B.E.

Fifth Semester Examination, December-2007

Computer Networks (IT-305-E)

Note : Attempt any five questions. All questions carry equal marks.

Q. 1. (a) What do you mean by Computer Network ? Discuss its various advantage and disadvantage. **20**

Ans. Computer Network to mean an interconnected collection of autonomous computers. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire; fibre optics, microwaves and communication satellites can also be used. By requiring the computers to be autonomous, we wish to exclude from our definition systems in which there is a clear master/slave relation. If one computer can forcibly start, stop, or control another one, the computers are not autonomous.

Advantages :

(i) Resource Sharing : This advantage make all programs, equipment and especially data available to anyone on the network without regard to the physical location of the resource and the user.

(ii) High Reliability : Network provide high reliability e.g., all files could be replicated on two or three machines, so if one of them is unavialable (due to a hardware failure), the other copies could be used. In addition, the presence of multiple CPUs means that if one goes down, the others may be able to take over its work, although at reduced performance.

(iii) Saving Money : Small computers have a much better price/performance ratio than large ones. Mainframes are roughly a factor of ten faster than personal computers, but they cost a thousand times more.

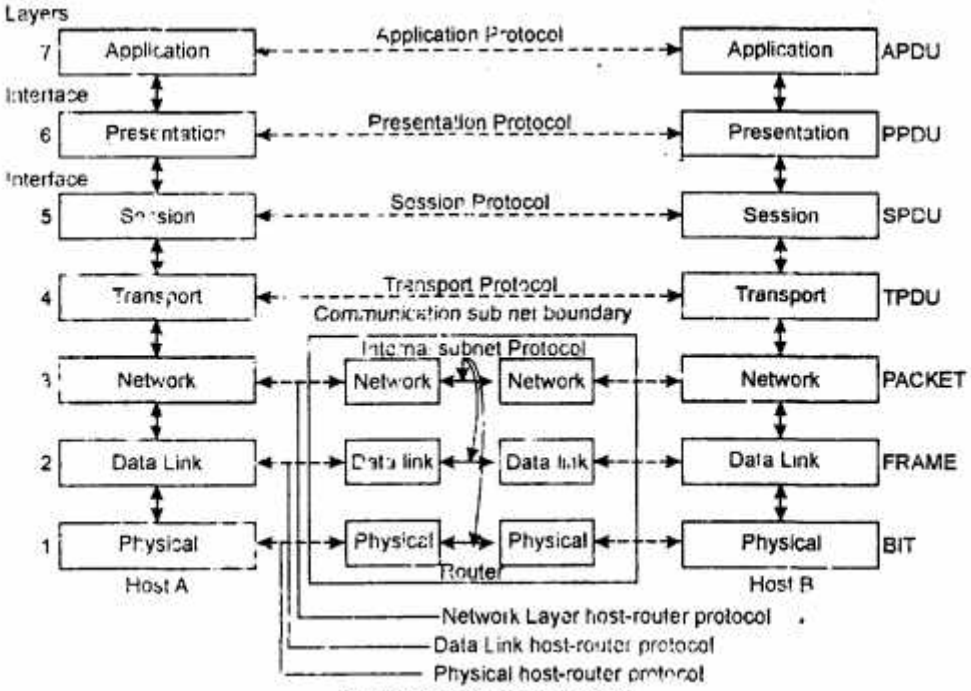
(iv) Scalability : Another networking advantage is scalability, the ability to increase system performance gradually as the workload grows just by adding more processors. With centralized mainframes, when the system is full, it must be replaced by a larger one, usually at great expense and even greater disruption to the users.

Disadvantages : The wide spread introduction of networking will introduce new social, ethical, political problems. A popular feature of many networks are news groups or bulletin boards where people can exchange messages with like minded individuals.

The trouble comes when news groups are set up on topics that people actually care about, like politics, religion or sex. High-resolution colour photographs and even short video clips can now easily be transmitted over computer networks. Some people take a live-and let-live view, but others feel that [illegible] certain material (e.g., child pornography) is simply unacceptable. Thus the debate rages.

Q. 1. (b) Explain OSI reference model in brief. **8**

Ans. This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers. The model is called the ISO OSI (Operating System Interconnection) reference model because it deals with connecting open systems-that is, systems that are open for communication with other systems.



The OSI reference Model

The OSI model has seven layers. The principles that were applied to arrive at the layers are as follows :

(i) A layer should be created where a different level of abstraction is needed.

(ii) Each layer should perform a well defined function.

(iii) The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

(iv) The layer boundaries should be chosen to minimize the information flow across the interfaces.

