MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer **Subject Code:** **17430**

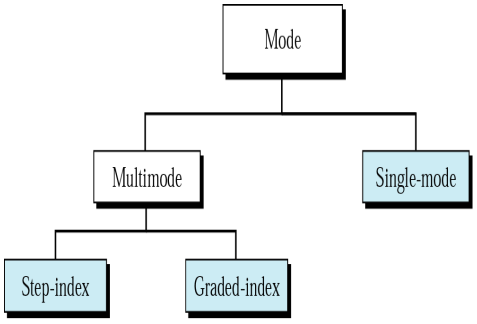
Important Instructions to examiners:

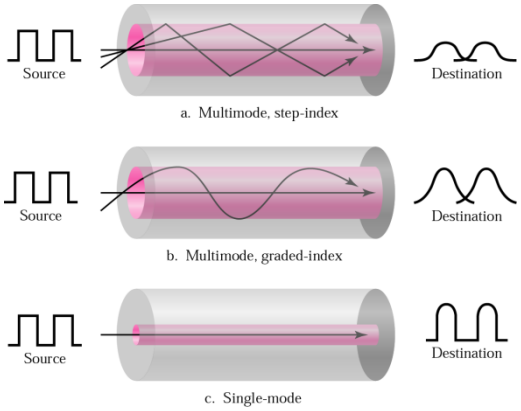
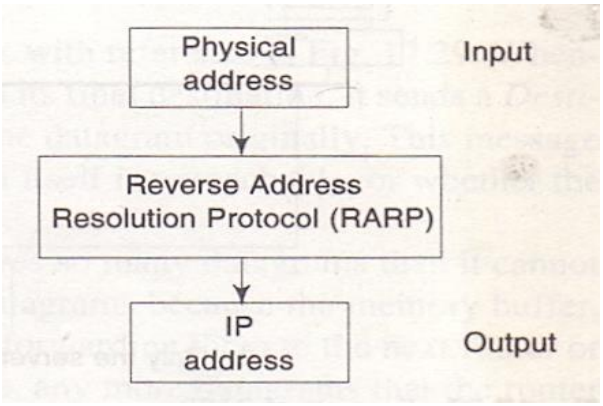
1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills).
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.

Q.No.	Sub Q.N.	Answer	Marking Scheme
1.	**a)**	**Attempt any SIX of the following:**	**12**
	(i)	**Define protocol? Why it is needed?**	***2M***
	Ans.	**Protocols** are sets of rules and convention for exchanging information. This exchange usually occurs much like a dialog between two computers. The sender and receiver are the two key parties in data communication must agree on common set of rules i.e protocol before they can communicate with each other. **Need of protocol:** ➢ Without rules and conventions two peoples/devices/machines cannot communicate. ➢ Protocol defines **syntax** (what is to be communicated?), **semantics** (How it is to be communicated?) and **timings** (When it is to be communicated?) ➢ Protocols were created to allow computers to communicate in an organized manner without any room for misinterpretation.	***Definition 1M*** ***Need 1M***
	(ii)	**Define the term for errors: Attenuation.**	***2M***
	Ans.	Attenuation is a communications term that refers to a reduction in signal strength commonly occurring while transmitting analog or digital signals over long distances. Attenuation is very small at short distances and increases with increase in distance.	***Definition 2M***

	(iii) Ans.	**Define BSS and ESS.** **IEEE 802.11 wireless LAN:** The 802.11 architecture define two types of services: **Basic services set (BSS):** 1) The basic services set contain stationary or mobile wireless station and central base station called access point (AP) 2) The use of access point is optional. 3) If the access point is not present, it is known as standalone network. Such a BSS cannot access such data to other BSSs. These types of architecture are known as adhoc architecture. 4) The BSS in which an access point is present is known as infrastructure network. **Extended services set (ESS):** 1) An extended service set is created by initializing two or more basic services set (BSS) having access points (APs) 2) These extended networks are created by joining the access points of basic station set through a wired LAN known as distribution system.	***2M*** ***1M for BSS*** ***1M for ESS***
	(iv) Ans.	**Give the Functions of Transport Layer.** **Transport layer is** responsible for process to process delivery of message and ensures that whole message arrives in order from source to destination. **Several other functions of Transport layer are:** 1. Service point addressing 2. Segmentation and reassembly 3. Connection control 4. Flow control: Flow control is performed end to end 5. Error control	***2M*** ***Functions of transport layer 2M***
	(v) Ans.	**List the different types of network connecting devices.** **Following is the list of network and internetwork connecting devices :** a) Hub b) Switch c) Repeaters d) Bridges e) Routers f) Gateways g) Modem	***2M*** ***Any 4 ½M each devices***

	(vi) Ans.	**What is IP address? Why it is required?** IP address is a logical address, 32 bit address having network_id & host_id that uniquely & universally identified over network or local network or to internet. Messages are routed in a network based on destination IP address. It has five classes: Class A, B,C,D,E. **OR** IP Address: IP Address is used in the source & destination address fields of the IP header it is 32 bit long. Each device has a unique IP Address. **Need:** 1. In a internetwork each device/computer should have unique address for identification and communication. IP addressing provides that facility. 2. In order to communicate with other devices in the network, there needs a global addressing scheme. IP addresses are used for logically addressing the computers. 3. It provides a network address and host address so routing becomes easy task. 4. It gives facility of subnetting and supernetting.	***2M*** ***Definition 1M*** ***Need 1M***
	(vii) Ans.	**What is Bridge? Give its types.** **A Bridge** is a device used to connect two or more LAN segments together. Bridge operates at the data link layer of OSI model. A Bridge provides packet filtering at data link layer, meaning that it only passes the packets that are destined for the other side of the network. **Types of Bridges:** Following types of Bridges are used in network: 1) Transparent Bridge. 2) Translational Bridge. 3) Source-route Bridge. Other than above, there are also Local Bridge, Remote Bridge, etc.	***2M*** ***Definition 1M*** ***Any 2 Types 1M***
	(viii) Ans.	**What is Gigabit Ethernate?** **Gigabit Ethernet provides the data rate of 1 Gbps or 1000 Mbps.** • IEEE created Gigabit Ethernet under the name 802.3z. • It is compatible with Standard or Fast Ethernet. • It also uses similarly 48 bit hexadecimal addressing scheme. • The frame format is also similar to standard Ethernet. • It operates in both half-duplex and full duplex mode. • In half duplex mode, CSMA/CD access method is used whereas in full duplex mode CSMA/CD is not required.	***2M*** ***2M for any 2 points***

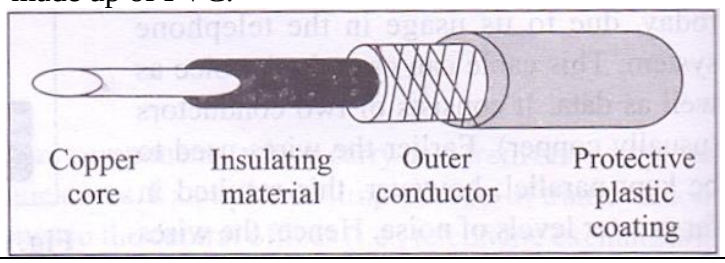
1.	**b)**	**Attempt any TWO of the following:**	**8**
	(i) Ans.	**Describe the characteristics of data communication system.** **The effectiveness of any data communications system depends upon the following four fundamental characteristics:** **1) Delivery**: The data should be delivered to the correct destination and correct user. **2) Accuracy**: The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data. **3) Timeliness**: Audio and Video data has to be delivered in a timely manner without any delay; such a data delivery is called real time transmission of data. **4) Jitter**: It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmitted.	***4M*** ***Any four - Each characteristics- 1M***
	(ii) Ans.	**Describe different modes of propagation of fibre optic cable.** Fibre optic cable supports two modes for propagating light along optical channels, each requiring fiber with different physical characteristics: **Multimode and Single Mode.** Multimode, in turn, can be implemented in two forms: step-index or graded index.  • **Multimode**: In this case multiple beams from a light source move through the core in different paths. • In **multimode step-index fiber**, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and cladding. At the interface there is an abrupt change to a lower density that alters the angle of the beam's motion. • In a **multimode graded-index fiber** the density is highest at the center of the core and decreases gradually to its lowest at the edge. • **Single mode** uses step-index fiber and a highly focused source of	***4M*** ***Each mode 1M***

