B.E.

Sixth Semester Examination, May-2009

Computer Networks (IT-305E)

Note : Attempt any *FIVE* questions out of eight.

Q. 1. What are network topologies? Explain any four in detail, with the help of diagrams and also enlist their practical applications.

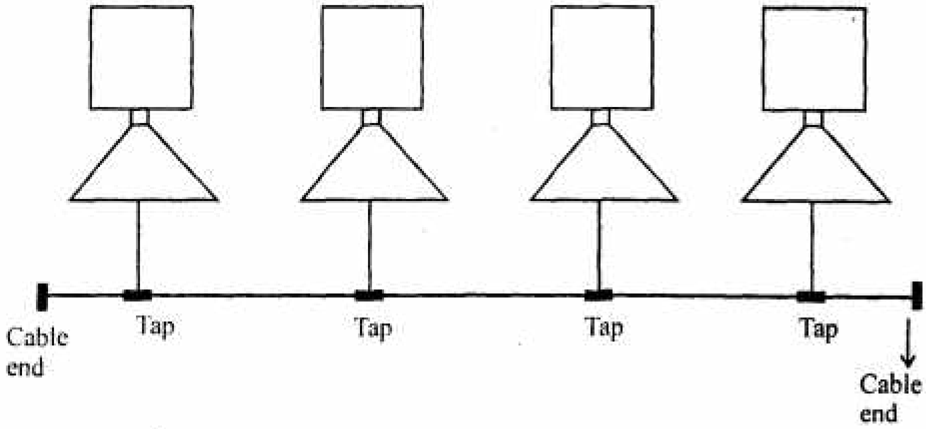
Ans. Network Topologies : Network topology describes the layout or appearance of a network that is, how the computers, cables and other components within a data communication network are interconnected both physically and logically. The physical topology describes the way in which a network is physically laid out and the logical topology describes how data actually flow through the network.

There are five basic network topology :

(i) Mesh topology
(ii) Star topology
(iii) Bus topology
(iv) Ring topology
(v) Tree topology.

(i) Bus Topology : A bus topology is a multipoint data communication circuit that makes it relatively simple to control data flow between and among the computers.

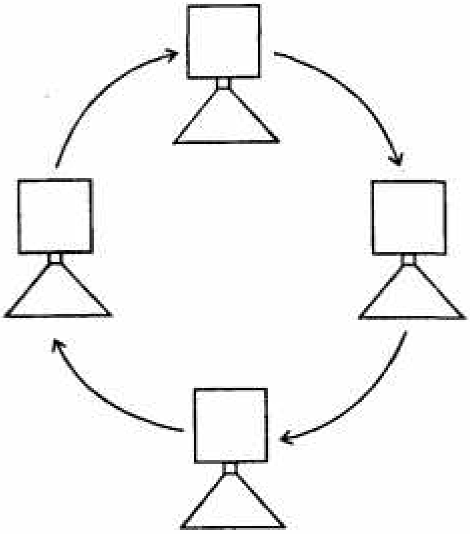
When one computer sends a signal upto the cable, all the computers on the network receive the information, but the one with the address that matches the one encoded in the message accepts the information while all others reject the message.



Bus Topology

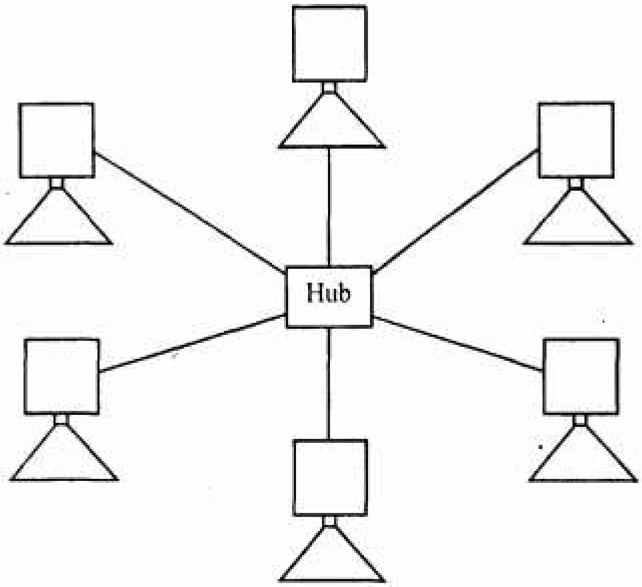
(ii) Ring Topology : In a ring topology, each computer is connected to the next computer, with the last one connected to the first as shown in fig.