(v) The number of layer should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

The OSI model itself is not a networking architecture because it does not specify the exact services and protocols to be used in each layer. It just tells what each layer should do. However, ISO has also produced standards for all the layers, although there are not part of the reference model itself. Each one has been published as a separate international standard.

Q. 2. Differentiate the following : **20**

(i) LAN, MAN, WAN

(ii) IPV6 and IPV4

(iii) Token bus and Token Ring

(iv) Bridges, Routers and Gateways

Ans. (i) LAN, MAN, WAN :

LAN : LAN (Local Area Network) is covered a short geographical distance to set a computer network. It may cover buildings, University Campus, Business Organization distance around 5 to 6 km maximum otherwise it remain with 1 or 2 km.

It is a high speed data exchange 10 mbps. It uses the expensive transmission media. It is a low error rate transmission. It covers maximum 1000 terminal in a network. It is privately owned network. It is a cheaper.

MAN (Metropolitan Area Network) : MAN is a bigger computer network than LAN. It cover nearly a corporate (business/commerical) offices in MAN. It is the extension of LAN networks. It covered entire city a geographical area distance can be around 40-50 km. The speed of MAN is 10-100 mbps, cable TV network or Telephone network is the example. A number of network of same or different topology and speed can connected via some interconnected devices may be bridge or repeaters etc.

WAN (Wide Area Network) : WAN is also like LAN but it covers long geographical distance to form networks. More than one dissimilar network can be communicated to each others.

There are two types of WAN :

(i) Public network run by government or group of company.

(ii) Private network run by company

Usage of WAN :

(i) It can connect computer to different site

(ii) It can connect more than one LAN

(iii) It operate at National level, Global World wide

(iv) Speed is slow instead of LAN

(v) Links and error are more than LAN.

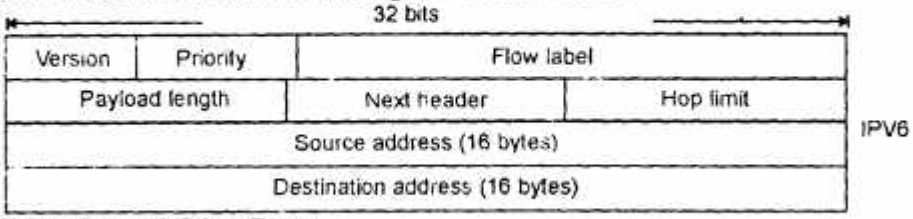
(ii) IPV6 and IPV 4 :

(i) The version fields is always 6 for IPV6 and 4 for IPV 4.

(ii) During the transition period from IPV4, which will probably take a decade, routers will be able to examine this field to tell what kind of packet they have.

(iii) The payload length field tells how many bytes follow the 40-bytes header. The name was changed from the IPV4 total length field because the meaning was changed slightly; the 40 header bytes are no longer counted as part of the length as they used to be.

(iv) The IPV6 address space is divided up. Addresses beginning with 80 zeros are reserved for IPV4 addresses. Two variants are supported, distinguished by the next 16 bits. These variants relate to how IPV6 packets will be tunneled over the existing IPV4 infrastructure.



(iii) Token Bus and Token Ring :

Token Bus : This standard, 802.4, describes a LAN called a token bus. Physically, the token bus is a linear or tree-shaped cable onto which the stations are attached. Logically, the stations are organized into

Version	IHL	Type of service	Total length
Identification		DF MF	Fragment offset
Time to live	Protocol	Header Checksum	
Source address			
Destination address			
Option (0 or more words)			

IPV4

a ring, with each station knowing the address of the station to its "left" and "right". When the logical ring

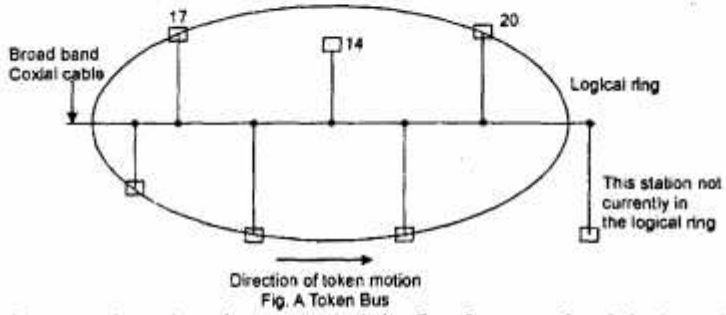


Fig. A Token Bus

is initialized, the highest numbered station may send the first frame. After it is done, it passes permission to its immediate neighbour by sending the neighbour a special control frame called a token. The token propagates around the logical ring, with only the token holder being permitted to transmit frames. Since only one station at a time holds the token, collisions do not occur.

