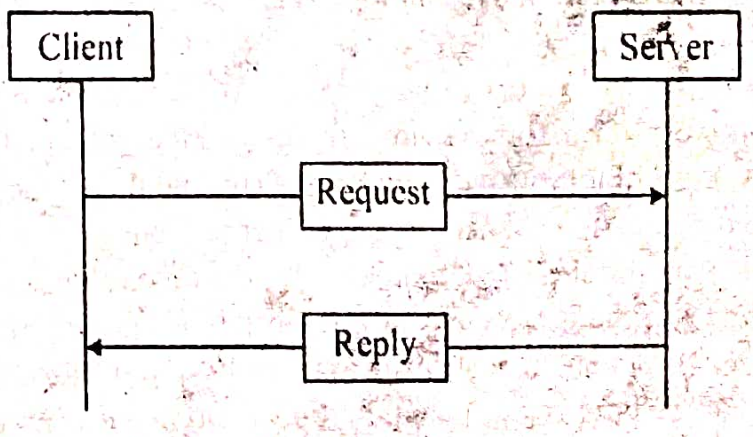


Fig.(1) : HTTP transaction

Ans.(d)Domain name system : The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.

Working of DNS : To map a name into an IP address, an application program calls a library procedure called the resolver. The name is passed on to the resolver as a paramter. The resolver sends a UDP packet to a local DNS server which looks up the name and returns the corresponding IP address to the resolver. The resolver then sends this address to the caller. Then the program can establish a tcp connection with the destination or send in the UDP packets.

The top level domains are of two types, namely, generic and countries.

DNS example : The DNS systemis a database, and no other databse on the planet gets this many requests. No other database on the planet millions of people changing it everyday, either. That is what makes the DNS system so unique!

For example :

(i) www.yahoo.com – the world's best known name.
(ii) www.mit.edu – a popular EDU name.
(iii) encarta.mas.com – a Web server that does not start with www.
(iv) www.bbc.co.uk – a name using four parts rather than three.
(v) ftp.microsoft.com – an FTP server rather than a Web server.
(vi) www.spce.ac.in – Server in India 'in' domain.

Section – C

Q.6.(a) What is Local Area Network ? Explain various features and components of LAN.

Ans. Refer Q.6(a) of paper May 2017. (10)

Q.6.(b) Explain various channel access methods in detail.

Ans. Refer Q.6(ii) of paper May 2018. (10)

Q.7.(a) Define Wide Area Network . What are the various WAN Technologies ?

Ans. WAN : It stands for wide area network. This is the largest network and can interconnect networks throughout the world and is not restricted to a geographical location. The Internet is an example of a worldwide public WAN. Most WANs exist to connect LANs that are not in the same geographical area. This technology is high speed and very expensive to setup. It is shown in fig.(c). (12)

WAN Technologies : A wide area network, or WAN spans a large geographical area, often as country or continent. It contains a collection of machines intended for running user (i.e., application) programs. We will follow traditional usage and call these machines hosts. The hosts are connected by a communication subnet, or just subnet for short. The hosts are owned by the customers (e.g. people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider. The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener. Separation of the pure communication aspects of the network (the subnet) from the application aspects (the hosts), greatly simplifies the complete network design.

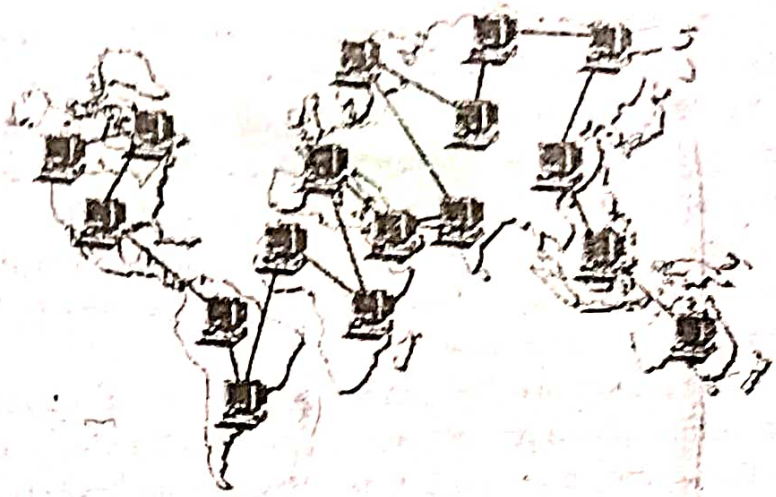


Fig.(c) : Wide area network

In most wide area networks, the subnet consists of two district component : transmission lines and switching elements. Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links. Switching elements are specialized computer that connect three or more transmission line. When data arrive on an incoming line, These switching element must choose an outgoing line on which to forward them. These swtiching element must choose an outgoing line on which to forward them. These switching computers have been called by various names in the past: the same router is now most commoly used. Unfortunately, some people pronounce it "router" and others have it rhyme with "douber". Determining the correct pronounciation will be left as an exercise for the reader. (Note : the perceived correct answer may depend on where you live).

In this model shown in Fig.(1) each host is frequently connected to a LAN on which a router is present, although in some cases a host can be connected directly to a router. The collection of communication lines and routers (but not the hosts) from the subnet.

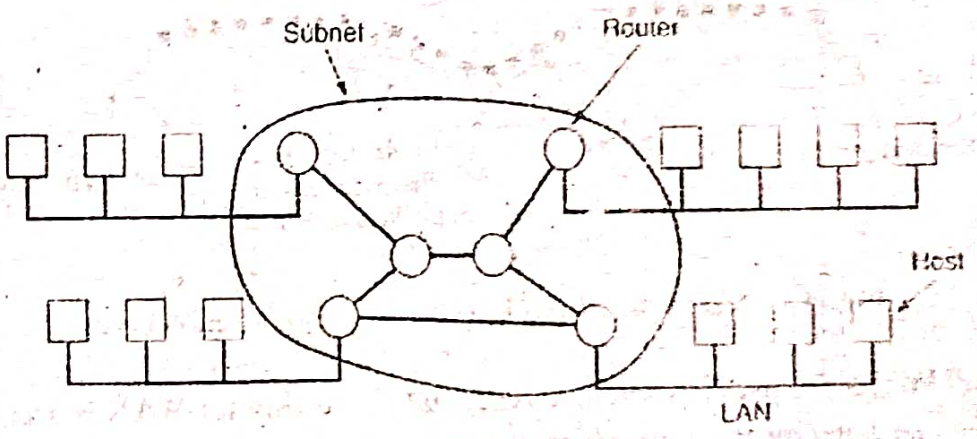


Fig.(1) : Relation betwen hosts on LANs and the subnet

A short comment about the term "subnet" is in order here. Originally, Its only meaning was the collection of routers and communication lines that moved packets from the source host to the destination host. However some years later, it also acquired a second meaning in conjuction with network addressing. Unfortunately, no widely used alternative exists for its initial meaning, so with some hesitation we will use it in both senses. From the context, it will always be clear which is meant.

In most WANs the network contains numerous transmission lines, each one connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers. When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded. A subset organied according to this principle is called a store and forward or packet switched subnet. Nearly all wide area networks (excets those being satellites) haves store and forward subnets. When the packets are small and all same size, they are often called cells.

The principle of a packet switched WAN is so important that it is worth devoting a few more words to it. Generally, when a process on some host has a message to be sent to a process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence. These packets are then injected into the network one at a time in quick succession. The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process. A stream of packets resulting from some initial message is illustrated in Fig.(2).

In this figure, all the packet follows the route *ACE*, rather than *ABDE* or *ACDE*. In some networks all packets from a given message must follow the same route; in others each packets is routed separately. Of course, if *ACE* is the best route, all packet may be sent along it, even if each packet is individually routed.

Rounting decisions are made locally. When a packet arrives at router *A*, it is up to A to decide if this packet should be sent on the line to *B* or the line to *C*. How *A* makes that decision is called the routing algorithm. Many of them exist.

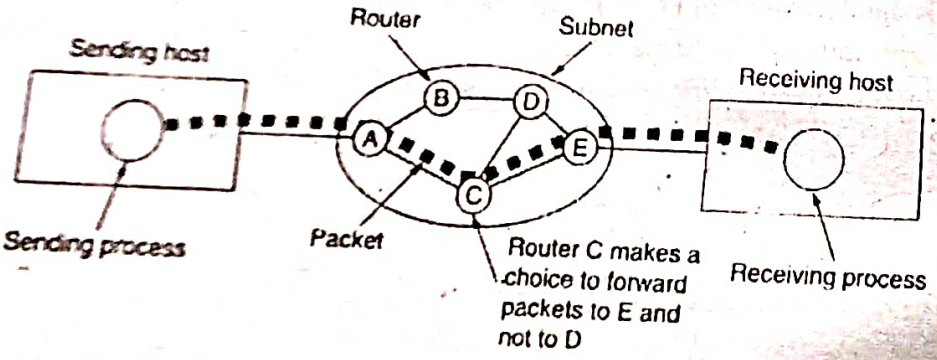


Fig.(1) : A stream of packets from sender to receiver.

Not all WANs are packet switched. A second possibility for WAN is a satellite system. Each router has an antenna through which it can send and receive. All routers can hear the output from the satellite, and in some cases they can also hear the upward transmissions of their fellow routers to the satellite as well. Sometime of outers connected to a substantial point to point subnet, with only some of them having a satellite antenna. Satellite neworks are inherently broadcast and are most useful when the broadcast property is important.

Q.7.(b) Briefly explain Distributed Queue Dual Bus (DQDB). **(8)**

Ans. Refer Q.7(b) of paper May 2017.