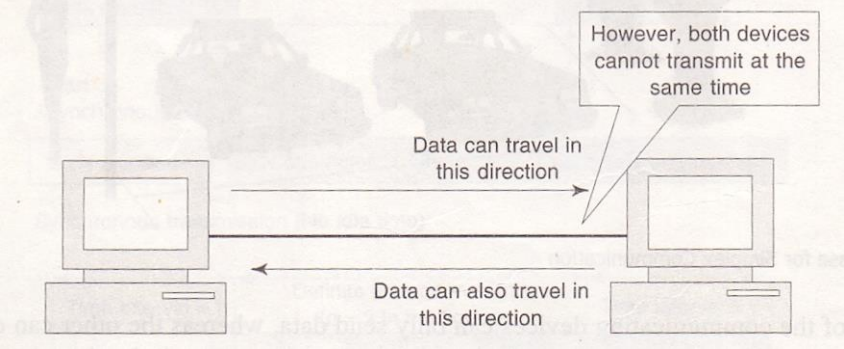
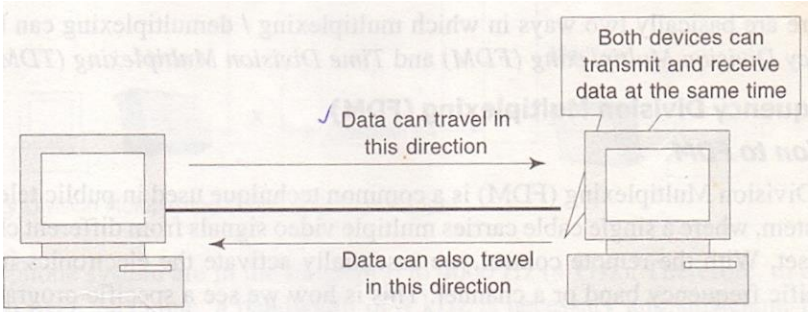
		light that limits beams to a small range of angles, all close to the horizontal.  	***Diagram 1M***
	(iii) Ans.	**Describe Reverse Address Resolution Protocol (RARP).** **RARP (Reverse Address Resolution Protocol):** 1) Reverse address resolution protocol is a network protocol used to resolve a data link layer address to the corresponding network layer address. 2) It is the RARP which designed for diskless workstations that have no means of permanently storing their TCP/IP configuration information or TCP/ IP settings. 3) RARP does the opposite of ARP. While ARP broadcasts an IP address in an effort to discover its equivalent hardware address, RARP broadcasts the systems hardware address. 4) RARP server responds by transmitting the IP address assigned to that client computer. RARP can supply IP address to all the systems on a network segment.  	***4M*** ***Explanation 3M*** ***Diagram 1M***

2.		**Attempt any FOUR of the following:**	**16**
	a) Ans.	**Define Standard. Name any four standard organizations.** 1) Standards are essential in creating and maintaining an open and competitive market for equipment Manufacturers and in guaranteeing national and international interoperability of data and telecommunication technology and processes. 2) They provide guidelines to manufacturers, Vendors, govt. agencies and other service providers to ensure the kind of interconnectivity necessary in today's market place and in international communication. **Standard organizations:** 1. International standard organization (ISO) 2. American National Standard institute (ANSI) 3. Institute of electrical & electronics engineers (IEEE) 4. The Electronics Industries Association. (EIA) 5. The International Telecommunications Union – Telecommunications Standard Sector(ITU-T)	***4M*** ***Definition 2M*** ***Any four-standard organizations 1/2M each***
	b) Ans.	**Compare FDM and TDM.** **Difference between FDM & TDM:**	***4M***

Sr. No.	FDM (Frequency Division Multiplexing)	TDM (Time Division Multiplexing)
1	Total frequency bands are divided into several users	Total available time is divided into several slots/user
2	Transmission of two or more signals on the same path, but at different times.	A multiplex system for transmitting two or more signals over a common path by using a different frequency band for each signal.
3	The signals multiplexed come from different sources/transmitters.	TDM imply partitioning the bandwidth of the channel connecting two nodes into finite set of time slots
4	FDM has less flexibility, as it cannot dynamically change the width of the allocated frequency.	TDM provides greater flexibility and efficiency, by dynamically allocating more time periods to the signals that need more of the bandwidth

Any four differences-1M each

		5	FDM, each signal uses a small portion of the bandwidth all of the time.	In TDM, each signal uses all of the bandwidth some of the time.	
		6	Channels in FDM can transmit at any time, their latencies would be much lower compared to TDM.	In TDM only one channel can transmit at a given time, and some data would often be delayed, though it's often only in milliseconds.	
		7	Synchronization is not required	Synchronization is required	
		8	FDM is simpler to implement than TDM	TDM is complex as compared to FDM.	
	c) Ans.	**Describe construction of co-axial cable with neat diagram.** The co-axial cable is also called as coax. It has an inner central conductor made up of solid material like copper or aluminum. The inner conductor is surrounded by an insulating sheath which in turn is enclosed in an outer conductor (shield). Outer conductor is made up of braided sheath. This acts not only as second conductor for completing the circuit but also act as shield against noise. The outer conductor is covered by a plastic cover mostly made up of PVC.  	***4M*** ***Description-2M*** ***Diagram-2M***
	d) Ans.	**Explain half duplex and full duplex communication.** **Half duplex**: In the half-duplex mode, both devices can transmit data, though not at the same time. When one device is sending data, the other must only receive it, and vice versa. This is conceptually similar to a street that has a single lane for vehicle traffic. When vehicles from one side are coming, the vehicles from the other side must wait. Thus, both sides take turns to send data as shown in diagram. This requires a definite turn around time during which the device changes form the receiving mode to the transmitting mode. Due to this delay, half-duplex communication is slower than simplex communication. However, it is more convenient than simplex communication, as both	***4M*** ***Definition of Half duplex 1M***

		the devices can send and receive the data.  Examples of half-duplex communication are conversations over walkie-talkie. **Full duplex:** In full duplex (or simply duplex) communication mode, both the devices can transmit data at the same time. It means that both devices are capable of sending as well as receiving data at the same time. This is like a two-way street with traffic flowing in both directions at the same time. It is also similar to a telephone conversation, where both parties can talk to each other simultaneously.  	***Diagram -1M*** ***Definition of full duplex 1M*** ***Diagram -1M***
	e) Ans.	**Draw OSI reference model. Explain working of any two layer.** OSI model (open system interconnection) model was developed by ISO (international standard organization)	***4M***