The token bus uses the 75-ohms broadband coaxial cable used for cable television. Both single and dual-cable systems are allowed, with or without head-ends.

Token Ring : Ring networks have been around for many years (Pierce, 1972) and have long been used for both local and wide area networks.

In a token ring a special bit pattern, called the token, circulates around the ring whenever all stations are idle. When a station wants to transmit a frame, it is required to seize the and remove it from the ring before transmitting.

An application of the token ring design is that the ring itself must have a sufficient delay to contain a complete token to circulate when all stations are idle. The delay has two components : the 1-bit delay introduced by each station and the signal propagation delay.

Ring interfaces have two operating modes, listen and transmit. In listen mode, the input bits are simply copied to output, with a delay of 1 bit time. In transmit mode, which is entered only ofter the token has been seized, the interface breaks the conection between input and output, entering its own data onto the ring.

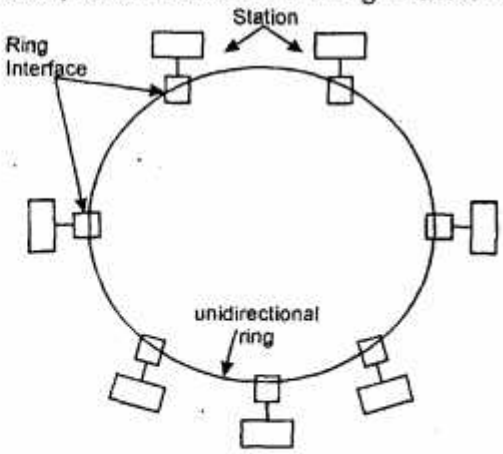
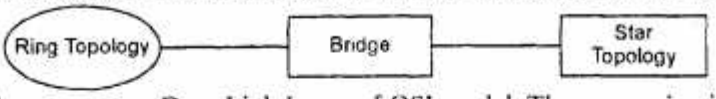


Fig. A RING NETWORK

(iv) Bridges, Routers and Gateways :

Bridges : It is a hardware device used to connect two or more different LAN of different topology

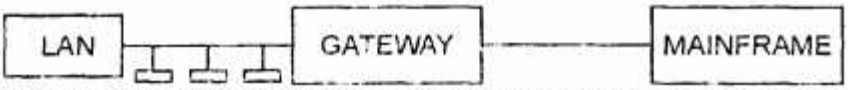


protocols. The bridge operate at Data Link Layer of OSI model. The processing is required minimal because all the protocol implement on Data Link Layer (DLL) Level.

Routers : It is a special hardware device connect two or more dissimilar LAN to form a WAN. Routers have an intelligent behaviour in all to send packets via correct path to reach the destination. It operates at network layer of OSI model. The different connected network can use similar or dissimilar protocols. Router have algorithms to calculate best suited path for packet-transmission over the network.

Gateways : It also used to connect two or more dissimilar LANs. It can share connection between LAN or MAIN FRAME or large packet switching network. It is a computer with microprocessor with memory hardware and related software etc.

Gateway convert the data packets of different size in one protocol format to another protocol format mean if a computer in network have TCP/IP protocol and other have IPX | SPX protocol use different size of packets. Gateway form or convert packet accordings to protocol needs by the destination network.



Q. 3. Explain ALOHA and CSMA protocols ? How CSMA/CD improve the performence of CSMA ? Explain. **20**

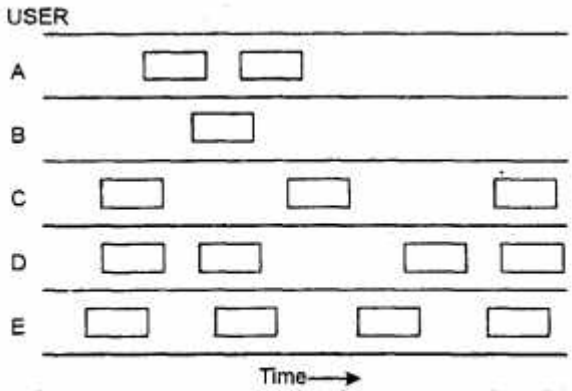
Ans. ALOHA : In the 1970s, Norman Abramson and his colleagues at the University of Hawaii devised a new and elegant method to solve the channel allocation problem. Abramson's work, called the ALOHA system, used ground-based radio broadcasting, the basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel.

There are two versions of ALOHA : pure and slotted. They differ with respect to whether or not time is divided up into discrete slots into which all frames must fit. Pure ALOHA does not require global time synchronization slotted ALOHA does.