Section – D

Q.8. Briefl explain : **(20)**

(a) Synchronous Digital Hierarch (SDH)

(b) Synchronous Optical Network (SONET)

(c) Frame Relay

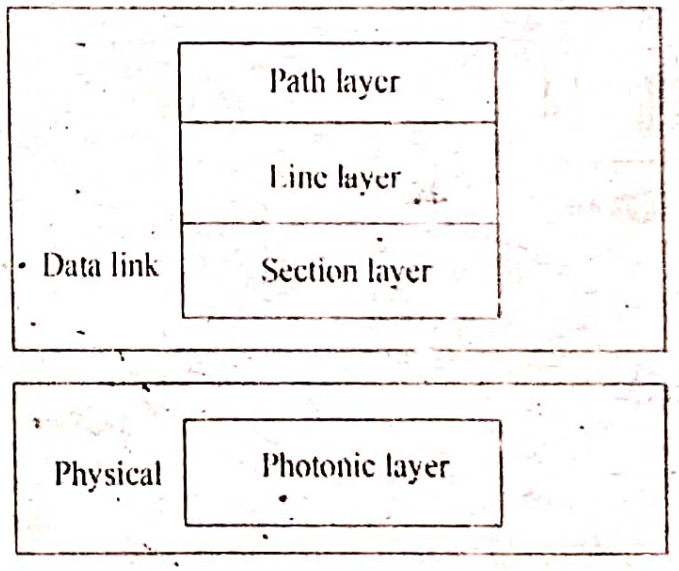
Ans.(a) Synchronous Digital Hierarch (SDH) : SDH (Synchronous Digital Hierarchy) is a standard technology for synchronous data transmission on optical media: It is the international equivalent of Synchronous Optical Network. Both technologies provide faster and less expensive network interconnection than traditional PDH (Plesiochronous Digital Hierarchy) equipment.

In digital telephone transmission, "synchronous" means the bits from one call are carried within one transmission frame. "Plesiochronous" means "almost (but not) synchronous," or a call that must be extracted from more than one transmission frame.

SDH uses the following Synchronous Transport Modules (STM) and rates: STM-1 (155 megabits per second), STM-4 (622 Mbps), STM-16 (2.5 gigabits per second), and STM-64 (10 Gbps).

Ans.(b)Synchronous Optical Network (SONET) : The ANSI standard is call the Synchronous Optical Network (SONET). The ITU-T standard is called the Synchronous Digital Hierarchy (SDH). SONET/SDH is a synchronous network using synchronous TDM multiplexing. All clock in the systems are locked to a master clock.

SONET LAYERS : The SONET standard includes four functional layers: the photonic, the section, the line, and the path layer. The correspond to both the physical and the data link layers (see Fig.).



Path Layer : The Path Layer is responsible for the movement of a signal from it optical source to its optical destination. At the optical source, the signal is changed from an electronic form into an optical form, multiplexed with other signals, and encapsulated in a frame. At the optical destination, the received frame is demultiplexed, and the individual optical signals are changed back into their electronic form. Path layer overhead is added at this layer.

Line Layer : The Line Layer is responsible for the movement of a signal across a physical line. Line layer overhead is added to the frame at this layer.

Section Layer : The Section Layer is responsible for the movement of a signal across a physical section. It handles framing, scrambling, and error control. Section layer overhead is added to the frame at this layer.

Photonic Layer : The Photonic Layer corresponds to the physical layer of the OSI model. It includes physical specifications for the optical fiber channel, the sensitivity of the receiver, multiplexing functions, and so on. SONET uses NRZ encoding with the presence of light representing 1 and the absence of light representing 0.

Ans.(c) 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 late 1980's and early 1990's. It is a connection oriented service. It can be imagined to be equivalent to a virtual leased line. On a virtual line data, bursts can be sent at full speed. Frame relay provides a service to determine the start and end of each frame. It also detects the transmission errors. But the frame relay does not have error control or flow control. If a frame contains errors, then the frame relay service simply discards it.

Frame Relay provides permanent virtual circuits and switched virtual circuits. Fig. shows an example of a Frame Relay network connected to the Internet. The routers are used, to connect LANs and WANs in the Internet. In the figure, the Frame Relay WAN is used as one link in the global Internet.

Some of the **advantages of frame relay** are as under :

(i) Streamlined communication process.
(ii) The number of functions of a protocol at the user-network interface is reduced.
(iii) Lower delay.
(iv) Higher throughout.
(v) Frame relay can be used at access speeds upto 2 Mbps.

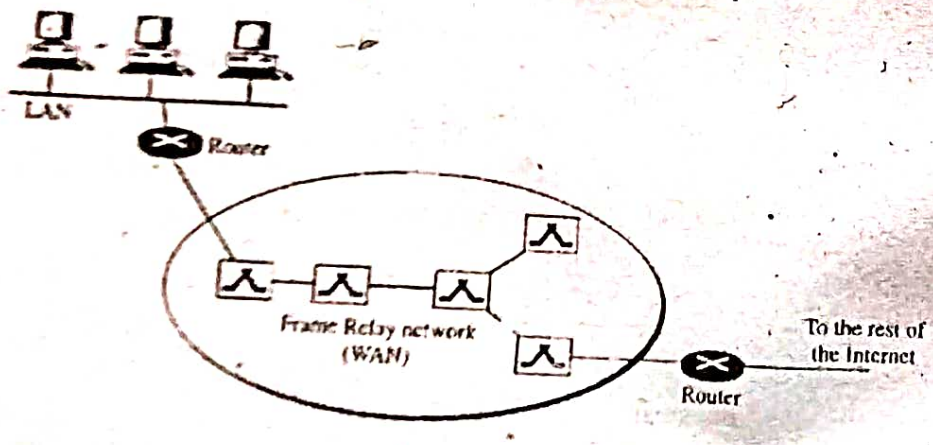


Fig : Frame Relay network

Q.9. Write a short note on : (20)

(a) IP address

(b) Security Management

(c) Client-Server Infrastructure

(d) Remote Monitoring Techhiques

Ans.(a) IP Address : An IP address is a unique address used to locate and identify a device over a network. That device can be an electronic device, a computer, a server, a router or even an IP phone. It is the addressing used for the transmission of data packets over a network working with the IP protocol.

It is classified as :

(i) *Class A address format* : The network field is 7 bit long as shown in fig.(a) and the host field is of 24 bit length. So the network field can have numbers between 1 to 127. But the host numbers will range from 0.0.0.0 to 127.255.255.255. Thus in class A, there can be 126 types of network and 17 million hosts. The "0" in the first field identifies that it is a class A network address.

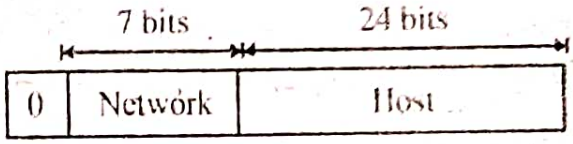


Fig. (a) : Class A IP Address formats

(ii) *Class B address Format* : The Class B address format is show in fig.(b).

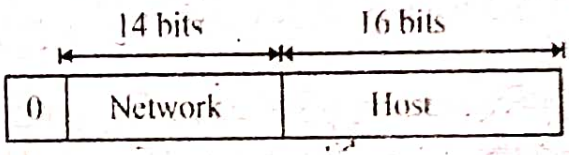


Fig. (b) : Class B Format

The first two fields identify the network, and the number in the first field must be in the range 128-191. Class B networks are large. Host numbers 0.0 and 255.255 are reserved. So there can be upto 65,234 (216-2) host in a class B network. Most of the 16.382 class B address have been allocated. The first block covers address from 128.0.0.0.0 in 128.255.255.255.255 and the last block covers from 191.255.0.0 to 191.255.255.255.

(iii) *Class C address format* : Class C address format is shown in fig.(c).

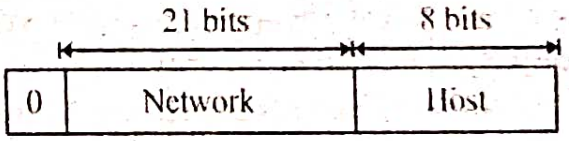


Fig. (c) : Class C Format

The first block in class covers addresses from 192.0.0.0 to 192.0.0.253 and the last block covers address from 223.255.255.0 to 223.255.255.255

(iv) *Class D format* : The class D address format is show in fig.(d).

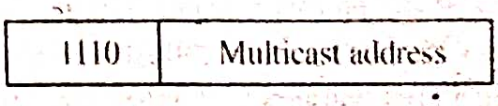


Fig. (d) : Class D Format

The class format allows for upto 2 million networks with upto 254 hosts each and class D format allows the multicast in which a datagram is directed to multiple hosts.

(v) *Class E address format* : Fig.(e) shows the address format for a class E address. This address begins with 1110 which shows that it is reserved for the future use.

1110	Reserved for future use

Fig. (e) : IP address for class E Network

The 32 bit (4 byte) network address are usually written in dotted decimal notation. In this notation each of the 4 bytes is written in decimal from 0 to 255. So the lowest IP address 0.0.0.0 i.e. all the 32 bites are zero and highest IP address is 255.255.255.255

Ans.(b)Security Management : Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

Homes & Small Businesses :

– A basic firewall or a unified threat management system.

– For Windows users, basic Antivirus software. An anti-spyware program would also be a good idea. There are many other types of antivirus or anti-spyware programs out there to be considered.

– When using a wireless connection, use a robust password. Also try to use the strongest security supported by your wireless devices, such as WPA2 with AES encryption.

– If using Wireless: Change the default SSID network name, also disable SSID Broadcast; as this function is unnecessary for home use. (However, many security experts consider this to be relatively useless).

– Enable MAC Address filtering to keep track of all home network MAC devices connecting to your router.

– Assign STATIC IP addresses to network devices.

– Disable ICMP ping on router.

Medium businesses :

– A fairly strong firewall or Unified Threat Management System

– Strong Antivirus software and Internet Security Software..

– For authentication, use strong passwords and change it on a bi-weekly/monthly basis.

– When using a wireless connection, use a robust password.

– Raise awareness about physical security to employees.

Large businesses :

– A strong firewall and proxy to keep unwanted people out.

– A strong Antivirus software package and Internet Security Software package.

– For authentication, use strong passwords and change it on a weekly/bi-weekly basis.

– When using a wireless connection, use a robust password.

– Exercise physical security precautions to employees.

– Prepare a network analyzer or network monitor and use it when needed.

– Implement physical security management like closed circuit television for entry areas and restricted zones.