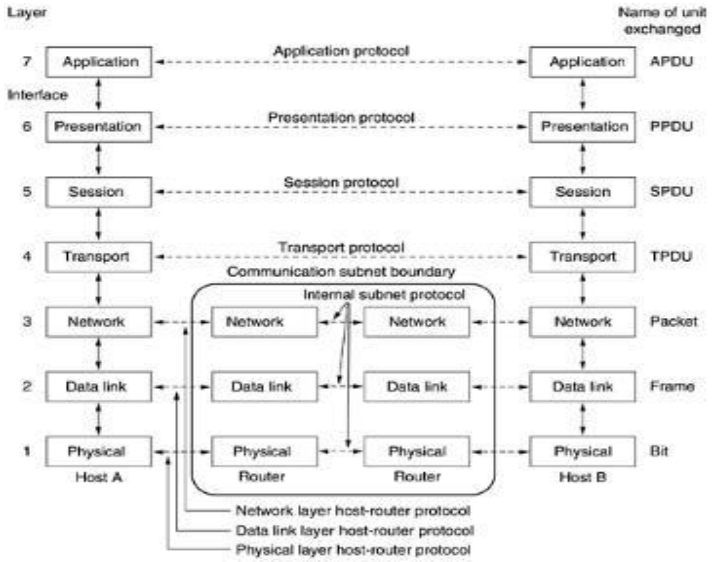


Fig. ISO-OSI reference model

Diagram of reference model- 2M

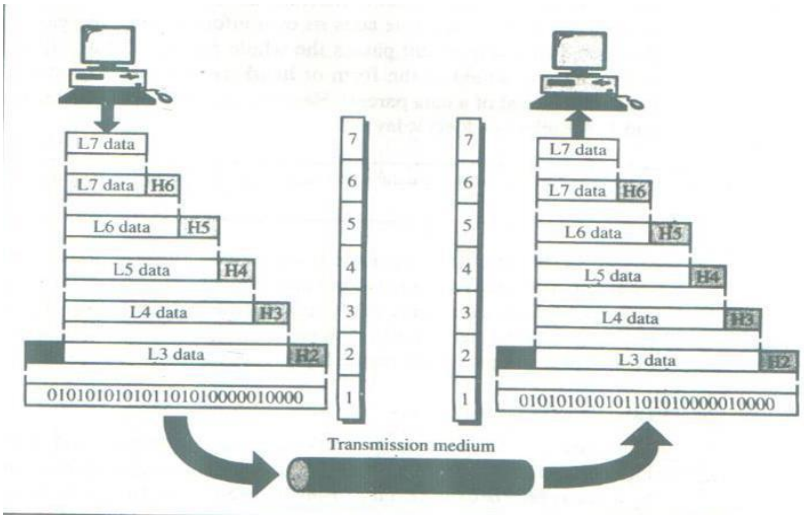
OSI model has following 7 layers as **Physical layer, data link layer, Network layer, Transport layer, Session layer, Presentation layer, Application layer**.
Following are the functions performed by the above layer

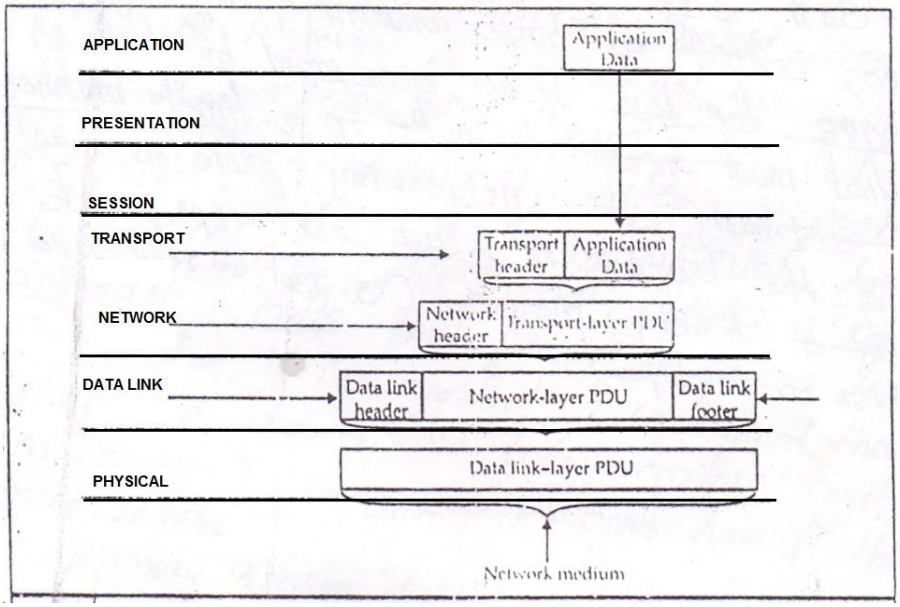
1. **Physical layer:** it deals with the mechanical and electrical specification of the interface and transmission medium.
   - Physical characteristics of interfaces and medium.
   - Representation of bits or signals.
   - Data rate
   - Synchronization of bit
   - Line configuration or connection type.
   - Physical topology
   - Transmission mode.

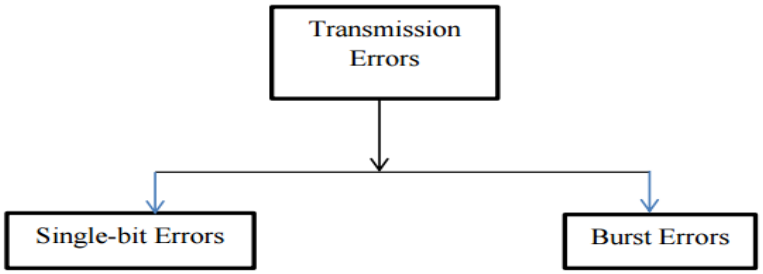
2. **Data link layer:** It performs node to node delivery of the data
It is responsible for transmitting group of bits between the adjacent nodes. The group of bits is called as frame.
   - Framing
   - Physical addressing
   - Flow control

Working any two - 1M each

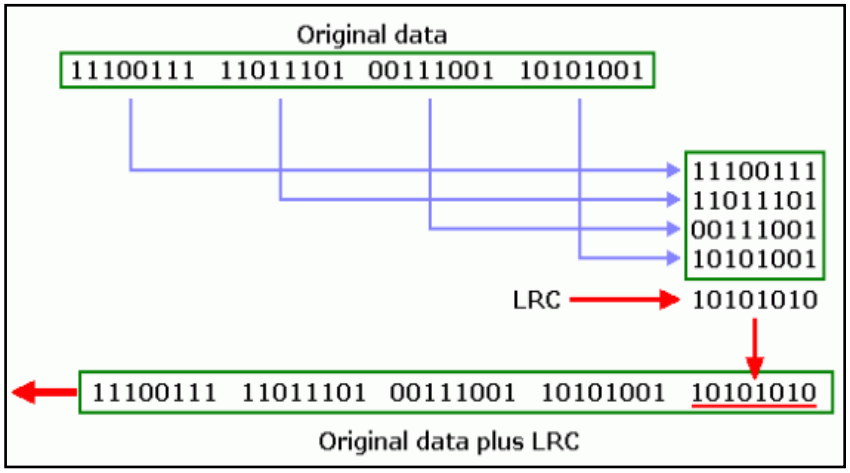
		➢ Error control ➢ Media access control ➢ Node to node delivery 3. **Network layer: It is responsible for routing the packets within the subnet i.e. from source** to destination. It is responsible for source to destination delivery of individual packets across multiple networks. It ensures that packet is delivered from point of origin to destination. ➢ Logical addressing ➢ Routing. ➢ Congestion control ➢ Accounting and billing ➢ Fragmentation ➢ Source host to destination host error free delivery of packet. 4. **Transport layer:** Responsibility of process to process delivery of message Ensure that whole message arrives in order. ➢ Service point addressing ➢ Segmentation and reassembly ➢ Connection control ➢ Flow control: Flow control is performed end to end ➢ Error control 5. **Session layer:** Establishes, maintains, and synchronizes the interaction among communication systems. It is responsible for dialog control and synchronization. ➢ Dialog control ➢ Synchronization ➢ Token Management ➢ Activity Management ➢ Data Exchange 6. **Presentation layer:** It is concerned with syntax, semantics of information exchanged between the two systems. ➢ Translation: presentation layer is responsible for converting various formats into required format of the recipient ➢ Encryption: Data encryption and decryption is done by presentation layer for security. ➢ Compression and Decompression: data to be transform compressed while sending and decompress while receiving	

		for reducing time of transmission. 7. **Application layer:** It enables user to access the network. It provides user interfaces and support for services like email, remote file access. ➢ Network virtual terminal. ➢ File transfer access and management. ➢ Mail services ➢ Directory services.	
	f) Ans.	**Describe the concept of data encapsulation.** ***(Any explanation with diagram shall be considered)*** The protocols operating at the various layers work together to supply a unified quality of service. Each protocol layer provides a service to the layers directly above and below it. The process of adding the **headers and trailers** to the data is called as **data encapsulation**. **OR** A packet(header and data) at level 7 is encapsulated in a packet at level 6.The whole packet at level 6 is encapsulated in a packet at level 5, and so on. In other words, the data portion of a packet at level N-1 carries the whole packet (data and header and maybe trailer) from level N. The concept is called **encapsulation.**  **OR**	***4M*** ***Description 3M*** ***Diagram 1M***