Pure ALOHA : In pure ALOHA, we have made the frames all the same length because the through put of ALOHA systems is maximized by having a uniform frame size rather than allowing variable length frames. Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be garbled. If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later. The checksum connot distinguish between a total loss & and near miss.

Slotted ALOHA : In 1972, Roberts published a method for doubling the capacity of an ALOHA system. His proposal was to divide time up into discrete intervals, each interval corresponding to one frame. This approach requires the users to agree of slot boundaries.

In Robert's method, which has come to be known as slotted ALOHA, in contrast to Abramson's pure ALOHA; a computer is no permitted to send. Whenever a carriage return is typed. Instead, it is required to wait for the beginning of the next slot.



In pure ALOHA, frames are transmitted at completely arbitrary times.

CSMA Protocol (Carrier Sense Multiple Access Protocols) : Protocols in which stations listen for a carrier (i.e., a transmission) and act accordingly are called carrier sense protocols. CSMA are persistent and non-persistent.

Persistent and Non-persistent CSMA : 1-persistent (Carrier Sense Multiple Access), when a station has data to send, it first listens to the channel to see if anyone else is transmitted at that movement. If the channel is busy, the station waits until it becomes idle. When the station detects one idle channel, it transmits a frame. If a collision occurs, the station waits a random amount of time and starts all over again. The protocol is called 1-persistent because the station transmits with a probability of 1 whenever it finds the channel idle.

A second carrier sense protocol is non-presistent CSMA. In this protocol, conscious attempt is made to be less greedy than in the previous one. Before sending, a station senses the channel. If no one else is sending, the station begins doing so itself. However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission. Instead, it waits a random period of time and then repeats the algorithm.

CSMA with Collision Detecion : Persistent and non-persistent CSMA protocols are clearly an improvement over ALOHA because they ensure that no station begins to transmit when it senses the channel busy. Another improvement is for stations to abort their transmission as soon as they detect a collision. In other words, if two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately. Rather than finish transmitting their frames, which are irretrievably grabled anyway, they should abruptly stop transmittimg as soon as the collision is deteed. Quickly terminating damaged frames saves time and bandwidth. This protocol, known as CSMA/CD (Carrier Sense Multiple Access with Collision Detection), is widely used on LANs in the MAC sublayer.

Q. 4. (a) Explain Transmission control and userdatagram Protocol ? **10**

Ans.Transmission Control Protocol : TCP (Transmission Control Protocol) is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It fragments the incoming byte stream into discrete messages and passes each one onto the internet layer.

At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make. Sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

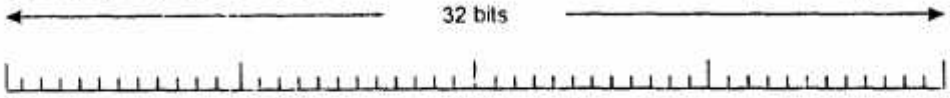
TCP was specifically designed to provide a reliable end-to-end byte stream over an unreliable inter network. An internetwork differs from a single network because different parts may have wildly different topologies, bandwidths, delays, packet sizes and other parameters. TCP was designed to dynamically adapt to properties of the interwork and to be robust in the face of many kinds of failures.

TCP was formally defined in RFC 793. TCP service is obtained by having both the sender and receiver create end points, called sockets. Each socket has a socket number (address) consisting of the IP address of the host and a 16-bit number local to that host, called a port. A TCP connection is a byte stream, not a message stream.

User Datagram Protocol (UDP) : The internet protocol suite also supports a connectionless transport protocol, UDP. UDP provides a way for applications to send encapsulated raw IP datagrams and send them wihout having to establish a connection.

A UDP segment consists of an 8-byte header followed by the data

The two ports serve the same function as they do in TCP : to identify the end points within the

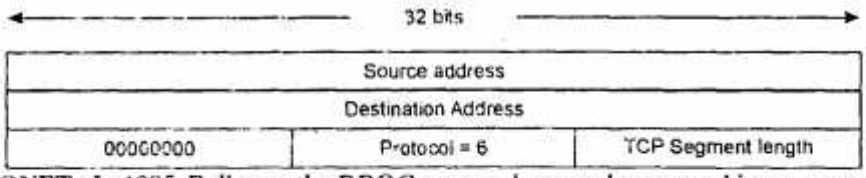


Source Port	Destination Port
UDP Length	UDP Checksum

The UDP Header

source and destination machines. The UDP length field includes the 8-byte header and the data. The UDP checksum includes the same format pseudo header, the UDP header and the UDP data, pool out to an even number of bytes if need be. It is optional and stored as 0 if not computed (a true computed 0 is stored as all 1s, which is the same in 1's complement).