School :

– An adjustable firewall and proxy to allow authorized users access from the outside and inside.

– Strong Antivirus software and Internet Security Software packages.

– Wireless connections that lead to firewalls.

– Children's Internet Protection Act compliance. (Only schools in the USA)

– Supervision of network to guarantee updates and changes based on popular site usage.

Large government :

– A strong firewall and proxy to keep unwanted people out.

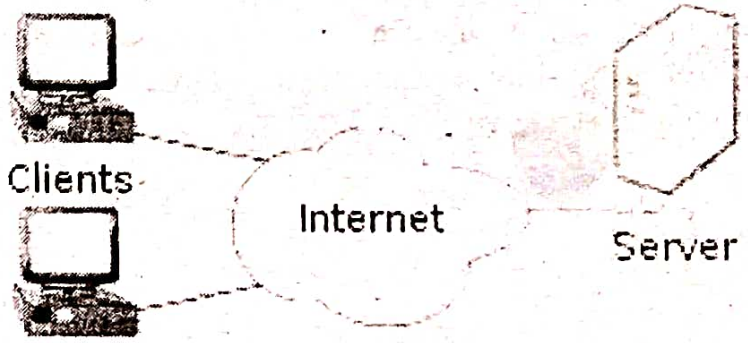
– Strong antivirus software and Internet Security Software suites.

– Strong encryption.

– Whitelist authorized wireless connection, block all else.

– All network hardware is in secure zones.

Ans.(c)Client-Server Infrastructure : In this architecture, each computer is either a client or a server. To complete a particular task, there exists a centralized powerful host computer known as server and a user's individual workstation known as client (fig.). The client requests for sercices (file sharing, resource sharing etc.) from the server and the server responds by providing that service. The servers provide access to resources, while the clients have access to the resource available only on the servers. In addition, no clients can communicate directly with each other in this architecture. A typical example of client/server architecture is accessing a website (server) from home with the help of a browser(client). When a client makes a request for an object to the server, then the server responds by sending the object to the client . In addition, it must be noticed that two browser's accessing the same website, never communicate with each other.



An advantage of client/server architecture is that the IP address of the server is always fixed and the server is always available on the network for clients. However, the disadvantage of this architecture is that with time as the number of client starts to increase, the number of requests to the server also increases rapidly. In this scenario, we might need more than one server to serve larger number of requests.

Ans.(d) Remote Monitoring Techniques : Remote monitoring enables various network monitors and console systems to exchange network-monitoring data. It is an extension of the SNMP Management Information Database (MIB).RMON is able to set alarms that will monitor the network based on certain criteria. RMON allows Administrators to manage local

networks as well as remote sites from one central location. It monitors at the Network Lay and below. RMON has 2 versions:

- RMON
- RMON2

The 2 components of RMON are the probe also known as the agent or monitor, and th client also known as the management station.

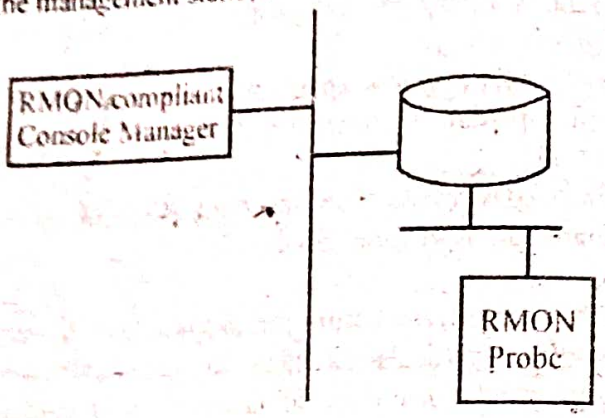


Fig. : RMON components

RMON uses 9 different monitoring groups to obtain information about the network.

(i) Statistics - stats measured by the probe for each monitored interface on this device.

(ii) History - records periodic statistical samples from a network and store for retrieval.

(iii) Alarm - periodically takes statistic samples and compares them with a set of thresholds for event generation.

(iv) Host - contains statistics associated with each host discovered on the network.

(v) HostTopN - prepares tables that describe top hosts

(vi) Filters - enable packets to be matched by a filter equation for capturing events

(vii) Events - controls generation and notification of events from a device

(viii) Token ring - supports token ring

COMPUTER NETWORKS

Mar - 2021

Paper Code:PCC-CSE-303-G

Note : *Attempt five questions in all, selecting one question from each Section. Question No. 1 is compulsory. All questions carry equal marks.*

Q.1. Write short note on :

(a) ARP (2.5)

(b) Subnetting (2.5)

(c) Types of Cipher (2.5)

(d) Token Ring (2.5)

(e) Framing in data link layer. (2.5)

(f) BOOTP (2.5)

Ans. (a) ARP (Address Resolution Protocol) : An internet consists of various types of networks and the connecting devices like routers. A packet starts from the source host, passes through many physical networks and finally reaches the destination host. At the network level, the hosts and routers are recongnised by their IP addresses.

IP Address : An IP address is an internetwork address. It is a universally unique address. Every protocol involved in internetworking requires IP address.

MAC Address : The packets from source to destination hosts pass through physical networks. At the physical level the IP address is not useful but the hosts and routers are recognized by their MAC address. A MAC address is a local address. It is unique locally but it is not unique universally. The IP and MAC address are two different identifiers both of them are needed, because a physical network can have two different protocols at the network layer at the same time. Similarly a packet may pass through different physical networks. Therefore, to deliver a packet to a host or a router. We require two levels of addressing, namely IP addressing and MAC addressing. Most importantly we should be able to map the IP address into a corresponding MAC address.

ARP is used for associating an IP address to its MAC address. For a LAN, each device has its own physical or station address as its identification. This address is imprinted on the NIC (Network Interface Card).

Ans.(b)Subnetting in IP : All the hosts in a network must have the same network number. But this property of IP addressing can be problematic as the network size increases. For example a company initially may have only one LAN but as the time passes by it might end up with many LANs each one having its own router and each one with its own class C network number. With increase in the number of distinct local networks, their management becomes a problem. Every time a new network number and then this number is to be announced worldwide. Another problem is that if a machine is to be moved from one LAN to another, then its IP address needs to be changed. This will require modification in its configurational files and its modified IP number needs to be announced to the world. The solution to this problem is that, the network is split into several smaller networks internally but it acts like a single network to the

outside world. The smaller parts of a network are called subnets. Now, continue with the same example taken at the beginning of this subsection. The growing company should start up with class B address instead of class C address and it can number the hosts from 1 to 254. When a second LAN is to be installed it can split the 16 bit host number into a 6-bit subnet number and 10 bit host number as shown in fig.(1).

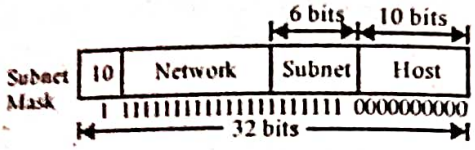


Fig.(1) : One of the ways to subnet a class B network

Due to this split it is possible to connect 62 LANs (0-1 are reserved) and each one can contain upto 1022 hosts. Outside the network, the subnetting is not visible. Hence, even if a new subnet is created it is not necessary to contact NIC or change any database.

Ans.(c) Types of Cipher : Different types of ciphers exist, some of which are :

Substitution Cipher: This offers an alternative to the plaintext. It is also known as Caesar cipher.

Polyalphabetic Substitution Cipher: In this cipher, a mixed alphabet is used to encrypt the plaintext, but at random points it would change to a different mixed alphabet which indicates the change with an uppercase letter in the Ciphertext.

Transposition Cipher: This cipher is also known as Rail Fence Cipher and is a permutation of the plaintext.

Permutation Cipher: The positions held by plaintext are shifted to a regular system in this cipher so that the ciphertext constitutes a permutation of the plaintext.

Private-key Cryptography: In this cipher, even the attacker is aware of the plaintext and corresponding ciphertext. The sender and receiver must have a pre-shared key. The shared key is kept secret from all other parties and is used for encryption as well as decryption. DES and AES algorithms are examples of this type of cipher. This cryptography is also known as "symmetric key algorithm".

Public-key Cryptography: In this cipher, two different keys - public key and private key - are used for encryption and decryption. The sender uses the public key to perform encryption, whereas the receiver is kept in the dark about the private key. This is also known as asymmetric key algorithm.

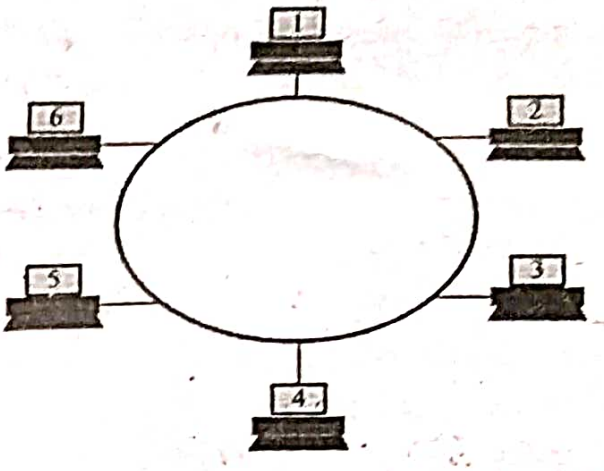
Ans.(d) Token ring : Token ring or is a network where all computers are connected in a circular fashion. The term token is used to describe a segment of information that is sent through that circle; when a computer on the network can decode that token, it receives data.

The data transmission process goes as follows:

– Empty information frames are continuously circulated on the ring.

– When a computer has a message to send, it seizes the token. the computer will then be able to send the frame.

– The frame is then examined by each successive workstation. The workstation that identifies itself to be the destination for the message copies it from the frame and changes the token back to 0.



– When the frame gets back to the originator, it sees that the token has been changed to 0 and that the message has been copied and received. It removes the message from the frame.

– The frame continues to circulate as an "empty" frame, ready to be taken by a workstation when it has a message to send.

Ans.(e) Framing in Data Link Layer : In the physical layer, data transmission involves synchronised transmission of bits from the source to the destination. The data link layer packs these bits into frames.