3.	**a)** Ans.	**Attempt any <u>FOUR</u> of the following:** **Explain different types of transmission errors.** **There are two types of errors:** 1. Single bit errors 2. Burst errors  **<u>Single bit errors:</u>** If the signal is carrying binary data, and if a value of 0 to changes to 1 or vice versa then it is known as single bit error. Single bit errors are more likely in the case of parallel transmission because it is likely that one of the eight wires carrying the bits has	**16** ***4M*** ***Single Bit Errors 2M***

		become noisy, resulting incorruption of a single bit of each byte. This can be a case of parallel transmission between the CPU and the memory inside a computer. **Burst errors:-** In burst error multiple bits of binary value are changed. In contrast, a burst changes at least two bits during data transmission because of errors. Note that burst errors can change any two or more bits in a transmission. These bits need not necessarily be adjacent bits. Burst errors are more likely in serial transmission, because the duration of noise is longer, which causes multiple bits to be corrupted.	***Burst Errors 2M***
	b) Ans.	**What is hub? Explain different types of hub.** It is defined as the networking device that is used to build a connection between the different computers to perform the tasks like a single network is called as the networking hub. The main function of the networking hub is to transfer the packet over the whole connected networks. **Passive Hub:** The first type of the networking hub is the passive hub. Passive hub does not perform any particular function but it just behaves like a bridge between the cables of connection and just receives the information and forwards it without any change in topology. It does not require electric power supply. **Active Hub:** Second type of the networking hub is the active hub. This type of hub is quite similar to that of the passive hub but can perform the additional tasks. Active hubs are those hubs that can work as connector between two regions but also has ability to regenerate/ amplify the information with the help of strong electrical signals. It is also called as the multi-port repeater. **Intelligent Hub:** In addition to signal regeneration intelligent hub performs some network management and intelligent path selection. A switching hub chooses only the port of the device where the signal needs to go than sending the signal along all paths. Basically this hub provides the opportunity to increase the speed of networking and also make the performance of the network efficient as compared to other devices. Addition to their specific work intelligent hubs can also perform the different functions that of routing, bridging etc. One advantage of this is that you can permanently connect all	***4M*** ***Definition of Hub 1M*** ***Description Types of hubs 1M each***

		transmission media segment because each segment will be used only when a signal is send to device using that segment.	
	c) Ans.	**Explain LRC and VRC for error detection.** **LRC:** In this error detection method, a block of bits is organized in a table with rows and columns. Then the parity bit for each column is calculated and a new row of eight bits, which are the parity bits for the whole block, is created. After that the new calculated parity bits are attached to the original data and sends to the receiver. ***Example:***  LRC increases the likelihood of detecting burst error. An LRC of n bits can easily detect a burst error of n bits. However, if two bits in one data unit are damaged and two bits in exactly the same positions in another data unit are also damaged, the LRC checker will not detect an error.	***4M*** ***Description of LRC 2M***

		1010*0*/1 0011*0*/1 11011101 11100111 10101010 (LRC) Calculate the LRC for Data Received 1010*0*/1 0011*0*/1 11011101 11100111 → LRC Calculated by Receiver 10101010 → Compare with LRC Received 10101010 **VRC:** • Vertical redundancy check (VRC), a parity bit is added to every data unit so that the total number of 1's become even. • VRC is most common & least expensive mechanism. • A redundant bit is called as parity bit. • After appending redundant bit to data unit if total number of 1's in the packet (including parity bit) becomes even then it is called even parity checking & if total number of 1's in the packet (including parity bit) becomes odd then it is called odd parity checking. • A parity bit is added to data packet for purpose of error detection. • Upon receipt of the packet, parity needed for data is recomputed & compared to parity received with the data. If any bit has changed state, parity will not match & error can be detected. • In fact, if an odd number of bits (not just one) have been altered, parity will not match. If even numbers of bits have been reversed, the parity will match even though error has occurred. ***Example:*** Suppose sender wants to send 1110111 data unit to receiver & both uses even parity checking. **Solution:** Original Data to send: Both sender & receiver 1 1 1 0 1 1 1 use Even parity checking. As total number of 1's in data unit are even i.e. six the parity bit added to end of data unit will be 0, so it maintains even	***Description of VRC 2M***

parity of data unit.
Actual data send by sender:

1	1	1	0	1	1	1	0

d) Ans.

Describe DNS in detail

4M

A domain name server is simply a computer that contains the database and the software of mapping between domain names and IP addresses. Every domain has a domain name server. It handles request coming to computers owned by it and also maintains the various domain entries. The DNS is completely distributed throughout the world on millions of computers.

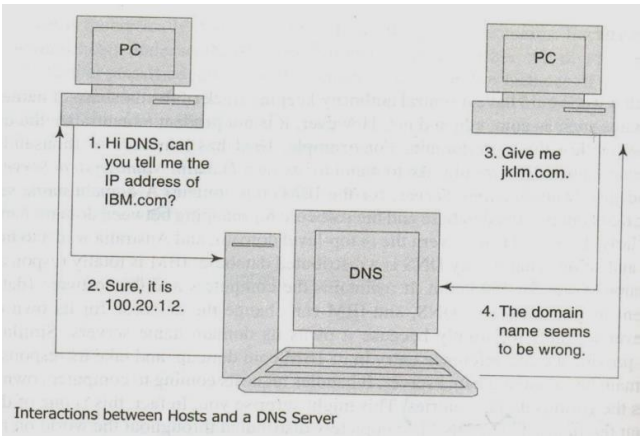
Any relevant description about DNS 4M

Table : Generic Domain Name

Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

The DNS works very similar to a telephone directory inquiry service. Basically, DNS server does two things tirelessly:

- Accept request from programs for converting domain names into IP addresses.
- Accept request from other DNS servers to convert domain names into IP addresses



Interactions between Hosts and a DNS Server

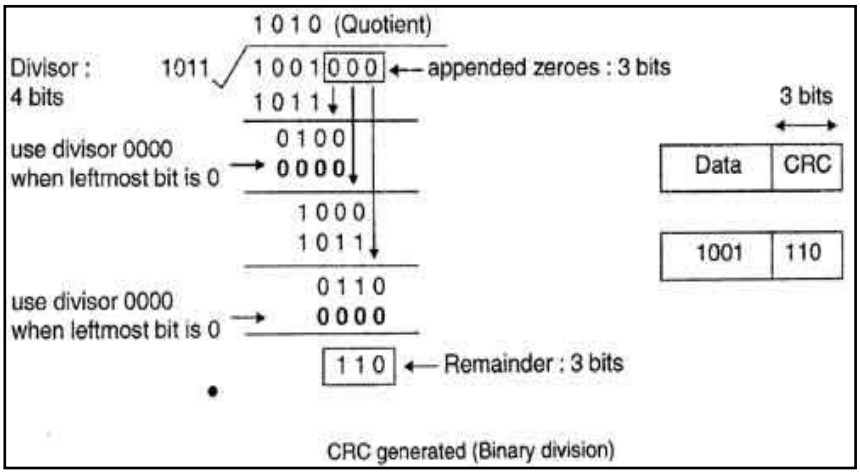
When such request comes in, a DNS server has the following options: It can supply the IP address because it already knows the IP address for the domain. It can contact another DSN server and try to locate the IP address for the name requested. It may have to do this more than once. Every DNS server has an entry called alternate DNS server, which is the DNS server it should get in touch with for unresolved domains. The DNS hierarchy specifies how the chains between the various DNS servers should be established for this purpose. It can simple say, "I do not know the IP addresses for the domains name you have requested, but here is the IP addresses for a name server that knows more than I do". In other word, it suggests the name of another DNS server. It can return an error message because the requested domain name is invalid or does not exist.