Q. 4. (b) Explain SONET. **10**



Ans. SONET : In 1985, Bellcore, the RBOCs research curve, began working on a standard, called SONET (Synchronous Optical Network).

The SONET design had four major goals. First and foremost, SONET had to make it possible for different carriers to interwork. Achieving this goal required defining a common signaling standard with respect to wavelength, timing, framing structure and other issues.

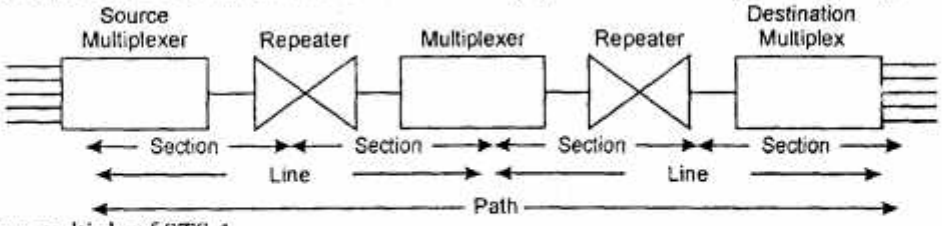
- Second, some means was needed to unity the U.S, European and Japanese digital system, all of which were based on 64-kbps PCM channels, but all of which combined them in different ways.

- Third, SONET had to provide a way to multiplex multiple digital channels together. At the time SONET was devised, the highest speed digital carrier actually used widely in the United States was T_3 , at 44.736 mbps. T_4 was defined , but not used much and nothing was even defined above T_4 speed.
- Fourth, SONET had to provide support for operation, administration and maintenance (OAM).

A SONET system consists of switches, multiplexes and repeaters, all connected by fibre. In SONET terminology, a fibre going directly from any device to any other device, with nothing in between is called a section. A run between two nultiplexer is called a line. Finally, the connection between the source and destination is called a path. The SONET topology can be mesh, but is often a dual ring.

The basic SONET frame is a block of 810 bytes put out every 125μ sec. Since SONET is synchronous, frames are emitted whether or not there are any useful data to send. Having 8000 frames/sec exaclty matches the sampling rate of the PCM channels used in all digital telephony systems.

The 810-byte SONET frames are best described as a rectangle of bytes, 90 columns wide by 9 rows high. Thus, $8 \times 810 = 6480$ bits are transmitted 8000 times per second, for a gross data rate of 51.84 mbps. This is the basic SONET channel and is called STS-1 (Synchronous Transport Signal-1). All SONET



trunks are a multiple of STS-1.

Q. 5. Explain following : **20**

(i) WAN Technologies

(ii) Wireless links

(iii) DQDB

Ans. (i) WAN Technologies : A wide area network or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user programs (hosts). The turn end system is sometimes also used in the literature. The hosts are connected by a communication subnet, or just subnet for short.

In most wide area networks, the subnets consists of two distinct components : Transmission lines and switching elements. Transmission lines (also called circuits, channels, or trunks) move bits between machines.

In most WANs, the network contains numerous cables or telephone lines, each one connecting a pair of routers. If two routers that do not share a cable nevertheless 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 subnet using this principle is called a point-to-point, store-and-forward or packet-switched subnet. Nearly all wide area networks (excepts those using satellites) having store-and forward subnets.

(ii) **Wireless Links :** Mobile computers, such as notebook computers and personal digital assistants (PDAs), are the fastest-growing segment of the computer industry. Many of the owners of these computers have desktop machines on LANs and WANs back at the offices and want to be connected to their home base even when away from home or en route. Since having a wired connection is impossible in cars and air planes, there is a lot of interest in wireless networks.

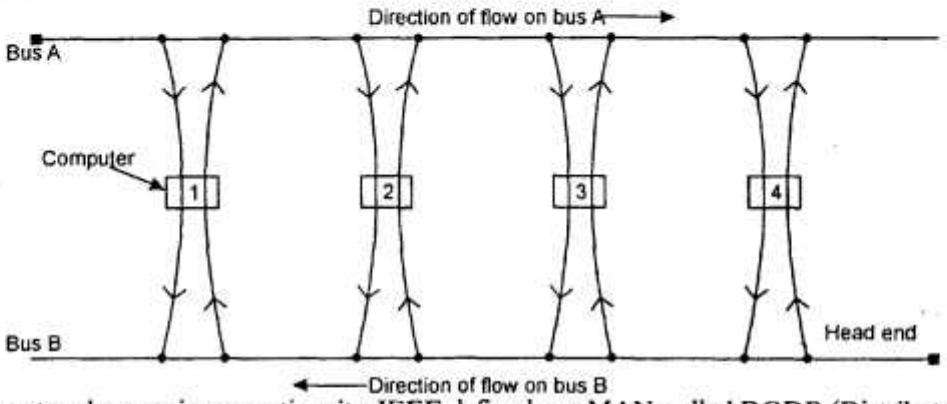
Wireless links have many uses :

(i) A common one is the portable office. People on the road often want to use their portable electronic equipment to send and receive telephone calls, faxes and electronic mail, read remote files, login or remote machines and so on and do this from anywhere on land, sea, or air.