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

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

Parts of a Frame : A frame has the following parts :

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

Ans.(f) BOOTP : Bootstrap Protocol (BOOTP) is a TCP/IP protocol and service that allows diskless workstations to obtain their IP address and their boot image file from a server.

BOOTP stands for Bootstrap protocol, is a TCP/IP protocol and service that allows diskless workstations to obtain their IP address, other TCP/IP configuration information, and their boot image file from a bootstrap protocol (BOOTP) server.

The network interface card (NIC) on these diskless workstations contains a programmable read-only memory (PROM) chip containing code necessary to initialize the client.

Working : When a BOOTP client is started, it has no IP address, so it broadcasts a message containing its MAC address onto the network. This message is called a "BOOTP request," and it is picked up by the BOOTP server, which replies to the client with the following information that the client needs:

- The client's IP address, subnet mask, and default gateway address
- The IP address and host name of the BOOTP server
- The IP address of the server that has the boot image, which the client needs to load its operating system

When the client receives this information from the BOOTP server, it configures and initializes its TCP/IP protocol stack, and then connects to the server on which the boot image is shared. The client loads the boot image and uses this information to load and start its operating system.

The Dynamic Host Configuration Protocol (DHCP) was developed as an extension of BOOTP. BOOTP is defined in Request for Comments (RFC) 951 and 1084.

Section – A

Q.2.(a) What is OSI model ? Explain the working of OSI model in details. (7.5)

Ans. The ISO-OSI Reference Model : This reference model is proposed by International standard organization (ISO) as a a first step towards standardization of the protocols used in various layers in 1983 by Day and Zimmermann. This model is called Open system Interconnection (OSI) reference model. It is referred OSI as it deals with connection open systems. That is the systems are open for communication with other systems. It consists of seven layers.

Fig. shows the seven layer architecture of ISO-OSI reference model.

– The Physical Layer (Layer 1) : Functions of the physical layer are as follows:

(i) To activate, maintain and deactivate the physical connection.

(ii) To define voltages and data rates needed for transmission.

(iii) To convert the digital bits into electrical signal.

(iv) To decide whether the transmission is simplex, half duplex or full duplex.

– Data Link Layer (Layer 2) : Functions of the data link layer are as follows :

(i) Functions of the data link layer are synchronization and error control for the information which is to be transmitted over the physical link.

(ii) To enable the error detection, it adds error detection bits to the data which are to be transmitted.

(iii) The encoded data are then passed to the physical layer.

(iv) These error detection bits are used by the data link on layer on the other side to detect and correct the errors.

(v) At this level, the outgoing messages are assembled into frames, and the system waits for the acknowledgments to be received after every frame transmitted.

(vi) Correct operation of the data link layer ensures reliable transmission of each message. Examples of data link layer protocols are HDLC, SDLC and X.25 protocols.

– The Network Layer (Layer 3) : The functions of network layer are as follows :

(i) To route the signals through various channels to the other end.

(ii) To act as the network controller by deciding which route data should take.

(iii) To divide the outgoing messages into packets and to assemble incoming packets into messages for the higher levels.

– Transport Layer (Layer 4) : The functions of the transport layer are as listed below :

(i) It decides if the data transmission should take place on parallel paths or single path.

(ii) It does the functions such as multiplexing, splitting or segmenting on the data.

(iii) Transport layer guarantees transmission of data from one end to the other.

(iv) It breaks the data groups into smaller units so that they are handled more efficiently

by the network layer.

– **The Session Layer (Layer 5) :** The functions of the session layer are as listed below :

(i) This layer manages and synchronizes conversations between two different applications. This is the level at which the user will establish system to system connection.

(ii) It controls logging on and off, user identification, billing and session management.

(iii) In the transmission of data from one system to the other, at session layer streams of data are marked and resynchronized properly so that the ends of messages are not cut prematurely and data loss is avoided.

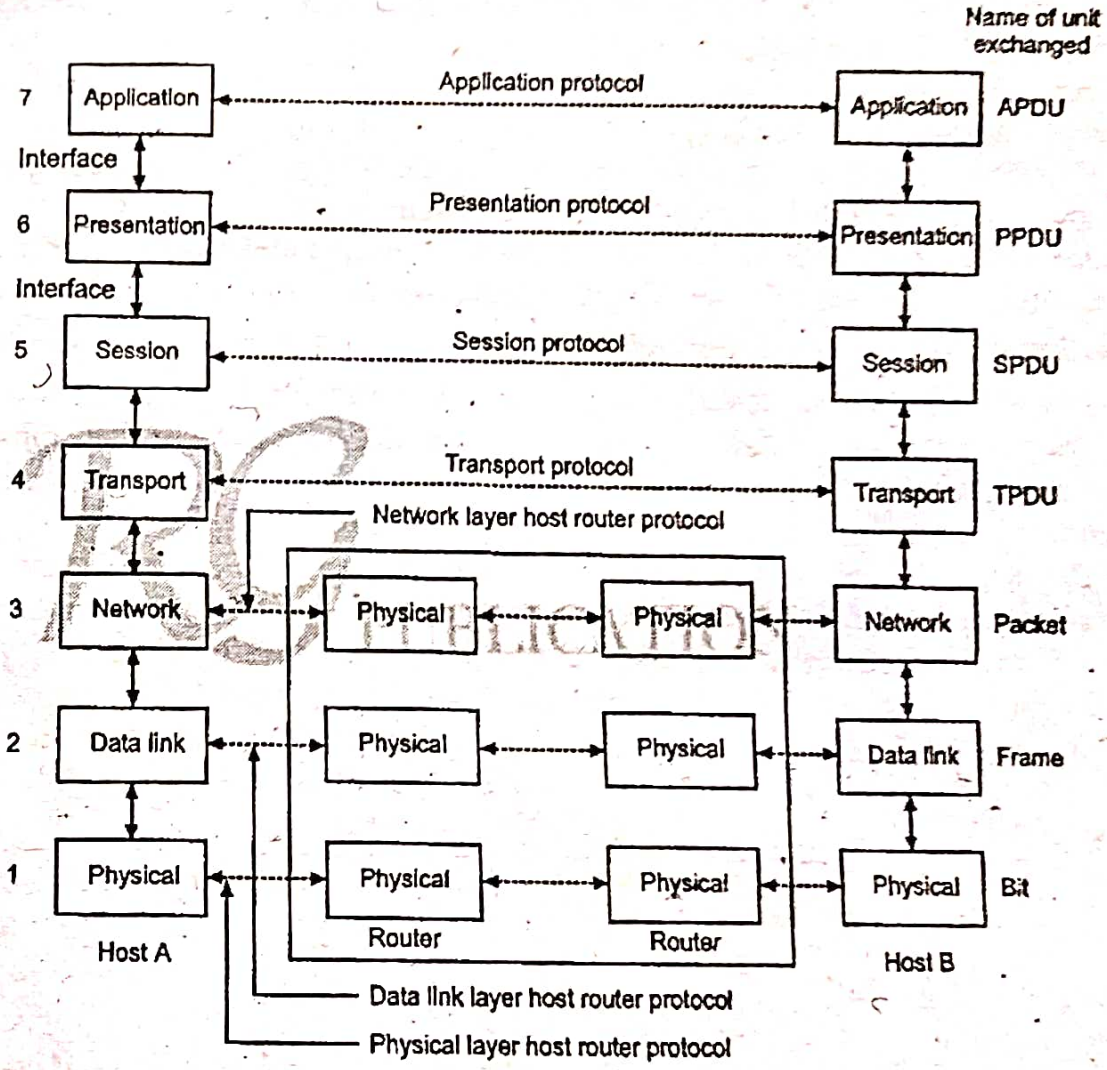


Fig. : The ISO-OSI reference model

– **The Presentation Layer (Layer 6) :** The functions of the presentation layer are as listed below :

(i) The presentation layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it.

(ii) The form and syntax (language) of the two communicating systems can be different e.g. one system is using the ASCII code for file transfer and the other one use IBM's EBCDIC.

(iii) Under such conditions, the presentation layer provides the translation from ASCII to EBCDIC and vice versa.

– Application Layer (Layer 7) : The functions of the application layer are as listed below :

(i) Application layer is at the top of all as shown in fig. It provides different services such as manipulation of information in various ways, retransferring the files of information, distributing the results etc. to the user who is sitting above this layer.

(ii) The functions such as LOGIN, or password checking are also performed by the application layer.

Q.2.(b) What do you mean by Sliding Window Protocol ? Explain. (7.5)

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

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

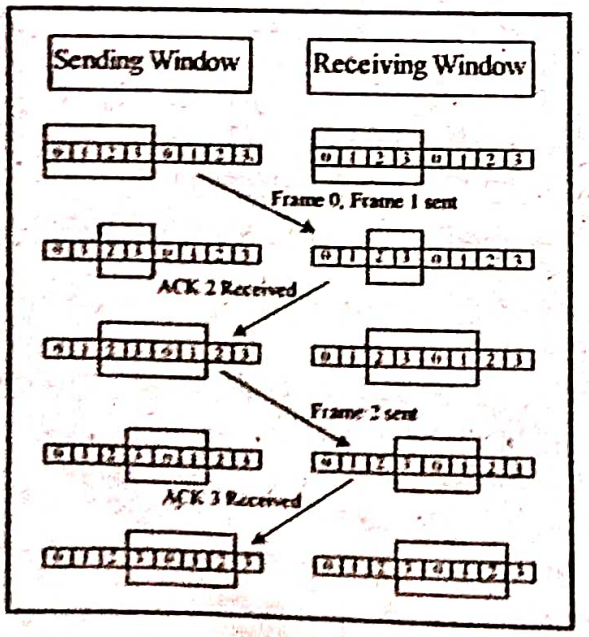
Working Principle : In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.

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

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

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

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



Types of Sliding Window Protocols : The Sliding Window ARQ (Automatic Repeat reQuest) protocols are of two categories :

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

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

Q.3.(a) Give a brief description about Computer Network and its historical development. **(7.5)**

Ans. Computer Network : Computer network is a system which allows communication amoung the computers connected in the network. A network must be able to meet certain criteria. The most important of them are:

1. Performance
2. Relaibility
3. Security

1. *Performacnce* : Performance can be measured in many ways. We can measure it in terms of transit time and response time.