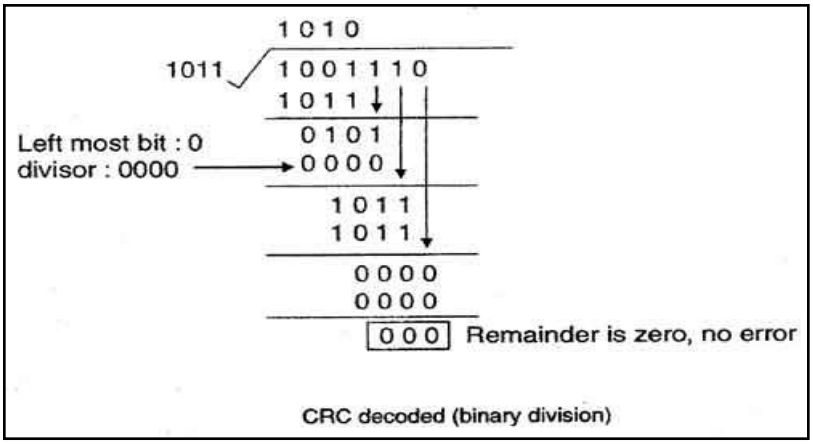
e) Ans.

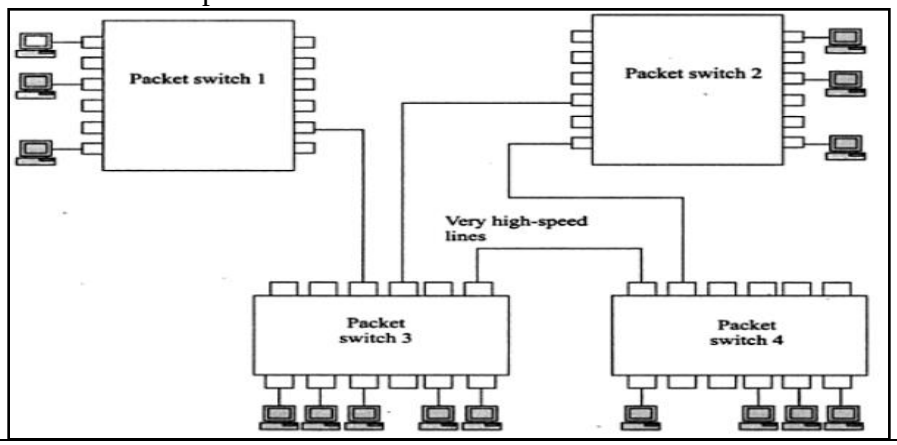
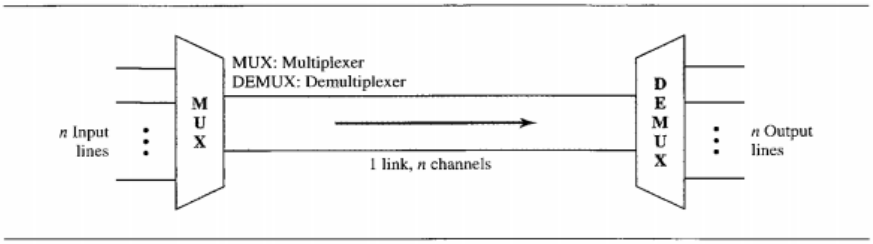
Describe cyclic redundancy check (CRC) with an example. ***4M***

Cyclic Redundancy Check (CRC): ***Description 2M***

CRC is one of the most common and powerful error detecting code which can be describe as follows. The polynomial code also known as CRC with co-efficient of 0s and 1s. In this method the sender and receiver must agree upon generator polynomial g(x) in advance. Both the high and low order bits of the generator (divisor) must be 1. To compute the checksum for some frame (data) with m bits, the frame must be longer than generator polynomial. The idea is to append checksum to the end of frame in such a way that the polynomial represented by the checksum frame is divisible by g(x). When the receiver gets the checksum frame it tries dividing it by g(x). If there is remainder there has been a transmission error and zero remainder means no error in the transmission. r is degree of g(x) polynomial

		Step by step procedure: 1. Append a string of r zero bits to the lower order end of data word where r is less than the number of bits pre-decided divisor by 1 bit i.e. if divisor = 5 bits then r = 4 zeros. Now data word contains m+r bits 2. Divide the newly generated data unit in step 1 by the divisor. It is module – 2 division 3. The remainder obtained after division is the r bit CRC. 4. This CRC will replace the r zeros appended to the data unit to get the codeword to be transmitted. ***Example:*** 1. Data unit 1011000 is divided by 1011.  1010 (Quotient) Divisor : 4 bits 1011 / 1001000 ← appended zeroes : 3 bits 1011 0100 use divisor 0000 when leftmost bit is 0 → 0000 1000 1011 0110 use divisor 0000 when leftmost bit is 0 → 0000 110 ← Remainder : 3 bits 3 bits Data | CRC 1001 | 110 CRC generated (Binary division) 2.During this process of division, whenever the leftmost bit of dividend or remainder is 0, we use a string of Os of same length as divisor. Thus in this case divisor 1011 is replaced by 0000.	***Example till step- 2 2M (Step-3 onwards optional)***

		3.At the receiver side, data received is 1001110.  CRC decoded (binary division) 4. This data is again divided by a divisor 1011. 5. The remainder obtained is 000; it means there is no error.	
	f) Ans.	**Compare SLIP and PPP.** **Sr. No.** | **SLIP (Serial Line Internet Protocol)** | **PPP (Point-to-Point Protocol)** 1 | SLIP does not perform error detection & correction. | PPP performs error detection & correction. 2 | SLIP supports only IP | PPP supports multiple protocols. 3 | IP address is assigned statically. | IP address is assigned dynamically 4 | SLIP does not provide any authentication. | PPP provides authentication. 5 | SLIP is not approved Internet standard. | PPP is approved Internet standard. 6 | SLIP is a connectionless protocol | PPP is a connection-oriented protocol 7 | SLIP is not a group of protocols | PPP is a group of protocols	***4M*** ***Any 4 relevant points 1M each***
4.	**a)** Ans.	**Attempt any FOUR of the following:** **Explain the architecture of WAN.** When numbers of packet switches are connected together a WAN is formed. A packet switch has multiple I/O ports. Thus it can connect too many different computers or other switches to form a variety of topologies. A figure given below shows a WAN formed by four Switches and 15 computers connected together. From figure we can	**16** ***Description 2M***

		say that WAN need not need to be a symmetric network. There can be any number of packet switches, and the packet switches connect to each other and the host. For instance, packet switch 1 connects to only three hosts, whereas packet switch 3 connects to 5 hosts. The packet switches are connected to each other using very high speed lines, such as T1. The hosts local to a particular packet switch connect to that packet switch.  	***Architecture Diagram 2M***
	b) Ans.	**What is multiplexing? Give its type.** Multiplexing divides the physical line or a medium into logical segments called channels. In multiplexing, different channels carry data simultaneously over the same physical medium. Hardware equipment called multiplexer (or mux in short) combines (or multiplexes) the inputs from different sources, and loads them on different channels of a medium. The combined data traverses over the medium simultaneously. At the destination, a demultiplexer (also called demux) separates (or demultiplexes) the signals meant for different destinations. The demultiplexer sends these separated signals appropriately to the different destinations. This is depicted in fig. This is cheaper than having separate lines.  Thus, the mux is responsible for both multiplexing and demultiplexing.	***4M*** ***Description 2M*** ***Diagram 1M***

		Types of Multiplexing There are basically two ways in which multiplexing and de-multiplexing can be achieved as follows. **1. Frequency Division Multiplexing (FDM):-** FDM divides the channel into multiple, but smaller frequency ranges to accommodate more users. **2. Time Division Multiplexing (TDM).** TDM divides a channel by allocating a time period for each channel.	***Listing of Types 1M***
	c) Ans.	**Describe the role of presentation layer.** The presentation layer is sixth layer of OSI model, concerned with preserving the meaning of information sent across a network. This layer concerns with semantics of the data, meaning of the data should be preserved. The presentation layer may represent (encode) the data in various ways (e.g., data compression, or encryption), but the receiving peer will convert the encoding back into its original meaning. The presentation layer concerns itself with the following: 1. **Data Format/Translation/Encoding**: Converting the complex data structures used by an application — strings, integers, structures, etc. — into a byte stream transmitted across the network. Representing information in such a way that communicating peers agree to the format of the data being exchanged. E.g., how many bits does an integer contain? Whether it supports ASCII or EBCDIC character set? 2. Compressing data to reduce the amount of transmitted data and hence its saves the money. 3. Security and Privacy issues: a. **Encryption:** Scrambling the data so that only authorized participants can unscramble the messages of a conversation. b. **Authentication:** Verifying that the remote party really is the party they claim to be rather than an impostor.	***4M*** ***Any 2 Role 2M each***
	d) Ans.	**Compare LAN and WAN (any Four points)**	***4M*** ***Any 4 Points 1M each***