Ring are used in high performance networks where large bandwidth is essential e.g., time attractive features such as video and audio.



Ring Topology

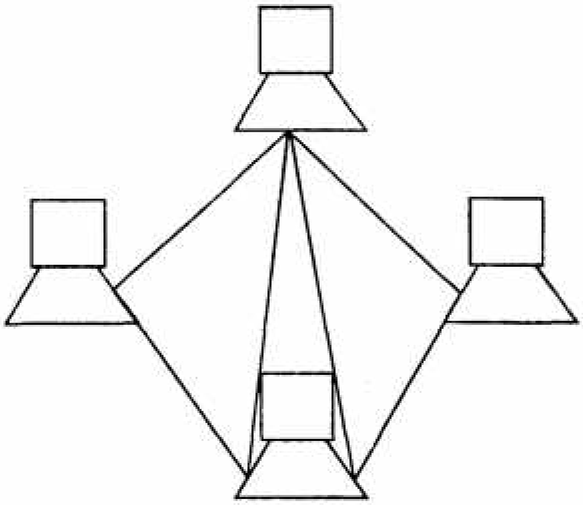
3. Star Topology : In star topology, all the cables run from the computers to a central location where they are all connected by a device called a hub.



Star Topology

Stars are used in concentrated networks, where the end points are directly reachable from a central location when network expansion is expressed and when the greater reliability of a star topology is required.

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



Mesh Topology

The term dedicated means that the link carries traffic only between two devices it connects. A fully connected mesh network therefore. has $n(n-1)/2$ physical channels to link, n_n devices.

To accommodate those links, every device on the network must have $(n-1)$ input output ports.

Q. 2. What is OSI Model? Explain function of each layer in detail. Also explain protocols of each layer.

Ans. OSI Model : OSI model is based on a proposal developed by a International Standards Organization (ISO) as a first step toward international standardization of protocols used in various layers. The model is called ISO. OSI (Open Systems Interconnection) reference model because it deals with connecting open system.

OSI model has seven layers :

(i) Physical Layer : The physical layer is concerned with transmitting raw bits over a communication channel.

(ii) Data Link Layer : Function of this layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer.

(iii) The Network Layer : The network layer controls the operation of subnet. A key design issue is determining how packets are routed from source to destination.

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

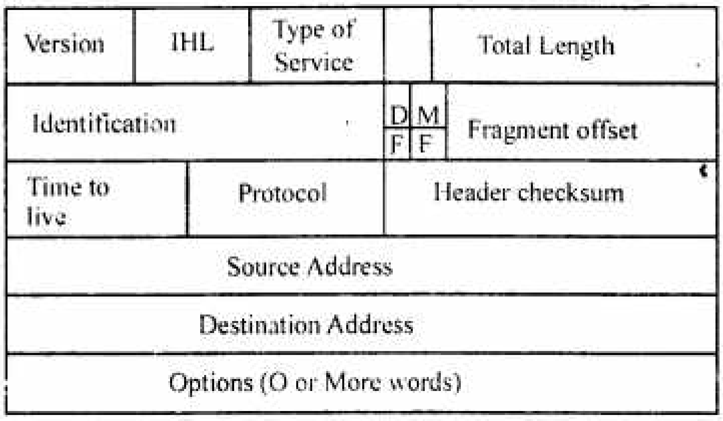
5. The Session Layer : The session layer allows user on different machines to establish sessions between them. Sessions offer various services, including dialog control, token management and synchronization.