(a) Transit time is defined as the amount of time required for a message to travel from one device to the other.

(b) Response time: It is the time elapsed between enquiry and response.

The other factors deciding the performance are as follows:

(i) Number of users

(ii) Type of transmission medium

(iii) Capability of connected hardware

(iv) Efficiency of software.

2. *Reliability :* The network reliability is important because it decides the frequency at which network failure takes place. It also decides the time taken by the network to recover and its robustness in the catastrophe.

3. *Security :* The network secutiry refers to protection of data from the unauthorized user or access.

Historical development of Computer Network :

Year	Event
1961	In this year, Leonard Kleinrock proposed the earliest computer networks, which was the idea of ARPANET.
1965	In 1965, Donald Davies coined the term "packet" to describe how to send data between computers on a network.
1969	Although In 1966, the development of ARPANET began, officially started ARPANET in 1969. It was considered one the first computer networks in which first two nodes, UCLA and SRI (Stanford Reserch Institute) were connected, and to use packet switching.

1969 On 29 August 1969, the first IMP and network switch were sent to UCLA. On ARPANET, the first data transmission was sent by using it.

1970 NCP, stands for NetWare Core Protocol, released by Steve Crocker and a team at UCLA for use with NetWare.

1971 In 1971, the first e-mail was sent to across a network to other users by Ray Tomlinson.

1973 While working at Xerox PARC, Robert Metcalfe developed the Ethernet in 1973. In the same year, ARPA deployed the first international network connection, known as SATNET.

1974 In this year, the use of first router was began, but they were not considered true IP routers.

1978 In 1978, the TCP/IP protocol was developed and invented by Bob Kahn for networks; it was developed with help from Vint Cert.

1981 In the United States, between IBM mainframe systems, BITNET was created in 1981 as a network. The U.S. National Science Foundation developed the CSNET (Computer Science Network) in the same year 1981.

1983 For using TCP/IP, ARPANET finished the transition. The first DNS implement by jon Postel and Paul Mockapetris in 1983.

1986 This is the year in which a backbone for ARPANET, the National Science Foundation Network was came online, which finally took the place of ARPANET in 1990s. In the same year, Digital Equipment Corporation developed it. This paper had the detail about the first firewall, known as a packet filter firewall.

1990 The first network switch was developed and introduced by a U.S. network hardware company named kalpana in 1990.

1996 In 1996, an IPv6 was introduced as an improvement over IPv4, as well as embedded encryption, improved routing.

1997 In June 1997, the 802.11 standards, containing transmission speeds up to 2 Mbps, for Wi-Fi were introduced.

1999 The 802.11 a standard, containing transmission speeds up to 25 Mbps to use the 5 GHz band, was officially made in 1999. Another standard 802.11b was available to use for the public in mid-1999, which offered transmission speeds up to 11 Mbps. In September 1999, for use with 802.11b, the WEP encryption protocol was released.

2003 802.11g devices, contained transmission speeds up to 20 Mbps, were available to the public in January 2003. In the same year, for use with 802.11g, the WPA encryption protocol is released.

2004 In 2004, as a replacement for WPA, the WPA2 encryption protocol was intorduced. By 2006, WPA2 certification ws compulsory for all Wi-Fi devices.

2009 The 802.11n standard can operate on the 2.4 GHz and 5 GHz bandwidths and offers higher transfer speeds over 802.11a and 802.11g. Officially, it was made in 2009.

2018 In January 2018, WPA3 encryption was released by the Wi-Fi Alliance, which comprises security enhancements over WPA2.

Q.3.(b) Explain Data link layer functions and services in detail. (7.5)

Ans. Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate. Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Data link layer has two sub-layers:

- *Logical Link Control* : It deals with protocols, flow-control, and error control
- *Media Access Control* : It deals with actual control of media

Functionality of Data-link Layer : Data link layer does many tasks on behalf of upper layer. These are:

(i) *Framing* : Data-link layer takes packets from Network Layer and encapsulates them into Frames.Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.

(ii) *Addressing* : Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

(iii) *Synchronization* : When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

(iv) *Error Control* : Sometimes signals may have encountered problem in transition and the bits are flipped.These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

(v) *Flow Control* : Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.

(vi) *Multi-Access* : When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

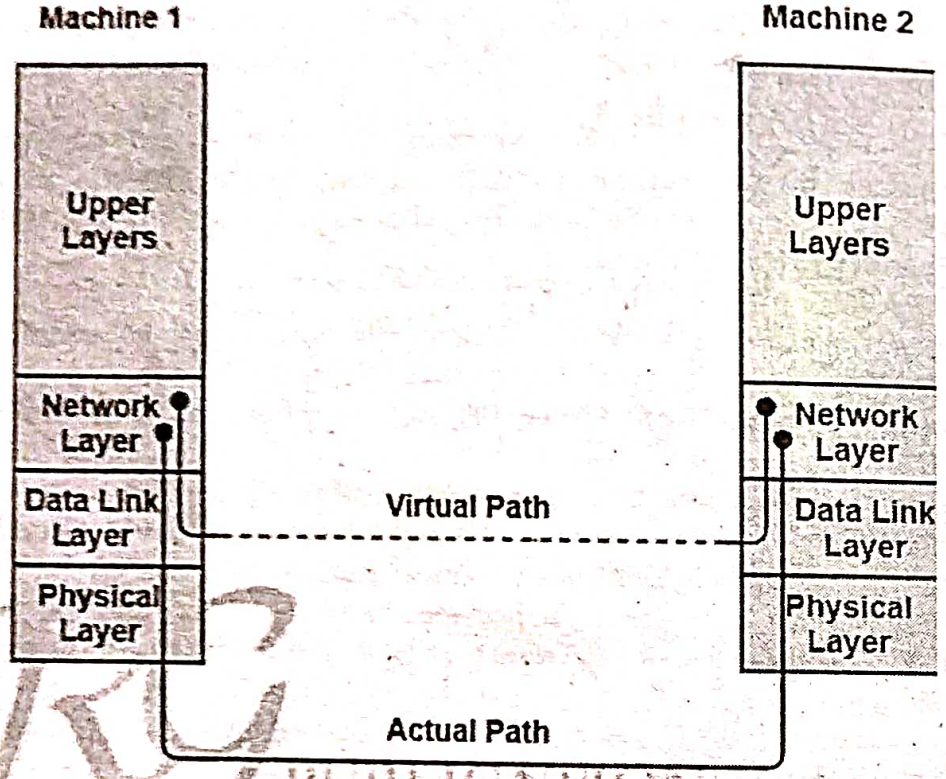
Service Provided to Network Layer : The important and essential function of Data Link Layer is to provide an interface to Network Layer. Network Layer is third layer of seven-layer OSI reference model and is present just above Data Link Layer.

The main aim of Data Link Layer is to transmit data frames they have received to destination machine so that these data frames can be handed over to network layer of destination machine. At the network layer, these data frames are basically addressed and routed.

This process is shown in diagram :

1. Actual Communication : In this communication, physical medium is present through which Data Link Layer simply transmits data frames. The actual path is Network Layer -> Data link layer -> Physical Layer on sending machine, then to physical media and after that to Physical Layer -> Data link layer -> Network Layer on receiving machine.

2. Virtual Communication : In this communication, no physical medium is present for Data Link Layer to transmit data. It can be only be visualized and imagined that two Data Link Layers are communicating with each other with the help of or using data link protocol.



Types of Services provided by Data Link Layer : The Data link layer generally provides or offers three types of services as given below :

1. Unacknowledged Connectionless Service
2. Acknowledged Connectionless Service
3. Acknowledged Connection-Oriented Service

(1) Unacknowledged Connectionless Service : Unacknowledged connectionless service simply provides datagram styles delivery without any error, issue, or flow control. In this service, source machine generally transmits independent frames to destination machine without having destination machine to acknowledge these frames.

This service is called as connectionless service because there is no connection established among sending or source machine and destination or receiving machine before data transfer or release after data transfer.

In Data Link Layer, if anyhow frame is lost due to noise, there will be no attempt made just to detect or determine loss or recovery from it. This simply means that there will be no error or flow control. An example can be Ethernet.

(2) Acknowledged Connectionless Service : This service simply provides acknowledged connectionless service i.e. packet delivery is simply acknowledged, with help of stop and wait for protocol.

In this service, each frame that is transmitted by Data Link Layer is simply acknowledged individually and then sender usually knows whether or not these transmitted

data frames received safely. There is no logical connection established and each frame that is transmitted is acknowledged individually.

This mode simply provides means by which user of data link can just send or transfer data and request return of data at the same time. It also uses particular time period that if it has passed frame without getting acknowledgment, then it will resend data frame on time period.

This service is more reliable than unacknowledged connectionless service. This service is generally useful over several unreliable channels, like wireless systems, Wi-Fi services, etc.

(3) Acknowledged Connection-Oriented Service : In this type of service, connection is established first among sender and receiver or source and destination before data is transferred.

Then data is transferred or transmitted along with this established connection. In this service, each of frames that are transmitted is provided individual numbers first, so as to confirm and guarantee that each of frames is received only once that too in an appropriate order and sequence.

Section – B

Q.4. Explain the following in detail : **(15)**

(a) DHCP

(b) IPv4

Ans. (a) DHCP (Dynamic Host Configuration Protocol) : DHCP (Dynamic Host Configuration Protocol) is a protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. If a machine uses Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments).

DHCP does the following :

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

There are many versions of DCHP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

How DHCP works : DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

The DHCP lease process works as follows :

- First of all, a client (network device) must be connected to the internet.
- DHCP clients request an IP address. Typically, client broadcasts a query for this information.
- DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes time period, called a lease, for which the allocation is valid.
- When refreshing an assignment, a DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

Components of DHCP

When working with DHCP, it is important to understand all of the components. Following are the list of components :

DHCP Server : DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.

DHCP client : DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.

IP address pool : IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.

Subnet : Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.

Lease : Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.