Parameters	LAN	WAN
Geographic area	It covers small area with multiple buildings or campus.	It covers Much larger area like country/continent
Speed	High Speed compared to WAN	Less speed compared to LAN
Installation cost	Low	High
Communicati	Connected through	Computers connected to a

		on medium	Cables like twisted pair, co-axial and optical fibre.	wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.	
		Distance coverage	Limited coverage, about upto 10KM.	Unlimited (usually in 1000Km) range, uses repeater and other connectivity for range extension	
		Technologies used for medium	Locally installed, twisted pair, fiber optic cable, wireless (e.g. WLAN, Zigbee)	Mostly used WAN and other wireless technologies including satellite, cellular networks etc, along with twisted pair wires, fiber optic, coaxial cable.	
		Ownership	Single organization	Multiple organization	
		Topology use	It uses symmetric topology like star, bus, ring etc.	It uses irregular topology	
	e) Ans.	**What is subnetting in IP network? Explain with suitable example.** **(*Any relevant Example shall be considered)*** **Sub-netting** Subnetting is a process of breaking large network in small networks known as subnets. Subnetting happens when we extend default boundary of subnet mask. Basically we borrow host bits to create networks. Every computer on network has an IP address that represents its location on network. Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic. Each data link on a network must have a unique network ID, with every node on that link being a member of the same network. If you break a major network (Class A, B, or C) into smaller subnetworks, it allows you to create a network of interconnecting subnetworks. Each data link on this network would then have a unique network/subnetwork ID. Any device, or gateway, that connects n			***4M*** ***Description 2M***

networks/subnetworks has n distinct IP addresses, one for each network / subnetwork that it interconnects.
In order to subnet a network, extend the natural mask with some of the bits from the host ID portion of the address in order to create a subnetwork ID. For example, given a Class C network of 204.17.5.0 which has a natural mask of 255.255.255.0, you can create subnets in this manner:

Network Identifier	Subnet Identifier	Host Identifier

Example
Default MASK: 255.255.255.0 (For CLASS C)
I/P ADDRESS (I) 204.17.5.65
MASK (M): 255.255.255.224
Subnet Mask in binary is as follows:
11111111 11111111 11111111 11100000
Here the bit 1 represents the network id and 0 bit represents the host id. In this case we have borrowed 3 bits from the host id (class c) so we will be having 2^3= 8 subnets and in each subnet 2^5 = 32 hosts.

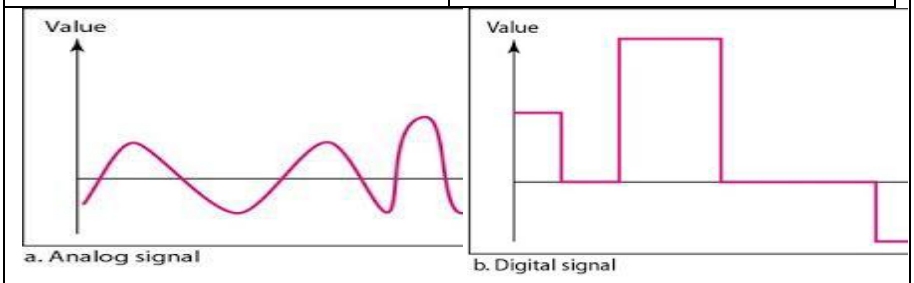
Example 2M

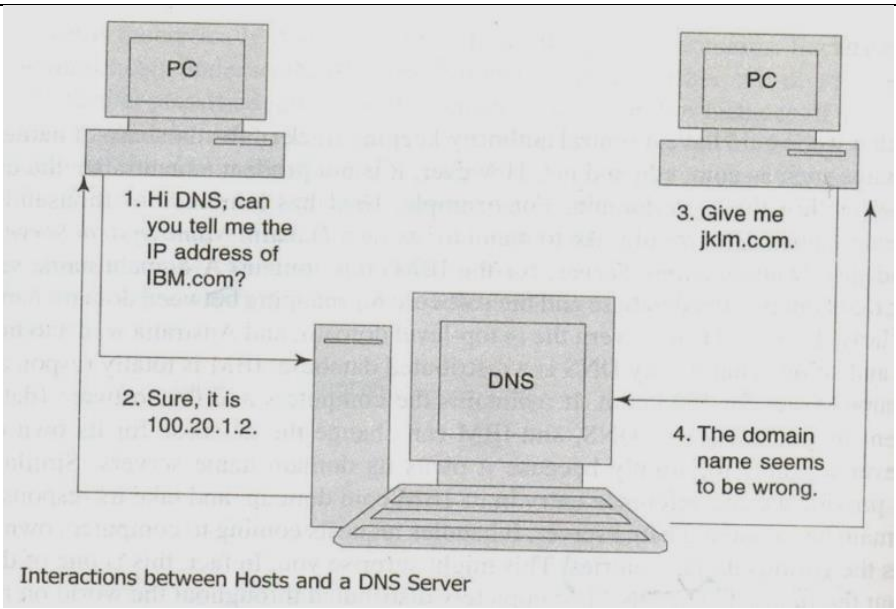
By extending the mask to be 255.255.255.224, you have taken three bits (indicated by "sub") from the original host portion of the address and used them to make subnets. With these three bits, it is possible to create eight subnets. With the remaining five host ID bits, each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device *since host ids of all zeros or all ones are not allowed* (As all zeros referred to loop back address and all ones are for broadcasting message in given subnet). So, with this, these subnets have been created.

204.17.5.0	255.255.255.224	host address range 1 to 30
204.17.5.32	255.255.255.224	host address range 33 to 62
204.17.5.64	255.255.255.224	host address range 65 to 94
204.17.5.96	255.255.255.224	host address range 97 to126
204.17.5.128	255.255.255.224	host address range 129 to 158
204.17.5.160	255.255.255.224	host address range 161 to 190
204.17.5.192	255.255.255.224	host address range 193 to 222
204.17.5.224	255.255.255.224	host address range 225 to 254

f) Ans. **Compare analog signal and digital signal.** ***4M***

Analog signal	Digital signal
An analog signal has infinitely many levels of intensity over a	A digital signal has only a limited number of values along

		period of time. / its value. As the wave moves from value A to value B. it passes through and includes an infinite number of values along its path. / Although each value can be any number, it is often as simple as 1 and 0. Analog signals are continuous in nature. / Digital signals are discrete in nature.  Analog signals are higher density. / Digital signals are lower density. Loss and Distortion is high. / Loss and Distortion is low. Analog signals are less secure as compare with Digital signal. / Digital signals are more secure Less bandwidth is require for transmission / High bandwidth is requiring for transmission. Synchronization not present / Synchronization present. Examples like Human voice in air, signals in analog electronic devices. / Examples include Computers and other digital electronic devices. Analog signal is best suited for audio and video transmission. / Digital signal is best suited for computing and digital electronic	***Any 4 Points 1M each***
5.	**a)** Ans.	**Attempt any FOUR of the following:** **Describe the process of DNS resolution.** Domain Name Resolution is the process of converting domain names to their corresponding IP address. DNS processes and interactions involve the communications between DNS clients and DNS servers during the resolution of DNS queries	**16** ***4M***



Interactions between Hosts and a DNS Server

When a DNS client needs to look up a name used in a program, it queries DNS servers to resolve the name. Each query message the client sends contains three pieces of information, specifying a question for the server to answer:

1. A specified DNS domain name, stated as a fully qualified domain name (FQDN).
2. A specified query type, which can either specify a resource record (RR) by type or a specialized type of query operation.
3. A specified class for the DNS domain name. For DNS servers running the Windows operating system, this should always be specified as the Internet (IN) class.