(ii) Another use is for rescue workers at disaster sites (fires, floods, earthquakes etc.) where the telephone system has been destroyed. Computers there can send messages, keep records and so on.

(iii) Finally, wireless links are important to the military. If you have to be able to fight a war anywhere on earth on short notice, counting on using the local networking infrastructure is probably not a good idea. It is better to bring your own.

(iii) **DQDB :** Distributed Queue Dual Bus consists of two unidirectional buses (cables) to which all the computers are connected. Each bus has a head-end, a device that initiates transmission activity. Traffic that is destined for a computer to the right of the sender uses the upper bus. Traffic to the lift uses the lower one.



For networks covering an entire city, IEEE defined one MAN, called DQDB (Distributed Queue Dual Bus) as standard 802.6. According to diagram, two parallel, unidirectional buses shake through the city, with stations attached to both buses in parallel. Each bus has a head-end, which generates a steady stream of 53-byte cells. Each cell travels downstream from the head-end. When it reaches the end, it falls off the bus.

Q. 6. (a) Explain Network Operating System ? Explain. **10**

Ans. NOS (Network Operating System) : NOS is a piece of software that controls a network and its message (e.g., packet) traffic and queues, controls access by multiple users to network resources such as files and provides for certain administrative functions including security.

(i) A NOS is most frequently used with local area network and WANs, but could also have applications to larger network systems.

(ii) The upper 5 layer of OSI reference model provides the foundation upon with many network operating system are based.

NOS was also the name of propriety time-sharing operating system on the CDC 60-bit 6000 and cyber series mainframe computers, in the mid 1980s. NOS was replaced with NOS/VE on the 64-bit cyber-ISO systems. NOS is an operating system that includes special functions for connecting computers and devices into a local-area network or inter-working. Some popular NOSs for DOS and windows system include Novell Netware, Window NT, 2000, 2003, 2008 server etc.

Features :

(i) Provide basic operating system features such as support for processors, protocols, automatic network detection and support multiprocessing of application.

(ii) Security features such as authentication, authorization, logon restrictions and access control.

(iii) Provide name and directing services.

(iv) Provide file, print, web services, back-up and replication services.

Q. 6. (b) What are popular remote monitoring Techniques ? Explain. **10**

Ans. Remote Monitoring Techniques :

Remote Monitoring : Directed Circuit Approach : The directed circuit approach to Remote Monitoring offers a numbers of benefit over the ageold remote monitoring models of VPNs and direct modem lines. If you are considering outsourcing the monitoring of critical data center infrastructures, the directed CKT approach offer security and reliability over traditional remote monitoring technique.

As more enterprises demand remote monitoring over their critical systems, they face two options. Remote monitoring has used a direct modem line to send alarms to are offsite vendor. This method cache reliability because the modem connection in a single point of failure, and the information transmitted from equipment contact closure is far from descriptive for diagnostic and troubleshouting processes.

Remote Monitoring a directed circuit uses a couple of models. First, there is the vender offering Remote monitoring Through a directed circuit for its customers. There are also MSPs (Manajed service Providers) that deploy apphance-based solution.

Emerson Liebert's directed circuit approach leverages a network-monitoring model consisting of SNMP and NIC to communicate more specific alarm information to a remote monitoring center.

The firewall is often the main challenge when uniprinting a remote monitoring solution. Other Remote Monitoring Techniques are VPNs as a secure tunnel through a corporate firewall.

Q. 7. Explain network topologies with their merits and demerits ? What is basic role if topologies in Computer Networking ? Which topology is widely used ? Why ? **20**

Ans. Computer Network : Computer Network to mean an interconnected collection of autonomous computers. Two computers are said to be interconnected if they are able to exchange information. By requiring the computers to be autonomous, if one computer can forcibly start, stop, or control another one, the computers are not autonomous.

The network contains numerous cables or telephone lines, each one connecting a pair of 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 lines it free, & then forwarded. A subnets using this principle is called a point-to-point, store and forward or packet switched subnet.