6. The Presentation Layer : This layer is concerned with syntax and semantics of the information transmitted. The presentation layer manages there abstract data structured and allows higher-level data structures, to be defined and exchanged.

7. The Application Layer : This layer contains a variety of protocols that are commonly needed by user. One widely used protocol is HTTP (Hyper Text Transfer Protocol).

Q. 3. (a) Compare and contrast Internet and transmission control protocols.

Ans. Internet Protocol : The format of Internet Protocol consist of IP datagrams. An IP datagram consist of a header part and text part. The header has 20 byte fixed part and a variable length optional part. The header format is shown in fig.



Internet Protocol Header

It is transmitted in bigendian order : from left to right, with the high order bit of the version field going first. Since the reader length is not constant, a field in the header. IHL is provided to tell how long the header is, in 32 bit words.

The type of service is one of the few fields that has changed its meaning over the years.

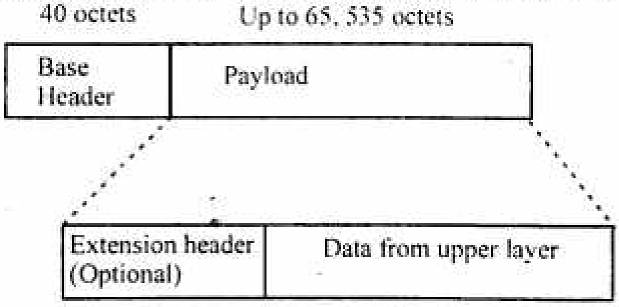
Transmission Control Protocol : TCP was specifically designed to provide a reliable end to end byte stream over an unreliable internet work. An internet work differs from a single network because different parts may have widely different topologies, delays bandwidth, packet sizes and other parameters.

Each machine supporting TCP has a TCP transport entity, either a library procedure, a user process or part of kernel. It manages TCP stream sand interfaces to IP layer. A TCP entity accepts user data streams from local processes, breaks them up into pieces not exceeding 64KB and sends each piece as a separate IP datagram. When datagrams containing TCP data arrive at a machine. They are given to the TCP entity which reconstructs the original byte stream.

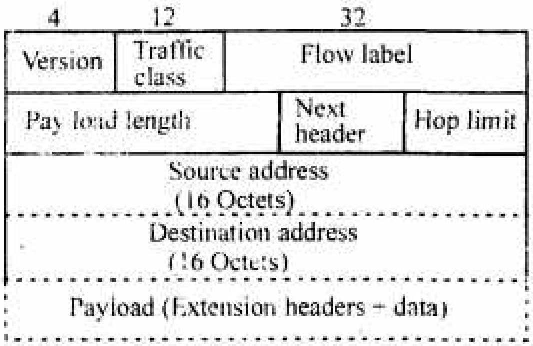
Q. 3. (b) What is IP version 6? Explain with the help of a suitable example.

Ans. IP Version 6 (IPV6) Internet Protocol : IPV6 is the next generation of internet protocol that will replace IPV4.

Format of IPV6 Packet : Fig. shows the format of IPV6 packet. It consists of a fixed base header followed by payload. The payload consists of optional extension headers and data octets from the upper layer.



(a)


4
12
32
Version
Traffic class
Flow label
Pay load length
Next header
Hop limit
Source address (16 Octets)
Destination address (16 Octets)
Payload (Extension headers + data)

(b)

Fig. IPV6 Packet Format

The base header has fixed length of 40 octets. It consist of the following fields :

(i) Version (4 bits) : It indicates the version of internet protocol which is 6 for IPV6.

(ii) Traffic Class (8 bits) : It is used for specifying the class of traffic to which the IP packet belongs. It decides the priority level to IP packets by a router.

(iii) Flow Label (20 bits) : It is used to identify all the packets in an individual flow.

(iv) Payload Length (16 bits) : It indicates number of octets present in the pay load. Muximum payload length can be 65, 535 octets.

(v) Next Header (8 bits) : It describes the next header after the base header. The next header can be an extension header or header of the upper layer.