DHCP relay : A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

Benefits of DHCP : There are following benefits of DHCP:

(i) *Centralized administration of IP configuration* : DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

(ii) *Dynamic host configuration* : DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

(iii) *Seamless IP host configuration* : The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

(iv) *Flexibility and scalability* : Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

Ans.(b)IPv4 : Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) Internet, and routes most traffic on the Internet.

The IPv4 Header fields are discussed as follows :

(i) *Version* : Indicates the version of IP currently used.

(ii) *IP Header Length* (IHL) : Indicates the datagram header length in 32-bit words.

(iii) *Types of Service* : Specifies how an upper-layer protocol would like a current datagram to be handled and assigns datagrams various levels of importance.

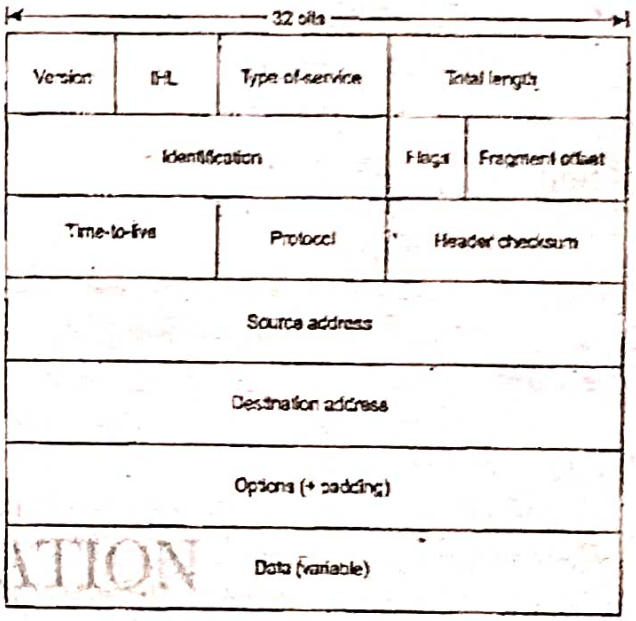


Fig. : IPv-4 Header

(iv) *Total Length* : Specifies the length in bytes of the entire IP packet, including the data and header.

(v) *Identification* : Contains an integer that identifies the current datagram. This field is used to help piece together datagram fragments.

(vi) *Flags* : Consists of a 3-bit field of which the two low-order (least-significant) bits control fragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether the packet is the last fragment in a series of fragmented packets. The third or high order bit is not used.

(vii) *Fragment Offset* : Indicates the position of the fragment's data relative to the begining of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.

(viii) *Time-to-Live* : Maintains a counter that gradually decrements down to zero, at which point the datagram is discarded. This keeps packets from looping endlessly.

(ix) *Protocol* : Indicates which upper layer protocol receives incoming packets after IP processing is complete.

(x) *Header Checksum* : Helps ensure IP header integrity.

(xi) *Source Address* : Specifies the sending node.

(xii) *Destination Address* : Specifies the receiving node.

(xiii) *Options* : Allows IP to support various options such as security.

(xiv) *Data* : Contains upper-layer information.

Q.5.(a) What do you mean by MAC ? Explain its functions in details. (7.5)

Ans. Medium Access Control (MAC) : The MAC is a protocol which controls the access to the transmission medium for an orderly and efficient use of the transmission capacity of the network.

Such a control can be exercised in two different ways :

(*i*) Centralized control

(*ii*) Decentralised control

(*i*) Centralized Control : In the centralized control, the controller has the authority to grant access to the network. A station who wishes to transmit its data on the network has to wait till a permission is received from the controller.

(*ii*) Decentralized Control : In a decentralized network, the stations collectively perform the medium access control function to determine the order in which the stations transmit.

Advantages of Centralized Control :

(*i*) It can exercise greater control.

(*ii*) It can use simple access logic at each station.

(*iii*) It avoids the problems of distributed co-ordination.

Disadvantages of Centralized Control :

(*i*) It creates a single point of failure. If this point fails, then it causes the entire network to fail.

(*ii*) It may act as a bottleneck to reduce the performance.

Functions of Media Access Control Sublayer :

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

Q.5.(b) Explain different network devices in details. (7.5)

Ans. LANs do not normally operate in isolation. They are connected to one another or to the Internet. To connect LANs, or segments of LANs, we use connecting devices. Connecting devices can operate in different layers of the Internet model.

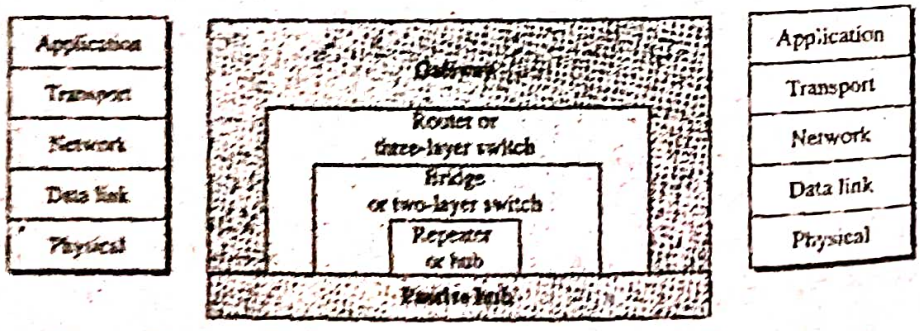


Fig (a) : Five categories of connecting devices.

– **Passive Hub:** A passive hub is just a connector. It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point. This type of a hub is part of the media; its location in the Internet model is below the physical layer.

– **Repeater:** A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern. The repeater then sends the refreshed signal. A repeater can extend the physical length of a LAN, as shown in fig.(b).

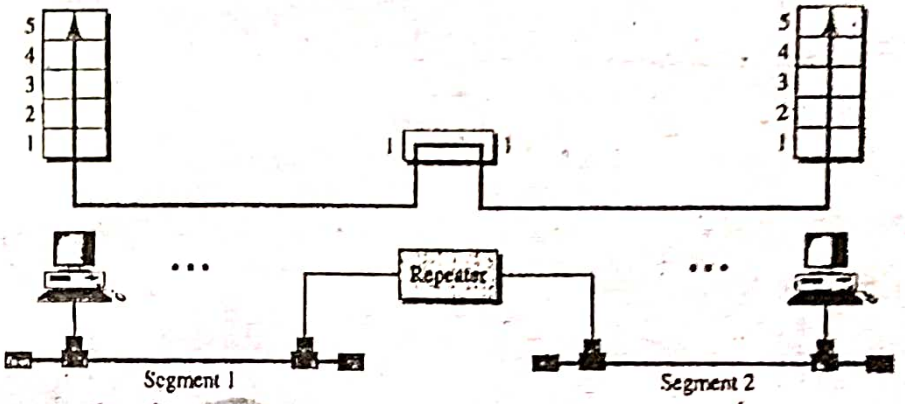


Fig (b) : A repeater connecting two segments of a LAN

– **Active hub :** An active hub is actually a multiport repeater. It is normally used to create connections between stations in a physical star topology.Hubs can also be used to create multiple levels of hierarchy. The hierarchical use of hubs removes the length limitation of 10Base-T (100 m).

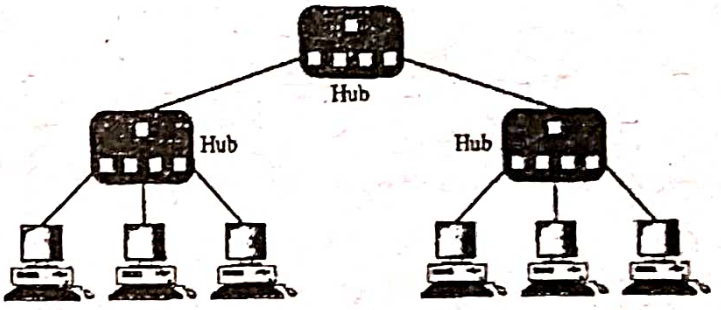
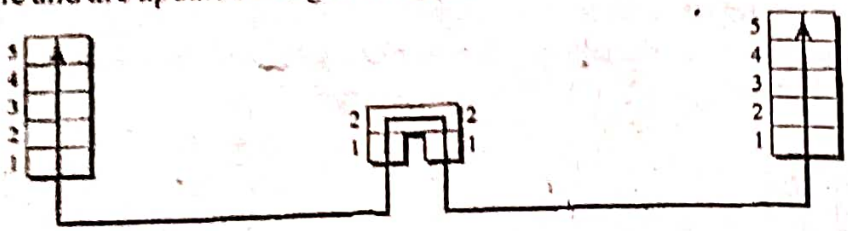


Fig (c) : A hierarchy of hubs

– **Gateway:** A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model. A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internet works that use different models. For example, a network designed to use the OSI model can be connected to another network using the Internet model. The gateway connecting the two systems can take a frame as it arrives from the first system, move it up to the OSI application layer, and remove the message. It can provide security and is used to filter unwanted application, layer messages.

– **Bridge:** A bridge operates in both the physical and the data link layer. The bridge can check the physical (MAC) addresses (source and destination) contained in the frame.

– **Router:** A router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing). A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route. The routing tables are normally dynamic and are updated using routing protocols.



Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	1
64:2B:13:45:61:12	2
64:2B:13:45:61:13	2

Bridge Table

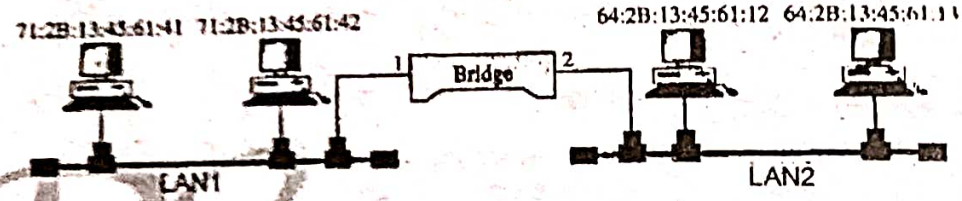


Fig (d) : A bridge connecting two LANs

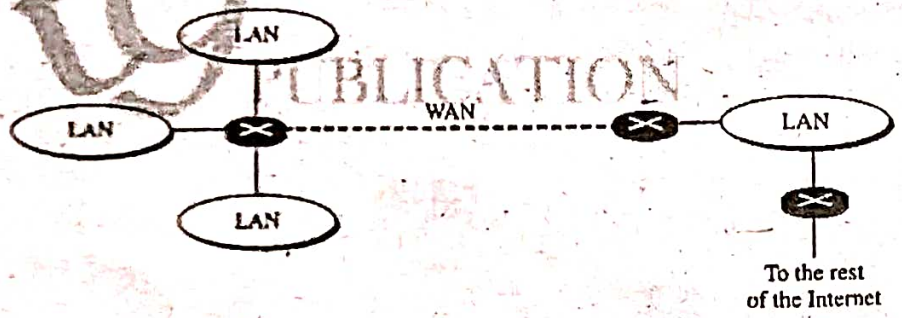


Fig (e) : Routers connecting independent LANs and WANs

Section – C

Q.6. Explain Link State and Distance Vector Routing with the help of example. (15)

Ans. Link State Routing : Distance vector routings was used in ARPANET upto 1979. After that is was replaced by the link state routing. Variants of this algorithm are now widely used. The link state routing is simple and each router has to perform the following five operations :

Router Operations :

(*i*) Each router should discover its neighbours and obtain their network addresses.

(*ii*) Then it should measure the delay or cost to each of these neighbours.

(*iii*) It should construct a packet containing the network addresses and the delays of all the neighbours.

(*iv*) Send this packet to all other routers.

(*v*) Compute the shortest path to every other router.

The complete topology and all the delays are experimentally measured and this information is conveyed to each and every router.

Then a shortest path algorithm such as Dijkstra's algorithm can be used to find the shortest path to every other router.

Protocols : Link state routing is popularly used in practice. The OSPF protocol, which is used in the Internet, uses the link state algorithm. IS-IS *i.e.* Intermediate system – Intermediate system is the other protocol which uses the link state algorithm. IS-IS is used in Internet backbones and in some digital cellular systems such as CDPD.

Distance Vector Routing : In this algorithm, each router maintains a table called vector, such a table gives the best known distance to each destination and the information about which line to be used to reach there. This algorithm is sometimes called by other names such as,

(*i*) Distributed Bellman-Ford routing algorithm.

(*ii*) Ford-Fulkerson algorithm.

In distance vector routing, each router maintains a routing table. It contains one entry for each router in the subnet.

The entry has two parts :

(*i*) The first port shows the preferred outgoing line to be used to reach the destination, and

(*ii*) Second part gives an estimaate of the time or distance to the destination.

The first means used can be one of the following :

(*i*) Number of hops

(*ii*) Time delay

(*iii*) Number of packets in a queue etc.

Q.7. Explain the following in detail : **(15)**

(a) DNS

(b) SNMP

Ans.(a) Domain Name System (DNS) :

Addressing : For communication to take place successfully, the sender and receiver both should have addresses and they shoud be knwon to each other. The addressing in aplication program is different from that in the other layers. Each program should have its won addrsss format. For example, ane-mail address is like sachinshaba@vsnl.net whereas the address to access a web page is like: http:// www.google.com/. It si important to note that there is an alias name for the address of remote host. The applicaion program uses an alias instead of an IP address. This type of address is very convenient for the human beings to remember and use. But it is not suitable for the IP portocol. So the alias address has to be mapped to the IP address. For this, an application program needs service of another entity. This entity is an application program clled DNS. Not that DNS is not used directly by the user. It is used by another application programs fo carrying out the mapping.

Working of DNS : To map a name into an IP address, an application program calls a library procedure called the resolver. The name is passed on to the resolver as a paramter. The resolver sends a UDP packet to a local DNS server which looks up the name and returns the

corresponding IP address to the resolver. The resolver then sends this address to the caller. Then the program can establish a tcp connection with the destination or send in the UDP packets.

The DNS Name Space : Conceptually, the Internet has been divided into hundreds of top level domains. Each domain covers many hosts. Each domainis divided into several subdomains and they are further partitioned and so on. These doamains can be represented by a tree as shown in fig.

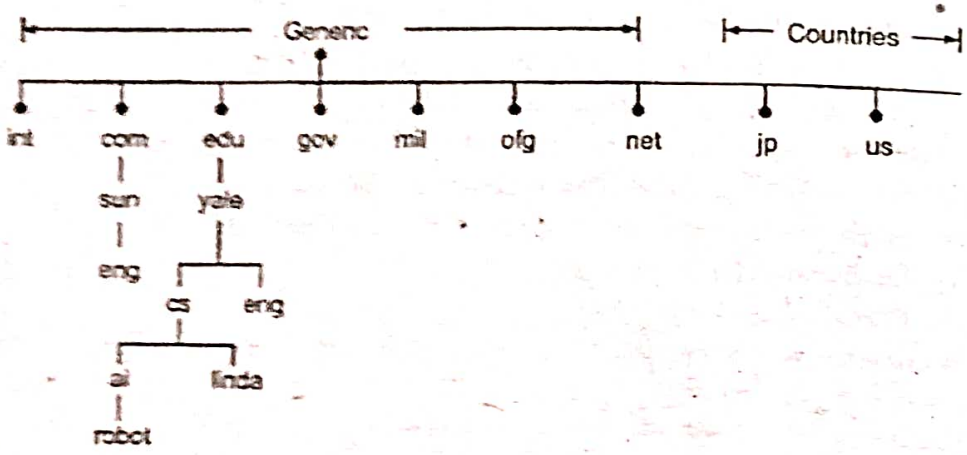


Fig. : A portion of internet domain name space

The top level domains are of two types, namely, generic and countries.

DNS example: The DNS systemis a database, and no other databse on the planet gets this many requests. No other database on the planet millions of people changing it everyday, either. That is what makes the DNS system so unique!

For example :

(i) www.yahoo.com – the world's best known name.
(ii) www.mit.edu – a popular EDU name.
(iii) encarta.mas.com – a Web server that does not start with www.
(iv) www.bbc.co.uk – a name using four parts rather than three.
(v) ftp.microsoft.com – an FTP server rather than a Web server.
(vi) www.spce.ac.in – Server in India 'in' domain.

Ans.(b) Simple Network Management Protocol (SNMP) : SNMP is an application layer protocol which uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults and sometimes even used to configure remote devices.

SNMP components : There are 3 components of SNMP:

1. SNMP Manager : It is a centralised system used to monitor network.It is also known as Network Management Station (NMS)

2. SNMP agent : It is a software management software module installed on a managed device. Managed devices can be network devices like PC, router, switches, servers etc.

3. Management Information Base : MIB consists of information of resources that are to be managed. These information is organised hierarchically. It consists of objects instances which are essentially variables.

SNMP messages : Different variables are :

1. GetRequest : SNMP manager sends this message to request data from SNMP agent. It is simply used to retrieve data from SNMP agent. In response to this, SNMP agent responds with requested value through response message.

2. GetNextRequest : This message can be sent to discover what data is available on a SNMP agent. The SNMP manager can request for data continuously until no more data is left. In this way, SNMP manager can take knowledge of all the available data on SNMP agent.

3. GetBulkRequest : This message is used to retrieve large data at once by the SNMP manager from SNMP agent. It is introduced in SNMPv2c.

4. SetRequest : It is used by SNMP manager to set the value of an object instance on the SNMP agent.

5. Response : It is a message send from agent upon a request from manager. When sent in response to Get messages, it will contain the data requested. When sent in response to Set message, it will contain the newly set value as confirmation that the value has been set.

6. Trap : These are the message send by the agent without being requested by the manager. It is sent when a fault has occurred.

7. InformRequest : It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is same as trap but adds an acknowledgement that trap doesn't provide.

SNMP security levels : It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely:

1. noAuthNoPriv : This (no authentication, no privacy) security level uses community string for authentication and no encryption for privacy.

2. authNopriv : This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.

3. authPriv : This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses DES-56 algorithm.

SNMP versions : There are 3 versions of SNMP:

1. SNMPv1 : It uses community strings for authentication and use UDP only.

2. SNMPv2c : It uses community strings for authentication. It uses UDP but can be configured to use TCP.

3. SNMPv3 : It uses Hash based MAC with MD5 or SHA for authentication and DES-56 for privacy.This version uses TCP. Therefore, conclusion is the higher the version of SNMP, more secure it will be.

Section – D

Q.8. What do you mean by Cryptography ? Explain its working with proper diagram. **(15)**

Ans. Cryptography refers to the science and art of transforming messages to make them secure and immune to attacks. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration but can also be used for user authentication.

Components : There are various components of cryptography which are as follows :

(i) *Plaintext and Ciphertext* : The original message, before being transformed, is called plaintext. After the message is transformed, it is called ciphertext. An encryption algorithm transforms the plaintext into ciphertext; a decryption algorithm transforms the ciphertext back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

(ii) *Cipher* : We refer to encryption and decryption algorithms as ciphers. The term cipher is also used to refer to different categories of algorithms in cryptography. This is not to say that every sender-receiver pair needs their very own unique cipher for secure communication. On the contrary, one cipher can serve millions of communicating pairs.

(iii) *Key* : A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key, and plaintext. These create the ciphertext. To decrypt a message, we need a decryption algorithm, a decryption key, and the ciphertext. These reveal the original plaintext.

Techniques used For Cryptography : In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

1. *Confidentiality* : Information can only be accessed by the person for whom it is intended and no other person except him can access it.

2. *Integrity* : Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

3. *Non-repudiation* : The creator/sender of information cannot deny his or her intention to send information at later stage.