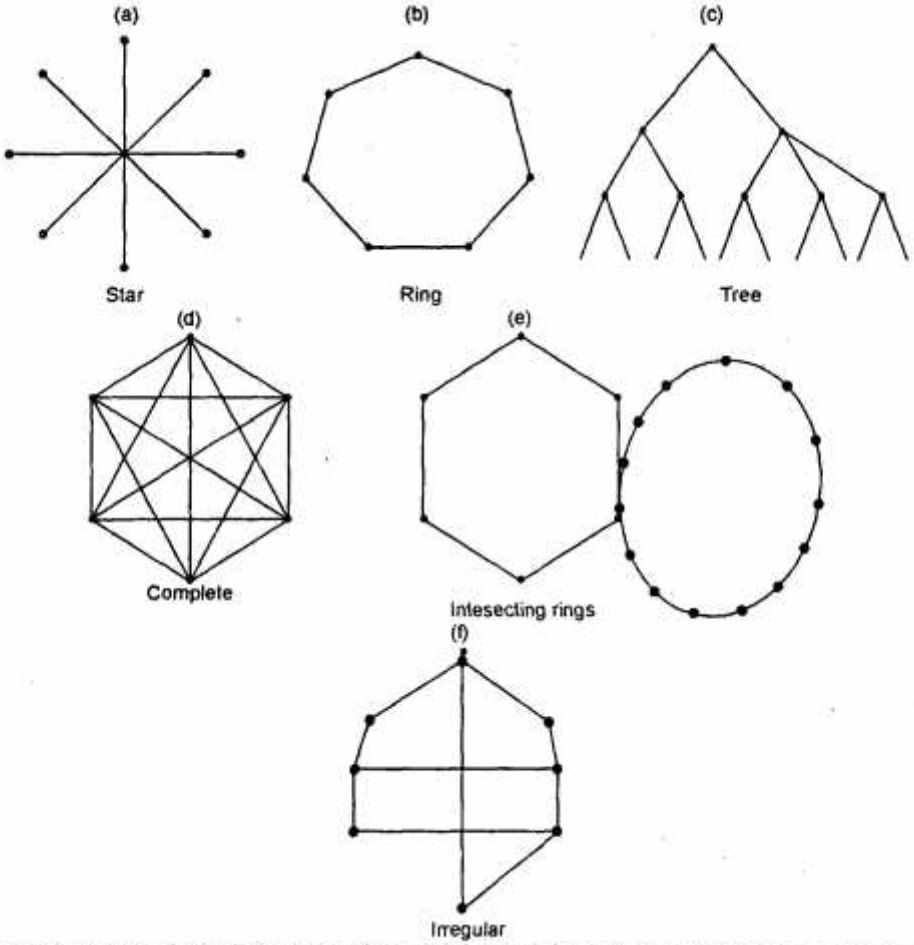


Figure shows several possible topologies. Local networks that were designed as such usually have a symmetric topology. In contrast, wide area networks typically have irregular topologies.

Bus Topology : Bus networks use a common backbone to connect all devices. A single cable, the backbone functions as a shared communication medium that devices attach int with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient centerally accept and processes the message.

Ring : In a ring network, every device has exactly two neighbours for communicate purposes. All messages travel through a ring in the same direction (either "clockwise" or "counter clockwise"). A failure in any cable or device breaks the loop and take down the entire network.

Star : Many home networks use the star topology. A star network features a central connection point called a "hub" that may be a hub, switch or router. Compared to the bus topology, a star network generally requires more cable but a failure in any star network cable will only take down one computer's network access and not the entire LAN.

Tree Topology : Tree topology integrate mutiple star topologies onto a bus. In its simplest form, only hub devices connect directly to the tree bus, and each hub function as the "root" of a tree of devices.

Mesh Topology : Mesh topology involve the concepts routers. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination.

Q. 8. Explain the following (Attempt any five) : **5×4=20**

(i) ARP **(ii) POP** **(iii) NNTP**

(iv) ATM **(v) Windows NT/200** **(vi) SDH**

Ans. (i) ARP (Address Resolution Protocol) : ARP solves the problem of finding out which Ethernet address corresponds to a given IP address. Almost every machine on the internet runs it. It is defined in RFC 826.

The advantage of using ARP over configuration files is the simplicity. The system manager does not have to do much except assign each machine an IP address and decide about subnet mask, ARP does the rest.

Various optimizations are possible to make ARP more efficient. To start with, once a machine has run ARP, it caches the result in case it needs to contact the same machine shortly. Next time it will find the mapping in its own cache, thus, eliminating the need for a second broadcast.