(vi) Hop Limit (8 bits) : It is decremented by one on each hop.

Q. 4. (a) Explain in detail IEEE 802 standards.

Ans. IEEE 802 standards : The institution of electrical and electronics engineers (IEEE) has developed the layered architecture and other standards of LAN. 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 → Metropolian Area Network (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

Q. 4. (b) Explain various LAN interconnecting devices.

Ans. (I) Repeater : This is a physical layer device that restores data and collision signals and transmits all traffic between segments including collision information. It increases network diameter and allows additional users access while acting as an amplifier to boost the signal. Today's advance repeater or hub can detect and disconnect faulty segments by applying an "auto-partition" scheme. An example of repeater (hub) implementation in an enterprise network is given in Fig. The link between two hubs or repeaters is called an IRL or inter-repeater link. It is a point-to-point link which extends the whole distance between the segments. A number of link media types are available, such as fiber optic IRL (1000 m), coax IRL, and vendor dependent IRL.

(II) Switch : Traditionally, to resolve an overloaded LAN, bridges were used to segment the network. Since then more and more demand on bandwidth network management, traffic analysis and faster transmission has driven engineers to develop a faster bridge with less cost per port, and a bigger back plane or exoplane to accommodate traffic today. Actually, Ethernet switches represent an expansion of the concepts in Ethernet bringing. A number of attributes differentiate bridges from switches. They are as follows :

(i) Switches are designed to provide high speed.

(ii) Each port represents a segment providing a number of LAN segments within a switching limit.

(iii) Switches can be "cut-through" and "store and forward."

(iv) Switch can provide second-layer, third-layer and fourth-layer (under experiment) support.

(v) Advance filtering and management capability.

(vi) Exotic backplane, typically 2 Gbps.

(vii) Multilink trunk (MLT) capability.

(viii) Stack or non-stack options etc.

(III) Bridge : A bridge is a data link layer device connecting two or more collision domains. MAC multicastes are throughout "extended LAN". An overloaded LAN can be segmented using a bridge. According to the IEEE 802.1 D specification, a MAC bridge in an 802.3 LAN works under the MAC service boundary, that is MAC service and LLC layers are transparent to it. Today, bridges are mostly replaced by switches. A bridge copies frames from one LAN to another of the same type or some extent to a different type of LAN. Bridges make decisions about which frames to copy, based on observations of SAs in received frames. This makes them extremely useful for traffic management in LANs. They can also usually be configured to filter frames based on address. A bridge port (or network interface) operates in promiscuous mode, accepting all frames. Frames are internally buffered, and the DA is compared to all of the addresses in a forwarding database.

IV) Routers : Routers work in a manner similar to switches and bridges, in that they filter network traffic by specific protocols rather than doing so by packet address. The devices were bron out of the necessity for the logical division of a network instead of a physical division. For example, an IP router can divide a network into various subnets so that traffic destined for a particular IP address can pass between segments. Such filtering takes more time than that used by a switch or bridge which only looks at the Ethernet address. When implementing a router in more complex network, network efficiency improves. Until now, very few switches have been able to provide interfaces such as Packet over SONET. Frame Relay, ATM over SMDS, SONET and or TI technologies. Therefore, a router still has significant and diversified features often unavailable in a switch.

Gateway : The traditional approach of bridges and routers is to solve internetwork problems in an environment where all of the device implement compatible protocols at the corresponding layers of the OSI model. For example, layer 3 protocols (IP, IPX, etc.) for routers and layer 2 (MAC) for bridges. The implementation of bridges and routers is the ideal situation towards which a business organization should strive. However, there are circumstances where one internetworking architecture needs to talk with a different architecture : For example, OSI to SNA and or DEC-Net to SNA internetworking support. The gateway provides a way to permit the coexistence of OSI-based and proprietary products, and gives the manager the tools needed to plan and implement a smooth migration to an exclusive OSI strategy. We should not confuse it with the "gateway" word in the IP addressing scheme, which is used to identify the pathway for a host to different routed segment or hop. For example, if a station with IP address 192.97.4.200 wants to reach another station (192.97.6.17), it has to depend on the gateway or routed interface 192.97.4.1 as shown in fig. The gateway that we are trying to understand is the "application-level gateway."