Generally queries can be classified as follows:

Recursive Resolution:

1. The resolver asks for a recursive answer from a DNS server.
2. The server must respond with the complete answer.
3. If it does not know the answer the server itself asks a parent server in the hierarchy.
4. If the parent does not know, the parent asks a higher level server in the hierarchy.
5. Eventually the resolver will be told the answer by the first DNS server the resolver contacted.

Iterative Resolution:

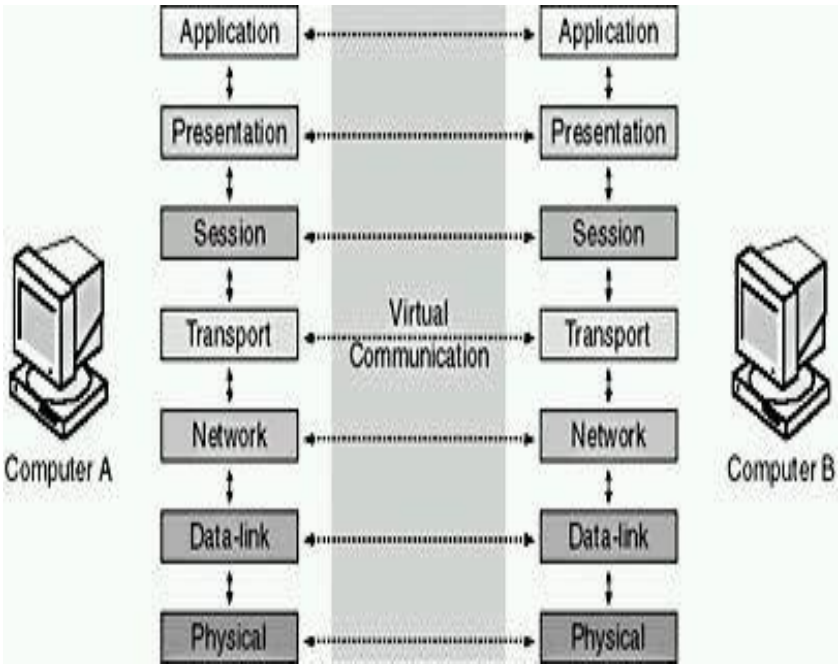
1. If client does not specify a recursive answer, client will get an iterative answer.

Relevant description 4M

		2. This means if the first server contacted does not know the answer, the server returns 3. The IP address of what the server thinks is a smarter server. 4. This continues until the answer is found.	
	b) Ans.	**Describe leased line connection. Give its need.** A leased line is a dedicated, fixed-bandwidth, symmetric data connection. A permanent. telephone connection between two points set up by a telecommunications common carrier. Typically, leased lines are used by businesses to connect geographically distant offices. Unlike normal dial-up connections, a leased line is always active. The fee for the connection is a fixed monthly rate. The primary factors affecting the monthly fee are distance between end points and the speed of the circuit. Because the connection doesn't carry anybody else's communications, the carrier can assure a given level of quality. Telephone companies & ISP‟s have come up with the option of offering more BW from their premises & let the organizations divide it internally the way they want. What is a leased line used for? It is used to link two locations together. The first location is typically a corporate office. The second location is typically another corporate office, a data center that's connected to the Internet or a data center that's connected to the company's existing Wide Area Network. **Lease line connection's need:** 1. For High bandwidth communication. 2. Dedicated and uninterrupted connectivity. 3. Fast and Secure communication between different offices. 4. Cost effective for large volume of data.	***4M*** ***Description 3M*** ***Any 2 needs 1M***
	c) Ans.	**State and Explain features of TCP.** **Features of TCP :** 1. Connection oriented: An application requests a "connection" to destination and uses connection to transfer data – IP does not uses "connections" - each datagram is sent independently! 2. Point-to-point: A TCP connection has two endpoints (no broadcast/multicast) 3. Reliability: TCP guarantees that data will be delivered without loss, duplication or transmission errors. 4. Full duplex: Endpoints can exchange data in both directions simultaneously 5. Reliable connection startup: TCP guarantees reliable, synchronized startup between endpoints (using "three-way	***4M*** ***Any 4 features with Explanation 1M each***

		handshake") 6. Gracefully connection shutdown: TCP guarantees delivery of all data after endpoint shutdown.	
	d) Ans.	**State advantages and disadvantages of mesh topology.** **Advantages :** 1. Use of the dedicated links guaranteed that each connection can carry its own data load 2. It is robust 3. A fault identification and diagnosed easily 4. Provides security and privacy 5. A faulty node won't affect the transmission of data in a mesh network. 6. Each node is connected to several other nodes which make it easier to relay data. 7. A faulty device will be ignored by the signals and will then find a new one that is connected with the node. **Disadvantages :** 1. There are high chances of redundancy in many of the network connections. 2. Overall cost of this network is way too high as compared to other network topologies. 3. Set-up and maintenance of this topology is very difficult. 4. Administration of the network is difficult. 5. The sheer bulk of wiring can be greater than the available space.	***4M*** ***2 advantages – 1M each*** ***2 Disadvantages – 1M each***
	e) Ans.	**Explain virtual communication between layers.** 1. Communication between software or hardware elements running at the same layer on different machines is called as " Virtual Communication" 2. Virtual Communication also called as Horizontal Communication. 3. Communication between peer processes is virtual, i.e. indirect. Each layer provides services to the next-higher layer and shields the upper layer from the details of how the services below it are actually implemented. At the same time, each layer appears to be indirect communication with its associated layer on the other computer. This provides a logical or virtual communication between peer layers, as shown in Figure. In reality, actual communication between adjacent layers takes place on one	***4M*** ***Explanation 3M***

computer only. At each layer, software implements network functions according to a set of protocols.



(Dashed line shows virtual communication between layers)

Diagram 1M

f) Ans.

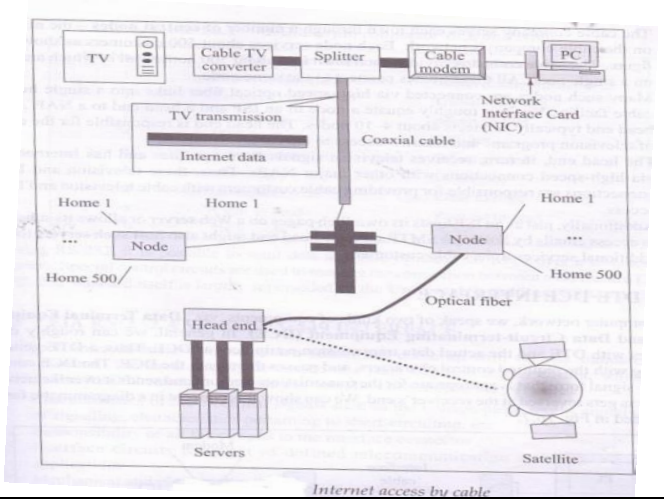
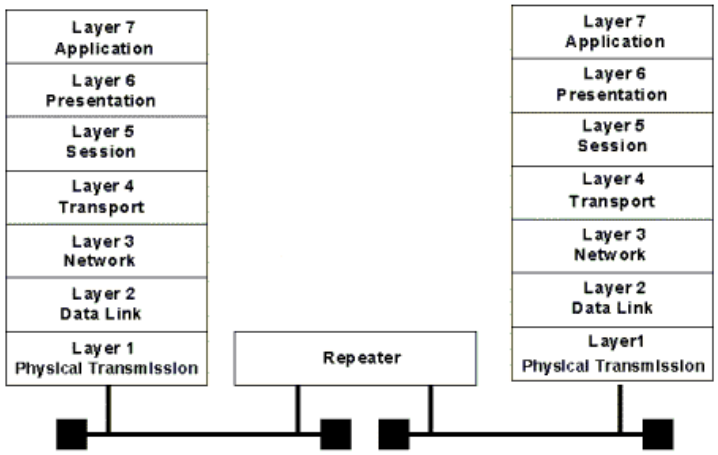
Compare OSI and TCP/IP.