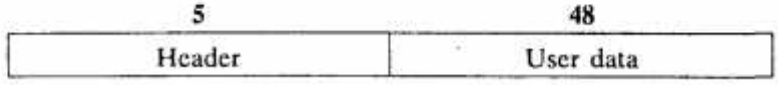
"The process of connecting internet address or IP address to a physical network address is known as Address Resolution. The software involved in this conversion is known as Address Resolution Protocol (ARP)".

(ii) POP (Point of Presence) : Any 1×C that wishes to handle calls originating in a Local Address and Transport areas (LATAs) can build a switching office called a POP (Point of Presence). The registration forms are available on the internet itself on the websites of the ISPs. An ISP provides subscribers with access to the Internet for a free. Customers can dial the ISP's point of presence (POP) through the Public Switched Telephone Network (PSTN) or over a described, " always-on" connection. A POP is like a telephone company's switching office, where all of the ISP's equipment and personnel are located.

(iii) NNTP (Network News Transfer Protocol) : NNTP, which is defined in RFC 977. NNTP has something of the same flower as SMTP, with a client issuing commands in ASCII and a server issuing responses as decimal numbers coded in ASCII. Most USENET machines now use NNTP.

NNTP was designed for two purposes. The first goal was to allow news articles to propagate from one machine to another over a reliable connection (e.g., TCP). The second goal was to allow users whose desktop computers cannot receive news to read news remotely. Both are widely used, but we will concentrate on how news articles speed out over the network using NNTP.

(iv) ATM (Asynchronous Transfer Mode) : The basic idea behind ATM is to transmit all information in small, fixed-size packets called cells. The cells are 53 bytes long, of which 5 bytes are header and 48 bytes are payload.



An ATM cell

ATM is both a technology and potentially a service (visible to the users). Sometimes the service is called cell relay, as an analogy to frame relay.

ATM networks are connection-oriented. Making a call requires first sending a message to set up the connection. After that, subsequent cells all follow the same path to the destination. Cell delivery is not guaranteed, but their order is. If cells 1 and 2 are sent in that order, then if both arrive, they will arrive in that order, never first 2 then 1.

ATM networks are organized like traditional WANs, with lines and switches (routers). The intended speeds for ATM networks are 155 mbps and 622 mbps. The 155-mbps speed was chosen because this is about what is needed to transmit high definition television. The exact choice of 155.52 mbps was made for compatibility with AT & T's SONET transmission system. The 622 mbps speed was chosen so four 155 mbps channels could be sent over it. By now it should be clear why some of gigabit test beds operated at 622 mbps : they used ATM.

(v) Window NT/2000 : Window is graphics user interface (GUI) based operating system in which the tasks are performed by clicking, double clicking, mouse move and other events associated with mouse. It is an operating system by Micro Soft Corporation. These are many windous operating system develc ped by Micro Soft Corporation like Windows 3.1,Windows 95, Windows 98, Windows 2000, Windows NT, Windows ME and WindowsXP. Window NT/2000 is more advance than previous ones. It is multi tasking, multi threading, multi user operating system i.e., many tasks and many user can work on it simultaneously in contrast to DOB which is single user and single tasking.

Components of Windows NT/2000 :

- **Desktop :** Main screen of computer visible after the start windows. Contains icons like my computer, recycle bin, network, internet explorer etc.
- **Taskbar :** This is bottom of desktop screen, contains start button, minimized files and other icons.
- **Tool Bar :** There are many toolbars like format drawing etc.
- **Icons :** Icons are images seen any where in the window location.
- **Buttons :** There are many buttons like minimized , maximize, restore, format.
- **Scroll Bar :** There are two types of scroll bars-horizontal and vertical scroll bars attached with various types of windows.

(vi) SDH (Synchronous Digital Hierarchy) : In the early days of fibre optics, every telephone company had its own proprietary optical TDM system. After AT & T was broker up in 1984, local telephone companies had to connect to multiple long-distance carriers, all with different optical TDM systems, so the need for standardization become obvious. In 1985, Bellcore, the RBOCs research arm, began working on a standard, called SONET (Synchronous Optical Network). Later, CCITT joined the effort, which resulted in a SONET standard and a set of parallel CCITT recommendations. The CCITT recommendations are called SDH (Synchronous Digital Hierarchy).

The 810-bytes SONET frames are best described as a rectangle of bytes, 90 columns wide by 9 rows high. Thus, $8 \times 810 = 6480$ bits are transmitted 8000 times per second, for a gross data rate of 51.84 mbps. This is the basic SONET channel and is called STS-1 (Synchronous Transport Signal-1).