Q. 5. (a) What is congestion in WAN? How it is controlled?

Ans. Congestion in WAN : Congestion is a network may occur if users send data into the network at a rate greater than that allowed by network resources.

For Example : Congestion may occur because the switches in a network have a limited buffer size to store arrived packets before processing.

Congestion Avoidance : For congestion avoidance, the frame relay network uses two bits in the frame to explicitly warn the source and the destination of the presence of congestion.

(a) BECN : The backward explicit congestion notification (BECN) bit warns the sender of congestion in network. One might ask how this is accomplished since the frames are travelling away from the sender. There are two methods :

(i) The switch can use response frames from the receiver or else.

(ii) Switch can use a predefined connection to send special frames for this specific purpose.

(b) FECN : The forward explicit congestion notification (FECN) bit is used to warn the receiver of congestion in the network. It might appear that the receiver cannot do anything to relieve the congestion.

For Example : If there is an acknowledgment mechanism at this higher level, the receiver can delay the acknowledgement. Thus, forcing the sender to slow down.

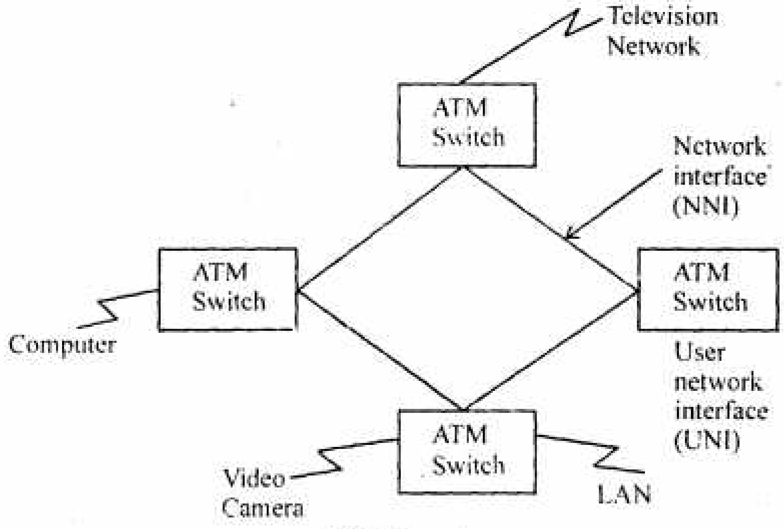
Four Situations : When two DTES are communicating using a Frame Relay network, Four situations may occur with regard to congestion. Fig. (2) shows there four situations.

Four Situations : When two DTEs are communicating using a Frame Relay network, Four situations may occur with regard to congestion. Fig. (2) shows there four situations.

Discarding : If users do not respond to the congestion notices, the frame relay network has to discard frames. Which frames are discarded called traffic control.

Q. 5. (b) Explain ATM? Why it is used? What are the various security concerned related to it? How they can be reduced or eliminated?

Ans. ATM (Asynchronous Transfer Mode) : ATM is a cell switched network. The user access devices, called the end points are connected through a user to network interface (UNI) to the switches, inside the network. The switches are connected through network to network interfaces (NNIs).



ATM Network

Virtual Connection : Connection between two endpoints is accomplished through transmission paths (TPs), virtual paths (VPs) and virtual circuits (VCs).

A transmission path (TP) is the physical connection (wire, cable, satellite and so on) between an end point and a switch or between two switches.

A virtual path (VP) provides a connection or a set of connections between two switches.

Cell networks are based on virtual circuits (VCs).

ATM in WAN : ATM is used to connect WANs or LANs together with router serving as an end point. The router has two stacks of protocols; one belonging to ATM and other belonging to other protocol.