4. *Authentication* : The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography : In general there are three types Of cryptography:

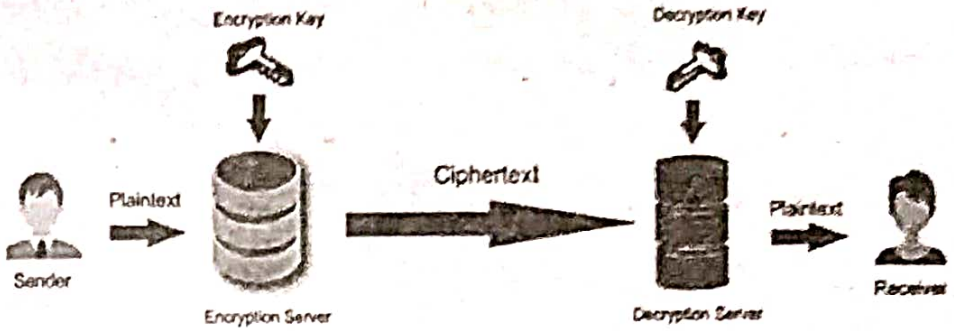
1. *Symmetric Key Cryptography* : It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

2. *Hash Functions* : There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

3. *Asymmetric Key Cryptography* : Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is

known by everyone the intended receiver can only decode it because he alone knows the private key.

Working Of Cryptography :



As shown above in the figure this is working of cryptography. There are two parties named as sender and receiver. The original message is called as Plaintext. This Plaintext sends sender in the encryption server. Where encryption algorithm is applied with the secret key and gives encrypted output as Ciphertext.

This Ciphertext is encrypted output which goes from public domain into the decrption server. Where decryption algorithm is applied with the secret key and gives output Plaintext or original message.

Q.9. Explain the following : (15)

(a) QoS Improving Techniques

(b) WAN

Ans. (a) Techniques to Improve QoS : Techniques that can be used to improve the quality of service as follows scheduling, traffic shaping, admission control and resource reservation.

(i) Scheduling : Packets from different flows arrive at a switch or router for processing. A good scheduling technique treats the different flows in a fair and appropriate manner. Several scheduling techniques are designed to improve the quality of service. Three of them here: FIFO queuing, priority queuing, and weighted fair queuing.

(1) *FIFO Queuing* : In first-in, first-out (FIFO) queuing, packets wait in a buffer (queue) until the node (router or switch) is ready to process them. If the average arrival rate is higher than the average processing rate, the queue will fill up and new packets will be discarded. Fig.(1) shows a conceptual view of a FIFO queue.

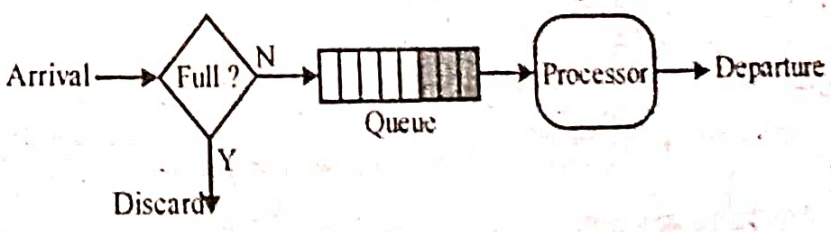


Fig.(1) : FIFO queue

(2) *Priority Queuing* : In priority queuing, packets are first assigned to a priority class. Each priority class has its own queue. The packets in the highest-priority queue are processed first. Packets in the lowest-priority queue are processed last. Note that the system does not stop serving a queue until it is empty.

Fig.(2) shows priority queuing with two priority levels (for simplicity).

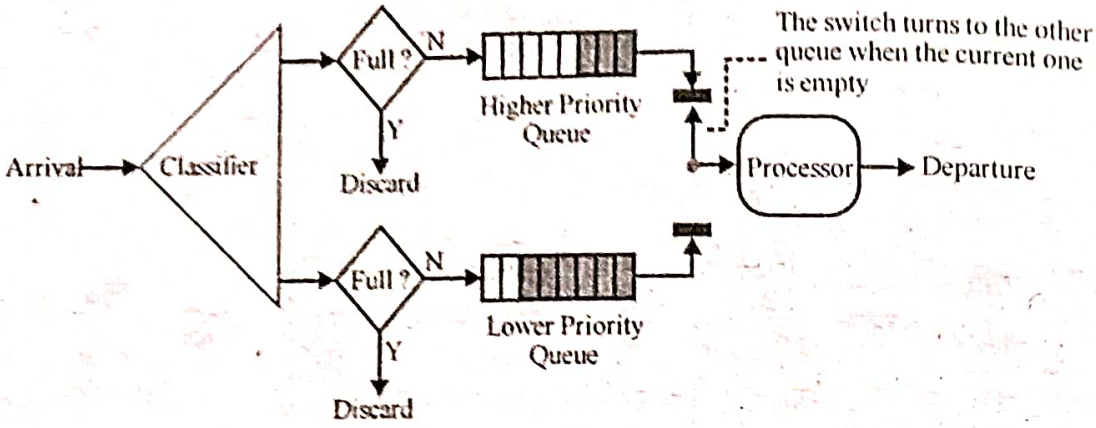


Fig.(2) : Priority queuing

A priority queue can provide better QoS than the FIFO queue because higher priority traffic, such as multimedia, can reach the destination with less delay.

(3) *Weighted Fair Queuing* : A better scheduling method is weighted fair queuing. In this technique, the packets are still assigned to different classes and admitted to different queues. The queues, however, are weighted based on the priority of the queues; higher priority means a higher weight. The system processes packets in each queue in a round-robin fashion with the number of packets selected from each queue based on the corresponding weight.

(ii) Traffic Shaping : Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network. Two techniques can shape traffic: leaky bucket and token bucket.

(1) *Leaky Bucket* : A technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate.

A simple leaky bucket implementation is shown in Fig.(3). A FIFO queue holds the packets. If the traffic consists of fixed-size packets, 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.

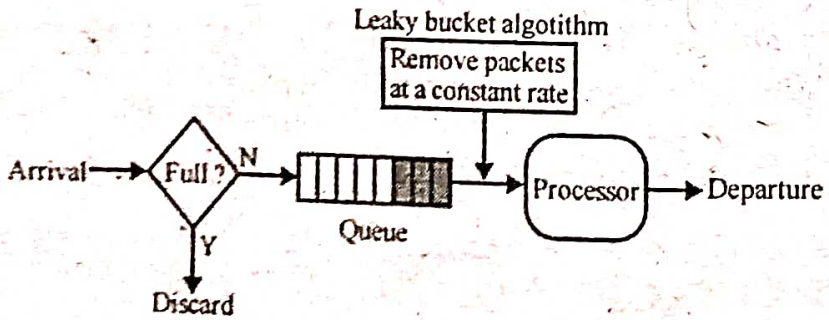


Fig.(3) : Leaky bucket implementation

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.

(2) *Token Bucket* : The token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens. For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every cell (or byte) of data sent. For example, if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens. Now the host can consume all these tokens in one tick with 10,000 cells, or the host takes 1,000 ticks with 10 cells per tick. In other words, the host can send bursty data as long as the bucket is not empty. Fig.(4) shows the idea.

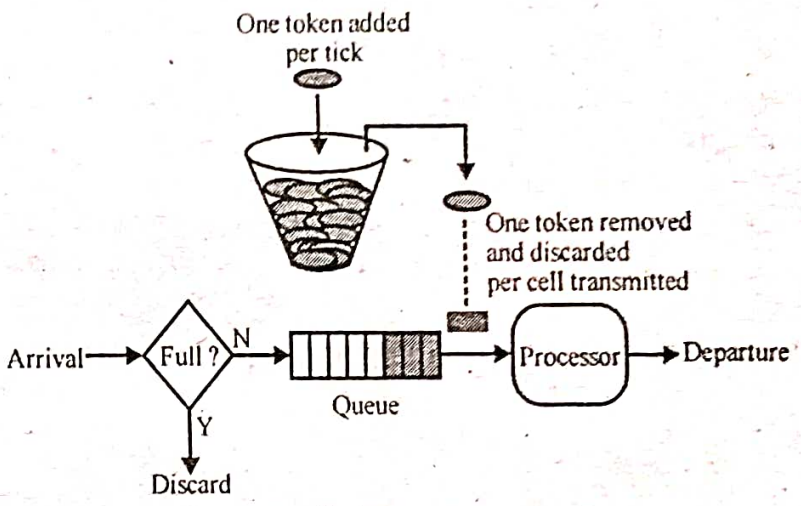


Fig.(4) : Token bucket

(iii) Resource Reservation : A flow of data needs resources such as a buffer, bandwidth, CPU time, and so on. The quality of service is improved if these resources are reserved beforehand.

(iv) Admission Control : Admission control refers to the mechanism used by a router, or a switch, to accept or reject a flow based on predefined parameters called flow specifications. Before a router accepts a flow for processing, it checks the flow specifications to see if its capacity (in terms of bandwidth, buffer size, CPU speed, etc.) and its previous commitments to other flows can handle the new flow.

Ans.(b) Introduction to Wireless LAN : Wireless LAN stands for Wireless Local Area Network. It is also called LAWN (Local Area Wireless Network). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.

The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). It also uses an encryption method i.e. wired equivalent privacy algorithm. Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.

In some instance wireless LAN technology is used to save costs and avoid laying cable, while in other cases, it is the only option for providing high-speed internet access to the public. Whatever the reason, wireless solutions are popping up everywhere.

Examples of WLANs that are available today are NCR's waveLAN and Motorola's ALTAIR.

Advantages of WLANs : (i) *Flexibility* : Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).

(ii) *Planning* : Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.

(iii) *Design* : Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.

(iv) *Robustness* : Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.

(v) *Cost* : The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, after providing wireless access to the wireless network via an access point for the first user, adding additional users to a network will not increase the cost. And second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.

(vi) *Ease of Use* : Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

Disadvantages of WLANs :(i) *Quality of Services* : Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.

(i) *Proprietary Solutions* : Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.

(ii) *Restrictions* : Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.

(iii) *Global operation* : Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.

(iv) *Low Power* : Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.

(v) *License free operation* : LAN operators don't want to apply for a special license to be able to use the product. The equipment must operate in a license free band, such as the 2.4 GHz ISM band.

(vi) *Robust transmission technology* : If wireless LAN uses radio transmission, many other electrical devices can interfere with them (such as vacuum cleaner, train engines, hair dryers, etc.).Wireless LAN transceivers cannot be adjusted for perfect transmission is a standard office or production environment.