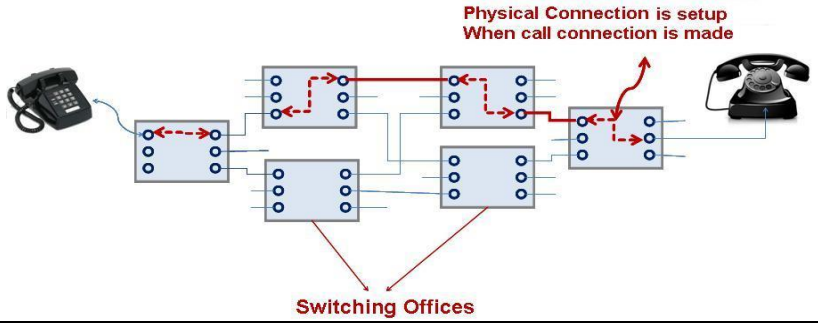
OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets	2. In TCP/IP model the transport layer does not guarantees delivery of packets.
3. OSI model has a separate Presentation layer and Session layer.	3. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are	5. TCP/IP model is, in a actual implementation of protocols

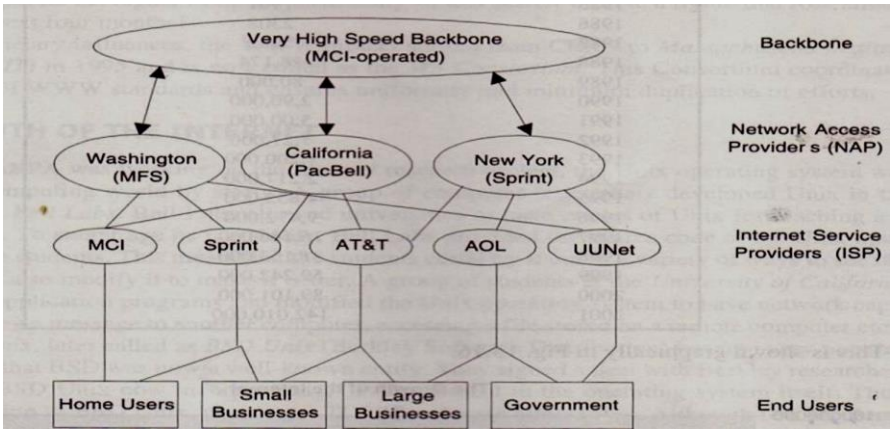
4M

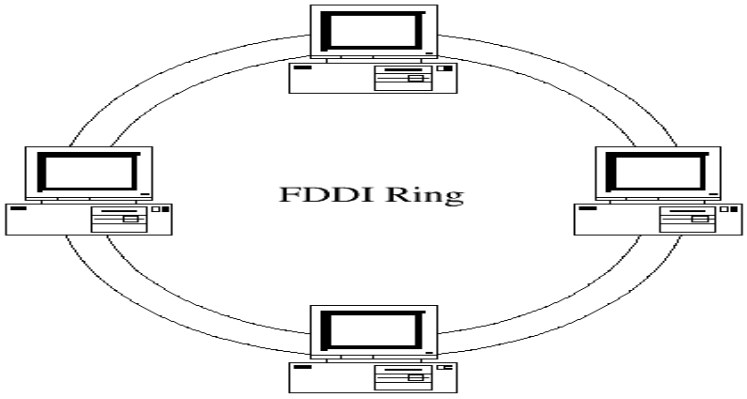
Any four points : 1M each

		built. Generally it is used as a guidance tool.	which we use on day to day basis.	
		6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.	
		7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model has its own set of protocols for each layer.	
		8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP protocols are well known and not easy to replace.	
		9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.	
		10. It has 7 layers	10. It has 4 layers	
6.		**Attempt any FOUR of the following:**		**16**
	a) Ans.	**Describe Cable modem with neat diagram.** Cable modems means CATV modems i.e. cable TV or network adapter modem. To install a cable modem, usually a power splitter and a new cable is required. The splitter divides the signal for "old" installations and the new segment connecting a cable modem. The transmitted signal from the cable modem is sometimes 80 strong that the TV set may get disturbed for while the isolation of splitter, a high pass filter is used. The HF allows only the TV Channel frequency to pass, at the same time blocks the upstream frequency band as well as low frequency of in house wiring. The term cable refers to a modem operates over the ordinary cable TV network. The cable modem is connected to TV outlet the cable TV and cable TV operator connects a cable modem termination system (CMTs) in the end (Head end). Again it works basically like a local area network interface. Thus CMTs device is used for connecting the cable TV network to a data network like the internet	***4M*** ***Description 3M***

		 *Internet access by cable*	***Diagram 1 M***
	b) ***Ans.***	**Explain with neat sketch repeaters in OSI model. State its advantages.** A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do no amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.  **Advantages of Repeater:** 1. A repeater is used to regenerate the signal. 2. It can be used to connect two segments. 3. A repeater allows extending the physical length of a network. 4. A repeater is used to boost the weak signal when the signal loses	***4M*** ***Explanation 2M*** ***Diagram 1M*** ***Advantage 1M***

		the strength as it passes along the cable. 5. A repeater does not have filtering capacity; It forwards every frame. 6. Repeaters are cheaper when compared to other networking devices.	
	c) Ans.	**Explain circuit switching with suitable diagram.** Circuit switching is primarily used in Telephone networks and not in Computer networks. In circuit switching, 1.An End to end circuit (path) is first reserved using a separate signaling protocol 2.Data transfer proceeds only after the circuit establishment phase 3.All data of that session passes through the same circuit 4.No other user can use this circuit till this session is completed 5.No signaling information is sent along with the data 6.Circuit is released after data transfer using the signaling protocol.  	***4M*** ***Explanation 3M*** ***Diagram 1M***
	d) Ans.	**Describe following :** **(i) Periodic Signal** **(ii) Non-periodical Signal** **(iii) Bandwidth** **(iv) Data transmission rate** **(i) Periodic Signal:** A **signal** is a **periodic signal** if it completes a pattern within a measurable time frame, called a period and repeats that pattern over identical subsequent periods. **(ii) Non-periodical Signal:** A ***signal*** that does not repeats its pattern over a period is called ***aperiodic signal*** or ***non periodic***. **(iii) Bandwidth:** The information carrying capacity of a signal or a medium, calculated using the difference between the highest and the lowest frequency. A range of frequencies within a given band, in particular that used for transmitting a signal.	***4M*** ***Description of each term 1M***

		Bandwidth (signal processing) or *analog bandwidth*, *frequency bandwidth* or *radio bandwidth*: a measure of the width of a range of frequencies, measured in hertz. **(iv) Data transmission rate:** The speed with which **data** can be **transmitted** from one device to another. **Data rates** are often measured in megabits (million bits) or megabytes (million bytes) per second. These are usually abbreviated as Mbps and MBps respectively. Another term for **data transfer rate** is **throughput.**	
	e) Ans.	**Explain the internet topology.** Internet is the worldwide network of computer networks. It is organized to form a hierarchy that makes it very simple to understand and operate. The following figure shows different parts of the hierarchy. At the very top, there is a very high speed backbone and at the other end there are the users and businesses. There are intermediate layers of network access provider (NAC) and Internet Service Providers (ISPs).  A home user dials into an ISP using a telephone connection with a modem. The ISP routes the call to a Network Access Provider (NAP) which in turn connects to a high speed back bone at a convenient network access point. This completes the circuit. Now, the user can send/ receive any message to anyone else connected to the Internet.	***4M*** ***Explanation 2M*** ***Diagram 2M***
	f) Ans.	**Describe Fiber Distributed Data Interface (FDDI) technology**. Fiber distributed data interface (FDDI), which is an optical data communication standard used for long distance networks provides communication with fiber optic lines up to 200 kilometers at a speed	***4M***

		of 100 megabit per second (Mbps). Fiber Distributed Data Interface (FDDI) is usually implemented as a dual token-passing ring within a ring topology (for campus networks) or star topology (within a building). The dual ring consists of a primary and secondary ring. The primary ring carries data. The counter-rotating secondary ring can carry data in the opposite direction, but is more commonly reserved as a backup in case the primary ring goes down.  	***Description 3M*** ***Diagram 1M***