ATM in LANs : ATM is a connection oriented protocol, while traditional LANs are connectionless. The addressing is different in connectionless protocols. Traditional LANs offer multicasting and broadcasting of packets, whereas ATM does not.

Q. 6. Explain in detail all the remote monitoring schemes while managing a network.

Ans. Remote Monitoring :

The invention discloses a remote network monitoring method of computer network. It is an improvement of the RMON (Remote Network Monitoring) alarm group. The method mainly includes: Setting an alarm-extended table in the RMON alarm group; Defining a combination object in MIB (Management Information Base) that is an expression with two or more than two independent objects; A network management center sends a Set-Request packet with the expression to managed devices to initiate a RMON monitoring process; The expression is calculated and its value is compared with a threshold; When calculated value of the expression exceeds the threshold, processing steps preset by the network management center are taken. The invention supports SNMP (Simple Network Management Protocol), optimizes network performance, and saves network bandwidth and CPU resource of the network management center.

(i) A remote computer network monitoring method is that a network management center supports Simple Network Management Protocol (SNMP) and implements remote network monitoring alarm through describing an independent object of a managed device and its attribute in a Manage Information Base (MIB) and comparing statistic value of the independent object with a preset threshold; comprising : A in the MIB, defining an alarm extended table of Remote Network Monitoring (RMON) that has a combination object combined with at least two independent objects through operation expression; B sending a Set-Request packet with said operation expression to the managed device by the network management center; C in the managed device, sampling values of every independent object in the operation expression and calculating said combination object according to the operation expression, and then comparing calculated result with the preset threshold; if calculated result exceeds the threshold, then making process with steps preset by said network management center.

(ii) The remote computer network monitoring method according to claim 1, further comprising, defining a set of objects which concern about monitoring duration in said alarm-extended table; ending a monitoring process automatically until the monitoring process exceeds its monitoring duration.

(iii) The remote computer network monitoring method according to claim 1, said step B comprising, through running an alarm-extended application program, the network management center sending the SNMP Set-Request packet to the managed device and setting the combination object and its attribute.

(iv) The remote computer network monitoring method according to claim 1, executing said step C based on a preset sampling period.

(v) The remote computer network monitoring method according to claim 1, before step C further comprises a step of checking and analyzing the operation expression, which includes parsing a character-string data information of the operation expression from said Set-Request packet and checking whether said character-string data information satisfies syntax rules of four fundamental operations of arithmetic, analyzing whether all independent objects of said in the operation expression can be sampled at said managed device; initiating a monitoring process for the combination object if said checking and analyzing have been passed.

(vi) The remote computer network monitoring method according to claim 5, further comprising, if said character-string data information cannot satisfy syntax rules of four fundamental operations of arithmetic, reporting to said network management center that said Set-Requesting is failure and ending; if said independent objects cannot be sampled from the managed device, reporting to said network management center that set request is failure and ending.

(vii) The remote computer network monitoring method according to claim 5, the combination object is OCTECT STRING data type and each of the independent objects is represented by integers separated by points.

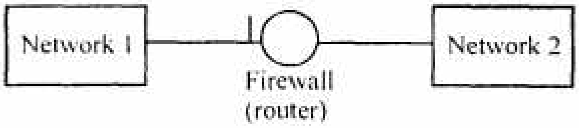
(viii) The remote computer network monitoring method according to claim 1, said managed device is a node device or an interface device for network signal transmission supporting SNMP of sub-networks.

(ix) The remote computer network monitoring method according to claim 1, the step of making process with steps preset by said network management center in the step C comprising, sending Trap packet to the network management center or logging.

Q. 7. (a) What is the concept of firewall? How they are installed? Upto what extent they are effective as far as security is concerned?

Ans. Firewalls : Firewall is a specially programmed router. It is programmed to filter packets that flow through it.

For Example : It may discard IP packets addressed to a particular address or TCP port.



There are two category of firewalls :

(i) Filter based firewalls.

(ii) Proxy-based firewalls.

(i) Filter Based Firewalls : There are simple and widely deployed. A filter based firewall router is configured with a table of addresses that decides whether a packet will be forwarded or not.

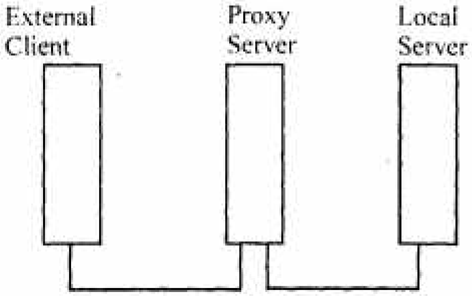
This approach is simple but with following limitations :

(i) The number of well known ports keeps growing. So, the filter is to be continuously updated.

(ii) Port number can be assigned dynamically and users can chore their own port numbers. Thus, tracking port numbers is impossible for filter configuration.

(iii) The firewall can be penetrated using tunneling where in an IP packet is encapsulated in another packet.

(ii) Proxy Based Fire Walls : Proxy is a process that sets between a client and server. To the client, it appears to be the server and to the server it appears to be client. Fig. shows proxy based firewalls.



Proxy Based Firewall

Remote users log into the proxy server and send their HTTP request that contains the URL. The proxy server establishes TCP connection to the local server if the requested page is allowed. When it receives response from the local server, the proxy forwards it to the client. If the requested page is not allowed, the proxy does not establish connection to the local server. It responds on its own to the client giving indication of an error.

Proxy Based Firewalls Having Some Limitations :

(i) It does not provide security against the internal attacks, i.e., a client within a network, may breach the security.

(ii) With advent of wireless communications any user can have at least physical access to the network. If access is allowed to a genuine mobile user. There is nothing to prevent on unauthorized user to gain access to the network.

Q. 7. (b) What is the need of network operating system? Draw and explain the architecture of client server.

Ans. Uses of Network Operating Systems :

(i) Business Application : May companies have a substantial number of computers. For example a company may have separate computers to monitor production, keep track of inventories and do the payroll. Initially, each of computers may have worked in isolation from others, but at some point, management may have decided to connect them to be able to extract and correlate information about the entire company.

(ii) Home Applications : The biggest example for this application is Internet access.

Some of the popular uses of internet for home users are as follows :

(i) Access to remote information.

(ii) Person to person communication.

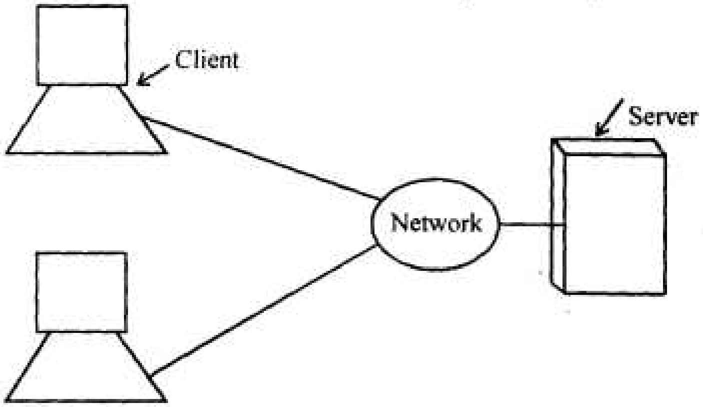
(iii) Interactive entertainment.

(iv) Electronic commerce.

(iii) Mobile Users : Mobile computers, such as note book, computers and personal digital assistants, are one of the fastest growing segments of computer industry.

(iv) Social Issues : The wide spread introduction of networking has introduced new social, ethical, and political problems. A popular feature of many networks are news groups on bulletin boards whereby people can exchange messages with like minded individuals.

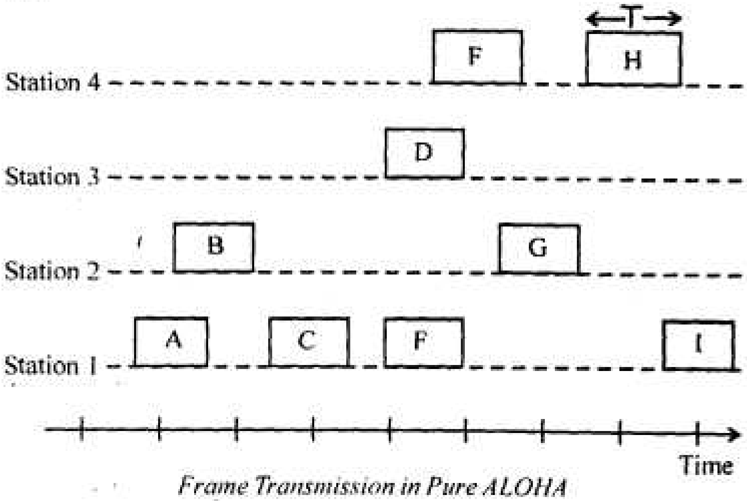
Client Server Model : In this model, data are stored on powerful computers called servers often there are centrally housed and maintained by a system administrator. In contrast, the employees have simpler machines, called clients, on their desk with which they access remote data. For example to include in spreadsheets. They are constructing. The client and server machines are connected by a network, as shown in fig. (1).



Q. 8. Write short notes on :

(a) ALOHA **(b) HTTP** **(c) SONET.**

Ans. (a) ALOHA :



Frame Transmission in Pure ALOHA

ALOHA contention access mechanism derives its name from its first implementation in ALOHA Packet Radio Network. The network was based on a single radio channel for several stations to communicate with each other. The original contention access mechanism is so, referred to as Pure ALOHA. The basic scheme is as follows :

(i) All the stations share a common radio channel for transmitting their data frames.

(ii) A station can transmit its data frame on the radio channel whenever it wants. There is a pre-assigned time or sequence in which the station transmit.

(iii) When a transmission is in progress if another station initiates its transmission, collision of two transmission occurs.

(iv) A mechanism to detect collision is established.

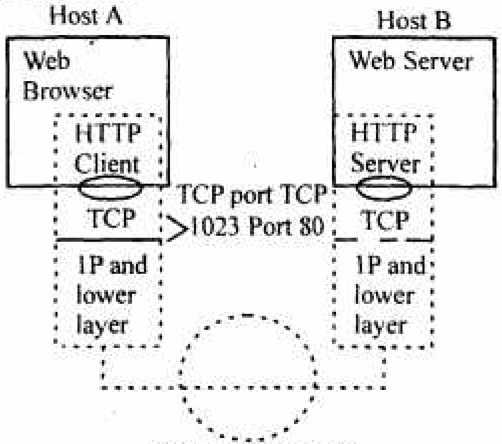
Fig. shows transmission of data frames by four stations. Data frames A, B, C, D, E and F get corrupted during transmission due to collisions with other frames. Data frames C, G, H and I are successfully transmitted.

(b) HTTP : Hypertext Transfer Protocol (HTTP) : HTTP is used for transporting WWW documents between the client (web browser) and server (web server). HTTP is running on the well known TCP port 80 for the server. The basic operation consists of three steps :

(i) The client opens a TCP connection and sends request for a document.

(ii) The server responds with the document.

(iii) The server closes the connection.



HTTP Architecture

HTTP messages from the client to the server are called HTTP request messages. HTTP messages from the server to the client are called response messages. There message consist of a header and a body. The body contains data described by a MIME header. The data can be HTML document (web page), graphic, video or sound.

(c) SONET : The ANSI standard is called SONET and the ITU-T standard is called SDH. Both standards are nearly identical.

A single clock handles the timing of transmission and equipment across the entire network. This network wide synchronization adds a level of predictability to the system.

A SONET regenerator takes a received optical signal and regenerates it. The SONET regeneration also replaces some of the existing overhead information with new information.

The photonic layer includes physical specifications for the optical fibre channel. The receiver and multiplexing functions as well as specifications regarding the method of encoding. The session layer handles framing, scrambling and error control. The line layer is responsible for moving the signal across a physical line.